REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
16-11-2015	Final Report	1-Jul-2009 - 30-Jun-2017

4. TITLE AND SUBTITLE

SoS Lablet;

Perpetually Available and Secure Information Systems

5a. CONTRACT NUMBER
W911NF-09-1-0273

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
611102

6. AUTHORS
William Scherlis, Monika De Reno, Virgil Gligor, Michael Balderson

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
Carnegie Mellon University
5000 Forbes Avenue

Pittsburgh, PA 15213 -3815

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS (ES)
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)
ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
56390-CS.343

12. DISTRIBUTION AVAILIBILITY STATEMENT
Approved for Public Release; Distribution Unlimited

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT

Carnegie Mellon University's CyLab built substantially upon the research thrusts and projects established under each of the main research thrusts of the original proposal. In the most recent year, over 35 research projects were approved for funding, totaling over $6.1 million and involving over 43 researchers and faculty.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Pradeep Khosla
UU	UU	UU	UU		19b. TELEPHONE NUMBER 412-268-5090

Standard Form 298 (Rev 8/98)
Prescribed by ANSI Std. Z39.18

Report Title

SoS Lablet;

Perpetually Available and Secure Information Systems

ABSTRACT

Carnegie Mellon University's CyLab built substantially upon the research thrusts and projects established under each of the main research thrusts of the original proposal. In the most recent year, over 35 research projects were approved for funding, totaling over $6.1 million and involving over 43 researchers and faculty.

Enter List of papers submitted or published that acknowledge ARO support from the start of the project to the date of this printing. List the papers, including journal references, in the following categories:

(a) Papers published in peer-reviewed journals (N/A for none)

Received	Paper
11/24/2014 20.00	Khalil Ghorbal, Jean-Baptiste Jeannin, Erik Zawadzki, André Platzer, Geoffrey J. Gordon, Peter Capell. Hybrid Theorem Proving of Aerospace Systems: Applications and Challenges, Journal of Aerospace information systems, (10 2014): 702. doi: 10.2514/1.I010178
TOTAL:	**1**

Number of Papers published in peer-reviewed journals:

(b) Papers published in non-peer-reviewed journals (N/A for none)

Received	Paper
09/05/2014 10.00	Pang Wu, Jiang Zhu, Joy Ying Zhang. MobiSens: A Versatile Mobile Sensing Platform for Real-World Applications, Mobile Networks and Applications , (02 2013): 1. doi:
TOTAL:	**1**

Number of Papers published in non peer-reviewed journals:

(c) Presentations

SoS Lablet

1) Arbob Ahmad and Robert Harper, "An Epistemic Formulation of Information Flow Analysis" - SoS Quarterly Lablet PI Meeting, Carnegie Mellon University, Pittsburgh, PA, July 1-2, 2014

2) Kathleen Carley, "Crisis Mapping: Big Data from a Dynamic Network Analytic Perspective" - World Summit on Big Data and Organization Design, Paris, France, May 16-17, 2013 - Invited Plenary

3) Kathleen Carley. "Geo-Spatial Network Analysis: Applications and Challenges" - 4th International Workshop on Location-Based Social Networks (LBSN 2012) at UBICOM, Pittsburgh, PA. September 8, 2012 - Invited Keynote

4) Kathleen Carley. "Dynamic Network Analysis: Security Applications" - Creighton University, Omaha Nebraska, 7/2013 - Invited Talk

5) Kathleen Carley. "Network-Centric Simulation and Virtual Experimentation" - 21st Behavioral Representation in Modeling and Simulation (BRiMS) Conference. Amelia Island, FL, March 12-15, 2012

6) Kathleen Carley. "Multi-Level Resilience Modeling: Evaluating Organizational Topologies for their Resilience to Attacks" - ONR sponsored Workshop on Social Cyber Security, Pittsburgh PA, 6/2013 - Poster Presentation

7) Kathleen M. Carley, “Analyzing and Simulating Dynamic Networks” - Rand Conferece, Arlington, VA, March 2014

8) Kathleen M. Carley, “Dynamic Network Analytics for Cyber Warfare” - CENTCOM Technical Exchange, Tampa, FL, March 2014

9) Kathleen M. Carley, “Network Analysis and Visualization” - Approaches to Dynamic Network and Scientometric Analysis within the IC, Washington DC, November 2013

10) Kathleen M. Carley, “Networks and Agents: The Value of a Multi-Level Approach to Agent-Based Dynamic- Network Modeling” - Statistical and Applied Mathematical Sciences Institute (SAMSI), Raleigh-Durham, NC, August 2013

11) Kathleen M. Carley, “Dynamic Network Analysis: Security Applications” - Creighton University, Omaha Nebraska, July 2013

12) Geoffrey Morgan, “Construct” - CASOS Summer Institute, Carnegie Mellon University, Pittsburgh, PA, June 15-22, 2014

13) Kathleen Carley. "Crisis Mapping: Big Data from a Dynamic Network Analytic Perspective." - World Summit on Big Data and Organization Design, Paris, France, May 16-17, 2013 - Invited Plenary

14) Kathleen Carley. "Geo-Spatial Network Analysis: Applications and Challenges." - 4th International Workshop on Location-Based Social Networks (LBSN 2012) at UBICOM, Pittsburgh, PA. September 8, 2012 - Invited Keynote

15) Kathleen Carley. "Dynamic Network Analysis: Security Applications." - Creighton University, Omaha Nebraska, July 2013 - Invited Talk

16) Ghita Mezzour. "International Cyber Attack Network Analysis." - ONR sponsored Workshop on Social Cyber Security, Pittsburgh PA, 6/2013 - Poster Presentation

17) Kenneth Joseph and Kathleen Carley. "Group-based Constructuralism: modeling the evolution of groups, ties, culture, and cognition" - CASOS Summer Institute, Carnegie Mellon University, Pittsburgh, PA, June 15-22, 2014 - Poster Presentation

18) Ghita Mezzour and Kathleen Carley. "Putting Cyber-Attacks on the World Map" - CASOS Summer Institute, Carnegie Mellon University, Pittsburgh, PA, June 15-22, 2014 - Poster Presentation

19) Geoffrey Morgan and Kathleen Carley. "Organizational Resilience and the Meta-Network Formalism" - CASOS Summer Institute, Carnegie Mellon University, Pittsburgh, PA, June 15-22, 2014 - Poster Presentation

20) Geoffrey Morgan and Kathleen Carley. "Modeling Organizational Resiliency to Cyber-Attacks" - Carnegie Mellon University Lablet Meeting, Pittsburgh, PA, July 1-2, 2014 - Poster Presentation

21) Ghita Mezzour, Kathleen Carley, and Richard Carley. "Global Mapping of Cyber Attacks" - Carnegie Mellon University Lablet Meeting, Pittsburgh, PA, July 1-2, 2014 - Poster Presentation

22) Kathleen M. Carley, "Dynamic Network Analytics for Cyber Warfare" - CENTCOM Technical Exchange, Tampa, FL, March 2014

23) Kathleen M. Carley, "Network Analysis and Visualization" - Approaches to Dynamic Network and Scientometric Analysis within the

IC, Washington DC, November 2013

24) Kathleen M . Carley, "Dynamic Network Analysis" - Soft Power Solutions, Chantilly VA, June 2014

25) Kathleen M. Carley, "Remote CBRNE Assessment using Dynamic Network Methods" - Defense Threat Reduction Agency, Washington DC, May 2014

26) Kathleen M. Carley, "A Global Perspective on Cyber Attacks" - NSA Security Lablet, Carnegie Mellon University, Pittsburgh, PA, September 2013

27) Kathleen M. Carley, "Dynamic Network Analysis: Security Applications" - Creighton University, Omaha Nebraska, July 2013 - Invited Talk

28) Jon Storrick, "Geo-Spatial Networks" - CASOS Summer Institute, Carnegie Mellon University, Pittsburgh, PA, June 15-22, 2014

29) Ghita Mezzour, "Nuclear, Bio, and Cyber Networks Social Influence Modeling" - CASOS Summer Institute, Carnegie Mellon University, Pittsburgh, PA, June 15-22, 2014

30) Geoff Morgan, "Validation Extended Construct" - CASOS Summer Institute, Carnegie Mellon University, Pittsburgh, PA, June 15-22, 2014

31) Geoff Morgan, "Resiliency Modeling" - CASOS Summer Institute, Carnegie Mellon University, Pittsburgh, PA, June 15-22, 2014

32) Wei Wei, "Geo-temporal Networks" - CASOS Summer Institute, Carnegie Mellon University, Pittsburgh, PA, June 15-22, 2014

33) Alain Forget, S. Komanduri, Alessandro Acquisti, Nicolas Christin, Lorrie Cranor, Rahul Telang. "Security Behavior Observatory: Infrastructure for Long-term Monitoring of Client Machines" - Symposium and Bootcamp on the Science of Security (HotSoS) 2014, ACM. Raligh, NC, April 8-9, 2014

34) Alain Forget, Alessandro Acquisti, Nicolas Christin, Lorrie Cranor, Rahul Telang. "Deploying the Security Behavior Observatory: An Infrastructure for Long-term Monitoring of Client Machines" - NSA Science of Security Lablet Meeting, July 2014. Carnegie Mellon University, Pittsburgh, PA, July 1-2, 2014, - Poster Presentation

35) Alain Forget, Alessandro Acquisti, Lorrie Faith Cranor, Nicolas Christin, Rahul Telang. "Security Behavior Observatory. Lightning talk at the Symposium on Usable Privacy and Security" - ACM, July 2013, Newcastle, UK.

36) Alain Forget. "Flying South For The Career." - Invited talk at the ISSNet 2013 Annual Workshop, NSERC, April 23-26, 2013, Victoria, Canada.

37)Alain Forget, Alessandro Acquisti, Lorrie Faith Cranor, Nicolas Christin, Rahul Telang. "Security Behavior Observatory." Lightning talk at the CyLab Usable Privacy and Lunch seminar, CMU, March 2013, Pittsburgh, USA.

38) Nathan Fulton, Cyrus Omar, and Jonathan Aldrich. "Statically Typed String Sanitation Inside a Python" - PSP 2014 : First International Workshop on Privacy and Security in Programming, Portland, OR, October 20-24, 2014

39) Darya Kurilova, Alex Potanin, and Jonathan Aldrich. "Wyvern: Impacting Software Security via Programming Language Design" - Workshop on Evaluation and Usability of Programming Languages and Tools (PLATEAU), 2014, SPLASH, Portland, OR, October 20-24, 2014

40) Michael Coblenz, Jonathan Aldrich, Brad Myers, and Joshua Sunshine. "Considering Productivity Effects of Explicit Type Declarations" - Workshop on Evaluation and Usability of Programming Languages and Tools (PLATEAU), 2014, SPLASH, Portland, OR, October 20-24, 2014

41) Jonathan Aldrich. "Extensible Languages" IFIP TC2 working group on programming language design (#2.16), Aarhus, Denmark, August 21-25, 2013

42) Cyrus Omar, Benjamin Chung, Darya Kurilova, Alex Potanin, and Jonathan Aldrich. "Type Directed, Whitespace-Delimited Parsing for Embedded DSLs". - Presentation at First Workshop on Domain Specific Languages Design and Implementation (DSLDI), 2013, Montpellier, France, July 1, 2013

43) Jonathan Aldrich. "Architectural Control" Presentation at the IFIP Workging Group on Language Design, Portland, OR, June 6, 2014

44) Sam Malek. "Toward the Making of Software that Learns to Manage Itself" Keynote at the 27th Brazilian Symposium on Software Engineering (SBES 2013). Brasilia, Brazil, Sept 29 - October 4, 2013.

45) Sam Malek. "Automated Security Testing of Mobile Applications" FedMobileCamp hosted by NGA/InnoVision, Reston, VA, August 2013.

46) Sam Malek and Marija Mikic-Rakic. "A Framework for Improving a Distributed Software System's Deployment Architecture" Delft University of Technology, Delft, Netherlands, June 2013

47) David Garlan, Mary Shaw. "Software Architecture: Reflections on an Evolving Discipline" - International Conference on Software Engineering and Applications (ICSE), San Francisco, CA, May 18-26, 2013, Keynote

48) David Garlan. "Software Architecture: Perspectives and Challenges" - 7/2014 Beihang University

49) David Garlan. "Self-Healing Systems" - 2/2014 Samsung Electronics

50) Andre Platzer. "Logical Foundations of Cyber-Physical Systems" - Invited talk at High Confidence Software and Systems Conference, 2014 (HCSS'14), Annapolis, MD, May 20, 2014

51) Andre Platzer. "Foundations of Cyber-Physical Systems" - Invited course at MAP-i, Universities of Minho, Braga, Porto and Aveiro, Portugal, March 2014

52) Andre Platzer. "Logical Foundations of Cyber-Physical Systems" - NSF Workshop for Aspiring PIs in Cyber-Physical Systems, Washington, DC, February 18-19, 2014

53) Andre Platzer. "Developing a Successful NSF Proposal" - NSF Workshop for Aspiring PIs in Cyber-Physical Systems, Washington, DC, February 18-19, 2014

54) Andre Platzer. "Logic of Dynamical Systems" - Invited Research School at École Normale Supérieure (ENS) de Lyon, France, January 2014

55) Andre Platzer. "Hybrid Systems Verification" - Invited talk at 4th Workshop Formal Methods for Robotics and Automation, Berlin, Germany, June 27, 2013

56) Andre Platzer. "How to Explain Cyber-Physical Systems to Your Verifier" - Invited talk at 5th Working Conference on Verified Software: Theories, Tools, and Experiments (VSTTE'13), Atherton, CA, May 17-19, 2013

57) Andre Platzer. "Logic of Hybrid Games" - Invited talk at LCCC Focus Period and Workshop on Formal Verification of Embedded Control Systems, Lund, Sweden, April, 2013

58) Erik Zawadzki, Geoffrey J. Gordon, and André Platzer. "A projection algorithm for strictly monotone linear complementarity problems" - Neural Information Processing Systems Foundation (NIPS), Lake Tahoe, NV, December 5-10, 2013

59) Limin Jia. "Proving Trace Properties of Programs that Execute Adversary-supplied Code" - Presented at PLClub at University of Pennsylvania, June 7, 2013

60) Limin Jia. "Proving Trace Properties of Programs that Execute Adversary-supplied Code" - Presented at Seminar at Princeton University, June 20th, 2013

61) Limin Jia. "Proving Trace Properties of Programs that Execute Adversary-supplied Code" - INRIA, Paris Rocquencourt, June 5, 2014

62) Frank Pfenning. "Concurrent Programming in Linear Type Theory" Workshop on the Mathematical Structures of Computation, Lyon, France, February 2014

63) Frank Pfenning. "Linear Logic and Session Types" 4-lecture course at the BETTY Summer School on Behavioral Types, Lovran, Croatia, June/July 2014

64) Ju-Sung Lee, Juergen Pfeffer. "Measurement Accuracy in Samples of Online Communication Networks" - EUSN, 1st European Conference on Social Networks, Barcelona, Spain, July 1-4 2014

65) Ju-Sung Lee, Juergen Pfeffer. "Robustness of Network Metrics in the Context of Cyber Communication Data" - Quarterly Lablet meeting, Carnegie Mellon University, Pittsburgh, PA, July 1-2 2014. - Poster Presentation

66) Ju-Sung Lee, Jürgen Pfeffer. "Approximating Network Measures for Large Scale Networks of Varying Size, Density, Typologies, and Subsampling Levels" - Sunbelt Network Analysis Conference, March 19-23, 2014

67) Jürgen Pfeffer, Kathleen M. Carley, Bradley Schmerl, David Garlan. "Network Analysis for Big Data in Resource-Constrained Environments" - Sunbelt Network Analysis Conference 2013, Hamburg, Germany, May 21-26, 2013

68) Jurgen Pfeffer. "Composability of Big Data and Algorithms for Social Networks Analysis Metrics" - Quarterly Lablet meeting at Urbana-Champaign, IL, May 1, 2014

69) Jurgen Pfeffer. "Describing Structural Change in Networked Systems" - Quarterly Lablet meeting at Urbana-Champaign, IL, May 1, 2014

Perpetually Available and Secure Information Systems

1) Aveek Purohit and Pei Zhang, SensorFly: A Collaboratively-Mobile Sensor Network (Poster), Cylab Partners Conference, Carnegie Mellon University, Pittsburgh, PA, September 2009.

2) Sasha Romanosky. Data Breaches and Identity Theft: When is Disclosure Optimal? – presented at the Sixth Annual Forum on Financial Information Systems and Cybersecurity: A Public Policy Perspective, University of Maryland, October 2009

3) Onur Mutlu, Designing High-Performance and Fair Shared Multi-core Memory Systems: Two Approaches. Presented the following venues and dates: Gigascale Systems Research Center E-Seminar, March 23, 2010; ARM, Inc., Austin, TX, April 8, 2010; Advanced Micro Devices, Austin, TX, April 9, 2010; Microsoft Research, Redmond, WA, April 27, 2010; HP Laboratories, Palo Alto, CA, May 25, 2010; VMware, Palo Alto, CA, May 26, 2010; Intel Corporation, Hillsboro, OR, May 27, 2010.

4) Onur Mutlu, Rethinking Memory System Design in the Nanoscale Many-Core Era. Presented the following venues and dates: Intel Memory Hierarchy Workshop, Hillsboro, OR, January 22, 2010; ASPLOS Workshop on Architecting Memory Technologies, Pittsburgh, PA, 14 March 2010.

5) Onur Mutlu, ATLAS: A Scalable and High-Performance Scheduling Algorithm for Multiple Memory Controllers. Presented the following venues and dates: Advanced Micro Devices Research Lab, Redmond, WA, October 2009; Freescale Semiconductor, Austin, TX, April 8, 2010.

6) Xin Zhang, Yanlin Li, and Onur Mutlu. More is Less: Denial-of-Service Attacks and Solutions in Many-Core On-Chip Networks. IEEE Symposium on Security and Privacy, May 2010.

7) Nancy Mead, Future Challenges of Security Requirements. Panelist, Grace Symposium on Security Requirements, June 9, 2008, National Institute of Informatics (NII), Tokyo, Japan.

8) Nancy Mead. Requirements Engineering for Improved System Security. Grace Symposium on Security Requirements, June 9, 2008, National Institute of Informatics (NII), Tokyo, Japan

9) Jonathan McCune. A Contractual Anonymity System: Experiences Building an Anonymity System using Trusted Computing.

10) Roy Maxion. Validity of Experiments in Trustworthy Computing. Johns Hopkins Applied Physics Laboratory, August 12, 2010

11) Roy Maxion. When Science Meets Security. Presented the following venues and dates: Pacific Northwest National Laboratory Roundtable on Cyber Security, August 27, 2010; RAID – Recent Advances in Intrusion Detection, September 24, 2009, St. Malo, France; . Information Security Institute: Mathematics Workshop on CyberSecurity, April 22, 2010, Gold Coast, Australia; Victoria University of Wellington, New Zealand, May 4, 2010

12) Roy Maxion. Dependability in the Time of Forensics, Latin American Dependability Symposium. Joao Pessoa, Brazil, September 2, 2009.

13) Roy Maxion. Keystroke Biometrics with Number-Pad Input. Queensland University of Technology, Australia, May 12, 2010.

14) K. Mai. Securing Emerging Non-Volatile Memory Technologies. Following venues and dates: Intel Symposium on Memory Hierarchy, January 2010; CMOS Emerging Technologies, May 2010.

15) Stephen Fienberg. Networks, E-commerce, and Privacy. Keynote Address for Conference on Statistical Challenges in Electronic Commerce Research, Heinz College, Carnegie Mellon University, May 31, 2009.

16) Stephen Fienberg. Rethinking the Risk-Utility Tradeoff Approach to Statistical Disclosure Limitation. Joint Statistics Meetings,

Washington DC. August 3, 2009.

17) Rob Hall. Secure Multiparty Computation for Multiple Regression Computation. Joint Statistics Meetings, Washington DC, August 3, 2009.

18) Jiashin Jin. Privacy protection for sparse data, Workshop on Statistical and Learning-Theoretic Challenges in Data Privacy, IPAM, UCLA. February 24, 2010.

19) Rob Hall. Secure multiple linear regression based on homomorphic encryption, Workshop on Statistical and Learning-Theoretic Challenges in Data Privacy, IPAM, UCLA. February 25, 2010.

20) Stephen Fienberg. Towards a Bayesian Characterization of Privacy Protection & the Risk-Utility Tradeoff. Workshop on Statistical and Learning-Theoretic Challenges in Data Privacy, IPAM, UCLA, February 25, 2010.

21) Yuval Nardi. Secure Logistic Regression with Distributed Databases. Workshop on Statistical and Learning-Theoretic Challenges in Data Privacy, IPAM, UCLA, February 26, 2010.

22) Anind K. Dey. Intelligence and Context-Aware Applications. ICEIS 2010.

23) Anind K. Dey. Real-World Context-Aware Applications. Summer school, Oulu, Finland.

24) Laura Brandimarte, Alessandro Acquisti, and George Loewenstein. Privacy Concerns and Information Disclosure: An Illusion of Control Hypothesis. INFORMS Annual Meeting, 2009.

25) Laura Brandimarte, Alessandro Acquisti, and George Loewenstein. Privacy Concerns and Information Disclosure: An Illusion of Control Hypothesis. Computer Freedom and Privacy (CFP) Research Showcase, 2009.

26) Laura Brandimarte, Alessandro Acquisti, and George Loewenstein. Privacy Concerns and Information Disclosure: An Illusion of Control Hypothesis. Computer Freedom and Privacy (CFP) Research Showcase Poster, 2009.

27) Laura Brandimarte, Alessandro Acquisti, and George Loewenstein. Privacy Concerns and Information Disclosure: An Illusion of Control Hypothesis. iConference, 2009.

28) Alessandro Acquisti. Privacy, Behavior, and Economics: The Illusion of Control Hypothesis. The following venues and dates: TRUST (Team for Research on Ubiquitous Secure Technologies), National Science Foundation Site Visit, April 2010; TRUST (Team for Research on Ubiquitous Secure Technologies) Autumn 2009 Conference, October 2009.

29) Aleecia McDonald and Lorrie Cranor. An Empirical Study of How People Perceive Online Behavioral Advertising. Privacy Law Scholars Conference, June 3, 2010.

30) Lorrie Cranor. Nuts & Bolts of Online Privacy, Advertising, Notice & Choice. The Progress & Freedom Foundation Capitol Hill Briefing, Washington, DC, May 24, 2010.

31) Lorrie Cranor. Consumer Expectations and Disclosures. Federal Trade Commission Exploring Privacy Roundtable, Washington, DC, December 7, 2009.

32) Alessandro Acquisti. Consumer Expectations and Disclosures. Federal Trade Commission Exploring Privacy Roundtable, Washington, DC, December 7, 2009.

33) Alessandro Acquisti. Online Information and Privacy Policy. Technology Policy Institute's Capitol Hill Briefing, Rayburn Building, Washington DC, July 2009.

34) Norman Sadeh. Are Social Networking and Privacy Irreconcilable? ICTI Annual Conference, Portugal, June 2010.

35) Norman Sadeh. What Will the App Store of the Future Look Like? Expert Address, Hong Kong University, May 2010.

36) Norman Sadeh. More Control --> More Sharing. Mobile Social Networking Asia, May 2010.

37) Norman Sadeh. User-Controllable Security and Privacy: Lessons from the Development and Deployment of Location Sharing Apps. Joint Intelligence/ISR/CyLab seminar, April 2010.

38) Norman Sadeh. User-Controllable Security and Privacy: Lessons from the Development and Deployment of Location Sharing Apps.

Google, March 2010.

39) Norman Sadeh. User-Controllable Security and Privacy. CyLab Partners Conference, October 2010.

40) Michael Benisch, Patrick Gage Kelley, Norman Sadeh, Tuomas Sandholm, Janice Tsai, Lorrie Faith Cranor and Paul Hankes Drielsma. The Impact of Expressiveness on the Effectiveness of Privacy Mechanisms for Location-Sharing. Poster presentation SOUPS 2009.

41) Eran Toch, Ramprasad Ravichandran, Lorrie Cranor, Paul Hankes Drielsma, Jason Hong, Patrick Kelley, Norman Sadeh and Janice Tsai. Analyzing Use of Privacy Policy Attributes in a Location Sharing Application. Poster presentation SOUPS 2009.

42) Ramprasad Ravichandran, Michael Benisch, Patrick Gauge Kelley, and Norman Sadeh. Capturing Social Networking Privacy Preferences: Can Default Policies Help Alleviate Tradeoffs between Expressiveness and User Burden? Poster presentation SOUPS 2009.

43) Bruno Sinopoli. Cyber-Physical Systems: a few results, a new direction and an application. CCDC seminar, UC Santa Barbara, February 2010.

44) Bruno Sinopoli. Secure Control Against Replay Attacks. ITA Workshop, UC San Diego, February 2010.

45) Bruno Sinopoli. Smart-Grid Security. Senate committee briefing, Washington, DC, January 2010.

46) Bruno Sinopoli. Secure Control Against Replay Attacks. TRUST Autumn Conference, Washington, D.C. October 2009.

47) Bruno Sinopoli. Secure Control of Cyber-Physical Systems, Sixth Cylab Partner's conference, Pittsburgh, PA October 2009.

48) Bruno Sinopoli. A Tutorial on Networked Control Systems, Necsys 2009, Venice, Italy, September 2009.

49) Frank Pfenning. Possession as Linear Knowledge. Proceedings of the 3rd International Workshop on Logics, Agents, and Mobility (LAM'10), Edinburgh, Scotland, July 2010.

50) Michelle Mazurek. Access Control for Home Data Sharing. Fall 2009 PDL Visit Day.

51) Rich Shay. Exploring Reactive Access Control (poster). CHI 2010.

52) Andrew Moore, Adam Cummings. Insider threat workshop, SEI (Arlington, VA.), May 19-20, 2010.

53) Nicolas Christin. Secure or insure? Following venues and dates: A game theoretic analysis of information security games. INI Seminar, November 2009; University of Toronto, October 2009

54) Nicolas Christin. National CyberLeap Year Summit. August 2009.

55) Randy Trzeciak. Insider Threat: A Real Problem for Financial Institutions (panel discussion). 2010 FS-ISAC, FSTC, BITS Annual Summit, May 4, 2010

56) Dawn Cappelli, Adam Cummings. Insider threat workshop, SEI (Arlington, VA.), May 3-5, 2010

57) Dawn Cappelli. Risk Mitigation Strategies: Lessons Learned from Actual Insider Attacks. 6th Annual Cyber Security and Information Intelligence Research Workshop, 4/23/2010

58) Dawn Cappelli, Mike Hanley. Insider Theft of Intellectual Property: A Profile of the Crime. INFOSEC World 2010 Conference, 4/21/2010

59) Dawn Cappelli. Insider Threat: Your Greatest Risks. Information Security Media Group, 4/1/2010

60) Dawn Cappelli. Overcoming Policy, Legal and Privacy Issues in the Fight Against Insider Threats (panel discussion). Government Security Expo and Conference 2010, March 23, 2010

61) Dawn Cappelli. Keys to Successful Monitoring for Detection of Insider Attacks. RSA Conference 2010, March 4, 2010

62) Andrew Moore. Under Attack: Threats to Deposit Accounts. BAI, 3/1/2010

63) Dawn Cappelli, Randy Trzeciak. Insider Threat Workshop. Fifty CIOs from Fortune 500 companies, March 1, 2010

64) Dawn Cappelli. Insider Threat. DC3 Conference, January 21-24, 2010.

65) Dawn Cappelli. Securing the Weakest Link: Cyber Security Awareness & Education. National Association of State Chief Information Officers (NASCIO) 2009 Annual Conference, October 27, 2009.

66) Dilsun Kaynar. Towards Differential Privacy for Systems. CyLab Student Seminar, October 2009.

67) Dilsun Kaynar. Reasoning about Privacy in Distributed Information Sharing Systems. Koc University Engineering Seminar, Istanbul, Turkey, December 2009

68) David Andersen, System and Algorithmic Adaptation for Flash Proc. Non-volatile Memories Workshop, San Diego, CA, April 2010

69) William Scherlis and Jonathan Aldrich. Application-Specific Software Assurance, CyLab ARO review presentation, August 2009.

70) Jonathan Aldrich. Design Intent: a Principled Approach to Application Security. CyLab seminar, September 2009.

71) Jonathan Aldrich. Design Intent: a Principled Approach to Application Security. Presentation at Boeing Application Security Developer's Forum on behalf of CyLab, September 2009.

72) Alessandro Acquisti. From the Illusion of Control to Discounting the Past: Privacy and Behavior. Usenix Security Symposium, San Francisco, August 2011.

73) Alessandro Acquisti. The Theater of Privacy. Microsoft’s Innovation Outreach Program, New York, April 2011. (Opening speaker for Day 2)

74) Alessandro Acquisti.Privacy and Social Networks. Microsoft’s Innovation Outreach Program, New York, April 2011.

75) Alessandro Acquisti. Samuelson Law, Technology & Public Policy Clinic's Spring 2011 Privacy Speaker Series, "Privacy and the Illusion of Control," Berkeley, 2011.

76) Alessandro Acquisti. The Economics of Privacy. OECD Roundtable on the Economics of Personal Data and Privacy, Paris, December 2010.

77) Alessandro Acquisti. Privacy and control. OECD 30th Annual Privacy Guidelines conference. Jerusalem, October 2010. (Plenary talk.)

78) Alessandro Acquisti. Consent: Illusion or Reality? International Data Protection and Privacy Commissioners Conference, Jerusalem, October 2010.

79) V. Bhagavatula: Super-resolution face recognition, invited seminar at Penn State University, State College, PA, March 3, 2011.

80) V. Bhagavatula. Signal processing approaches for biometric recognition, IEEE Pittsburgh Chapter, Pittsburgh, PA, April 8, 2011.

81) Onur Mutlu. Research funded by this grant was presented at the CyLab Partners Conference in fall of 2010; the 3-day PDL retreat and the PDL spring visit day (where it was the subject of several posters and talks); an invited talk at the International Workshop on Mobile Security 2010 (Santa Clara, CA, October 28, 2010); and a number of informal interactions with industry researchers (e.g., from Intel, Cisco).

82) Onur Mutlu. Memory Systems in the Many-Core Era: Challenges, Opportunities, and Solution Directions. Joint Keynote Talk, International Symposium on Memory Management (ISMM) and ACM Workshop on Memory System Performance and Correctness (MSPC), San Jose, CA, 5 June 2011

83) Onur Mutlu. Architecture and System-Level Challenges Related to Memory. Focus Center Research Program Memory Cross-Cut Workshop, Cambridge,MA, 12 May 2011.

84) Onur Mutlu. Architecting and Exploiting Asymmetry in Multi-Core Architectures: Two Studies. Intel, Santa Clara, CA, 9 March 2011.

85) Onur Mutlu. Towards Practical Bufferless On-Chip Networks. Intel, Santa Clara, CA, 9 March 2011.

86) Onur Mutlu. PCM (NVM) as Main Memory: Opportunities and Challenges. Carnegie Mellon University, Parallel Data Lab Retreat, Pittsburgh, PA, October 25, 2010.

87) Onur Mutlu. Research Challenges in Future Computing Platforms. Carnegie Mellon University, ECE Department Faculty Retreat, Wheeling, WV, August 12, 2010.

88) Onur Mutlu. Multi-core Architectures and Shared Resource Management: Fundamentals and Recent Research. Seoul National University, Lecture Series (12 hours), Seoul, Korea, July 6-9, 2010. Korea Advanced Institute of Science and Technology, Global Lecture Series (15 hours), Daejeon, Korea, July 26-29, 2010.

89) Onur Mutlu. End-to-end QoS-aware, High-Performance and Customizable Many-Core Memory Systems. Intel Memory Hierarchy Meeting, Hillsboro, OR, 8 October 2010.

90) William Scherlis and Jonathan Aldrich. Application-Specific Software Assurance. CyLab ARO review presentation, August 2009.

91) Jonathan Aldrich. Design Intent: A Principled Approach to Application Security. CyLab seminar, September 2009. Presentation at Boeing Application Security Developer's Forum on behalf of CyLab, September 2009.

92) K. Mai. Securing Storage Class Memories. Intel Memory Hierarchy Workshop, January 22, 2010.

93) K. Mai. Efficient Secure Digital Logic and Memory, C2S2 FCRP Portable Theme Meeting, July 26, 2010.

94) K. Mai. Side-Channel Attack Resistant ROM-Based AES S-Box, University of Cambridge Computer Laboratory Security Group Meeting, July 30, 2010.

95) K. Mai. Side Channel Attack Resistant ROM-Based AES Implementations, C2S2 FCRP E-Seminar, May 16, 2011.

96) K. Mai. Efficient Secure Digital Logic and Memory, C2S2 FCRP Enterprise Theme Meeting, July 11, 2011.

97) Patrick Tague. Adaptive Attack and Defense in Wireless Communication Systems, presentation at CyLab-Silicon Valley corporate partners' event, Nov, 2010.

98) Patrick Tague. Adaptive Attack and Defense in Wireless Networks", presentation at CMU-INI Graduate Seminar, Feb, 2011

99) Sasha Romanosky, David Hoffman (Beasley School of Law, Temple University), Alessandro Acquisti. Empirical Analysis of Data Breach Litigation. 39th Research Conference on Communication, Information and Internet Policy (Telecommunications Policy Research Conference, George Mason University Law School, Arlington, VA, September 23-25, 2011. Fourth Annual Privacy Law Scholars Conference (PLSC), Berkeley, CA, June 2-3, 2011. Seventh Annual Forum on Financial Information Systems and Cybersecurity: A Public Policy Perspective, University of Maryland, College Park, MD, January 19, 2011. Fifth Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection, Dartmouth College Hanover, NH, March 23–25, 2011

100) Stephen E. Fienberg. Privacy and network data, SAMSI Workshop on Dynamic Network Analysis. (January 12, 2011)

101) Stephen E. Fienberg. Participant in CMU Privacy Day panel discussion, Heinz College, Carnegie Mellon University. (January 26, 2011)

102) Stephen E. Fienberg. Statistical Disclosure Limitation & the Challenge of Societal-Scale Data, CMU Privacy Seminar. (March 24, 2011)

103) Stephen E. Fienberg. Getting Back to Basics: The Why and How of Statistical Disclosure Limitation vs. Privacy Protection, IAB Workshop on Privacy and Disclosure, Nuremberg, Germany. (June 30, 2011)

104) Rob Hall: January 26: Secure multi-party statistical computations, (poster) Carnegie Mellon Annual Data Privacy Day

105) Veek Purohit and Pei Zhang, SensorFly: A Collaboratively-Mobile Sensor Network (Poster), Cylab Partners Conference, Carnegie Mellon University, Pittsburgh, PA, September 2009.

106) Sasha Romanosky. Data Breaches and Identity Theft: When is Disclosure Optimal? – presented at the Sixth Annual Forum on Financial Information Systems and Cybersecurity: A Public Policy Perspective, University of Maryland, October 2009

107) Onur Mutlu, Designing High-Performance and Fair Shared Multi-core Memory Systems: Two Approaches. Presented the following venues and dates: Gigascale Systems Research Center E-Seminar, March 23, 2010; ARM, Inc., Austin, TX, April 8, 2010; Advanced Micro Devices, Austin, TX, April 9, 2010; Microsoft Research, Redmond, WA, April 27, 2010; HP Laboratories, Palo Alto, CA, May 25, 2010; VMware, Palo Alto, CA, May 26, 2010; Intel Corporation, Hillsboro, OR, May 27, 2010.

108) Onur Mutlu, Rethinking Memory System Design in the Nanoscale Many-Core Era. Presented the following venues and dates: Intel Memory Hierarchy Workshop, Hillsboro, OR, January 22, 2010; ASPLOS Workshop on Architecting Memory Technologies, Pittsburgh, PA, 14 March 2010.

109) Onur Mutlu, ATLAS: A Scalable and High-Performance Scheduling Algorithm for Multiple Memory Controllers. Presented the following venues and dates: Advanced Micro Devices Research Lab, Redmond, WA, October 2009; Freescale Semiconductor, Austin, TX, April 8, 2010.

110) Xin Zhang, Yanlin Li, and Onur Mutlu. More is Less: Denial-of-Service Attacks and Solutions in Many-Core On-Chip Networks. IEEE Symposium on Security and Privacy, May 2010.

111) Nancy Mead, Future Challenges of Security Requirements. Panelist, Grace Symposium on Security Requirements, June 9, 2008, National Institute of Informatics (NII), Tokyo, Japan.

112) Nancy Mead. Requirements Engineering for Improved System Security. Grace Symposium on Security Requirements, June 9, 2008, National Institute of Informatics (NII), Tokyo, Japan

113) Jonathan McCune. A Contractual Anonymity System: Experiences Building an Anonymity System using Trusted Computing.

114) Roy Maxion. Validity of Experiments in Trustworthy Computing. Johns Hopkins Applied Physics Laboratory, August 12, 2010

115) Roy Maxion. When Science Meets Security. Presented the following venues and dates: Pacific Northwest National Laboratory Roundtable on Cyber Security, August 27, 2010; RAID – Recent Advances in Intrusion Detection, September 24, 2009, St. Malo, France; . Information Security Institute: Mathematics Workshop on CyberSecurity, April 22, 2010, Gold Coast, Australia; Victoria University of Wellington, New Zealand, May 4, 2010

116) Roy Maxion. Dependability in the Time of Forensics, Latin American Dependability Symposium. Joao Pessoa, Brazil, September 2, 2009.

117) Roy Maxion. Keystroke Biometrics with Number-Pad Input. Queensland University of Technology, Australia, May 12, 2010.

118) K. Mai. Securing Emerging Non-Volatile Memory Technologies. Following venues and dates: Intel Symposium on Memory Hierarchy, January 2010; CMOS Emerging Technologies, May 2010.

119) Stephen Fienberg. Networks, E-commerce, and Privacy. Keynote Address for Conference on Statistical Challenges in Electronic Commerce Research, Heinz College, Carnegie Mellon University, May 31, 2009.

120) Stephen Fienberg. Rethinking the Risk-Utility Tradeoff Approach to Statistical Disclosure Limitation. Joint Statistics Meetings, Washington DC. August 3, 2009.

121) Rob Hall. Secure Multiparty Computation for Multiple Regression Computation. Joint Statistics Meetings, Washington DC, August 3, 2009.

122) Jiashin Jin. Privacy protection for sparse data, Workshop on Statistical and Learning-Theoretic Challenges in Data Privacy, IPAM, UCLA. February 24, 2010.

123) Rob Hall. Secure multiple linear regression based on homomorphic encryption, Workshop on Statistical and Learning-Theoretic Challenges in Data Privacy, IPAM, UCLA. February 25, 2010.

124) Bruno Sinopoli. Asymptotic Performance of Distributed Detection over Random Networks, The 2011 Santa Barbara Control Workshop: Decision, Dynamics and Control in Multi-Agent Systems, Santa Barbara, June 2011

125) Bruno Sinopoli. Detection Mechanisms for Integrity Attacks on Sensing and Control Software Systems, Northrop Grumman Corp. Research Consortium, Spring symposium, MacLean, VA April 2011

126) Bruno Sinopoli. Secure Control of Cyber-Physical Systems, TCIPG seminar, UIUC, April 2011

127) Bruno Sinopoli. Security of Smart Grids, A Cyber-Physical Perspective, CMU Silicon Valley Briefing, March 2011

128) Bruno Sinopoli. Secure Control of Cyber-Physical Systems, ISL Colloquium, Stanford University, March 2011

129) Bruno Sinopoli. Models and Control Strategies for Data Center Energy Efficiency, NCSU/SRI Workshop on Cyber-Physical Applications in Smart Power Systems, NCSU, February 2011

130) Bruno Sinopoli. A mean field games approach to nonlinear estimation, ITA Workshop, UC San Diego, February 2011

131) Bruno Sinopoli. Secure Control Against Replay Attacks, UC Berkeley, October 2010

132) Joy Ying Zhang. Oct. 2012: CyLab partners' annual meeting.

133) Joy Ying Zhang. "Mobile Sensing for Behavior-aware Mobile Computing A Language Approach," Language Technologies Institute Seminar, CMU, Pittsburgh, PA, May 3rd, 2012.

134) Joy Ying Zhang. "Mobile Sensing for Behavior-aware Mobile Computing," TechniColor Lab Seminar, Feb. 22, 2012.

135) Joy Ying Zhang. "Mobile Sensing for Behavior-aware Mobile Computing," Colloquium of Information, University of Northern Texas, Denton, TX, March 13, 2012.

136) Joy Ying Zhang. "Mobile Sensing for Behavior-aware Mobile Computing," Ericsson Research Lab Seminar, San Jose, CA, Dec. 8, 2011.

137) Joy Ying Zhang. "Mobile Sensing for Behavior-aware Mobile Computing," Nokia Research Center Seminar, Palo Alto, CA, Oct. 6, 2011.

138) Joy Ying Zhang. "Mobile Sensing for Behavior-aware Mobile Computing," Qualcomm Contextual Awareness Symposium, San Diego, CA, September 29-30, 2011.

139) Fienberg: Rob Hall, Alessandro Rinaldo, Larry Wasserman: "Differential privacy in reproducing kernel Hilbert spaces," ICML 2012 Workshop on Reproducing Kernel Hilbert Spaces.

140) B. DeBruhl, Y. S. Kim, and P. Tague, "A Toolbox to Explore the Interaction of Adaptive Jamming and Anti-Jamming", demo at INFOCOM 2012 (abstract available at http://wnss.sv.cmu.edu/papers/infocom-12dD.pdf).

141) Y. S. Kim and P. Tague, "Jamming-resistant Distributed Path Selection on Wireless Mesh Networks", demo at INFOCOM 2012 (abstract available at http://wnss.sv.cmu.edu/papers/infocom-12dK.pdf)

142) Michelle Mazurek: Towards usable access control for shared personal storage. PDL retreat, November 9, 2011.

143) Limin Jia: Run-time enforcement of information-flow properties on Android. Max Planck Institute for Software Systems. October 17, 2012.

144) "Are There Evolutionary Roots to Privacy Concerns?" Alessandro Acquisti, Laura Brandimarte, and Jeff Hancock, Security and Human Behavior workshop (SHB), 2012.

145) "An Experiment in Hiring Discrimination via Online Social Networks" Alessandro Acquisti and Christina Fong. Privacy Law Scholars Conference (PLSC), 2012.

146) "An Experiment in Hiring Discrimination via Online Social Networks" Alessandro Acquisti and Christina Fong. INFORMS Marketing Science Conference, 2012.

147) "An Experiment in Hiring Discrimination via Online Social Networks" Alessandro Acquisti and Christina Fong. 10th ZEW Conference on the Economics of Information and Communication Technologies, 2012.

148) "An Experiment in Hiring Discrimination via Online Social Networks" Alessandro Acquisti and Christina Fong. 40th Research Conference on Communication, Information and Internet Policy (TPRC), 2012.

149) "An Experiment in Hiring Discrimination via Online Social Networks" Alessandro Acquisti and Christina Fong. International Economic Science Association Conference, NYU, 2012.

150) "An Experiment in Hiring Discrimination via Online Social Networks" Alessandro Acquisti and Christina Fong. Bay Area Behavioral and Experimental Economics Workshop, 2012.

151) "An Experiment in Hiring Discrimination via Online Social Networks" Alessandro Acquisti and Christina Fong. Utah Winter Conference on Business Intelligence, 2012.

152) Sadeh: "Empowering Users to Make Sense of Android Permissions", Google Seminar, Google, Mountain View, October 2012

153) Sadeh: "Livehoods: Understanding the Dynamics of our Cities", TEDxTalk, Yale, October 2012.

154) Sadeh: “The SENSEable City”, Panel, Personal Democracy Forum, New York, June 2012

155) Sadeh: “Can We Reconcile Privacy and Usability?”, Computer Science Seminar Series, Hong Kong University of Science and Technology, May 2012

156) Sadeh: “Mobile Privacy: Technology and Human Consideration”, Expert Address, Hong Kong University, May 2012

157) Sadeh: “Smartphone Security and Privacy: What Should We Teach our Users and How?”, invited presentation, FISSEA 2012, NIST, March 2012

158) Sadeh: “User-Controllable Privacy: An Oxymoron?”, MIT CSAIL Seminar, March 2012

159) Sadeh: “From Today’s Android Permission System to Intelligent Security and Privacy Agents”, Google Seminar, Pittsburgh, December 20“Mobile and Pervasive Computing: Future Opportunities and Privacy Challenges”, keynote, Mobile Day, Pitney Bowles, Stamford, CT, October 2011.

160) Sadeh: Privacy Panel, panelist, Qualcomm’s Context Awareness Symposium, San Diego, September 2011

161) Zheng Sun, Aveek Purohit, Kathleen Yang, Neha Pattan, Dan Siewiorek, Asim Smailagic, Ian Lane, and Pei Zhang. “CoughLoc: Location-Aware Indoor Acoustic Sensing for Non-Intrusive Cough Detection”. In the International Workshop on Emerging Mobile Sensing Technologies, Systems, and Applications. Mobisense 2011 in conjunction with Pervasive, San Francisco, CA, June 2011.

162) Z. Sun, A. Purohit, Kathleen Yang, N. Pattan, D. Siewiorek, A. Smailagic, I. Lane, P. Zhang, VMA: An Inexpensive Indoor Acoustic Sensing Platform for In-home Patient Monitoring, The 8th International Conference on Mobile Systems, Applications, and Services. June, 2010.

163) B.V.K. Vijaya Kumar: Multiple uses of correlation filters for biometrics,” Keynote speech, International Conference on Hand Biometrics, Hong Kong, November 17, 2011.

164) B.V.K. Vijaya Kumar: “Correlation filters for biometrics,” Seminar at Department of Electrical and Computer Engineering, University of Houston, Houston, TX, December 9, 2011.

165) B.V.K. Vijaya Kumar: “Multiple uses of correlation filters for biometrics,” CYLab, Carnegie Mellon University, Pittsburgh, March 5, 2012.

166) B.V.K. Vijaya Kumar: “Matching challenging ocular images,” invited talk, SPIE Conference on Biometric Technology for Human Identification IX, Baltimore, April 23, 2012.

167) B.V.K. Vijaya Kumar: “Correlation filters for biometrics,” invited talk, Institute for Infocomm Research (I2R), Singapore, June 26, 2012.

Number of Presentations: 236.00

Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Received	Paper
08/05/2014	09.00 Alain Forget, , S. Komanduri, Alessandro Acquisti, Nicolas Christin , Lorrie Cranor, Robert Telang. Building the Security Behavior Observatory: An Infrastructure for Long-term Monitoring of Client Machines, Symposium and Bootcamp on the Science of Security (HotSoS) 2014, ACM. 31-JAN-14, . : ,
11/17/2014	72.00 Alexander H. Levis , Bahram Yousefi. Multi-Formalism Modeling for Evaluating the Effects of Cyber Exploits, 28th European Conference on Modeling and Simulation (ECMS2014). 27-MAY-14, . : ,
11/18/2014	76.00 Alain Forget, , S. Komanduri, , Alessandro Acquisti,, Nicolas Christin, , Lorrie Cranor, , Rahul Telang. Building the Security Behavior Observatory: An Infrastructure for Long-term Monitoring of Client Machines, Symposium and Bootcamp on the Science of Security (HotSoS) 2014, ACM. Raligh, NC, April 8-9, 2014. 08-APR-14, . : ,
11/19/2014	87.00 Nathan Fulton. Domain Specific Security through Extensible Type Systems, Proceedings of the SPLASH Student Research Competition, 2012. Tucson, AR, October 19-26, 2012. 19-OCT-12, . : ,

TOTAL: **4**

Number of Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Peer-Reviewed Conference Proceeding publications (other than abstracts):

Received	Paper
08/26/2013	92.00 David Garlan, Bradley Schmerl, Rui Abreu, Paulo Casanova. Diagnosing architectural run-time failures, 8th International Symposium on Software Engineering for Adaptive and Self-Managing Systems (SEAMS). 20-MAY-13, . : ,
08/26/2013	07.00 Nathan Fulton. Domain Specific Security through Extensible Type Systems, SPLASH Student Research Competition. 19-OCT-12, . : ,
08/26/2013	06.00 Simin Chen. Declarative Access Policies based on Objects, Relationships, and States, SPLASH Student Research Competition. 19-OCT-12, . : ,
08/26/2013	05.00 Darya Kurilova, Stephanie Balzer, Benjamin Chung, Alex Potanin, Jonathan Aldrich, Ligia Nistor. Wyvern: A Simple, Typed, and Pure Object-Oriented Language, Mechanisms for Specialization, Generalization, and Inheritance, 2013. 01-JUL-13, . : ,
08/26/2013	03.00 Blase Ur, Patrick Gage Kelley, Saranga Komanduri, Joel Lee, Michael Maass, Michelle Mazurek, Timothy Passaro, Richard Shay, Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor. How Does Your Password Measure Up? The Effect of Strength Meters on Password Creation, 21st USENIX Security Symposium. 08-AUG-12, . : ,
08/26/2013	95.00 Cyrus Omar, Benjamin Chung, Darya Kurilova, Alex Potanin, Jonathan Aldrich. Type-Directed, Whitespace-Delimited Parsing for Embedded DSLs, International Workshop on Globalization of Domain Specific Languages. 02-JUL-13, . : ,
09/09/2014	13.00 Tingting Yu, Witawas Srisa-an, Gregg Rothermel. SimRT: An Automated Framework to Support Regression Testing for Data , International Conference on Software Engineering (ICSE)Hyderabad, India. 2014. 31-MAY-14, . : ,
09/09/2014	21.00 Cyrus Omar, , Darya Kurilova, , Ligia Nistor, , Benjamin Chung, , Alex Potanin, , Jonathan Aldrich. Safely Composable Type-Specific Languages, Proc. European Conference on Object-Oriented Programming, 2014. 28-JUL-14, . : ,
09/09/2014	22.00 Joshua Sunshine, , James Herbsleb, , Jonathan Aldrich. Structuring Documentation to Support State Search: A Laboratory Experiment about Protocol Programming, Proc. European Conference on Object-Oriented Programming, 2014.. 28-JUL-14, . : ,
09/09/2014	23.00 Filipe Militão, , Jonathan Aldrich, , Luís Caires. Rely-Guarantee Protocols, Proc. European Conference on Object-Oriented Programming, 2014. 28-JUL-14, . : ,
09/09/2014	24.00 Michael Maass, , Jonathan Aldrich, , William Scherlis. In-Nimbo Sandboxing, Proc. Science of Security (HotSOS), 2014. 08-APR-14, . : ,
09/09/2014	25.00 Ligia Nistor, , Jonathan Aldrich, , Stephanie Balzer , Hannes Mehnert. Object Propositions, In Formal Methods, 2014.. 12-MAY-14, . : ,
09/09/2014	26.00 Jonathan Aldrich, , Luís Caires, Filipe Militão, . Substructural Typestates, In Programming Languages meets Program Verification, 2014.. 21-JAN-14, . : ,
09/09/2014	34.00 Cyrus Omar, , Darya Kurilova,, Ligia Nistor, , Benjamin Chung, Alex Potanin,, Jonathan Aldrich. Safely Composable Type-Specific Languages , The European Conference on Object-Oriented Programming, 2014.. 28-JUL-14, . : ,

09/09/2014 35.00 Alireza Sadeghi, Naeem Esfahani, Sam Malek. Mining the Categorized Software Repositories to Improve the Analysis of Security Vulnerabilities,
17th International Conference on Fundamental Approaches to Software Engineering (FASE 2014), Grenoble, France, April 2014.. 05-APR-14, . : ,

09/09/2014 37.00 Paulo Casanova, David Garlan, Bradley Schmerl, Rui Abreu. Diagnosing Unobserved Components in Self-Adaptive Systems,
9th International Symposium on Software Engineering for Adaptive and Self-Managing Systems, Hyderabad, India, 2-3 June 2014. . 01-JUN-14, . : ,

09/09/2014 38.00 Jonathan Aldrich, Cyrus Omar, Alex Potanin, Du Li. Language-Based Architectural Control,
International Workshop on Aliasing, Capabilities, and Ownership (IWACO '14), 2014. 29-JUL-14, . : ,

09/09/2014 36.00 Eric Yuan, Naeem Esfahani, Sam Malek. Automated Mining of Software Component Interactions for Self-Adaptation,
9th International Symposium on Software Engineering for Adaptive and Self-Managing Systems. Hyderabad, India, June 2014. . 01-JUN-14, . : ,

09/10/2014 52.00 A. Forget, , S. Komanduri,, A. Acquisti, , N. Christin, , L.F. Cranor, , R. Telang. Building the Security Behavior Observatory: An Infrastructure for Long-term Monitoring of Client Machines,
Symposium and Bootcamp on the Science of Security (HotSoS) 2014, ACM.. 08-APR-14, . : ,

09/10/2014 55.00 Bradley Schmerl, , Javier Camara, , Je ´ ffrey Gennari, , David Garlan,, Paulo Casanova, , Gabriel A. Moreno, , Thomas J. Glazier, , Jeffrey M. Barnes. Architecture-Based Self-Protection: Composing and Reasoning about Denial-of-Service Mitigations,
HotSoS 2014: 2014 Symposium and Bootcamp on the Science of Security, Raleigh, NC, USA, 8-9 April 2014. . 08-APR-14, . : ,

09/10/2014 56.00 Javier Camara, Gabriel Moreno, David Garlan. Stochastic Game Analysis and Latency Awareness for Proactive Self-Adaptation,
9th International Symposium on Software Engineering for Adaptive and Self-Managing Systems, Hyderabad, India, 2-3 June 2014. . 02-JUN-14, . : ,

09/10/2014 57.00 David Garlan. Software Architecture: A Travelogue,
Future of Software Engineering, Pages 29--39, ACM, New York, NY, USA , 2014. ISBN 978-1-4503-2865-4. Also available from ACM. 04-JUN-14, . : ,

11/19/2014 94.00 Blase Ur, , Patrick Gage Kelley, , Saranga Komanduri, , Joel Lee, , Michael Maass, , Michelle Mazurek, , Timothy Passaro, , Richard Shay, , Timothy Vidas, , Lujo Bauer, , Nicolas Christin,, Lorrie Faith Cranor. How Does Your Password Measure Up? The Effect of Strength Meters on Password Creation,
Proceedings of 21st USENIX Security Symposium, Bellevue, WA, August 8-10, 2012 . 08-AUG-12, . : ,

11/19/2014 95.00 Jonathan Aldrich. The power of interoperability,
the 2013 ACM international symposium. 29-OCT-13, Indianapolis, Indiana, USA. : ,

11/19/2014 84.00 Cyrus Omar, , Benjamin Chung, , Darya Kurilova, , Alex Potanin, , Jonathan Aldrich. Type Directed, Whitespace-Delimited Parsing for Embedded DSLs,
Proceedings of International Workshop on Globalization of Domain Specific Languages (GlobalDSL), 2013. Montpellier, France, July 2, 2013. 02-JUL-13, . : ,

11/19/2014 85.00 Ligia Nistor, , Darya Kurilova, , Stephanie Balzer, , Benjamin Chung,, Alex Potanin, , Jonathan Aldrich. Wyvern: A Simple, Typed, and Pure Object-Oriented Language,
Proceedings of Workshop on Mechanisms for Specialization, Generalization, and Inheritance (MASPEGHI), 2013. Montpellier, France, July 1, 2013. 01-JUL-13, . : ,

11/19/2014 86.00 Simin Chen. Declarative Access Policies based on Objects, Relationships, and States,
Proceedings of the SPLASH Student Research Competition, 2012. Tucson, AR, October 19-26, 2012. 19-OCT-12, . : ,

11/19/2014 88.00 Cyrus Omar, , Darya Kurilova, , Ligia Nistor, , Benjamin Chung,, Alex Potanin, , Jonathan Aldrich. Safely Composable Type-Specific Languages,
European Conference on Object-Oriented Programming (ECOOP), 2014. Uppsala, Sweden, July 28 - August 1, 2014. 28-JUL-14, . : ,

11/19/2014 89.00 Joshua Sunshine, , James Herbsleb, , Jonathan Aldrich. Structuring Documentation to Support State Search: A Laboratory Experiment about Protocol Programming,
European Conference on Object-Oriented Programming (ECOOP), 2014. Uppsala, Sweden, July 28 - August 1, 2014. 28-JUL-14, . : ,

11/19/2014 90.00 Filipe Militão, , Jonathan Aldrich, , Luís Caires. Rely-Guarantee Protocols,
European Conference on Object-Oriented Programming (ECOOP), 2014. Uppsala, Sweden, July 28 - August 1, 2014. 28-JUL-14, . : ,

11/19/2014 91.00 Michael Maass, , Jonathan Aldrich, , William Scherlis. In-Nimbo Sandboxing,
Proc. Symposium and Bootcamp on the Science of Security (HotSOS), 2014. Raleigh, NC, April 8-9, 2014. 08-APR-14, . : ,

11/19/2014 92.00 Ligia Nistor, , Jonathan Aldrich, , Stephanie Balzer , Hannes Mehnert. Object Propositions,
FM 2014: 19th International Symposium on Formal Methods, Singapore, May 12-16, 2014. 12-MAY-14, . : ,

11/19/2014 93.00 Filipe Militão, , Jonathan Aldrich, , Luís Caires. Substructural Typestates,
In Programming Languages meets Program Verification (PLPV), 2014. San Diego, CA, January 21, 2014. 21-JAN-14, . : ,

11/19/2014 78.00 Tingting Yu, , Witawas Srisa-an, , Gregg Rothermel. SimRT: An Automated Framework to Support Regression Testing for Data Races,
In Proceedings of the International Conference on Software Engineering (ICSE) 2014. Hyderabad, India, May 31 - June 7, 2014. 31-MAY-14, . : ,

11/20/2014 02.00 Eric Yuan, , Sam Malek, , Bradley Schmerl, , David Garlan, , Jeff Gennari. Architecture-Based Self-Protecting Software Systems,
Proceedings of the Ninth International ACM Sigsoft Conference on the Quality of Software Architectures (QoSA 2013), Vancouver, BC, Canada, June 17-21, 2013. 17-JUN-13, . : ,

11/20/2014 03.00 Cyrus Omar, , Darya Kurilova, , Ligia Nistor, , Benjamin Chung, , Alex Potanin, , Jonathan Aldrich. Safely Composable Type-Specific Languages,
European Conference on Object-Oriented Programming (ECOOP), 2014. Uppsala, Sweden, July 28 - August 1, 2014. 28-JUL-14, . : ,

11/20/2014 04.00 Filipe Militão, , Jonathan Aldrich, , Luís Caires. Rely-Guarantee Protocols,
European Conference on Object-Oriented Programming (ECOOP), 2014. Uppsala, Sweden, July 28 - August 1, 2014. 28-JUL-14, . : ,

11/20/2014 05.00 Alireza Sadeghi, , Naeem Esfahani, , Sam Malek. Mining the Categorized Software Repositories to Improve the Analysis of Security Vulnerabilities,
17th International Conference on Fundamental Approaches to Software Engineering (FASE 2014), Grenoble, France, April 2014.. 05-APR-14, . : ,

11/20/2014 06.00 Eric Yuan, , Naeem Esfahani, , Sam Malek. Automated Mining of Software Component Interactions for Self-Adaptation,
9th International Symposium on Software Engineering for Adaptive and Self-Managing Systems. Hyderabad, India, June 2014. . 03-JUN-14, . : ,

11/20/2014 07.00 Paulo Casanova, , David Garlan, , Bradley Schmerl, , Rui Abreu. Diagnosing Unobserved Components in Self-Adaptive Systems,
9th International Symposium on Software Engineering for Adaptive and Self-Managing Systems, Hyderabad, India, 2-3 June 2014. . 03-JUN-14, . : ,

11/20/2014 08.00 Jonathan Aldrich, , Cyrus Omar, , Alex Potanin,, Du Li. Language-Based Architectural Control, International Workshop on Aliasing, Capabilities, and Ownership (IWACO '14), 2014, Uppsala, Sweden, July 29th, 2014. 29-JUL-14, . : ,

11/20/2014 09.00 Cyrus Omar, , Benjamin Chung, , Darya Kurilova, , Alex Potanin, , Jonathan Aldrich. Type-Directed, Whitespace-Delimited Parsing for Embedded DSLs,
Globalization of Domain Specific Languages (GlobalDSL), 2013. 01-JUL-13, . : ,

11/20/2014 15.00 Radu Vanciu , Ebrahim Khalaj , Marwan Abi-Antoun. Comparative Evaluation of Architectural and Code-Level Approaches for Finding Security Vulnerabilities,
Workshop on Security Information Workers, co-located with the ACM Conference on Computer and Communications Security (CCS), 2014. Scottsdale, AZ, November 7, 2014. 07-NOV-14, . : ,

11/20/2014 14.00 Marwan Abi-Antoun , Sumukhi Chandrashekar , Radu Vanciu , Andrew Giang. Are Object Graphs Extracted Using Abstract Interpretation Significantly Different from the Code?,
IEEE International Working Conference on Source Code Analysis and Manipulation (SCAM), 2014. Victoria, BC, Canada, September 28-29, 2014. 28-SEP-14, . : ,

11/20/2014 16.00 Ebrahim Khalaj , Radu Vanciu , Marwan Abi-Antoun. Is There Value in Reasoning about Security at the Architectural Level: a Comparative Evaluation?,
Symposium and Bootcamp on the Science of Security (HotSoS), 2014. Raleigh, NC, April 8-9, 2014. 08-APR-14, . : ,

11/20/2014 17.00 Radu Vanciu , Marwan Abi-Antoun. Finding Architectural Flaws using Constraints,
IEEE/ACM Conference on Automated Software Engineering (ASE), 2013. Palo Alto, CA, November 11, 2013. 11-NOV-13, . : ,

TOTAL: 46

Number of Peer-Reviewed Conference Proceeding publications (other than abstracts):

(d) Manuscripts

Received		Paper
08/26/2013	96.00	Jonathan Aldrich. The Power of Interoperability: Why Objects are Inevitable, Onward! (10 2013)
09/09/2014	14.00	Tingting Yu, Witawas Srisa-an, Gregg Rothermel. ReflexScope: A Hybrid Analysis Approach to Demystify Reflection Usage in Android Apps, TBD (01 2014)
09/09/2014	15.00	Tingting Yu, Witawas Srina-an, Gregg Rothermel. RaceDr: A Just-in-time Atomicity Violation Repair Framework, To be submitted for publication (01 2015)
09/09/2014	16.00	Tingting Yu, Witawas Srisa-an, Gregg Rothermel. Leverage Redundancy in Hardware Transactional Memory to Improve System Reliability , TBD (01 2015)
11/20/2014	12.00	Jonathan Aldrich. The Power of Interoperability: Why Objects are Inevitable, Onward! (10 2013)
TOTAL:		**5**

Number of Manuscripts:

Books

Received	Book
08/26/2013 93.00	Ladan Tahvildari, Norha M. Villegas, Thomas Vogel, Danny Weyns, Kenny Wong , Jochen Wuttke, Rogério de Lemos, Holger Giese, Oscar Nierstrasz, Mauro Pezzè, Christian Prehofer, Wilhelm Schafer, Rick Schlichting, Serge Mankovskii, Bradley Schmerl, Dennis B. Smith, João Pedro Sousa, Gabriel Tamura, Marin Litoiu, Antonia Lopes, Jeff Magee, Sam Malek, Raffaela Mirandola, John Mylopoulos, Hausi A. Muller, Mary Shaw, Jesper Andersson, Luciano Baresi, Basil Becker, Nelly Bencomo, Yuriy Brun, Bojan Cukic, Ron Desmarais, Schahram Dustdar, Gregor Engels, Kurt Geihs, Karl M. Goeschka, Alessandra Gorla, Vincenzo Grassi, Paola Inverardi, Gabor Karsai, Jeff Kramer. Software engineering for self-adaptive systems: A second research roadmap, Berlin Heidelberg: Springer-Verlag, (05 2013)
08/26/2013 98.00	Kathleen Carley, Geoffrey Morgan. Modeling Formal and Informal Ties Within an Organization: A Multiple Model Integration, Global: Emerald Group Publishing Ltd, (11 2012)
11/17/2014 66.00	Kathleen Carley, Geoffrey Morgan . Modeling Formal and Informal Ties within an Organization: A Multiple Model Integration," The Garbage Can Model of Organizational Choice: Looking Forward at Forty, unknown: Emerald Group Publishing Limited, (11 2012)
TOTAL:	**3**

Received	Book Chapter
TOTAL:	

Patents Submitted

SoS Lablet

Michael Maass, Bill Scherlis, Jonathan Aldrich - Language and Framework for Development of Secure Mobile Apps "In-Nimbo Sandboxing"

Perpetually Available and Secure Information Systems

1) Yang Cai, Object-Based Multi-Resolution Video Streaming (US Patent)
2) Yang Cai, Eye-Tracking Based Multi-Resolution Video Streaming (US Patent)
3) Alessandro Acquisti. U.S. Nonprovisional Patent Application Serial No.: 13/177,157; Filed: 7/6/2011 Title: Validating Legitimacy of a Social Security Number or Other Identifier Inventors: Alessandro Acquisti et al. CMU Reference No.: 2009-012 DRM File No.: 13556-017USU1
4) Yang Cai. The patent application on Context-Based Multiple Resolution Video Compression was filed on July 17, 2008 (our docket number 2007-014). It was published by the USPTO on 9/16/10.
5) Yang Cai. The patent application on Eye Tracking Based Network Data Flow Control was also filed on July 17, 2008 (our docket number 2007-015. Published by the UPSTO on 11/11/10.
6) Shawn Blanton. None, but an IP disclosure to the university is forthcoming.

Patents Awarded

Perpetually Available and Secure Information Systems

---

1) Pei Zhang, Zheng Sun, Aveek Purohit, Trevor Pering, PANDAA: A Physical Arrangement Detection Technique for Networked Devices through Ambient-Sound. 12/12/2011

2) Pei Zhang, Zheng Sun, Aveek Purohit, Trevor Pering, POLARIS: Orientation through Ambient Images.

Awards

Kathleen Carley - Learned Resiliency in Multi-Level Systems

1)Kathleen Carley - Member of the NAS/NRC Committee on Digital Math Library, 2012-13

2) Kathleen Carley - DHS Homeland Security Science and Technology Advisory Committee, HSSTAC, SGE. Also member of special sub-group on cyber-security, 2012-13

3) Kathleen Carley - IEEE Fellow, 2013

4) Kathleen Carley - Allen Newell Award for Research Excellence - “For the creation of empirical methods to rigorously establish the impact of human communication on software quality.” 2014

5) Kathleen Carley - Member of the NAS ARL Review Panel, 2014

Kathleen Carley, Geo-Temporal Characterizations

1) Kathleen Carley - Member of the NAS/NRC Committee on Digital Math Library, 2012-13

2) Kathleen Carley, DHS Homeland Security Science and Technology Advisory Committee, HSSTAC, SGE , Also member of special sub-group on cyber-security, 2012-13

Jonathan Aldrich, A Language and Framework for Development of Secure Mobile Apps

1) Nathan Fulton, Cyrus Omar, and Jonathan Aldrich. "Statically Typed String Sanitation Inside a Python," PSP Best paper award

2) Cyrus Omar, Darya Kurilova, Ligia Nistor, Benjamin Chung, Alex Potanin, and Jonathan Aldrich. "Safely Composable Type-Specific Languages" awarded ECOOP 2014 Distinguished Paper Award

David Garlan, Jonathan Aldrich, Bradley Schmerl - Science of Secure Frameworks

1) Sam Malek, Mason Emerging Researcher/Scholar/Creator Award

2) David Garlan, ACM Fellow

Perpetually Available and Secure Information Systems

1) David Brumley received DARPA CSSG Award.
2) Vijayakumar Bhagavatula elected 2010 IEEE Fellow.
3) Vijayakumar Bhagavatula named co-chair of the SPIE 2010 conference on Biometric Technology for Human Identification VII.
4) PhD student Patrick Kelley a winner in ACM Student Research Competition Grand Finals.
5) Greg Ganger received HP Innovation Partnership Award.
6) Greg Ganger awarded Jatras Chair.
7) Bruno Sinopoli received 2009 NSF Career Award.
8) Alessandro Acquisti named EPIC advisory board member.
9) Alessandro Acquisti won Heinz College ISM Teaching Award.
10) Stephen Fienberg received Founders Award, American Statistical Association.
11) Yang Cai received AFRL 2010 Summer Faculty Fellowship.
12) Eiman Ebrahimi, Chang Joo Lee, Onur Mutlu, and Yale N. Patt received Best Paper Award for Fairness via Source Throttling: A Configurable and High-Performance Fairness Substrate for Multi-Core Memory Systems, 15th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS), 2010.
13) Onur Mutlu received NSF CAREER Award, Scalable, High-Performance, and QoS-Aware Many-Core Memory Systems, 2010.
14) Aveek Purohit and Pei Zhang received Best Demo Award for SensorFly: a controlled-mobile aerial sensor network. In Proceedings of the 7th ACM, 2009.
15) Best paper award at ACM Conference on Wireless Network Security (WiSec), March 2010. Ahren Studer and Adrian

Perrig. Paper title: ``Mobile User Location-specific Encryption (MULE): Using Your Office as Your Password."
16) Adrian Perrig won the Information Security Magazine, Security 7 award in the category of education, “Improving SSL/TLS Security Through Education and Technology”, 2009.
17) Alessandro Acquisti. Future of Privacy Forum's Best Privacy Papers for Policy Makers Competition. (Author of 2 out of 6 selected Leading papers), 2010. Alessandro Acquisti. Privacy and the Control Paradox, Best Student Paper Award (Lead author: Laura Bradimarte), CIST 2010. (Also Runner-up for best paper award), 2010.
18) Alessandro Acquisti. Opening Speaker: Privacy Symposium: Vie Privie & Riseaux Sociaux en Ligne: Nouveaux Comportements et Nouvelles Regulations, "From the Illusion of Control to Discounting the Past: Privacy and Behavior," Universite Paris-Sud, Faculte Jean Monnet, March 2011.
19) Alessandro Acquisti. Keynote: Computers, Freedom, and Privacy Conference (CFP), "Privacy in the Age of Augmented Reality," Washington DC, June 2011.
20) Nicolas Christin. CHI 2011 “Honorable mention” for the paper above cited (Komanduri et al.).
21) Lorrie Cranor. CHI 2011 paper received best paper honorable mention
22) V. Bhagavatula. Co-author, 2010 Best Innovative Paper award at the Biometrics: Theory, Applications and Systems (BTAS) conference.
23) V. Bhagavatula. Co-chair of the April 2011 SPIE conference on Biometric Technology for Human Identification VIII.
24) Onur Mutlu. IEEE Computer Society Technical Committee on Computer Architecture Young Computer Architect Award, 2011.
25) Onur Mutlu. Best paper award at ASPLOS 2010 - Fairness via Source Throttling: A Configurable and High-Performance Fairness Substrate for Multi-Core Memory Systems.
26) Onur Mutlu. Best paper award at VTS 2010 Concurrent Autonomous Self-Test for Uncore Components in System-on-Chips.
27) Onur Mutlu. Three papers (of 11 total) selected for IEEE Micro’s “op Picks from Computer Architecture Conferences 2010 – Thread Cluster Memory Scheduling: Exploiting Differences in Memory Access Behavior, Aergia: Exploiting Packet Latency Slack in On-Chip Networks, Data Marshaling for Multi-core Architectures.
28) Dean F. Sutherland and William L. Scherlis. Best paper finalist (one of two): Composable Thread Coloring. Principles and Practice of
29) Parallel Programming (PPoPP) 2010, January 2010.
30) Bryan Parno, ACM Dissertation Award, May 2011.
31) Adrian Perrig, Benjamin Richard Teare Teaching Award from the College of Engineering, Carnegie Mellon University, March 2011.
32) Bruno Sinopoli. 2010 CIT George Tallman Ladd Research Award, made to a faculty member within the Carnegie Institute of Technology in recognition of outstanding research and professional accomplishments and potential.
33) Greg Ganger invited to testify before U.S. Congress on the benefits and risks of moving federal IT functions to the cloud
34) Greg Ganger: HP Innovation Partnership Award
35) Greg Ganger: Jatras Chair awarded
36) Christin: Invited plenary keynote at GameSec 2011.
37) P.Tague, NSF CAREER Award, “Inference-Based Adaptation Techniques for Next Generation Jamming and
38) Anti-Jamming Capabilities”, 2012-2017.
39) Michelle Mazurek was awarded a Facebook Fellowship for academic year 2012-13.
40) Acuisti:
41) “Are There Evolutionary Roots to Privacy Concerns?” Alessandro Acquisti, Laura Brandimarte, and Jeff Hancock.
42) National Science Foundation SATC grant (about 350k, 2012-2014).
43) 2012 Information Systems Research – Best paper published in 2011
44) 2012 IAPP Privacy Law Scholars Conference Best Paper Award.
45) 2012 Selected, Future of Privacy Forum's "Privacy Papers for Policy Makers" 2012.
46) 2011-2012 Member, National Academies’ Committee on “Public Response to Alerts and Warnings Using Social Media and Associated Privacy Considerations.”
47) 2012 Visiting Fellow, Becker/Friedman Institute for Research in Economics, University of Chicago.
48) 2012 Nominated, Heinz College Martcia Wade Teaching Award.
49) 2012 Amsterdam Privacy Conference, Amsterdam, October 2012. (Keynote.)
50) 2012 Annual Privacy Forum, Cyprus, October 2012
51) 2012 TED MidAtlantic, University of Maryland College Park, October 2012. (Invited speaker.)
52) International Association of Privacy Professionals - European Annual Conference, "Privacy in the Age of Augmented Reality," London, April 2012. (Keynote)
53) ISchool, UC Berkeley, "An Experiment in Hiring Discrimination via Online Social Networks," Berkeley, April 2012. (Dean's Lecture)
54) Wall Street Journal, Data Transparency Weekend, New York, April 2012. (Invited speaker.)
55) Stanford CIS Speaker Series, “Privacy in the Age of Augmented Reality,” Stanford University, April 2012. (Invited speaker.)
56) Metricon Workshop (RSA Conference 2012), "Valuating Privacy," San Francisco, February 2012. (Opening Speaker)
57) Conference on the Economics of Privacy, "The Economics of Privacy," University of Colorado, Boulder, December

2011. (Keynote)
58) International Association of Privacy Professionals - Australia and New Zealand - Annual Conference, "Privacy in the Age of Augmented Reality," Melbourne, November 2011. (Keynote)
59) SCL 6th Annual Policy Forum: The New Shape of European Internet Regulation, "Privacy, Behavior, and Regulation,"
60) London, September 2011. (Keynote)
61) Conference on the Economics of Information and Communication Technologies, "Privacy, Economics, and Behavioral Economics," Paris, October 2011. (Keynote)
62) Sadeh: June 2012: Best Paper Award - 6th International AAAI Conference on Weblogs and Social Media (ICWSM-12)
63) Zhang, Pei: Best Demo Award, 13th International Conference on Ubiquitous Computing (UBICOMP'11).
64) B.V.K. Vijaya Kumar: Co-chair of the April 2012 SPIE conference on Biometric Technology for Human Identification
65) B.V.K. Vijaya Kumar: Chair, IEEE Biometrics Council Fellow Evaluation Committee

Graduate Students

NAME	PERCENT_SUPPORTED	Discipline
Arbob Ahmad	0.93	
Michael Arntzenius	0.29	
Vishal Dwivedi	0.04	
Hanan Hibshi	0.12	
Kuen-Bang Hou	0.60	
Krutika Kamilla	0.03	
Kurilova Darya	0.89	
Momin Malik	0.07	
Ghita Mezzour	0.49	
Geoffrey Morgan	0.61	
Cyrus Omar	0.37	
Jigar Patel	0.08	
Ashwini Giridhar Rao	0.36	
Cassandra Urmano	0.09	
Wei Wei	0.10	
Erik Zawadski	0.92	
Shahriyar Amini	0.27	
Michael Abd-El-Malek	0.02	
Ramzi Abi Antoun	0.02	
Mohammadreza Aghajani	0.01	
Michael Ashley-Rollman	0.01	
Arjun Athreya	0.07	
Rachata Ausavarungnirun	0.02	
Athanasios Avgerinos	0.08	
Pranjal Awasthi	0.10	
Yogesh Makarand Badwe	0.00	
Athula Balachandran	0.15	
Aniruddha Basak	0.11	
Avni Baveja	0.00	
Rahul Baxi	0.19	
Jonathan Becker	0.15	
Nels E Beckman	0.01	
Aravind Bharadwaj	0.02	
Mudit Bhargava	0.01	
Aditya Bhave	0.02	
Ashwini Anant Bijwe	0.00	
Yasodekshna Vishnu Boddeti	0.28	
Joanna Bresee	0.01	
Senaka Buthpitiya	0.02	
Cagla Cakir	0.11	
Sang Kil Cha	0.02	
Rohan S Chabukswar	0.05	
Anne-Sophie Charest	0.15	
Clifford Chen	0.05	
Eric Chen	0.09	
Heng-Tze Cheng	0.03	
Travis W Christian	0.00	
James A Cipar	0.11	
Michele Cossalter	0.02	
Justin B Cranshaw	0.01	
Scott Ian Davidoff	0.06	
Bruce E Debruhl	0.05	
Sweta Deivanayagam	0.01	
Yun Du	0.18	
Rituik Dubey	0.00	

Tudor Dumitras	0.15
Vishal Dwivedi	0.16
David Guido Eggerschwiler	0.00
Christopher I Fallin	0.01
Dhenuka Ganesh	0.00
Jared G Goerner	0.03
Anuj Gupta	0.02
Pragna Halder	0.01
Robert J Hall	0.40
Michael Hanley	0.01
Diana Mary Hazel	0.00
Kuen-Bang Hou	0.43
Matthew Robert Houy	0.12
Hsu-Chun Hsiao	0.01
Xinyao Hu	0.01
Lin-Shung Huang	0.22
Alexa Huth	0.03
Eui Seok Hwang	0.15
Dinesh D Israni	0.01
Mehul Jain	0.01
Umar Javed	0.03
Leslie K John	0.05
Da-Cheng Juan	0.02
Abhinav R Kadiri	0.00
Keisuke Kamataki	0.01
Arvind Kandhalu Raghu	0.11
Miray Kas	0.00
Patrick G Kelley	0.09
Kevin Killourhy	0.19
Hyun Jin Kim	0.01
Jung Soo Kim	0.17
Yoongu Kim	0.15
Yu Seung Kim	0.08
Peter F Klemperer	0.13
Saranga Komanduri	0.08
Himanshu Shishir Koshe	0.08
Meghana Koushik	0.01
Elie Krevat	0.11
Abhinandan Krishnan	0.19
Avijit Kumar	0.01
Kumar Kunal	0.05
Shing-Hon Lau	0.36
Patrick Lazik	0.20
Jason Lee	0.21
Sihyung Lee	0.26
Nektarios Leontiadis	0.50
Kyriaki Levanti	0.17
Yuan Liang	0.24
Daniel R Licata	0.01
Hyeontaek Lim	0.05
Lynly Marie Lumibao	0.00
Weinan Ma	0.17
Lawrence S Maccherone	0.12
Chris Martens	0.02
Mark Mccartney	0.22
Sean Thomas Mclaughlin	0.25
Eric R Menendez	0.05
Margaret Menis	0.00
Justin Meza	0.20

Ghita Mezzour	0.00
Yilin Mo	0.01
Iulian Moraru	0.20
Jamie Morgenstern	0.19
Reinhard Richard Munz	0.13
Karl Bascom Naden	0.21
Cheong Kin Ng	0.01
Jacob Oresick	0.16
Fatih Kursat Ozenc	0.04
Rahul Pandey	0.01
Varokas Panusuwan	0.01
Luca Parolini	0.09
Vishal Patel	0.02
Huan-Kai Peng	0.25
Soila Pertet	0.14
Stephanie Rosen Pomerantz	0.01
Nithin Prahalah Betegeri	0.01
Rahul Rajan	0.16
Sureshbabu Rajasekaran	0.03
Abhishek Ramani	0.04
Ashwini Giridhar Rao	0.06
John A Reppert	0.04
Andres Rodriguez-Perez	0.02
Sasha L Romanosky	0.19
Raunak Rungta	0.04
Guillermo Salas	0.02
Raja Raman Sambasivan	0.10
Akkarit Sangpetch	0.02
Thejas Sasidhara Varier	0.00
Edward J Schwartz	0.24
Divya Sharma	0.01
Tarun Sharma	0.29
Richard J Shay	0.02
Or Sheffet	0.15
Stephen Siena	0.06
Arunesh Sinha	0.18
Parineeta Sinha	0.02
Shafeeq Sinnamohideen	0.06
Kristina Sojakova	0.33
Sudheer Someshwara	0.01
Derrick Spooner	0.04
Ahren M Studer	0.01
Madhusudan Subbu	0.00
Lavanya Subramanian	0.34
Orathai Sukwong	0.01
Zheng Sun	0.30
Priya Krishnan Sundararajan	0.02
Joshua S Sunshine	0.02
Karen Pei-Yi Tang	0.01
Kanat Tangwongsan	0.02
Kanupriya Tavri	0.01
Craig R Teegarden	0.21
Quoc N Tran	0.01
Janice Y Tsai	0.00
Michael Carl Tschantz	0.58
Andrew Turner	0.23
Fnu Unni Prasad	0.01
Vijay Vasudevan	0.11
Shreyas Venugopalan	0.02

Shankar Viswanathan	0.00
Matthew Wachs	0.02
Hongfei Wang	0.47
Xiao Wang	0.08
Benjamin J Weaver	0.00
Robert Weiland	0.01
James E Weimer	0.16
Zachary Weinberg	0.18
Roger E Wolff	0.27
Kai-Chiang Wu	0.15
Guang Xiang	0.24
Lianghong Xu	0.35
Shishir K Yadav	0.01
Xiaolin Yang	0.10
Xiaoqi Yin	0.05
Hanbin Yoon	0.05
Luke Thomas Zarko	0.26
Sabina Zejnilovic	0.13
Yi Zhang	0.25
Yu Zhang	0.03
Zongwei Zhou	0.10
Jiang Zhu	0.15
FTE Equivalent:	**23.47**
Total Number:	**195**

Names of Post Doctorates

NAME	PERCENT_SUPPORTED
Stephanie Balzer	0.47
Nikou Gunnemann-Gholizadeh	0.99
Du Li	0.84
Alex Potanin	0.10
New Entry	0.00
Haw Wuen Chan	0.15
Deepak Garg	0.13
Limin Jia	0.17
Benjamin Edward Johnson	0.28
Yung-Wei Kao	0.03
Zeliha Dilsun Kaynar	0.23
Jong Hyup Lee	0.01
Soo Bum Lee	0.31
Natalie Linnell	0.04
Ganeshraj Manickaraju	0.03
Robert M Mcguire	0.13
Balakrishnan Narayanaswamy	0.16
James E Springfield	0.01
Ngyuen Thanh	0.01
Osman Yagan	0.21
FTE Equivalent:	**4.30**
Total Number:	**20**

Names of Faculty Supported

NAME	PERCENT_SUPPORTED	National Academy Member
Alessandro Acquisti	0.10	No
Jonathan Aldrich	0.14	
Travis Breaux	0.20	
Kathleen Carley	0.17	
Nicolas Christin	0.08	
Lorrie Cranor	0.09	
Anupam Datta	0.09	
David Garlan	0.01	
Juergen Pfeffer	0.06	
Frank Pfenning	0.15	
Andre Platzer	0.05	
William Scherlis	0.17	
Bradley Schmerl	0.16	
Limin Jia	0.04	
David J Farber	0.03	No
David Garlan	0.04	No
Virgil D Gligor	0.20	No
Daniel R Golovin	0.03	No
Martin Griss	0.12	No
Eija Haapalainen	0.02	No
Chin Hyuk Hong	0.13	No
Aldrich, Jonathan E	0.11	
Ljudevit Bauer	0.23	No
Yang Cai	0.19	
Charles Cranor	0.23	
Anupam Datta	0.22	
John M. Dolan	0.02	
Collin Jackson	0.19	No
Kenneth W Mai	0.03	No
Jonathan Mccune	0.17	No
Yuval Nardi	0.01	No
James Newsome	0.20	No
Adrian Perrig	0.13	No
Anthony Rowe	0.05	No
William L Scherlis	0.03	No
Bradley Schmerl	0.03	No
Edwin Selker	0.03	No
Daniel P Siewiorek	0.03	No
Asim Smailagic	0.03	No
Dean F Sutherland	0.25	No
Patrick Tague	0.04	No
Denzil Socrates Teixeira Ferreira	0.02	No
Eran Toch	0.16	No
Shomir Wilson	0.13	No
Jeannette Wing	0.18	No
Pei Zhang	0.16	No
Ying Zhang	0.24	No
FTE Equivalent:	**5.19**	
Total Number:	**47**	

Names of Under Graduate students supported

NAME	PERCENT_SUPPORTED	Discipline
Benjamin Chung	0.93	
Jia Jun Brandon Lum	0.37	
Rahul Manne	0.38	
Wen Jay Tan	0.59	
New Entry	0.00	
Maryam A Aly	0.01	
Andrew Bunn	0.02	
Lucian J Cesca	0.29	
Emily Marie Durbin	0.10	
Ian Gillis	0.01	
Ankur Goyal	0.01	
Rachael A Harding	0.12	
Aaron Hsu	0.01	
Nikhil K Khadke	0.05	
Joseph H Lee	0.01	
Sizhe Liu	0.08	
Brian Pak	0.18	
Hannah Post	0.01	
David Schlesinger	0.19	
Ayman J Singh	0.32	
Elizabeth Solomon	0.07	
Apaorn Suveepattananont	0.06	
Wennie Tabib	0.11	
Ian Voysey	0.25	
FTE Equivalent:	**4.17**	
Total Number:	**24**	

Student Metrics

This section only applies to graduating undergraduates supported by this agreement in this reporting period

The number of undergraduates funded by this agreement who graduated during this period: 0.00

The number of undergraduates funded by this agreement who graduated during this period with a degree in science, mathematics, engineering, or technology fields:..... 0.00

The number of undergraduates funded by your agreement who graduated during this period and will continue to pursue a graduate or Ph.D. degree in science, mathematics, engineering, or technology fields:..... 0.00

Number of graduating undergraduates who achieved a 3.5 GPA to 4.0 (4.0 max scale):..... 0.00

Number of graduating undergraduates funded by a DoD funded Center of Excellence grant for Education, Research and Engineering:..... 0.00

The number of undergraduates funded by your agreement who graduated during this period and intend to work for the Department of Defense 0.00

The number of undergraduates funded by your agreement who graduated during this period and will receive scholarships or fellowships for further studies in science, mathematics, engineering or technology fields:..... 0.00

Names of Personnel receiving masters degrees

NAME	
Michael Lanham	
Joshua Sunshine, December 2013	
Joanna Bresee	
Rituik Dubey	
Jared G Goerner	
Jung Soo Kim	
Yuan Liang	
Stephanie Pomerantz	
John Reppert	
Parineeta Sinha	
Craig Teegarden	
Hongfei Wang	
Hanbin Yoon	
Total Number:	**13**

Names of personnel receiving PHDs

NAME	
Michael Lanham, exp May '15	
Joshua Sunshine, December 2013	
Radu Vanciu, May 2014	
Naeem Esfahaini, August 2014	
Yasodekshna Vishnu Boddeti	
James V Hendricks	
Eui Seok Hwang	
Sihyung Lee	
Kyriaki Levanti	
Lawrence S Maccherone	
Mark Mccartney	
Sasha Romanosky	
Shafeeq Sinnamohideen	
Janice Tsai	
Jijay Vasudevan	
Kai-Chiang Wu	
Total Number:	**16**

Names of other research staff

NAME	PERCENT_SUPPORTED
Monika DeReno	0.10
Jamie Hagerty	0.21
Tiffany Todd	0.01
Alain Forget	0.10
Michael Kowalchuck	0.18
Lee Ju-Sung	0.10
Jeremy Thomas	0.25
Amit Thomas	0.14
Michael Balderson	0.22
Chandrasekhar Bhagavatula	0.13
Madhusudan Bhagavatula	0.25
Andrew Bun	0.08
Christopher Canning	0.02
William V Courtright	0.03
Nichole Dwyer	0.12
Zisimos Odyss Economou	0.03
Michael Farb	0.30
Mitchell Franzos	0.11
Reto Grieder	0.18
Ralph Gross	0.16
Marco Gruteser	0.09
Aaron Jaech	0.25
Chaitra Kamath	0.03
Yung-Wei Kao	0.03
Khoa Luu	0.27
Jonathan M Mccune	0.11
Andrea Meythaler	0.08
James Duran Newsome	0.31
Thanh Le Nguyen	0.03
Karoly D Pados	0.01
Rahul Pandey	0.08
Richard Power	0.12
Nithin Prahalad	0.31
Manish Prasad	0.10
Shivkant Ranade	0.14
Steven Rosenberg	0.06
Sharat Sannabhadti	0.11
Cathy Schaefer	0.22
Elizabeth Solomon	0.28
Jean Stamberger	0.03
Michael Stroucken	0.11
Pat Sweeney	0.03
Amit Vasudevan	0.06
Spencer Whitman	0.07
Tina Yankovich	0.23
Xiaolin Zang	0.11
FTE Equivalent:	**5.99**
Total Number:	**46**

Sub Contractors (DD882)

Inventions (DD882)

Scientific Progress

SoS Lablet

Jonathan Aldrich - Race Vulnerability Study and Hybrid Race Detection

•We finished the implementation to adapt the results of static analyses with dynamic analyses by feeding static analysis to the JVM when it launches. This increases the start-up time of JVM, but this overhead pays off for long-running applications.

•We created a database of race-related vulnerabilities and associated artifacts. The database now includes race-related vulnerabilities from the four major browsers (IE, Chrome, Safari, and Firefox). Vulnerabilities were culled from the National Vulnerability database, project bug repositories, and security mailing lists (e.g. Full Disclosure). For open source browsers, Chrome and Firefox, tests to replicate vulnerabilities and patches to fix vulnerabilities are included in the database.

•We formalized our race detection algorithm. The formalization consists of static and dynamic semantics that are consistent with the program analyses we implemented in our hybrid race detection system.

•We are working to develop dynamic analysis techniques inside Just-In-Time compilers. As static analysis tools become more effective at detecting security vulnerabilities, malware writers have to rely more on dynamism of today's software to deliver malicious intents. For example, the use of custom class loaders to dynamically load malicious code segments or the use of reflection to invoke external malicious methods provides ways for malware to escape detection efforts by static analysis tools. As code segments are being loaded through these mechanisms, we must be able to inspect them for potential malicious intents. They propose an approach to use a JIT compiler to detect dynamically loaded code for potential vulnerabilities during deployment. We are currently modifying the JIT compiler in OpenJDK to detect information leakage. As of now, the work is about 65% complete.

•We are also developing dynamic taint analysis framework to monitor information flow during deployment. Activity 1 provides us with the capability to detect potential vulnerabilities in dynamically loaded classes. To verify whether these vulnerabilities are real, we need to observe information that is flowing into methods of these classes. For example, if our approach detects that a method can store information to the SD card, it flags this method as containing a potential vulnerability. The real vulnerability can be confirmed by observing if sensitive information, such as entries from the address book, can actually reach this method. To do so, we need to be able to perform dynamic taint analysis. We are currently building the dynamic taint analysis framework in OpenJDK. The work is about 70% complete.

Jonathan Aldrich - A Language and Framework for Development of Secure Mobile Applications

Activity in progress:
•We developed a formal system for safely composing separately defined type system fragments with modular type constructors. We establish several strong semantic guarantees, notably type safety, stability of typing under extension and conservativity: that the type invariants that a finite set of fragments maintain are conserved under extension.

•The implementation of the Wyvern language continued. We added several important language features (e.g. type parameters), improved interoperability with Java, and completed a first implementation of language extensibility.

•We continued to define Wyvern in its specification. The working draft is available at http://www.cs.cmu.edu/~aldrich/securemobileweb/spec-rationale.html

Major results:
•In-Nimbo Sandboxing (HotSOS '14). In-Nimbo Sandboxing is a new concept that encapsulates untrusted or hard-to-assure computation by running it on ephemeral computing resources in a cloud computing environment. It has the advantage that any malicious state resulting from the computation will not persist in a high-value environment even if other controls on the computation fail. In-Nimbo Sandboxing can provide additional security in a mobile, desktop, or web environment. As a proof of concept, we built a sandbox for Adobe Reader, which has been repeatedly compromised in the past. We also developed a novel scheme for analyzing the level of security provided by a sandbox, enabling sandboxing techniques to be compared effectively.

•Safely Composable Type-Specific Languages (ECOOP '14). Command injection vulnerabilities are common in part because programmers compose commands by combining strings rather than using more structured, but inconvenient, representations such as prepared SQL statements. A promising mitigation is to provide programmers with mechanisms for constructing commands that are as convenient as strings while being as secure as prepared SQL statements. Mechanisms for embedding domain-specific languages (DSLs) for constructing commands within a programming language exist, but none have achieved widespread use, in part because prior techniques were unmodular, so that separately-defined embedded DSLs could not be

used together. We describe a novel mechanism called type-specific languages that supports modular DSL embeddings by associating a unique DSL with appropriate types. When the programmer wants to construct an instance of such a type--a database query, for example--he or she can define the instance using the associated DSL (SQL, in this example). Our paper describes the mechanism and states safety and composability properties of the design. The paper also includes results from an empirical study suggesting that strings are in very widespread use for constructing domain-specific object structures, indicating that our approach should have broad applicability.

•Structuring Documentation to Support State Search: A Laboratory Experiment about Protocol Programming (ECOOP '14). Incorrect use of libraries that require developers to follow a protocol is at the core of significant security vulnerabilities, such as the SSL libraries described in the CCS'12 paper "The most dangerous code in the world: validating SSL certificates in non-browser software." We developed a novel tool-supported intervention that makes the states defined in a library more visible in automatically generated documentation such as Javadoc. We then performed a quantitative study to find out whether this approach could help programmers use state-based libraries more quickly and with fewer errors. We found that the intervention makes programmers 2 times faster at performing state-related tasks. Furthermore, programmers using the documentation intervention made 7 times fewer mistakes in answering questions about the code they were writing. Overall, our results contribute to the science of security by demonstrating that better documentation of library code can assist programmers in writing code more quickly and accurately in the context of state-based libraries such as SSL. The paper also provides one of the first empirical results that directly supports the productivity benefits of putting security-related design intent into code.

David Garlan, Bradley Schmerl, Jonathan Aldrich - Science of Secure Frameworks

•We have almost completed a model of probe placement, reporting on the foundational theory at SEAMS 2014 that deals with a formalism and proofs for determining upper and lower bounds on required probes. system. Building on this work will allow us to reduce potential vulnerabilities that could be introduced by the monitoring required for self-adaptation by allowing us to reason about the minimal set of required probes to be able to diagnose issues in the system (including security issues).

•We refined our scientific approach to mitigating CSRF attacks based on architectural design intent relating to web interaction protocols. Two conference papers were accepted, and while they were supported primarily via other sources, they will contribute to the Science of Secure Frameworks project. [Omar et al. 2014], supported by the sister lablet project "A Language and Framework for Development of Secure Mobile Applications," describes language extensibility mechanisms that can be used by frameworks to provide secure extension points to their plugins. [Militao et al. 2014] describes an approach to specifying and verifying interaction protocols that we plan to leverage in mitigating CSRF vulnerabilities.

•Developed a tool called ARMOUR that leverages novel data mining techniques to detect security attacks from the interactions that arise in the system’s runtime architecture. One of the obstacles with using a tool such as ARMOUR to detect anomalous behavior in arbitrary systems is that there is no universal optimal value for the underlying mining algorithms’ parameters. That is, for each system, parameters such as support and confidence have to be carefully selected to effectively detect anomalous behavior. GMU team developed a novel approach for the selection of parameters based on the behavioral characteristics of the system to minimize the false positive and negative rates. The approach automatically selects and tunes the parameters based on the observed historical variability in the system and its use cases.

•Developed and tested an approach for detecting data flow vulnerabilities, called Scoria, that uses static analysis to determine dataflow between components in the system. This was tested on over 30 test cases from the DroidBench benchmark, and extended the benchmark with additional test cases.

Travis Breaux - Usability and Secure Requirements

In progress: security patterns produced from expert knowledge by applying Situation Awareness, which is a technique for eliciting experts' descriptive and prospective thoughts, to security problems.

In progress: a security pattern construction protocol based on the requirements inquiry-cycle model, which allows security analysts to incrementally update a pattern to address emerging security challenges.

In progress: a security pattern catalogue based on attributes extracted from security standards using text analysis and machine learning.

Kathleen M. Carley - Geo-Temporal Characterization of Security Threats

**See Attachments for graphs

Objective

The objective of this project is to empirically characterize the nature of the current threat environment and to test a series of existing hypotheses about that threat environment using Symantec data. Our focus is global. The basic theory is that the potential severity of the threat is a function of the political environment rather than the technology. Questions to be addressed empirically include:

4.What is the likelihood of a catastrophic threat? Hypothesis: Most attacks are small.

5.How does the likelihood differ by type of threat? Hypothesis: there are no differences by type of threat.

6.Do these answers differ by country? Hypothesis A: Once GDP, internet penetration, and the number of attacks are accounted for there are no differences by country. Hypothesis B: The likelihood of a company being attacked depends on their position in the alliance/enmity network.

Background

In their 2011 survey Symantec found that the number one cyber risk business concern was external cyber-attacks, followed by concerns about both unintentional insider error (2nd risk) and intentional insider error (3rd risk) (Symantec, 2011, pg 9). Analysis by Verizon's cyber forensics team indicates that the massive increase in external threats overshadows insider attacks (Verizon, 2012b, pg 21). See also Richardson (2008). Despite the increase in external threats little is known about the source of such threats; or the global implications this evolving threat environment.

Wynne (2010) notes that the need to do attribution and forensics is critical to stem the tide of cyber-attacks. To meet this need, an understanding of the threat environment at the global level is needed. Cyber security, at the global level, is critical on a number of fronts including countering terrorism (Westby, 2007). At the global level, cyber security requires not only attribution and forensics, but harmonized laws and effective information sharing. In spite of this growing consensus there is still little empirical understanding of the global cyber threat environment, an understanding that is critical for forensics. We have found that most global information sharing is done through security providers and the data is only now becoming available and in restricted form given the dual privacy and security needs that must be met.

We note that reliance on anecdotal evidence can be damaging for the Science of Security. As empirical findings come to light, assumptions about the nature of cyber threat are changing. For example, in 2004, Byre and Lowe showed that process control and SCADA systems were not immune to attack using incidence data. Further basic assumptions are falling as new empirical evidence comes to light. This is creating a new baseline against which forensics can operate. While there are an increasing body of findings focused on specific threats and empirical assessments of key incidents; there is less understanding of the human socio-behavioral factors, particularly at the global level.

At the global level, multiple conceptual frameworks abound. For example, Kshetri (2005) argues that country level differences in the regulative, normative and cognitive legitimacy of different types of web attacks lead to differences in the extent to which organized crime can use the internet in those countries. BSA (2010) provides guiding principles for global cyber security. Broadhurst (2006) argues that cyber-attacks are traditional crimes in a new venue which makes traditional forensic methods obsolete. And so on. Despite the recognition of the global nature of the cyber threat there is little characterization of that threat.

Approach

The basic approach used was to develop code for extracting country level indicators of attacks and attack paths from the Symantec data. The analysis is based on the Symantec WINE telemetry data set. WINE is a platform through which external researchers can access data sets used within Symantec Research labs. To the best of our knowledge, Symantec is currently the only security company that makes such platform available to external researchers. The telemetry data set consists of attack reports from more than 10 million Symantec customer computers worldwide.

This was then combined with other open-source data to create a global threat profile. An example of such additional open source data is the ICT index cira 2010 for all countries. The ICT index is a combined measure based on 11 indicators including adult literacy, internet access and so on. The data was fused to create a global indicators data set and was then assessed using network analytics and standard statistical procedures. Based on this data a network based model of the impact of hostilities and other factors on geo-cyber-attack-network was developed.

Summary of Key Results

There are two key aspects to this research. The first is the characterization of the threat profile. The second is the assessment of the over-all global threat with respect to cyber attacks.

In terms of the general threat profile, our results led to an empirical characterization of the change in cyber-threat over the past several years. This work indicated that web attacks account for the vast majority of attacks in the IPS catalog. Around 2003, worms and viruses were the most dominant threat types. At that time, the main malware distribution technique was infection propagation among computers. The main goal of attacks was to cause damage or to "show off". Since then, we have seen the emergence of new attack types that reflect either new distribution techniques (e.g. web attacks) or that mainly have monetary goal (fake anti-viruses, adware/spyware). 61% of attacks are transmitted from an exploiting machine, 37% of attacks are transmitted from malicious websites, 2% are from other sources not specified.

The results confirmed the hypothesis that most attacks are small, and so low severity threats. This result informed other research in the lablet. It Is important to recognize though that Symantec (as an example of key anti-virus vendor) prioritizes releasing attack signatures for fast propagating threats, but not necessarily for threats that might cause high damage.

We conducted a global assessment of the extent to which countries were threatened, threatening, or utilized for sending cyber-attacks. It was hypothesized that once GDP, internet penetration, and the number of attacks are accounted for there are no differences by country. This hypothesis was disconfirmed. While these factors do mitigate the effect, there are still country effects.
Developed countries are more likely to encounter web attacks and fake applications (such as fake anti-viruses) – see Figure 1. High ICT countries, e.g., US, are more likely to encounter fake applications and web attacks; whereas, mid ICT countries are more likely to encounter threats. Mid ICT countries are most likely to transmit attacks, e.g., Romania, Moldovia, Bosnia. And in general, the USA is exposed to more fake applications than other countries. It is possible that attackers target these countries because such attacks are likely to be more lucrative. From a statistical perspective - monetary and computing resources are the main factor that attracts attacks at the country level.
Further, we find that the global threat profile is complicated and does not match the standard view from political science of the US and one or two other countries mostly fighting with each other. This means that our results are counter to the standard wisdom which is case based. A general social-influence model is a better predictor than the traditional great-powers model.
How attacking computers' hosting varies across countries was analyzed and factors that explain such variation were identified. We found that many countries in Eastern Europe and Central America extensively host attacking computers. Such countries have a combination of good computing infrastructure and high levels of corruption. The high levels of corruption facilitates conducting cyber criminal activities such as registering malicious websites through the complicity of ISPs and law officials.
The international cyber attack network was analyzed. For web attacks and fake applications, most attacks are from Eastern Europe and Central America to developed countries in Western Europe and North America. See for example, the network of dominant attacks from the Ukraine in Figure 2. Exploits have a tendency to spread to geographically nearby countries.
The country-level specificity of the results means that diplomatic and soft-power solutions may be valuable in mitigating cyber-attacks. Many countries are cyber-crime friendly environments – see Figure 3. Some of these countries serve as wayports – and so are “usable” by others to send attacks. Globally – countries with weak cyber policies or poor enforcement or unsophisticated approach to cyber attacks are most “used” or serve as the “source” to spread attacks. Thus, countries in Eastern Europe and Central America host most cyber-attack infrastructure (such as malicious web sites and botnets). A combination of good computing infrastructure and lax policies makes the above countries attractive for hosting attack infrastructure. It is interesting to note that the Ukraine and several countries that were part of the USSR fall into this category.
We note that Russia is about to require all blogs to register and to add more control over the web. Based on this research and other research we have done on social media we expect this to a) impact the potential for state instability, and b) to alter the flow of web-based attacks that flow through the related countries. A possible future study might look specifically at the Russia/China/US cyber environment in more detail.

Bibliography
Broadhurst, Roderic, 2006, "Developments in the global law enforcement of cyber-crime", Policing: An International Journal of Police Strategies & Management, 29(3): 408 – 433
BSA, 2010, Global Cyber-Security Framework. Accessed from: http://www.bsa.org/country/Public%20Policy/~/media/Files/Policy/Security/CyberSecure/Cybersecurity_Framework.ashx
Byres, Eric and Justin Lowe, 2004, The Myths and Facts behind Cyber Security Risks for Industrial Control Systems, Proceedings of the VDE Kongress, 2004.
Kshetri, Nir, 2005, Pattern of Globalcyber War and Crime: A Conceptual Framework, Journal of International Management, 11 (4): 541–562.
Richardson, R., 2008, 2008 CSI Computer Crime and Security Survey. Accessed from: http://gocsi.com/sites/default/files/uploads/CSIsurvey2008.pdf
Symantec, 2011, 2011 State of Security Survey. Accessed from: http://www.symantec.com/content/en/us/about/media/pdfs/symc_state_of_security_2011.pdf
Verizon, 2012b, 2012 Data Breach Investigations Report. Accessed from: http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf
Wynne, Michael W., 2010, Report from the Stevens Institute Cybersecurity Policy Conference, January 19-20 Reagan Building Washington DC.

Kathleen M. Carley - Learned Resiliency in Multi-Level Systems
**See Attachments for graphs

Introduction
Increasingly organizations are under cyber-attack. These attacks may take many forms, with denial of service, data stealing or sabotage, being simple examples. These attacks have the potential to impede mission planning, reduce performance, and cause information to “leak” or “be-discovered” where inappropriate. The question arises, how can organizations be structured to mitigate these cyber-induced risks, to be resilient in the face of these cyber-threats? Using agent-based simulation thee questions are addressed. The results provide guidance for how to design for cyber-security resilience. In addition to the organizational design guidance, this work led to a novel agent-based technology, new metrics of resilience, and new visualization capabilities for simulation data.

Statement of the problem studied

Organization's face security risks from both human and computer (hardware or software) errors. These errors can compound, and grow worse as more individuals are connected to more people and more information technology (IT) in more ways (e.g., VoIP, direct interaction, email, social media …). Identifying the source of the errors, and responding to errors in a rapid and effective manner is often made more difficult when the organization is operating simultaneously at multiple levels of security – an example is the unclassified, classified secret and classified above-secret levels employed by many governments. The multi-level security impacts IT system, information and human segmentation due to controls on who can relay and access what information using what systems. The need to operate with multi-level security places added constraints on what organizational design solutions are possible to achieve high levels of resiliency in the face of cyber threats and events and increases the need to be resilient in the face of security risks. We ask, is it possible to design organizations that are operating at multiple levels of security to be resilient to cyber threats?

Objective

The objective of this project is to develop a theory of system resiliency for complex adaptive socio-technical systems. A secondary objective is to develop the modeling framework and associated metrics for examining the resiliency of complex socio-technical systems in the face of various cyber- and non-cyber-attacks, such that the methodology can be used to support both basic level simulation based experimentation and assessment of actual socio-technical systems. To meet these objectives multi-modeling is used to examine how to design and impact complex organizational systems in which information is segmented to multiple levels of security with all the attending issues for personnel access and IT usage.

Background

Much of the recent research on threatened complex socio-technical systems, in the security area, has focused on tracking (Lipson, 2002; Gao & Ansari, 2005), investigating (Nilson & Larson, 2008), characterizing (Kotapati et al, 2005), or measuring the damage caused by (Lala & Panda, 2001) cyber attacks. Such work, while providing a context for this research, does not address the issue of system resiliency in the face of such threats. Current approaches seeking to mitigate these threats, in complex socio-technical systems tend to either model cyber attacks at the IT level or provide guidelines to managers about how to handle the human side of the equation. For example, on the IT side, the CAML approach to modeling cyber attacks focuses on data streams and features of the IT system (e.g., Cheung, Lindqvist & Fong, 2003), and the DDoS attack detection models focus on network usage characteristics (Li, Li and Jiang, 2008). For example, on the organizational side, efforts have been made to provide managers with exercises for improving reaction to threat events (Andersen et al., 2004). One exception to this trend is the cyber command and control model (Scherrer & Grund, 2009) which is a conceptual model laying out processes and lines of authority for the DOD and which cannot be used for empirical assessment of resiliency, nor is it generally applicable beyond the DoD. We seek to develop a model that considers both the human and the IT side, such that the model supports empirical analysis of both hypothetical and real complex socio-technical systems. The other key exception is the service restoration model (Lee, Mitchell & Wallace, 2007) which uses highly theoretical and stylized organizations subject to generic attacks and assesses resilience along seven dimensions. Ws build on these dimensions but recast them, and formalize them, using network metrics.

In the area of cyber threat, relatively less is known about the human than the IT side of the equation (Stytz & Banks, 2008). In general, more work is needed on how humans and so organizations respond to varying cyber threats and events – especially those of significant impact and duration. Drawing on the work in high-reliability organizations, there are models of mitigation based on assumptions of human error and organizational design (LaPorte & Consolini, 1991; Bigley & Roberts, 2001). Admittedly the high reliability research was focused on types of threat other than cyber; nevertheless, this research speaks to the need for specialized organizational structures and norms when the socio-technical system must exhibit high reliability in the face of a highly volatile and potentially hostile environment. Organizations faced with high security needs are in a similar environmental situations and so too would need specialized structures and norms. In complex socio-technical systems, where security is a premium, a comprehensive model must account for both these IT and organizational issues. The proposed work is a step toward creating a joint human-IT framework for assessing the impact of cyber threat and the resiliency of the socio-technical system.

Current approaches to understanding the impact of threats and vulnerabilities on these systems tend to focus on the system as it was planned with some flexibility for how it was built – rarely do cyber or organizational security attempt to identify how the system(s) may evolve. However, the nature of the threat evolves, the threatened organization, its operating environment and its operating dependencies are changing, and the individuals in the organization are learning. While a full explication of these co-evolutionary processes is beyond this proposal we do focus in on the extent to which individual learning results in the evolution of trust, norms, and coordination practices that may support or be detrimental to overall system resiliency. For this we employ agent-based models of learning. The impact of learning on system behavior has been extensively studied. Key finding of relevance here are that: the type of learning employed impacts outcomes (Lant & Mezias, 1992); learning at the individual and group level can conflict resulting in a decrease in resiliency (Carley & Svaboda, 1996); organizational-complexity and the organizational structure impacts the leaning of norms (Harrison & Carroll, 1991) and so would impact the development of a security culture; in contrast to novices, experts models of complex phenomena are richer (Chi, Feltovich & Glaser, 1981), contain more detailed relations among factors (Klein & Hoffman, 1993) informed by experience (Klein, 1998) and so the experts should be less likely to under or over-react than novices; high personnel turnover in conjunction with a volatile and perhaps hostile environment can mitigate the impact of learning and decrease resilience (Lin & Carley, 2003).

Approach

To address these issues, an approach combining agent-based simulation and dynamic network analysis is used. The specific agent-based model that we extended is Construct (Carley 1990; Carley, Martin & Hirshman, 2009). The result was a new system that supports reasoning about both individuals and groups and can be used to assess multi-level security systems at the organizational level. Resiliency metrics based on a high-dimensional dynamic network representation of organizations were constructed. This representation is referred to as a meta-network representation of the socio-technical organization. A series of scenario driven virtual experiments were then used to assess the relative resiliency of organizations with different designs in either or both the lines of personnel authority and interaction or IT/data access. Over 2 million simulation runs were conducted generating over 900GB of simulated data. A response-surface visualizer was developed for visualizing the results, a set of compression and aggregation techniques were developed for data management. A new system for running the models through condor was developed.

Summary of Key Results

These simulations show that most organizations are reasonably resilient to small and medium cyber attacks. The attack must be large and fairly pervasive to have a major impact on performance and the ability to engage in and complete mission planning. We find this result to be consistent with the data findings from Symantec. Our results further indicate that hierarchies, overall, are among the top performers and exhibit high resilience when operating a multi-level security environment. When under cyber-attack resiliency is enhanced by organizations resort to direct human communication; however, that increases the chances of inadvertent information leaks. Results of these simulations further suggest that inadvertent information leaks are more likely to occur when the organization is under cyber-attack and are likely to occur in all organizations, regardless of their design. These can be thought of as “normal” accidents. However, such leaks, are most likely in mesh organizations and least likely in hierarchies – see Figure 1.

At one level, these results suggest that organizations to be resilient in the face of cyber-attacks should operate as a high-reliability organization (Weick & Roberts, 1993; Shulman, 2004; Roberts, 1990). Such organizations are ones that utilize management and design practices that enable them to avoid failure despite operating in high risk environments were errors can be expected due to both the complexity of the system and the level of external risk. High-tech multi-level security systems are inherently complex and the potential cost of errors due to cyber threats creates a high risk environment. In these simulations, those organizational designs that rely on personal expertise, and that support change in the face of attacks (commitment to resilience) operate at higher reliability.

At another level, these results refine the notion of what it takes to be a high reliability organization by providing explicit guidance for how to design for resiliency. In particular, our results indicate that:

•Redundancy leads to improved performance and resiliency but at the cost of increased opportunities for information leakage.
•Hierarchies are more impacted initially by a reliability attack, but are barely impacted by an integrity attack. Scale Free organizations are the opposite. In the absence of an attack, the Scale Free organizations have superior task performance.
•Although leadership may be relatively insulated from attacks, specific sub-populations of interest within the organization will be more impacted. IT and Human IT changes tend to improve the ability of the hierarchical organization to support these sub-populations, while such changes in the scale-free organizations are detrimental.
•Low magnitude attacks are unlikely to be noticed by leadership unless leadership is looking for them. To maintain high reliability, leadership needs to be vigilant to these attacks.
•Organizations with IT dependencies are able to shrug off minor attacks because information is not optimally distributed for efficiency.
•Increasing the number of information classification levels and distribution protocols, degrades robustness.
•Combinations of attacks are more harmful than single attacks.
•Cloud topologies suffer more in the short-term, but are more robust in the long.
•Hierarchical organizations with cloud IT are the most robust tested organization in the long-term.
•Stove-piped IT systems, where each system is maintained separately, tend to retain bad information longer and so are less resilient in the face of integrity attacks.
•Matrix Organizations, with their cross-functional teams, may be able to overcome knowledge gaps caused by cyber-attacks; but, are often to coherently finish any tasking once the attack has begun.

At a technical level, a key finding is that agent-based simulation modeling that employs “social” reasoning and so agents at both the individual and group level is a significant win as it enables increased accuracy, increased predictive capability in general, and increased speed/ number of actors modelable. Traditionally in agent-based modeling as you improve the model by making the agents more cognitively accurate, or by making the networks more realistic the number of agents that could be modeled or the speed of the model runs decreased. Our results demonstrate that adding social cognition to the model and the associated multi-level actions actually increased the number of agents modelable or the speed for the same number of agents, in the cyber-security domain.

At a measurement level, this research led to a temporal approach and a set of network of metrics for assessing organizational resiliency to cyber attacks and other organizational issues – see Figure 2. The basic idea is that a metric of interest can be used to assess immediate impact, persistent impact and recovery by varying the time period of interest. These metrics take the into account the lines of authority and communication among personnel, access to data and IT systems, mode of communication, and direct IT to IT connections. Both static and dynamic metrics were developed. In general, we find that the

dynamic metrics are more effective for assessing resiliency than the static.

Bibliography

Andersen, David, Dawn M. Cappelli, Jose J. Gonzalez, Mohammad Mojtahedzadeh, Andrew P. Moore, Eliot Rich, Jose Maria Sarriegui, Timothy J. Shimeall, Jeffrey M. Stanton, Elise A. Weaver, and Aldo Zagonel. 2004. Preliminary System Dynamics Maps of the Insider Cyber-threat Problem. Paper read at System Dynamics Modeling for Information Security: An Invitational Group Modeling Workshop, 16-20 February, at Pittsburgh, PA, USA.

Bigley, Gregory A. and Karlene H. Roberts. 2001. The incident command system: High-reliability organization for complex and volatile task environments. Academy of Management Journal, 44, 6, 1281-1300.

Carley & Svoboda, 1996. Kathleen M. Carley & David M. Svoboda, 1996, Modeling Organizational Adaptation as a Simulated Annealing Process. Sociological Methods and Research, 25(1): 138-168

Carley, Kathleen M., 1990, “Group Stability: A Socio-Cognitive Approach,” Advances in Group Processes: Theory and Research. Edited by Lawler E., Markovsky B., Ridgeway C. and Walker H. (Eds.), Vol. VII. Greenwhich, CN: JAI Press, 7: 1-44.

Carley, Kathleen M., Michael K. Martin and Brian Hirshman, 2009, “The Etiology of Social Change,” Topics in Cognitive Science, 1.4:621-650.Zhiang Lin and Kathleen M. Carley, 2003, Designing Stress Resistant Organizations: Computational Theorizing and Crisis Applications, Boston, MA: Kluwer.

Cheung, S.; Lindqvist, U.; Fong, M.W.; , "Modeling multistep cyber attacks for scenario recognition," DARPA Information Survivability Conference and Exposition, 2003. Proceedings , vol.1, no., pp. 284- 292 vol.1, 22-24 April 2003

Chi, M.T.H., Feltovich, P.J., & Glaser, R. , 1981. Categorization and representation of physics problems by experts and novices. Cognitive Science, 5, 121-152.

Dennis K. Nilsson and Ulf E. Larson. 2008. Conducting forensic investigations of cyber attacks on automobile in-vehicle networks. In Proceedings of the 1st international conference on Forensic applications and techniques in telecommunications, information, and multimedia and workshop (e-Forensics '08). ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), ICST, Brussels, Belgium

Gao, Zhiqiang and Ansari, N., 2005 , "Tracing cyber attacks from the practical perspective," Communications Magazine, IEEE , vol.43, no.5, pp. 123- 131, May 2005

Harrison, J.R. and G.R. Carroll. 1991. Keeping the Faith: A Model of Cultural Transmission in Formal Organizations. Administrative Science Quarterly, 36, 552-582.

Kameswari Kotapati, Peng Liu, Yan Sun and Thomas F. LaPorta, 2005, A Taxonomy of Cyber Attacks on 3G Networks Intelligence and Security Informatics Lecture Notes in Computer Science, Volume 3495/2005, 129-138

Klein, G. A., & Hoffman, R. R., 1993. Seeing the invisible: Perceptual-cognitive aspects of expertise. In Rabinowitz, M. (ed.), Cognitive science foundations of instruction. Hillsdale, NJ: Erlbaum. 203-226.

Klein, Gary A. 1998, "Sources of Power: How People Make Decisions", MIT Press, Cambridge, Mass, pp. 1-30.

La Porte, Todd R. and Paula M. Consolini. 1991. Working in Practice But Not in Theory: Theoretical Challengers of 'High-Reliability Organizations'. Journal of Public Administrative Research and Theory, 1, 1, 19-47.

Lala, C. and B. Panda, 2001, Evaluating damage from cyber attacks: a model and analysis, IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans, 31(4):300-310.

Lant, T.L. and S.J. Mezias, 1992, “An Organizational Learning Model of Convergence and Reorientation,” Organization Science, 3(1): 47-71.

Lee, Earl E. II, John E. Mitchell, and William A. Wallace. 2007. Restoration of Services in Interdependent Infrastructure Systems: A Network Flows Approach. Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on 37 (6):1303-1317.

Li, Muhai, Ming Li and Xiuying Jiang, 2008, DDoS attacks detection model and its application, WSEAS Transactions on Computers, 7(8).

Lipson, Howard F., 2002, Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues, Technical Report, Software Engineering Institute, Carnegie Mellon University

Roberts, K. H. (1990). Some Characteristics of High-Reliability Organizations. Organization Science, 1, 160-177.

Scherrer, Joseph H., and William C. Grund. 2009. A Cyberspace Command and Control Model. edited by U. A. Force. Maxwell AFB, AL: Air War College.

Schulman, P. R. (2004). General attributes of safe organizations. Quality and Safety in Health Care. 13, Supplement II, ii39-ii44.

Stytz, Martin & Sheila Banks, 2008, Advancing Cyber Warfare Simulation System Capabilities, SimTecT 2008 Simulation Conference: Simulation - Maximising Organisational Benefits (SimTecT 2008) Melbourne, Australia, May 12 – 15 , 2008

Weick, K. E., & Roberts, K. H. (1993). Collective Mind in Organizations: Heedful Interrelating on Flight Decks. Administrative Science Quarterly, 38, 357-381.

Lorrie Cranor - USE: User Security Behavior
**See Attachment

Anupam Datta, Limin Jia - Secure Composition of Systems and Policies

Problem studied:

Our research aims to develop compositional reasoning principles to verify systems that consist of trusted and adversarial components. In particular, our adversaries can supply code to be executed by trusted components.

Results:

We developed a program logic that can reason about systems that contain trusted and untrusted components. In particular, untrusted components can provide code to be executed by trusted components: e.g., via modifying the code region of trusted programs. Our program logic contains two novel typing rules that derive security properties of two commonly-used security mechanisms for executing untrusted code: sandboxing and code identification. We proved our program logic sound with regard to a step-indexed semantics. We demonstrate the expressiveness of our program logic by verifying the security property of the design of Memoir [1], a previously proposed trusted computing system for ensuring state continuity of isolated security-sensitive applications.

Robert Harper - An Epistemic Formulation of Information Flow Analysis

Problem studied:

We continue our investigation of using epistemic logic to formalize information flow analysis. We also began exploring applying epistemic logic to analyzing information flow in social networks.

Results:

The main development in the research is that we have begun to consider timing channels as these are important when there is a centralized certificate authority that interacts with multiple security sensitive processes. Timing channels are difficult to avoid as any branching on confidential inputs can create a timing leak if the branches do not take the exact same time to execute. We are seeking a reasonable approach that minimizes the probability of timing leaks by adding sleep delays into the program where necessary.

In addition, as a primarily exploration, we have extended the linear epistemic logic
in [2] to analyze information flows on social networking sites such as Facebook. More concretely, we extended [1] with names, a dedicated mechanism for global information,
list comprehension and membership testing for lists to model common constructs in social networking sites, such as access control lists.

Frank Pfenning - Proofs and Signatures

In the current year, Frank Pfenning, Dennis Griffith and Elsa Gunter have made significant strides both in the theory and implementation of a session-typed language (called SILL) for secure, distributed programming. On the theoretical side, we have integrated various form of resource management into the formal description of the language and established its fundamental properties. We have also developed techniques for reasoning about programs in the language using parametricity, which is particularly important in this setting since many security properties of programs are consequences of parametricity. On the implementation side, we have constructed and continually refined the prototype. This includes a much improved front-end, integrating new techniques for combining the type system of an ambient host language and the concurrency module. It also includes several back ends that are appropriate in different circumstances: two of them employs shared memory for synchronous or asynchronous communication, a third one is distributed and uses explicit message passing. This prototype has been used successfully in teaching at a summer school affiliated with a multi-site European project on behavioral types. We have also designed techniques to dynamically check the adherence of processes to prescribed communication protocols under a practical adversary model. This latter design is critical for purposes of technology transfer, but has not yet been integrated into the implementation.

Main Highlights
We have designed a programming language for secure distributed computation which supports both formal proof and digital signatures in order to establish trust.
We have established crucial properties of this language, such as session fidelity, deadlock freedom, type preservation, parametricity, and termination.
We have implemented a prototype that allows us to write, check, and execute concurrent, and distributed session-typed

programs.
We have designed and implemented a new type inference algorithm that modularly combines a background language with its concurrent extension.
We have designed and implemented an automatic resource control regime that is fully logically justified.
We have developed a system of dynamic checking and blame assignment towards a theory of causality and accountability in distributed computation.

André Platzer - Security Reasoning for Distributed Systems with Uncertainty

INTRODUCTION
This project is focused on understanding large systems in the presence of adversarial attacks, stochastic component failures and benign stochastic noise. The intuitive challenge is that sensor or measurement noise is ubiquitous, and noise makes it difficult to determine whether an anomalous component has been maliciously manipulated or has permanently failed. However, a reliable system should be robust to disruptions—we should design systems to shrug off both failure and attack, and still efficiently achieve their intended goal.

This is a critical security issue that will become increasingly important as autonomous and semi-autonomous devices—including cyber-physical systems (CPSs) like unmanned aerial vehicles (UAVs) and other robotic systems—become more widely adopted in governments, economic processes and militaries. Security vulnerabilities in these systems will cause serious real-world effect. Worryingly, security vulnerabilities in this setting could be extremely subtle.
As a speculative example: suppose that a particular UAV became a popular delivery vector for small packages in the near future. If a hostile entity were able to somehow manipulate of these devices—say by remotely tampering with sensor calibration—then this might be a multi-million dollar attack in terms of lost productivity. This manipulation might be something as explicit as inducing the UAVs to crash into the ground or other UAVs, but might be less obvious such as reducing the UAV's delivery efficiency. We want to develop techniques that can assess how susceptible a CPS is to manipulation. Furthermore, we want to invent techniques that allow use to automatically design controllers and policies for autonomous (or semi-autonomous) systems that are efficient, reliable and difficult to manipulate.
In previous years we have already made progress on aspects of this topic. In last year's ARO annual report we discussed # SAT. # SAT is a new computational problem designed to help analyze robustness in the presence of failure. A large class of reliabilities and robustness questions can be expressed as # SAT instances.
For example, we can model many deterministic planning problems in Boolean propositional logic. Once this has been done, we can declare parts of the model to be 'prone to failure' with a certain failure probability. Our interest is determining how likely is it that we can achieve an objective given independent failure of these failure-prone components. If the percentage is too low, this suggests that the system is not robust to the type of failures modeled, and should be redesigned with more redundancy.
In our paper "A generalization of SAT and #SAT for robust policy evaluation" we provided both a theoretical analysis and empirically successful algorithm for solving # SAT problems exactly.
This year we have been exploring the issue of controller synthesis. Our algorithm for # SAT is designed to estimate how robust a moderately-large design is to stochastic component failure. By itself it can be used as an inner loop of a heuristic controller design algorithm—some kind of local search, for example. Our work this year has been aimed at explicitly designing reliable controllers for systems that are much too large to handle using exact # SAT methods while, at the same time, providing explicit bounds on the quality of the policy.

SUMMARY OF MOST IMPORTANT RESULTS
We had several major results this year. They are summarized in our NIPS workshop paper "A projection algorithm for strictly monotone linear complementarity problems", and partially expounded upon in our journal paper "Hybrid theorem proving of aerospace systems: applications and challenges". We expect to complete a new paper on this topic relatively soon, as well.
Our principle focus this year has been on approximating large and continuous decision problems. We are particularly interested in control and decision problems stemming from CPS security. Robotic systems are good examples of a CPS. As a running example of a CPS we will use the problem of designing a controller for a UAV. However, part of the promise of our work is that it is a fundamental exploration into planning under uncertainty, adversarial disruption and robustness—the research will apply to many other security problems that bare little superficial resemblance to our UAV example.
Designing a controller for a UAV that maintains good performance in the face of benign uncertainty—e.g. uncertainty stemming from sensor noise and actuator imprecision—is an example of a core problem that has been explored from a number of different fields. Here the problem is based on finding a mapping from a UAV's current and past sensor measurements into an appropriate set of signals to its actuators that achieves some goal. For example, we want to determine a way of building a controller that takes in noisy sensor information (that could include GPS information, a camera feed, and information from an inertial measurement unit) and determine how this can be used to guide the UAV from point A to point B quickly without crashing into any other object along the way.
There are several existing ways of approaching this controller design problem. A standard way is to model the continuous flight dynamics of the UAV (using, for example, differential equations), then to discretize and linearly approximate these dynamics. This discrete linearization can be turned into a Markov decision process (MDP)—a popular formalism for sequential decision

making. Once the MDP has been formulated, an optimal policy for controlling the UAV can be found using dynamic programming algorithms.

One thing to note about this process is that by discretizing the system we have approximated the true continuous dynamics of the system. How accurate is this approximation? Any approximate representation degrades solution quality. The difference between the solution to the approximate problem and the solution to the ideal problem is called representation error.

There is a natural tradeoff, in the above example, between how finely state-space is gridded—and hence how accurate the approximation is—and how difficult it will be to find a policy with dynamic programming. As the number of continuous dimensions increases, the number of states in a finely-gridded representation will explode. Bellman dubbed this the curse of dimensionality in the 1950s. Finding a good control policy in continuous problems with dimensions much higher than 8 is a serious problem even for modern computers.

The above discussion raises some natural questions. How sensitive is the optimal discrete policy to the discretization schemes—if we grid more coarsely, how much worse will the optimal discrete policy be when applied to the continuous setting? Are there other ways to approximately represent the problem other than gridding? When do they offer a better trade-off between representation size and representation error? Our work this year has been focused on characterizing these representational issues in a broad class of decision problems and a general form of approximate representation.

We have been working on monotone linear complementarity problems (LCPs). Any decision problem with linear or convex quadratic objectives and linear constraints can be represented as a monotone LCP. MDPs are LCPs, so the above discussion on UAVs can be discussed using LCPs. Furthermore, linear programs (LPs; a nearly ubiquitous class of optimization problems), support vector machines (SVM; a classification model used widely in machine learning applications), and any convex quadratic program (QPs; a more general optimization framework than LPs) can all be cast as monotone LCPs.

A LCP, formally, is described by a square matrix and a vector . Monotonicity is a technical condition on that is important for ensuring the LCP is tractable. A vector is a solution to the LCP if three conditions hold, which can be concisely written as: . In other words, must be non-negative, its affine transformation must be non-negative, and must be orthogonal to . Together, the non-negativity and orthogonally tell us that for a solution , either or .

Readers familiar with optimization might notice a similarity between the definition of a solution to an LCP and KKT conditions—which a necessary and (usually) sufficient first-order conditions for optimality in convex programs. This is no accident: the connection between optimization and complementarity problems is deep. We will omit detailing this connection here, however

We note that the definition of an LCP can be extended to the continuous setting where becomes a linear operator and both and are functions in some function space, but we will neglect to do so in this document. This may be important for dealing with continuous decision problems, however, and we are actively working in this setting.

For a large or continuous LCP we need to approximate , , and . We do this with a general technique that can be called using a finite basis expansions. This representation is simple to describe, we represent a function as a linear combination of basis functions: . Here, is the vector that we are trying to, is the vector of fitting coefficients and is a set of basis vectors.

When , then is a low-dimensional representation of —we are representing the numbers of with the numbers in . In order for this low-dimensional representation to be relatively accurate want to be the projection of onto the range of , denoted by , which is the closest approximation of possible using the basis . This ideal of projection onto a low-rank space is central to our idea of approximation.

Our major contribution has been develop an approximate iterative algorithm for solving strictly monotone LCPs that uses these low-dimensional representations. This algorithm detailed in our paper “A projection algorithm for strictly monotone linear complementarity problems.” This algorithm is much faster than previous iterative algorithms for the same problem, and we have proved bounds on the approximation error that it induces—it is very accurate as long the actual solution of the LCP is not far from its projection

Critically, we have a stochastic version of the algorithm no longer has dependency on the size of the problem . This means that our algorithm can be totally liberated from issues associated with discretizing a continuous problem. It is based on sampling while it is running rather than using a ‘mesh’ of the state-space.

We consider this to be an important advance for any security problem that involves planning under uncertainty, such as any security problem involving robots, because it is a fast approximate, but also maintains an explicit bound on its approximation error. Exact solvers will be too slow to solve many problem instances, and many other approximate solvers do not have approximation guarantees—it will not be possible to use their solutions to formally reason about the security properties.

FUTURE DIRECTIONS

In the coming year we will primarily work on implementation of our algorithms, and extending them to more general settings. Our algorithms currently work on strictly monotone LCP, and we want to extend them so that they also apply to non-strictly monotone LCPs. Monotone LCPs can model more problems than strictly monotone LCPs, although there is usually a strictly monotone LCP approximation of any monotone LCP that can be formed with a simple regularization process.

We also want to showcase how our algorithm performs on a continuous two UAV collision problem. The goal is to find a good collision-avoiding control policy for a UAV using different high-dimension model of flight dynamics. We expect that our approach will be significantly faster than existing dynamic programming approaches and, again, will have the virtual of carrying formal bounds on its quality.

**See Attachments

Perpetually Secure and Available Systems

Re: A Principled Approach to Web Security, Anupam Datta reports: We have developed a formal framework for compositional reasoning about secure systems. A key insight is to view a trusted system in terms of the interfaces that the various components expose: larger trusted components are built by combining interface calls in known ways; the adversary is confined to the interfaces it has access to, but may combine interface calls without restriction. Compositional reasoning for such systems is based on an extension of rely-guarantee reasoning for system correctness to a setting that involves an adversary whose exact program is not known. At a technical level, our work includes an expressive concurrent programming language with recursive functions for modeling interfaces and a logic of programs in which compositional reasoning principles are formalized and proved sound with respect to trace semantics. We have applied the method on representative examples from web-based systems, network protocols, and access control with dynamic policies.

Re: Security the Digital Home, Lorrie Cranor, Lujo Bauer and Greg Ganger report: As digital content becomes more prevalent in the home, non-technical users are increasingly interested in sharing that content with others and accessing it from multiple devices. Not much is known about how these users think about controlling access to this data. To better understand this, we conducted semi-structured, in-situ interviews with 33 users in 15 households. We found that users create ad-hoc accesscontrol mechanisms that do not always work; that their ideal policies are complex and multi-dimensional; that a priori policy specification is often insufficient; and that people’s mental models of access control and security are often misaligned with current systems. One promising mechanism for helping non-expert users create accurate access-control policies is reactive policy creation, in which users can update their policy dynamically in response to access requests that cannot otherwise succeed. Our earlier study suggested that reactive policy creation may be a good fit for file access control at home. To test this theory, we designed and executed an experience-sampling study in which participants used a simulated reactive access-control system for a week, yielding rich data about users' access-control decisions. We found both quantitative and qualitative evidence of access-control policies that are hard to implement using traditional models but that reactive policy creation can facilitate. We found that when making policy decisions, people want more control and interactivity and rely on social norms, all areas where reactive policy creation can contribute. We also found that while there are some clear disadvantages to the reactive model, they do not seem insurmountable, and user opinions support the reactive model. Based on these results, we believe that reactive policy creation has considerable potential as one component of a usable access-control system. A promising approach to implementing access-control infrastructure is by specifying access-control policy as statements in a formal logic, and permitting an attempted access to succeed only when it is accompanied by a formal, logical proof that the access is consistent with this access-control policy. This approach brings high assurance of correctness due to its formal nature, while also permitting a great deal of flexibility in the access-control policies that it can support. Drawing on the results of the above-described user studies, as well as on recent prior work on the Perspective distributed file system; we have been investigating how to formalize the kinds of access-control policies that we believe will commonly occur in the context of a distributed, replicated file system. As part of this investigation, we have encoded in machine-verifiable form a set of example policies that illustrate common use cases in such a setting. Our investigation has so far touched on a number of interesting issues, such as information leakage through metadata-driven specification of access-control policies, policy specification for replicated objects within a global namespace, and necessary assumptions about trust in an environment where different system components are owned by different entities. The investigation carried out thus far has resulted in a preliminary design for an access-control infrastructure for Perspective, our distributed file system. In the next year we plan to finalize this design and use it to develop a prototype implementation.

Re: Privacy Decision Making, Lorrie Cranor and Alessandro Acquisti report: Earlier work has shown that consumers cannot effectively find information in privacy policies and that they do not enjoy using them. In our previous research on nutrition labeling and other similar consumer information design processes we developed a standardized table format for privacy policies. We compared this standardized format, and two short variants (one tabular, one text) with the current status quo: full text natural language policies and layered policies. We conducted an online user study of 789 participants to test if these three more intentionally designed, standardized privacy policy formats, assisted by consumer education, can benefit consumers. Our results show that providing standardized privacy policy presentations can have significant positive effects on accuracy of information finding, overall speed, and reader enjoyment with privacy policies.

Re: Survivable Distributed Storage: From Theory to Reality, Greg Ganger reports: Good decision-making processes require timely access to accurate information. In military settings, this often includes real-time intel. But, it always includes large quantities of previously acquired information (e.g., landscape images, behavioral tendencies, equipment capabilities, and so on). Thus, it is critically important to have large-scale distributed storage capable of retaining (and protecting) information for long periods of time and providing access to it, where it is needed, when it is needed. Distributed storage that truly supports military decision-makers should meet a number of difficult requirements. Of course, it should scale to sufficient storage capacities and provide sufficient access performance for the intensive decision-support systems utilizing the information repositories. But, it must also be able to protect the confidentiality of information from those who would seek to steal military secrets. It must be able to protect the integrity of information from those who would seek to destroy it or, worse, to corrupt it and

thereby mislead decision makers. It must be able to provide access to the information under duress; that is, it must be able to foil denial of service attacks that seek to block information availability during critical decision-making moments. In this project, we have developed and demonstrated technologies that would allow construction of survivable and secure distributed storage systems with most of the properties discussed above. We defined the PASIS architecture for survivable storage, developed protocols with desired survivability and security properties, and demonstrated their efficacy in prototypes. Along the way, we had regular in-depth discussions with industry leaders about how to transition these technologies to COTS offerings. In doing so, these leaders helped us understand roadblocks to making such systems available as COTS products for military (and other) usage. Although the storage industry is adopting results of our work, we have focused on addressing the roadblocks to wholesale adoption of survivable and secure storage into COTS offerings. Perhaps the largest concern has been that most customers would be unwilling to accept significant cost or performance overheads for most of their data, relegating survivable storage solutions to niche markets. Our response to this concern has been a focus on enabling and demonstrating versatility: a single storage system implementation should be able to simultaneously accommodate data that has strong survivability and security requirements, data that has neither but needs maximal efficiency at minimal cost, and anything in between. Such a capability would allow customers to pay only those costs necessitated by their data's requirements, and to specialize those costs/requirements for each dataset within a single storage infrastructure. Our approaches also focus on allowing the requirements, and associated costs, to be changed over time, as threat levels change and data moves through its lifecycle. In previous years, we developed and demonstrated that such versatility can be realized within the PASIS architecture, using new protocols that were developed. Just last year, however, we developed an approach that dramatically reduces the difference in overheads for attack-tolerant storage relative to simple crash-tolerant storage. To avoid the expensive techniques of previous protocols, this approach employs novel mechanisms to optimize for the common case when faults and concurrency are rare, including reduced roundtrips and a new form of checksum comprised of cryptographic hashes and homomorphic fingerprints. An implementation of this approach shows bandwidth within 10% of crash-tolerant protocols for writes and reads. We have demonstrated that it works, explained how to integrate it into the versatile storage model required for COTS providers, and worked on a prototype implementation that serves as a concrete example. We have also made significant progress on support for safe and rapid reconfiguration within a versatile storage system, delivering on the promise of dynamic versatility. COTS providers do have concerns that versatility will only serve to exacerbate the IT administration problems that plague their customers, thereby preventing adoption in the marketplace. To address this concern, we continue to develop new techniques for automating and simplifying survivable storage administration. For example, we have demonstrated new approaches to automatically identifying which server is faulty among a number of servers within a storage or data processing system. We have also developed new approaches to instrumenting distributed storage, based on end-to-end request flow tracing, and using such data to identify which components (software and hardware) are creating performance problems – for example, we have developed new approaches to using such information to compare system behaviors across time periods, which many companies (e.g., Google) are now pursuing. And, of course, we continue to develop new approaches to modeling and selecting appropriate configurations from among the options made available by versatility. A primary concern of COTS providers has been the potential for metadata service scalability limitations imposed by survivable storage architectures. We have been addressing this issue by developing new protocols for dynamically scalable metadata services that still provide correct behavior for operations involving multiple pieces of metadata that may be spread across multiple metadata servers. Traditionally, decentralized metadata services have involved complex, inefficient, non-scalable protocols for coordinating the activities of the metadata servers. Our approach, instead, allows each metadata server to operate independently and uses migration to centralize all pieces of metadata needed for a single operation. By doing so, we simultaneously eliminate some complex protocols from the system and increase scalability potential significantly. In addition, this approach has inspired a new approach to Byzantine fault-tolerant operations that should combine perfectly with this model: by temporarily locking subsets of metadata on distinct servers, in a Byzantine fault-tolerant fashion, the same scalability properties should be achievable, which would be unprecedented for Byzantine fault-tolerant services. In this year, both the basic approach and the Byzantine fault-tolerant version have matured to the point of being demonstrated and published in top-tier forums. Several companies are investigating their use to enhance existing products to eliminate existing metadata scalability limitations. We continue to focus on the availability aspects of survivability/security, in addition to confidentiality and integrity. Previously, we developed a storage server capable of preventing denial-of-service of services using it by other services using it. So, for example, compromising one service using the storage server could not lock out or even dramatically reduce the efficiency of other services. The solution was mechanisms and policies that explicitly bound the inefficiency that a particular service will see, within its configured fraction of server time, regardless of what other services are doing. During the previous and current year, we have extended this concept from a single server to the multi-server environment expected in a survivable storage solution, wherein data is distributed across the many servers. Our approaches to cache partitioning extended relatively easily, but the disk head time partitioning required some form of synchronization between the activities of servers over which each particular dataset is distributed. We developed protocols to synchronize loosely, with minimal overhead, and to co-schedule placements of dataset portions so as to minimize the complexity of finding an acceptable global schedule of disk head timeslices. The result is insulated performance for workloads in a distributed storage system. This past year, we demonstrated this concept and its efficacy, leading to a top-tier publication and continued work.

Re: Grey: Practical Logic-Based Access Control, Lujo Bauer reports: Today's computing environments are characterized by an ongoing dramatic increase in connectivity and data sharing. The number of computing devices and kinds of devices that can communicate with each other is increasing sharply, as is the amount of data and kinds of data that they store, generate, and exchange. The new functionality arising through this transformation is enabling increases in productivity, efficiency, and safety

and giving rise to fundamentally new applications in almost all aspects of our lives. A critical concern in this setting is access control---the ability to easily and quickly allow access to authorized users or devices, while preventing misuse, unauthorized access, and violations of privacy. Flexible and secure access-control mechanisms are part of what makes the new functionality and applications possible and sustainable. Authorization logics allow concise specification of flexible access-control policies, and are the basis for logic-based access-control systems. In such systems, resource owners issue credentials to specify policies, and the consequences of these policies are derived using logical inference rules. Proofs in authorization logics can serve as capabilities for gaining access to resources. Because a proof is derived from a set of credentials possibly issued by different parties, the issuer of a specific credential may not be aware of all the proofs that her credential may make possible. From this credential issuer's standpoint, the policy expressed in her credential may thus have unexpected consequences. To solve this general problem, we proposed a system in which credentials can specify constraints on how they are to be used. Building on the observation that a proof of access describes in full detail the manner in which a credential is used, our system allows credential issuers to specify constraints as functions over the proofs in which their credentials are used. This powerful mechanism allows our framework to capture a wide variety of constraints of practical interest, including the following: limiting (re-)delegation depth when delegating authority; enforcing strict revocation policies on all credentials used in a proof; preventing a credential from being used to access resources outside a particular set, which can be specified explicitly or by indirection; and constraining the size of the proof. To make it easier to understand and implement constraints, we classified them in two dimensions: in one, according to their intended use; and, in another, according to the information they need in order to be enforced. In addition to supporting a wider variety of constraints than other approaches, our framework for enforcing constraints exhibits desirable formal properties. We designed our framework to modularly build on existing authorization logics with robust proof theories. This makes it possible to apply our approach to different authorization logics, and at the same time makes it easy to prove meta-properties about the resulting system, thus providing a high assurance of correctness. We demonstrated this by applying our framework to a specific authorization logic.

Re: Robust, Secure, Efficient Networked Embedded Control Systems, Bruno Sinopoli reports: We formally defined Cyber-physical attack vectors and analyze the security of the most commonly used control systems with respect to integrity attacks. Leveraging initial results on the detection of replay attacks, we considered several extensions comprising injection of spurious sensor data in cyber-physical systems, with a special focus on Power networks. Combining predictions with measurement we can detect incongruence between the expected and the observed behavior of a system. We developed a model-based scheme to detect integrity attacks on control systems. A model of the system is required to compute its expected behavior. Any deviation can be measured and an alarm will be triggered when the probability of detection exceeds the threshold specified by the designer. In Secure Control against Replay Attack we consider the effect of a data replay attack on control systems. Suppose an attacker wishes to disrupt the operation of a control system in steady state. In order to inject an exogenous control input without being detected the attacker will hijack the sensors, observe and record their readings for a certain amount of time and repeat them afterwards while carrying out his attack. This is a very common and natural method for an attacker who does not know the dynamics of the system but is aware that the system itself is expected to be in steady state for the duration of the attack. In our work we showed the existence of conditions where such attack will be undetectable. Furthermore we provide detectability conditions that can guide the design of the estimator and controller algorithms to ensure that such attacks are always detected. We provided a quantitative tradeoff analysis relating the loss of performance to the detection probability and the speed of the detection. In False Data Injection Attacks in Control Systems we showed how an attacker can render certain classes of control systems unstable by changing a few sensor reading without being detected by commonly used fault detection schemes. In False Data Injection Attacks against State Estimation in Wireless Sensor Networks, we provide an algorithm to compute the extent of the disruption of an integrity attack on a control system. Finally in False Data Injection Attacks in Electricity Markets we show how electricity prices can be manipulated by changing load measurements on power transmission lines.

Re: BAP: The Binary Analysis Platform, David Brumley reports: We have added support for ARM to BAP, and added efficient directionless weakest precondition. This implementation creates verification conditions O(n^2) the size of a program of n statements. We have done extensive evaluation and shown that our approach is significantly more efficient than previous work

Re: Compressed Sensing for Face Recognition, Vijayakumar Bhagavatula reports: Our research progress has been on two fronts of importance to biometrics: use of compressed sensing or sparse representation for biometrics and a framework for binding and retrieving class-specific information from biometric image patterns using correlation filters. Linear models for images are very popular, whereby images representing the same class (e.g., images of the same face under different lighting conditions) are assumed to lie on a linear subspace. The main idea in the compressed sensing approach is that a test image is well represented by the training images of the same class rather than by training images from other classes. Thus, when we try to represent a test image as linear combination of training images from multiple classes, the weights of that linear combination will be mostly zero except for the weights of training images from the correct class. This observation can be turned into an optimization based on the L0 norm of the weight vector. However L0 norm optimization is NP-hard and compressed sensing theory allows us to use L1 norm instead (under some assumptions). The L1 norm optimization is more computationally feasible and we have investigated its use for face recognition and iris recognition. This problem formulation has been shown to handle up to 70% corruption by noise and up to 25% in image occlusion. These properties make it ideal to be applied to face and iris recognition, especially iris recognition since iris images usually suffer from eyelid and eyelash occlusions. The algorithm is able to handle as much occlusions and noise because of the redundancy in the images, i.e., there are more pixels in the image than

the dimensionality of the training images. Preliminary results are encouraging, but computational methods need to be improved so that we can handle reasonable sized images. Another important goal in biometrics research is to develop a method to bind an encryption key to a biometric signature such as a face image or an iris image. However, biometric encryption systems present several challenges. The main concern is that cryptography requires exact matches while biometric measurements are inherently noisy due to their natural variability. Hence combining cryptography with biometric recognition is challenging. Some requirements of biometric cryptographic systems are: 1. Revocability (i.e., the ability to revoke a compromised template), 2. Security (i.e., protection from various attacks), 3. Performance (i.e., satisfactory recognition rates) and 4. Diversity (i.e., ability to issue multiple templates for multiple applications, for the same person). Cross-correlation has been used successfully for matching a biometric pattern (e.g., a face image or an iris image) with a template. Traditional correlation filters lead to correlation outputs with strong peaks in response to authentic inputs and no such peaks in response to impostor images. We developed a new correlation filter design that leads to multiple correlation peaks at specified location in response to authentic input images. By using such advanced correlation filters to bind information to image patterns in addition to pattern discrimination, we developed a new framework to bind class-specific information to image patterns which can be retrieved by matching a query pattern with the correlation filter designed for that class of patterns. Moreover, these filters are designed to release the bound information only upon a successful match between the template pattern class and the query pattern. This new framework is also flexible enough to be able to spread the information to be bound over multiple pattern classes. This has been tested on multiple biometric databases including CMU PIE and CMU Multi-PIE face databases and has demonstrated excellent performance. The detailed results are being summarized in an IEEE T-PAMI submission.

Re: A Securable, Usable Context Toolkit for Mobile Applications, Martin Griss reports: We designed a novel system for detecting anomalies in GPS paths, using a vocabulary-based n-gram approach. The approach is quite accurate, and has broad applications to security, healthcare and other domains We designed a technique for verifying that an online component in a distributed sensor-based setting is secure and to be trusted. It supports remote code verification and access control in this setting, to be run on mobile phones and laptops, along with fixed computing. We developed a toolkit for supporting intelligibility in context-aware applications, allowing a developer to request that the system produce explanations of its behaviors for end-users, and having the system automatically produce the explanations.

Re: Security and Privacy Risk Management in Organizations, Nicolas Christin reports: We have considerably improved understanding of the impact of uncertainty in security decision making. In particular, we have provided 1) formal, quantitative evaluation of the impact of bounded-rational security decisions in the presence of limited information availability and externalities, and 2) the first formal study to quantitatively assess the impact of different degrees of information security expertise on the overall security of a network.

Re: Personal Information Security, Conflation of Dissemination and Access, and Illusion of Control, Alessandro Acquisti reports: We have introduced and test the hypothesis that control over publication of private information may influence individuals' privacy concerns and affect their propensity to disclose sensitive information, even when the objective risks associated with such disclosures do not change or worsen. We designed three experiments in the form of online surveys administered to students at a North-American University. In all experiments we manipulated the participants' control over information publication, but not their control over the actual access to and usage by others of the published information. Our findings suggest, paradoxically, that more (real or just perceived) control over the publication of their private information decreases individuals' privacy concerns and increases their willingness to publish sensitive information, even when the probability that strangers will access and use that information stays the same or, in fact, increases. On the other hand, less (real or just perceived) control over the publication of personal information increases individuals' privacy concerns and decreases their willingness to publish sensitive information, even when the probability that strangers will access and use that information actually decreases. Our findings have both behavioral and policy implications, as they highlight how technologies that make individuals feel more in control over the publication of personal information may have the paradoxical and unintended consequence of eliciting their disclosure of more sensitive information. Re On Privacy and Compliance, Annupam Datta reports: Major scientific accomplishments of our project fall under the two main lines of work. Specification and enforcement of privacy policies and laws using logic-based methods: In the context of this project we developed what we believe to be the most complete logical formalizations of the Gramm-Leach-Bliley Act (GLBA) and the Health Insurance Portability and Accountability Act (HIPAA) to date. Specifically, we formalized Sections 6802 and 6803 of GLBA and Sections 164.502, 164.506, 164.508, 164.510, 164.512, 164.514, and 164.524 of HIPAA, which include all the sections that are stated in terms of operational requirements (those that are not do not lend themselves to formalization). Despite a range of frameworks proposed for the formal specification and analysis of privacy policies and laws, there has been comparatively little work on expressing large fragments of actual privacy laws as we have done in our formalization. Hence, our work has filled a gap in this area by providing the public with a very substantial and comprehensive case study. From a technical point of view, our formalization is significant in that (i) it is the necessary first step for enforcing privacy laws in a rigorous manner, using model checking or proof theory; (ii) it gives one insight about the expressive power that is needed in a logic to adequately capture the meaning of clauses in a typical privacy regulation. In addition to producing a precise specification of GLBA and HIPAA the project also gave rise to a new logic (PrivacyLFP), which is an extension of an existing privacy logic (LPU) with real-time features and fixed point operators that provide the expressive power necessary to capture legal clauses found in GLBA and HIPAA involving bounded-time obligations and reuse of information [1]. Laws such as GLBA and HIPAA are enacted to regulate organizations such as banks and hospitals that collect and use personal information. Hence it is expected that these organizations have rules and processes

in place to comply with these regulations. In our project we also develop principles and methods to model organizational processes by assigning role-based responsibilities to agents, and to show that a process is in compliance with a regulation formalized in PrivacyLFP. An interesting technical approach we take is that our model of processes and specifications of responsibilities are also expressed in the same logic. To aid in designing processes that meet the specified privacy policies, we develop a semantic locality criterion to characterize responsibilities that agents (or groups of agents) have a strategy to discharge, and easily checkable, sound syntactic characterizations of responsibilities that meet this criterion. Policy enforcement is achieved through a combination of techniques: (i) a design-time analysis of the organizational process to show that the privacy policy is respected if all agents act responsibly, using a sound proof system we develop for PrivacyLFP; and (ii) a posthoc audit of logs of organizational activity that identifies agents who did not live up to their responsibilities, using a model checking procedure we develop for PrivacyLFP [2]. Sharing Aggregate Information with Differential Privacy Guarantees: The line of work discussed above mostly focuses on privacy as it relates to the flow of personal information about individuals within an organization. On the other hand, organizations such as banks and hospitals commonly have large databases where data can be analyzed to release aggregate information such as some statistics about financial status of account holders or about health issues that are of interest to the public. It is now well-acknowledged that unless appropriate measures are taken aggregate information released by organizations can be combined with information from other sources to infer sensitive personal information about individuals, violating their privacy. In our project we have also been investigating this aspect of privacy by focusing on a promising approach to privacy preserving data analysis called differential privacy, which was originally proposed by Dwork et. al. Differential privacy literature contains a well-developed theory for functions. Despite recent work on implementing database systems that aim to provide differential privacy, the problem of carrying over guarantees of differential privacy from mathematical functions to such implemented systems has not been adequately addressed. Our project presents the first results towards bridging this gap [3]. We lay out what we think are the basics of a formal approach for proving differential privacy guarantees for system models. We develop a formal probabilistic automaton model of differential privacy for systems by adapting prior work on differential privacy for functions. This formalization addresses challenges associated with nonterminating systems and mutable data sets. The main technical result to date is a sound proof technique based on a form of probabilistic bisimulation relation for proving that a system modeled as a probabilistic automaton satisfies mutable differential privacy. The technical novelty lies in the way we track quantitative privacy leakage bounds using a relation family instead of a single relation. We have illustrated our proof technique on a representative automaton motivated by PINQ, an implemented system that is intended to provide differential privacy.

Re: A Static Approach to Operating System Security III, Karl Crary reports: Devised and partially implemented the operational model for a static operating system. This specifies how programs (applications and device drivers) interact with the static OS kernel, particularly the scheduler and the shared heap’s garbage collector. Also designed a strongly-typed, low-level, imperative programming language intended for implementing the bulk of the static OS kernel. The language assimilates features from C, Algol, and Standard ML. Proved type-safety of the core of the language and began its implementation.

Re: User Controllable Security and Privacy for Mobile Social Networking, Norman Sadeh reports: Accomplishment 1: Expressiveness We conducted user studies where we tracked participants over several weeks and collected thousands of hours of audits: that is, users were shown their locations throughout the day and asked, for various times of the day, how comfortable they would have been disclosing their location to different types of social contacts (family, friends, etc.). Data was analyzed to see how different levels of expressiveness in privacy settings would compare when it comes to capturing these preferences. This analysis was also refined to take into account user burden considerations in the form of limits on the number of rules users can realistically be expected to specify. Results show that the privacy settings offered by today's location sharing applications (i.e., white lists) are unsuitable when it comes to capturing the wide array of privacy preferences revealed by our study. Without such settings, people simply err on the safe side and do a lot less sharing, which explains why all pull-based location sharing applications have failed so far. A similar analysis was also conducted to study people’s willingness to share their location with mobile advertisers. The results also show that people’s privacy preferences are fairly complex and will likely require more expressive settings than what is currently offered by Android or the iPhone OS. This work was published as a Tech Report and submitted for publication in a journal. Accomplishment 2: Location Naming in Location Sharing We have also gained a deeper understanding of how people name places that they share with others. For example, one could say that they are at Pittsburgh, Carnegie Mellon Campus, Newell Simon Hall, or Work. In what cases will a person use which name? We conducted a user study to understand how people describe the places they are at to different people in different situations. We identified factors that influence how people name places, the most salient of which are the recipient's perceived familiarity with a location and how public (or private) a place is. Based on this data, we also built a machine learning model that can predict with 85% accuracy what method a person would use to name a place. This work will be presented at Ubicomp2010 Accomplishment 3: Social Properties of Physical Locations We developed several quantitative measures for studying the social properties of a physical location, including location entropy, which measures the frequency and relative proportion of the unique users who visit a location. We showed that these measures prove valuable in analyzing human location data. In one study we showed that location entropy is positively correlated with the comfort the user has with sharing a location with others. Users are more comfortable sharing high entropy (public) places than low entropy (private) places. In another study we showed that location entropy can be used to predict the social structure of a set of users by analyzing their co-location patterns. From a privacy perspective, this result both illustrates the need for privacy controls over location data, and it also provides some groundwork for the development of systems which can aid users in understanding their privacy needs through a better understanding of their social network. This work will be presented at Ubicomp2010 We have begun analyzing location traces to see if we can form a

bridge between physical world contact and online contact. Using various machine learning techniques, we can predict whether people are likely to be friends on Facebook based solely on their co-location patterns. We also found a positive relationship between the mobility patterns of a user and the number of online friends the user has.

Re: Compiling Epistemic Specifications to Secure Distributed Code, Frank Pfenning reports: We have designed a secure distributed specification language based on linear epistemic logic. This is a significant theoretical advance, clarifying the role of linearity (to deal with state change) and epistemic modalities (to deal with local knowledge and possession) for specifying secure distributed computation. We intend to develop reasoning principles and an implementation the next reporting period.

Re: MERIT Insider Threat Laboratory, Dawn Cappelli reports: Incidents involving insiders that stole intellectual property were analyzed by the CERT Insider Threat team to better understand the trends and methods that insiders use to exfiltrate sensitive data from a company. Our research builds upon previous findings by Moore et al in Insider Theft of Intellectual Property for Business Advantage: A Preliminary Model which developed initial models and analysis of insider theft of IP cases. Our research expands upon these initial findings by studying the business assets and types of intellectual property that has been targeted by the insiders in order to better understand the threat. After learning about the ways insiders have stolen data from a company, we analyzed the types of controls that could be put in use to mitigate the occurrence of these incidents. Additionally, our research involves looking at the current state of vendor tools that claim to address the problem of data leakage from an organization. These tools are often known as data loss prevention (DLP) applications. Based on the actual data exfiltration methods observed in the CERT case library, we analyzed several major commercial and open source tools by its available DLP features. This analysis was done using a combination of product literature, independent research, and live testing (when possible) in a laboratory environment. Based on our analysis, we are able to draw some conclusions about gap areas that exist in the tool space with respect to combating theft of intellectual property by insiders. We sought to understand the focus of the market and leveraged our case studies of real incidents to draw conclusions and gap areas that exist in the industry. We have begun the construction of an Insider Threat Lab for MERIT. The ongoing analysis of cases has yielded recommended best practices, models of insider behavior, training materials and other useful results. As we begin to put this body of knowledge into practice, the Insider Threat Lab will allow us to begin to test our results in an actual environment. We can now start to determine the effectiveness of various controls and tools against the threat of malicious insiders and will be in a better position to make concrete, technical recommendations for prevention and mitigation. Currently, the lab has been used to recreate scenarios based on cases from the CERT Insider Threat database to help teach cyber-defenders how to use tools to protect their networks. These demonstrational videos have been presented at respected security conferences and CERT Insider Threat workshops. In the future, the Insider Threat Lab will greatly improve the research of insider threat and benefit organizations by creating cyber-defense exercises. The flexibility of this Insider Threat Lab provides a quick way to realistically study insider attacks and respective defense mechanisms. Through using the Insider Threat Lab, an in-depth study and analysis of current tools can be performed and a set of best practices will be developed for companies to utilize. Finally, by incorporating the Insider Threat Lab with CERT's XNET training environment, realistic training exercises can be performed by organizations to better equip their defenses against malicious insiders. We have also begun construction of an open-source, network-based data loss detection tool. Our hope is to produce a tool that will integrate with an existing Snort infrastructure to help detect the exfiltration of various types of sensitive data from a network.

Re: MERIT Insider Threat Metrics, Andrew Moore reports: The CERT/CyLab metrics research plan set forth several goals. At a high level, these included discovering and analyzing categories of interesting vulnerabilities associated with insider threat, ranking various combinations of these selected attributes in order of the impact/severity of the incident in question, and beginning to formulate models (specifically, regression models) to help understand the significance of each vulnerability. The goal here is to understand what, if any, vulnerabilities are more significant than others, and help organizations take steps to measure their effectiveness at combating insider threat through reducing vulnerabilities over time. Thus far, the project has benefitted from extensive vetting of various groups of vulnerabilities and exploits observed across the 350+ insider threat cases in our database. We have catalogued over 4000 vulnerabilities that belong to over 150 unique classes. These classes are abstracted into 8 high-level classes of security areas of interest, including logging and monitoring, behavioral risk management, and user access control. At this time, we are actively working through the data associated with the user account control vulnerabilities and working to rank order applicable cases in terms of a generalized impact scale so as to begin statistical modeling of the vulnerabilities in aggregate. Within this user account control grouping, we have identified 30 classes of specific vulnerabilities and actions, which are being used in concert with other case attributes to weight various aspects of observed insider activity against a standardized scale which attempts to order levels of impact in such a way that organizations of varying size and shape can relate to one another. Approximately 30 cases exist in the pool being used to create the first iteration of the proposed insider threat scoring metric.

Re: Autonomous Trustworthy Computing Platforms and Devices, Ole Menegshoel reports: The project has supported, fully or in part, Research Assistantships for four graduate students, two of which are Ph.D. students in the bi-coastal ECE program, and two of which are M.S. students on the Silicon Valley campus. The Ph.D. students started in January 2010, while the M.S. students started in September 2009. While not all four students have yet submitted publications, they are all in the process of developing publications, and several additional submissions are expected within the next 1-6 months. Below, I briefly describe the scientific progress and accomplishments made by students in collaboration with myself and other CMU faculty. One student has been engaged in improving the understanding of the relationships between the measurable properties of software (metrics)

and its quality (trustworthiness, specifically as measured by number of bugs). In this research, we have investigated Open Source projects (Java projects), and specifically collected their source code (*.java files). Various metrics (LOC, Defects/LOC, Number of comments, types of bugs in the projects, etc;) were then computed by processing the Java source code of these projects. These metrics were then used to create heuristics for identifying trustworthy/dependable software, using a machine learning approach. Different supervised machine learning algorithms, such as Bayesian networks, Naïve Bayes, and Decision Trees, have been and are being investigated. A conference/workshop paper, with tentative title Software Bug Prediction: A Machine Learning Approach is under development. Two students, partly funded by ARO, have been working on visual analytics for making comparisons across different parts of a data corpus and across multiple representational levels in a complex data set. This work has been concerned with developing multi-focus, multi-level, and multi-zoom visualization and analytical techniques that also preserve the structure of networks. Starting from a network overview, the approach and supporting software tools can be successfully used to analyze large-scale data sets. Several publications and posters are in progress in this research area. Finally, it has become clear over the last year that for the type of large-scale data sets that we are interested in, computational processing power is a serious concern. Consequently, we have during the first 6 months of 2010 obtained and installed a Hadoop cluster, consisting of 8 computers with a total of 32 cores, for data-intensive computing. Hadoop is a distributed computing framework for processing large amount of data. Compared with previous distributed frameworks, Hadoop has the following advantages: (1) fault tolerance; (2) easy of programming; (3) performance that improves linearly with the number of machines; (4) ease of program deployment. We have started using this capability with existing machine learning algorithms, are in the process of developing novel approaches, and expect that this will lead to publications in the next few months. In addition, the development of this Hadoop cluster will enable research and long-term improvements in the area of Computing Platforms, Data Centers, and Cloud Computing. The data centers of the Computing Infrastructure may contain multiple subsystems such as, for example, servers, switches, power systems, cooling systems, etc. The hardware and software of these sub-systems provide an infrastructure for communications, Web search, Web mail, and other software services, and keeping them operational and healthy is therefore of crucial importance. With the installation of this cluster and supporting software at CMU Silicon Valley, we now have a facility where research in this area can be performed.

Re: Visualizing Home Networks, Jason Hong reports: SafetyNet is a user interface we are developing to improve people's abilities to manage access control for home networks. We have done one round of prototyping and evaluating user interfaces. The first interface showed what devices could potentially interact through Venn Diagrams. Users could manipulate icons for devices in this interface, to modify access control policies. The second interface also showed devices, but used small icons near devices to represent what devices could potentially interact with one another. Our first round of evaluation showed that people could complete basic tasks in these two interfaces, though there were some challenges with respect to scale. We are also exploring the use of proximity as a way of managing access control for homes. Examples include scenarios like My children can only watch TV when I am at home, My children can only log into Facebook when I am also in front of the computer, and Guests can view my pictures only when I am at home. While we do not believe that proximity can solve all problems, we do believe that proximity can greatly simplify access control policies, are easier to understand and remember, and give people greater confidence that they got the rules right. We are currently preparing a series of user studies to evaluate how effective proximity rules can be in hypothetical scenarios. We will then proceed to build systems that make use of proximity, using ubiquitous computing technologies such as mobile phones, RFIDs, or simple cameras and computer vision. We have also been conducting a series of meetings with Intel Pittsburgh to examine points of collaboration. Currently, Intel Pittsburgh is purchasing a collection of equipment to install in homes, which will form the basis of a testbed for this work.

Re: Dynamically Reconfigurable Antenna Arrays for Anti-Jamming and High-Performance Applications, Jason Lohn reports: Our CyLab seed effort resulted in a low-cost system that was successfully able to adaptively thwart a jamming signal.

Re: Circuit-Level Secure-by-Design Digital Integrated Circuits, Ken Mai reports: A novel physical unclonable function (PUF) based on SRAM sense amplifiers was designed that demonstrates significantly lower latency and greater temperature stability than alternative PUF topologies. The PUF allows for post-manufacturing tuning for additional stability and reliability. The design, simulated in a 65-nm bulk CMOS process technology, demonstrates ~3x lower errors than alternative topologies across temperature and voltage variations. An exploration of implementing AES S-Boxes using custom power-analysis-resistant ROMs was undertaken. These ROMs demonstrate lower latency, power, and area than canonical standard cell logic S-Box implementations. Both secure and unsecure versions of the ROMs were designed in a 90nm bulk CMOS process. The secure ROM exploits the inherent similarity of ROM accesses to achieve over 10x higher power-analysis resistance than the logic implementation (as measured by the normalized energy deviation). The unsecure ROM achieves over 3x faster latency, 10x lower energy, and over 2x lower area than the logic implementation.

Re: Insider-Forensics - Keystroke Error Rates, Roy Maxion reports: We compared 14 different anomaly detectors on the same data set. The literature (keystroke dynamics, which we regard as an E. coli model organism for detection) strongly suggests that neural nets form the best anomaly detectors. Our research showed, however, that a detector based on a Manhattan distance metric outperformed all other detectors. No other investigators had compared a suite of detectors against the same data set; this is a first, and it debunks the common wisdom that neural nets are the top detection performers. Keystroke biometrics is used to identify users on the basis of their typing rhythms. Over the 30-year history of the field it had always been assumed that typing rhythms were unique to individuals, but this hypothesis had never been tested. We tested this idea in a tightly-controlled experiment, obtaining 99.97% correct detection. This result confirms scientifically what had been merely assumed for a long

time. With this confirmation we can go forward with confidence in using keystroke biometrics in applications such as two-factor authentication and continuous re-authentication.

Re: Contractual Anonymity, Jonathan McCune reports: We propose, develop, and implement techniques for achieving contractual anonymity. In contractual anonymity, a user and service provider enter into an anonymity contract. The user is guaranteed anonymity and message unlinkability from the contractual anonymity system unless she breaks the contract. The service provider is guaranteed that it can identify users who break the contract. The significant advantages of our system are that 1) the service provider is not able to take any action toward a particular user (such as revealing her identity or blacklisting her future authentications) unless she violates her contract, 2) our system can enforce a variety of policies, and 3) our system is efficient.

Re: Security Quality Requirements Engineering (SQUARE) Project, Nancy Mead reports: SQUARE was accepted as a CMU Master of Software Engineering (MSE) Studio Project. A team of 5 MSE students is producing a robust tool for SQUARE, to replace the current prototype tool. The new tool will be available September 2009. As planned, SQUARE was extended to address acquisition. A short working paper describing this extension was developed. In addition SQUARE is incrementally being extended to address privacy. This year there are three part-time CyLab-sponsored student interns working on the privacy aspects of SQUARE: Varokas Panusuwan, Prashanth Batlagundu, and Gowtham Sridharan. In addition, Dr. Saeed Abu Nimeh, a researcher at WebSense, is collaborating with the project as a volunteer. Seiya Miyazaki, a master's student of Justin Zhan at CMU Japan, worked at CMU Pittsburgh during the summer of 2008 under the supervision of Nancy Mead on a thesis project as part of his degree program. The thesis partially extended SQUARE concepts to include privacy aspects and this was built into the SQUARE prototype tool. Seiya sought the advice of Lorrie Cranor and other CMU Pittsburgh faculty members during this research project. Nancy Mead and Justin Zhan are on the organizing and program committees for a number of conferences and workshops addressing security and privacy.

Re: Attacking and Defending Unreliable Hardware, Onur Mutlu reports: We have developed novel attacks and methods to prevent denial of service attacks in three major critical shared resources in future/current multi-core computer systems: • Main memory controllers • On-chip interconnects/networks • Shared L2/L3/L4 caches Demonstration of new, cache locality-based thermal attacks and new defenses: We have demonstrated for the first time that the commonly-envisioned distributed shared cache organization that takes advantage of locality leads to a new thermal threat in multi-core architectures [Subramanian et al., USENIX Security 2010 submission]. We demonstrated that the most promising scalable multi-core designs are severely vulnerable to a new class of thermal attacks, exactly because the system is designed to maximize locality in shared caches. A malicious application, called a Locality-based Thermal Attacker (LTA), can repetitively access data in the shared cache to increase the temperature of both the shared resource, its core and connecting buses beyond the limits for which the chip is designed. As a result, the hardware wears out quickly, chip lifetime reduces, or overall performance degrades significantly in an attempt to contain the temperature within a tolerable range. To contain the LTA with minimal performance loss in the entire system, we devised new techniques that migrate frequently-accessed data far away from the LTA. Our results showed that the proposed defense mechanisms can effectively prevent LTAs, with minimal impact on performance. These attacks can especially hurt profit, productivity, and comfort in cloud computing, mobile, and interactive systems; therefore, solving them can lead to enabling new applications and systems. Demonstration of denial of service attacks in on-chip interconnects and new defenses: We have demonstrated that the on-chip interconnection networks, which are also envisioned to be a scalable way to build multi-core systems, are vulnerable to new denial of service attacks. A malicious attacker can inject traffic in the network and destroy the performance of all other co-executing applications as well as the entire system on the same multi-core chip. The attack can be launched by a single attacker or with multiple cooperating (intentionally or unintentionally) attackers, which constitutes distributed denial of service. The difficulty is that a malicious attacker can be very difficult to distinguish from a regular application We have developed many different solutions to this problem. These include ensuring QoS/fairness in on-chip networks via packet scheduling [Das et al., ISCA 2010], redesigning the on-chip network topology with QoS as a first class goal [Grot et al., MICRO 2010 submission], congestion control techniques for bufferless networks [Nychis et al., HotNets 2010 submission], and fair source throttling techniques [Ebrahimi et al., ASPLOS 2010]. The solutions are effective and provide high-performance. New main memory controller designs that provide QoS/fairness and prevent denial of service attacks: We have developed new insights into how to design memory controllers to satisfy QoS guarantees while at the same time providing very high performance. We have discovered that least attained service memory scheduling not only prevents denial of service attacks in the memory system but also provides a very high throughput substrate on top of which the operating system can build QoS policies [Kim et al., HPCA 2010]. The ATLAS memory controller is the first memory controller design that takes into account the existence of multiple memory controllers on chip and recognizes the need for them to be coordinated to ensure high QoS and high performance. More recently, we have devised the fairest as well as highest-performance memory scheduler that exploits very fine-grain changes in programs' memory access behavior to balance the amount of service each thread achieves. No previous work in memory controllers provided the best fairness as we as best system throughput at the same time. This work is currently under review [Kim et al., MICRO 2010 submission]. A new, generalized QoS substrate for multi-core systems: To tackle the denial of service issues in all shared memory resources in multi-core systems, we have developed a generalized new approach. The idea is to detect unfairness and denial of service using hardware monitoring mechanisms, feed back this information to a hardware or software controller, and have the controller adjust the throttling levels of the respective cores to prevent denial of service, improve fairness, and provide QoS. This work is a new approach to thinking about ho denial of service should be prevented end to end in the entire multi-core system. Previous works predominantly focused on preventing

denial of service in each shared resource but did not take a holistic view of the shared memory system. This work received the best paper award at ASPLOS 2010 [Ebrahimi et al., ASPLOS 2010].

Re: User Controllable Security and Privacy for Mobile Social Networking, Sasha Romanosky reports: In “Do data breach disclosure laws reduce identity theft?” we collected data from FOIA requests to the Federal Trade Commission over 2002-2009, we empirically estimated the effect of data breach disclosure (security breach notification) laws on consumer identity theft. Our findings suggest that these laws (requiring firms to notify consumers when their personal information is lost or stolen) reduced identity theft by about 6%, on average. This research fostered a great interest into general forms of policy mechanisms (laws) that can be employed to reduce externalities caused by companies. For instance, there is substantial literature that compares and contrasts mandated standards with legal liability regimes. In “Privacy Costs and Personal Data Protection: Economic and Legal Perspectives” we examine those two regimes in combination with information disclosure laws. We discuss the incentives that they are expected to drive for companies and consumers, and then contrast this with their practical outcomes (i.e., their limitations). We also attempt to assess their effectiveness in regard to data breaches and resulting consumer harms. Specifically, we identify a number of consumer behavioral biases that may prevent information disclosure from becoming very effective. For instance, while disclosure may empower consumers to take action to mitigate harm, it may also burden them, causing them to ignore the potential threat. Moreover, while mandated standards are useful for forcing companies to adopt minimum information security standards, it may drive companies to compliance, and not actually reduce the risk of future data breaches. Finally, while a legal liability regime may be useful to allow consumers to recover losses; these attempts often fail because victims are unable to demonstrate actual harm, as is required in negligence liability claims. Finally, in “Data Breaches and Identity Theft: When is Disclosure Optimal?” we analytically examine the effect that data breach disclosure laws should have on firm and consumer incentives. We leverage the economic analysis of accident (tort) law in order to identify the conditions under which these forms of laws can reduce overall social costs. Here, we find that disclosure laws will likely reduce consumer costs, while increasing firm costs. In cases when the firm bears only a small portion of consumer losses (i.e., when they provide only a small amount of consumer redress), a disclosure tax may be necessary in order to reduce overall social costs.

Re: As-If Infinitely Ranged Integer Model, Robert Seacord reports: The AIR integer model produces either a value that is equivalent to a value that would have been obtained using infinitely ranged integers or a runtime-constraint violation. AIR integers can be used for dynamic analysis or as a runtime protection scheme. At the -02 optimization level, our compiler prototype showed only a 5.58% slowdown when running the SPECINT2006 macro-benchmark. Although that percentage represents the worst-case performance for AIR integers (be-cause no optimizations were performed), it is still low enough for typical applications to enable this feature in deployed systems. AIR integers have also been proven effective in discovering vulnerabilities, crashes, and other defects in the JasPer image processing library and the FFmpeg audio/video processing library during testing with dumb (mutation) fuzzing.

Re: Collaborative Mobile Sensor Network Control with Extremely Noisy Measurements, Pei Zhang reports: We are working flying sensor nodes using very few sensors. Three universities are now using the novel platform. We have received significant press coverage for our research, including Physics of the Impossible. Discovery’s Science Channel, Sep 2010 (to appear), SwarmBots. BBC FOCUS MAGAZINE, Mar 2010, Aerobot Invasion, POPULAR SCIENCE, Mar 2010, Networked surveillance minicopters, NEW SCIENTIST, Nov 2009, SensorFly robots hunt in packs and can take a battering, WIRED, Nov 2009, Self-righting autonomous swarming robots, MAKEZINE, Nov 2009.

Re: VMA: Dynamic and Secure Heterogeneous System for Elder Care, Pei Zhang reports: We have designed a distributed far field audio event detection system for in-home patient monitoring. We have 50+ hours of sound traces.

Re: Soft Biometrics from Emerging Media (Project) Yang Cai reports: We have achieved significant progress in detecting anomalous sound patterns, super-resolution for video forensics and feature detection from hand-held videos. We have also built a remarkable link between Soft Biometrics and Multimedia Forensics for intelligence analytics. This has a major impact on theoretical and practical development of both fields. Our new concept Surreal Media has been accepted by ACM Multimedia conference in 2010 for the workshop on Surreal Media and Virtual Clone

Re: "Deep Software Assurance: Requirements, Techniques, Field Experience," Jonathan Alrich and William Scherlis report: Proved the soundness of our CyLab-funded architecture assurance technology, and carried out a case study applying the tool to verify secure information flow and find seeded defects in an application of moderate size. Carried out experiments with typestate verification at scale, and explored a wider application of the technology in the context of a novel programming language with a permission-based type system. Developed and published a new technique for assuring compliance with complex, security-relevant framework constraints.

Re: "Efficient Data-Intensive Computing in Support of Security Applications," David Andersen reports the following: This year featured two major advances: Improved algorithms for large-scale pattern matching, with applications to virus scanning, exfiltration prevention, and large-scale data analytics; and the CLAMP architecture for securing web sites against external attack. The algorithmic improvements result in a 2-6x improvement in speed for virus scanning, with a similar reduction in the amount of memory required, enabling today's virus scanning algorithms to remain scalable for several additional years of

growth in the amount of viruses. In addition, the basic algorithmic technique, described in the "Fast Cache" technical report, has applications well beyond virus scanning, both inside security and more broadly in data analytics. The algorithm speeds up searching large data corpuses for any item matching one of hundreds of thousands or millions of patterns.

Re: SCION: Scalability, Control, and Isolation On Next-Generation Networks, Adrian Perrig reports: We presented the first Internet architecture designed to provide route control, failure isolation, and explicit trust information for end-to-end communications. SCION separates ASes into groups of independent routing sub planes, called trust domains, which then interconnect to form complete routes. Trust domains provide natural isolation of routing failures and human misconfiguration, give endpoints strong control for both inbound and outbound traffic, provide meaningful and enforceable trust, and enable scalable routing updates with high path freshness. As a result, our architecture provides strong resilience and security properties as an intrinsic consequence of good design principles, avoiding piecemeal add-on protocols as security patches. Meanwhile, SCION only assumes that a few top-tier ISPs in the trust domain are trusted for providing reliable end-to-end communications, thus achieving a small Trusted Computing Base. Both our security analysis and evaluation results show that SCION naturally prevents numerous attacks and provides a high level of resilience, scalability, control, and isolation.

Re: The Impact of Online Social Networks on Firms' Hiring Practices and The Evolutionary Roots of Privacy and Security Concerns, Alessandro Acquisti reports: We completed studies on the re-identifiability of individuals based on face recognition and online social networks data. The results were presented at BlackHat USA 2011. We investigated the feasibility of combining online social network data with off-the-shelf face recognition applications for the purpose of individual re-identification. Two completed experiments demonstrated a high degree of success in identifying strangers online (for instance, on websites where individuals use pseudonyms, such as dating sites) and offline (for instance, on the street), based on the profile pictures they posted on a popular online social network. One ongoing experiment additionally showcases the ability to infer personal and even sensitive information about a stranger merely by combining, in real time, face recognition algorithms and access to online resources.

Re: Techniques for Compositional Security: Foundations, Mechanized Reasoning and Applications, Anupam Datta reports: We develop a formal framework for compositional reasoning about secure systems. A key insight is to view a trusted system in terms of the interfaces that the various components expose: larger trusted components are built by combining interface calls in known ways; the adversary is confined to the interfaces it has access to, but may combine interface calls without restriction. Compositional reasoning for such systems is based on an extension of rely-guarantee reasoning for system correctness to a setting that involves an adversary whose exact program is not known. At a technical level, we present an expressive concurrent programming language with recursive functions for modeling interfaces and trusted programs, and a logic of programs in which compositional reasoning principles are formalized and proved sound with respect to trace semantics. The methods are applied to representative examples of web-based systems and network protocols.

Re: Next-Generation Binary Analysis Techniques and Platform, David Brumley reports: Program analysis of binary (i.e., executable) code has become an important and recurring goal in software analysis research and practice. Binary code analysis is attractive because it offers high fidelity reasoning of the code that will actually execute, and because not requiring source code makes such techniques more widely applicable. BAP, the Binary Analysis Platform, is the third incarnation of our infrastructure for performing analysis on binary code. Like other platforms such as CodeSurfer/x86, McVeto, Phoenix, and Jakstab. BAP first disassembles binary code into assembly instructions, lifts the instructions to an intermediate language (IL), and then performs analysis at the IL level. BAP provides the following salient features: BAP makes all side effects of assembly instructions explicit in the IL. This enables all subsequent analyses to be written in a syntax-directed fashion. For example, the core code of our symbolic executor for assembly is only 250 lines long due to the simplicity of the IL. The operational semantics of the IL are formally defined and available in the BAP manual. Common code representations such as CFGs, static single assignment/three- address code form, program dependence graphs, a dataflow framework with constant folding, dead code elimination, value set analysis [3], and strongly connected component (SCC) basedvalue numbering. Verification capabilities via Dijkstra and Flanagan-Saxe style weakest pre- conditions and interfaces with several SMT solvers. The verification can be performed on dynamically executed traces (e.g., via an interface with Intel’s Pin Framework), as well as on static code sequences. BAP is publicly available with source code at http://bap.ece.cmu.edu/. BAP currently supports x86 and ARM. We have leveraged BAP in dozens of security research applications ranging from automatically generating exploits for buffer overflows to inferring types on assembly. A recurring task in our research is to generate verification conditions (VCs) from code either using forward symbolic execution or weakest preconditions. Generating VCs that are actually solvable in practice is important; we routinely solve VCs hundreds of megabytes in size that capture the semantics of 100,000s of assembly instructions using BAP.

Re: Cloud Computing and CyLab: Establishing a Shared Utility and Informing Assured Cloud Computing Research, Greg Ganger reports: This project had two primary goals, both of which it achieved: First, we established, maintained, and instrumented three shared clouds, one using each of the three most popular cloud computing models: (1) a Hadoop-based cloud for use running data-intensive computing applications using the MapReduce model. (2) a Tashi-based cloud for use running more general computing tasks in virtual machines, using a model akin to Amazon’s EC2. Tashi is an open source software infrastructure for cloud computing that CMU and Intel have developed collaboratively, and it is a primary part of the evolving OpenCirrus software stack and used for Intel’s OpenCirrus site. (3) a VMware-based cloud for use running general

computing tasks in virtual machines, building on the vcloud framework. These shared clouds have been used by various Carnegie Mellon researchers, for research described elsewhere in this report. Second, we have used the experiences, measurements and case studies from these shared clouds to gain insight informing our explorations into the new space of cloud computing and its associated security and assurance challenges. Among other things, the result has been the new research center described above. Also, the industry connections associated with this project have made our results (and software) highly transferable to industry – indeed, this was an explicit component of both the Intel and VMware connections

Re: Reconciling Privacy and Usability by Learning Default Privacy Policies, Norman Sadeh reports: In the past year, we have worked to better understand users' location-sharing preferences and developed user-oriented machine learning techniques to help users specify and refine privacy and security policies, focusing on the location-sharing domain. These results are further discussed below: Increasingly users interact with social networks and mobile applications that leverage a wide range of personal attributes. The business models of these networks and applications often depend on users sharing their personal information. This creates a tension because users have complex privacy preferences that determine when they wish to disclose information, and it is difficult for users to specify these preferences explicitly in a policy. To address this difficulty, we have been working on user-controllable policy learning (UCPL). UCPL applies machine learning in a user-friendly way to help users specify privacy policies. We have developed a two-pronged approach to UCPL that first identifies default personas that cover the space of different privacy policies. Once a user is mapped to a default persona, iterative refinement then helps the user to further update his/her policy so that it can even better capture some of the user's finer preferences. We have evaluated this approach with data collected from 60 users over a period of 3 weeks. The results strongly suggest that our approach can significantly help when it comes to helping users specify their privacy preferences. At the same time, further validation will be required in the context of longer live studies. We have also worked on adapting Gaussian mixture models to be used in UCPL. We have shown that Gaussian mixture models can be used to learn location-sharing policies of users that evolve gradually over time and should therefore be understandable. Gaussian mixture models open up several modern techniques in active and semi-supervised learning, which we intend to further explore. We are also investigating how machine learning in general can be used to assist users specify a broad range of policies and preferences. We know of no good overview of prior research in the area of user-oriented machine learning. Currently, the challenges associated with this area remain ill understood. In an attempt to remedy this situation, we have made substantial progress on a survey document that offers a taxonomy of research challenges along with an overview of relevant work that has been conducted in this and related areas – including our own. As a tool to investigate user preferences, we use a location sharing application called Locaccino (www.locaccino.org), which we have previously developed. We are creating a ``wizard'' with the goal of quickly and easily allowing a new user of Locaccino to identify a privacy policy that works best for him or her. The next step will be to try to configure the wizard using privacy personas identified by our machine learning algorithms. Additionally, Locaccino has been deployed to track the shuttle buses here at CMU. Students can now find the up-to-the-minute location of their preferred shuttle using a computer or smartphone. We expect this to contribute to the further uptake of the application and provide us with more data to analyze. To better understand users privacy preferences for location sharing, we also conducted several user studies: Studies focusing on the role of obfuscation settings in better capturing users location sharing privacy preferences. These studies show that beyond location and time restrictions on the conditions when someone is willing to share their location (e.g. "Only share my location with my colleagues on weekdays, 9am to 5pm, and when I'm on company premises), obfuscation can play a significant role in better capturing people's preferences (e. g. "share my location with friends during the weekend but only at the level of the city I am in and not at a finer level"). A three-week comparative study collecting location traces and location-sharing preferences from two comparable groups in the U.S. and China (29 from the U.S. and 30 from China). Our analysis examines different aspects of our participants' location-sharing preferences. This includes comparing mobility patterns and willingness to share locations with different types of recipients. It also includes looking for conditions under which different users are more or less willing to share their locations, such as particular days or times of the day and particular locations. Overall, the study showed that people in both groups had complex and diverse location sharing privacy preferences. At the same time, the study also revealed some subtle differences that may have an impact on the privacy settings one might want to expose to each group (as well as different privacy personas/profiles to chose from).

Re: Online Crime Economics: Modeling Advertising and Retail Operations, Nicolas Christin reports: Significantly improved understanding of tactics used by online miscreants to redirect web traffic to their businesses/activities (see USENIX'11, CCS'11 papers), and complemented these measurement studies with economic analysis of the structure of the groups behind such tactics, as well as the profits they can expect to make. Considerably improved our understanding of the effects of password policies on password security. Evidenced numerous possible attacks on mobile platforms in general, and Android in particular

Re: Improving the Security and Usability of Text Passwords, Lorrie Cranor reports: Text-based passwords are the most common mechanism for authenticating humans to computer systems. To prevent users from picking passwords that are too easy for an adversary to guess, system administrators adopt password-composition policies (e.g., requiring passwords to contain symbols and numbers). Unfortunately, little is known about the relationship between password-composition policies and the strength of the resulting passwords, or about the behavior of users (e.g., writing down passwords) in response to different policies. We conducted a large-scale study that investigates password strength, user behavior, and user sentiment across four password-composition policies. We characterize the predictability of passwords by calculating their entropy, and find that a number of commonly held beliefs about password composition and strength are inaccurate. We correlate our results with user behavior and sentiment to produce several recommendations for password-composition policies that result in strong passwords

without unduly burdening users. We performed an analysis of 12,000 passwords collected under seven composition policies via an online study. We developed an efficient distributed method for calculating how effectively several heuristic password-guessing algorithms guess passwords. Leveraging this method, we (a) examined the resistance of passwords created under different conditions to password guessing; (b) examined the performance of guessing algorithms under different training sets; (c) investigated the relationship between passwords created under a given composition policy and others that happen to meet the same requirements; and (d) investigated the relationship between guessability, as measured with password-cracking algorithms, and entropy estimates. We believe our findings advance understanding of both password-composition policies and metrics for quantifying password security.

Re: Impact of Sensor Fidelity on Residential Smart Meter, Anthony Rowe reports: This funding supported the development of a home automation and sensing platform that can collect data related to home energy usage and user activities. Initial data suggests that high-speed energy data can reveal information about high-level user activities, occupancy and even consumer appliance types. This platform has been integrated with the Sensor Andrew middleware (also partially CyLab funded).

Re: Efficient and Effective High Speed Network Logging for Digital Forensics, David Andersen reports: The work we have done in the prior year reflects technological advancements underpinning our creation of high-throughput, high-efficiency data recording and analysis systems. Our work encompasses two main thrusts: First, high-throughput search over large unstructured data streams. In particular, we have extended our work from the previous year on performing "multi-grep" (searching large corpuses of data for thousands of millions of patterns at once). Last year we collaborated with David Brumley to integrate these techniques into the ClamAV open source virus scanner, resulting in a 2x speedup and 2x reduction in memory use. Since then, we have completed a formal analysis of the behavior of our algorithm, and in the process, discovered several additional opportunities for optimization. To our knowledge, ours if the fastest algorithm for simultaneously searching for a large number of (fixed, non-wildcard) patterns in huge amounts of data. The second research thrust is high-performance, low-latency key-value storage. Key-value stores underlie many popular Internet services (facebook, twitter, etc.), and are fundamental building blocks for a large number of large-scale data retrieval systems. Our papers at SOSP (a leading operating systems conference) and SOCC (a new conference collaboration between the systems and database community) address two important issues for these systems: DRAM efficiency and load-balancing at high scale. We have created a new indexing algorithm for key-value storage systems that is the most memory-efficient yet known when storing data on flash devices, and have shown new theoretical and empirical results in load-balancing to help overcome performance bottlenecks when scaling these systems up. Lujo Bauer reports: Prototype Semantic File System We have continued developing our prototype of Perspective, our semantic file system, and supporting its ongoing deployment in several offices and the student lounge in our building. The goal of our efforts has been to improve the prototype to make it feasible to deploy more widely in a practical setting, e.g., on laptops that move between home and work, run different operating systems, and experience periods of poor or non-existent network connectivity. More specifically: • We developed a first cut of a Perspective appliance, which enables our file system to be deployed on a host inside a minimal virtual machine. In this mode, a Perspective instance always runs in a virtual machine and exports its file system to the host via CIFS or NFS. The goal of this was to make it easier to support multiple OS platforms; most importantly, Windows was previously unsupported due to incompatibility with some of the core libraries used in Perspective. • We developed infrastructure to allow Perspective instances to communicate across network boundaries. Previously, we relied on Linux and MacOS peer-to-peer discovery services, which were both unreliable and, even in the best case, limited to finding devices in the same subnet. • We demonstrated these new features to industry partners via a demo in which three Perspective instances, running on different OSes and attached to different networks, collaborated to allow real-time, ad-hoc photo sharing between users. Reactive Policy Creation We previously carried out user studies that suggested that reactive policy creation, in which users can update their policy dynamically in response to access requests that cannot otherwise succeed, may be a good fit for file access control at home. In the past year we completed a follow-up study: The goal of this second study was to explore whether reactive policy creation would seem be an appealing an option when people were using it— and hence experiencing its potential disadvantages or inconveniences—instead of just hypothesizing about using it. In particular, we wanted to know whether people have specific policy needs that match better to a reactive model than a traditional model, as well as whether reactive policy creation better matches users' mental models and preferences. We also wanted to know whether responding to requests would prove so tedious or annoying that the reactive model would be impractical. For this study, we chose to focus on how well the reactive model could work for file owners; we did not explore reactive policy creation from a requester's point of view. To address these questions as realistically as possible without building an actual reactive system, we designed and executed an experience-sampling study intended to simulate the experience of using a reactive policy creation system to manage file access. Our 24 participants provided names of files they have and people they know. For one week, each participant received and responded to simulated access requests drawn at random from these lists of people and files. We collected a rich set of data that bolsters the case for using reactive policy creation as one of the modes by which home users specify file-access-control policy. We found quantitative and qualitative evidence of dynamic, situational access-control policies that are hard to implement using traditional models but that reactive policy creation can facilitate. In particular: • Policies change over time. Our results indicate that participants' file-sharing policies change relatively often, in response to a variety of factors. Reactive policy creation is better suited to express these kinds of dynamic policies than traditional access-control models. Specifically, in the second round of the study participants chose to use reactive policy creation for 15% of the user-file pairs (i. e., 15% of an ACL or access matrix). Additionally, we found that users changed their policy preferences between the initial interview in which users described their policy and the simulated access request for a file covered by their policy—in fact, users responded to 12% of the simulated requests in a manner inconsistent with the policy they had previously specified.

Interestingly, 62% of all conflicts involved participant prohibiting an access statically (i.e., when filling out the access matrix on paper) but allowing a simulated request. This provides some evidence that people will share more reactively than proactively. • Policies are situational. Our results indicate that participants' policies are dynamic in part because their sharing decisions depend heavily on the details of the situation at the time the access-control decision is made. Again, this context-awareness is a natural fit for a reactive model, which allows users to make decisions at the relevant time rather than a priori. Participants frequently explained that the reason why someone wanted to access a file mattered in making policy. • Policies are also complex in other ways. Our findings indicate that many users' policy preferences are also complex in less dynamic ways. Some participants considered factors beyond the sensitivity of the information in question when making decisions. For example, a user denied a request from a friend for a Christmas photograph because "she doesn't celebrate Christmas and might be offended." Our study also showed that the reactive model supports many of our participants' policy creation needs, including the desire for more control and interactivity. Several of our participants found a request-based system appealing because they felt it provided added control over the dissemination of their files. This finding confirms that reactive policy creation continues to fit well into users' mental models after a week of simulated exposure to it. Six participants said they might use reactive policy creation to help them track who was accessing their files and when. Other participants liked that the reactive policy model incorporates the idea of requesting permission. Participants also said the reactive model helped them make better decisions; e. g., a user said the reactive model provides "more of an opportunity to really think about it." Re: Android App Scanner, Jason Hong reports: With the widespread adoption of smartphones, mobile apps have gained mainstream popularity. These apps can make use of a number of the smartphone's capabilities, including network access, data storage, personal data such as call logs and contacts list, and sensors detecting such things as motion, location, sound level, and so on. On the one hand, these capabilities allow developers to create rich and compelling applications. On the other hand, these same capabilities can also lead to new kinds of spyware, malware, and privacy intrusions, which we are just starting to see emerge. The potential risks are quite high, as smartphones become increasingly integrated with our lives, being able to access our email, social networking accounts, financial information, personal photos, and even our cars and homes. To address this problem, we are developing a system that combines automated analysis with crowdsourcing techniques to analyze and understand a mobile app's behavior and detect deviant behavior. We are also developing better user interfaces that can summarize these behaviors to individuals. So far, we have been able to instrument mobile applications to understand when they request location information, allowing us to know how often and at what granularity location information is gathered. We have also made some progress on deploying a virtual machine testbed for executing applications and doing this over a remote desktop connection, which is one possible path for crowdsourcing. Finally, we have mapped out several possible other ways of using crowdsourcing to analyze mobile applications.

Re: Bridging the Gap Between Systems Security and Language Security, Jonathan McCune reports: While millions of machines in enterprises have TPM chips installed in them, in most cases they are not enabled, and if enabled they are significantly underutilized. This work studies the challenges of automating the process of integrating Trusted Computing technologies and solutions into software during development. As first steps toward automation, we design a solution that builds a distributed application that utilizes Trusted Computing platforms from a simplified source language, with security annotations, that abstract most of the Trusted Computing details. The solution is built upon Cflow, a security-preserving compiler for distributed applications designed by Fournet et al., which produces an application with confidentiality, integrity, and control flow protection from a program written in a simplified typed-language with information flow policy enforcement. Our design, retaining all the security properties inherited from Cflow, adds much stronger confidentiality and integrity guarantees, that can also be remotely verified. Throughout the design process, we study the solutions and tradeoffs of several challenges that emerge when using Trusted Computing, without requiring an expert programmer, in a distributed application. In the current design, the developer still needs to identify which commands should be executed in a Trusted Environment. However, we present simple guidelines for correctly identifying these commands based on confidentiality and integrity policies at the source code level.

Re: Expanding Firewall Misconfiguration Detection based on Dynamic Routing Analysis for Large Networks, Hyong Kim reports: Our contributions are as follows: We include routing information in the model, allowing automatic discovery of possible routes and detection of misconfigurations in accordance with these routes. The routing information is directly obtained from the equipment's routing tables as they are at a certain point in time. With this information we can accurately detect connectivity and security issues that stem from the routing policies in place, and also have a realistic view of the routing state of the network. The application's testbed in a section of the network of a large European telecommunictaions provider. The section includes a total of 30 nodes (including Layer 3 switches, routers and firewalls from different vendors), with more than 350 rule sets and close to 12,000 ACL rules. We suggest a course of action for each detected misconfiguration, based on the data obtained from the static analysis performed over the filtering rules. Tracing the source of a failure: automatically determine which rule(s) caused a misconfiguration. For example: by pinpointing the origin of the misconfiguration, it is easier to automatically suggest a course of action for its correction. We offer a mechanism for testing a flow in order to determine whether it is able to cross the network, where it fails and why. We also generate an accurate diagram of the network topology being analyzed and provide the ability to quickly calculate and visualize real possible routes across the network. These features, more practical and operational in nature, are greatly appreciated by network operators in the field.

Re: Efficiently Securing Non-Volatile Storage in Portable Systems, Ken Mai reports: We have designed and implemented in Silicon ROM-based S-Box designs that show significantly improved area, power, and delay over synthesized logic versions. Additionally, side-channel secured versions of the ROM-based S-Box show side-channel leakage equivalent to secure logic

families (e.g., WDDL) at much lower area, power, and delay. Simulation results were published in the IEEE International Symposium on Hardware-Oriented Security and Trust in June 2010. The testchip was fabricated in a commercial 65nm bulk CMOS process and contains a stand-alone ROM-based S-Box, a synthesized AES encryption core using ROM-based S-Boxes, and a synthesized AES encryption core using standard logic S-Boxes (for comparison). Measured results show that the ROM S-Box can operate at up to 2GHz (at 1.25V Vdd) and is able to dissipate under 5pJ per 8b substituion (at 0.8V Vdd). The ROM AES encryption core shows improved power and performance over the standard core at approximately equivalent area. We have designed and implemented in Silicon a sense amplifier based physical unclonable function (PUF) that demonstrates high randomness, uniqueness, and reliability, as well as low power, area, and delay. Simulation results were published in the IEEE International Symposium on Hardware-Oriented Security and Trust in June 2010. The testchip was fabricated in a commercial 65nm bulk CMOS process and contains arbiter, ring oscillator, SRAM, and sense amplifier PUFs. All PUFs are fully functions and being tested for randomness, uniqueness, and reliability across voltage and temperature. We have designed and implemented in Silicon a SRAM and DRAM test structure to measure memory retention time and remanence effects. With the measured results from the testchip we plan on determining the amount of time data is retained in SRAM and DRAM structures after power down, and the precise nature of permanent data remanence effects in SRAM and DRAM structures in a modern IC fabrication technology. The testchip was fabricated in a commercial 65nm bulk CMOS process and contains two 16kb SRAMs and one 16kb DRAM (3T cells) instrumented to provide retention time and remanence data. We have tested the retention time at room temperature and are proceeding to test at different temperatures before proceeding with remanence testing (which will permanently alter the testchip samples, and thus must be performed last).

Re: Super-Resolution for Iris Recognition, V. Bhagavatula reports: Recognition of iris images captured under challenging conditions is error-prone since standard iris recognition algorithms require segmentation of the iris region from the rest of the eye image. However the images captured under challenging conditions are usually of poor quality suffering from low resolution. Standard iris recognition algorithms fail in this case (segmentation being the main failure mode), but we would still like to identify subjects under such conditions. In this effort, we developed and investigated a Super-Resolution (SR) algorithm on low-resolution iris images. Algorithm: Given the set of high-resolution gallery and low-resolution probe images, we extract features from both the high and low resolution images. In these experiments we use the Fisher features on principal components analysis (PCA) coefficients. During the testing phase given the low-resolution image y, we solve the following optimization problem using features from each class. The three residues (i.e., the three L2 norms below) are then used to determine the class to which the given low-resolution image belongs. In the equation above, B denotes the blurring operator, x is the super-resolved image, k is the claimed identity of the subject, L is an operator measuring the non-smoothness of the reconstruction, F is the operator for extracting the features and fk denotes the features computed from training images of the k-th subject (i.e., the claimed identity). Database: We applied the super-resolution algorithm on images obtained from the Iris Challenge Evaluation (ICE) database i.e., ICE Left with 84 classes and 1434 images and ICE Right with 85 classes and 1266 images. The ICE database has high resolution imagery (640x480). Experiments: We now describe the experiments that we conducted on images generated from the ICE database. Since the super-resolution algorithm requires the images to be registered, we applied a simple eye-detector to first locate the center of the eye and register the images. Several experiments were conducted. But we describe one experiment here that illustrates the benefit of our SR algorithm. In this experiment, we generated images of resolution 64x48 in which the iris is about 25 pixels across. These 64x48 images represent the high-resolution (HR) gallery images from which we artificially generate low-resolution (LR) images of size 32x24 with the iris being 13 pixels across. The images are cropped to 26x26 for the high-resolution and 13x13 for the low-resolution. Figure below shows examples of some of the HR gallery and LR probe images used. Top Row: Three 26x26 HR gallery images. Bottom Row: Three 13x13 LR probe images. The rank-1 IDAs for HR probe images matched against HR gallery images was 91.1% whereas it degraded to 75.2% when LR probe images were matched against HR probe images. By using our super-resolution algorithm, we were able to improve the rank-1 IDA to 88.4% when matching LR probe images against HR gallery images. Next Steps: We are currently investigating methods to improve the speed of super-resolution for iris recognition. Current method requires an optimization effort for each probe image and this can be time-consuming. We are looking at using subspace projection methods that will map HR and LR images to a common subspace where they can be compared. As this method avoids the optimization step, it can be computationally more attractive.

Re: Attacking and Defending Unreliable Hardware, Onur Mutlu reports: We have developed new mechanisms to defend attacks that appear due to unreliable and unfair design of hardware resources in future multi-core systems. We have especially focused on preventing unforeseen consequences of the security and robustness-unaware design of: - emerging memory technologies, such as Phase Change Memory and STT-RAM - memory controllers and on-chip interconnection networks - deep submicron technologies that are vulnerable to hard faults We have also demonstrated denial of service attacks that exploit algorithmic vulnerabilities in multiple thread management in parallel applications in multi-core systems and due to memory errors in new memory technologies (phase change memory). The following two submissions deal with how to prevent these attacks and can be obtained by emailing me. Eiman Ebrahimi, Rustam Miftakhutdinov, Chang Joo Lee, Onur Mutlu, Chris Fallin, Yale N. Patt, “Managing Inter-thread Memory System Interference for Parallel Applications,” submitted to MICRO, under review since July 2011. HanBin Yoon, Justin Meza, Rachata Ausavarungnirun, Rachael Harding, Onur Mutlu, “Row Buffer Locality-Aware Data Placement in Hybrid Memories,” submitted to MICRO, under review since July 2011. Several key improvements are briefly described below: Thread Cluster Memory Scheduling for Fair Memory Performance in Many-Core Systems (MICRO 2010): MEMORY SCHEDULERS IN MULTICORE SYSTEMS SHOULD CAREFULLY SCHEDULE MEMORY REQUESTS FROM DIFFERENT THREADS TO ENSURE HIGH SYSTEM PERFORMANCE AND FAIR, FAST PROGRESS OF EACH THREAD.

NO EXISTING MEMORY SCHEDULER PROVIDES BOTH THE HIGHEST SYSTEM PERFORMANCE AND HIGHEST FAIRNESS. THREAD CLUSTER MEMORY SCHEDULING IS A NEW ALGORITHM THAT ACHIEVES THE BEST OF BOTH WORLDS BY DIFFERENTIATING LATENCY-SENSITIVE THREADS FROM BANDWIDTH-SENSITIVE ONES AND EMPLOYING DIFFERENT SCHEDULING POLICIES FOR EACH. Slack based Packet Routing for Fair Interconnect Performance in Many-Core Systems (ISCA 2010): A TRADITIONAL NETWORK-ON-CHIP (NOC) EMPLOYS SIMPLE ARBITRATION STRATEGIES, SUCH AS ROUND ROBIN OR OLDEST FIRST, WHICH TREAT PACKETS EQUALLY REGARDLESS OF THE SOURCE APPLICATIONS' CHARACTERISTICS. THIS IS SUBOPTIMAL BECAUSE PACKETS CAN HAVE DIFFERENT EFFECTS ON SYSTEM PERFORMANCE. WE DEFINE SLACK AS A KEY MEASURE FOR CHARACTERIZING A PACKET'S RELATIVE IMPORTANCE. AE´RGIA INTRODUCES NEW ROUTER PRIORITIZATION POLICIES THAT EXPLOIT INTERFERING PACKETS' AVAILABLE SLACK TO IMPROVE OVERALL SYSTEM PERFORMANCE AND FAIRNESS. Online self test to prevent exploitation of hardware errors (VTS 2010): Concurrent autonomous self-test, or online self-test, allows a system to test itself, concurrently during normal operation, with no system downtime visible to the end-user. Online self-test is important for overcoming major reliability challenges such as early-life failures and circuit aging in future System-on-Chips (SoCs). To ensure required levels of overall reliability of SoCs, it is essential to apply online self-test to uncore components, e.g., cache controllers, DRAM controllers, and I/O controllers, in addition to processor cores. This is because uncore components can account for a significant portion of the overall logic area of a multi-core SoC. In this paper, we present an efficient online self-test technique for uncore components in SoCs. We achieve extremely high test coverage by storing high-quality test patterns in off-chip non-volatile storage. However, a simple technique that stalls the uncore-component-under-test can result in significant system performance degradation or even visible system unresponsiveness. Our new techniques overcome these challenges and enable cost-effective online self-test of uncore components through three special hardware features: 1. resource reallocation and sharing (RRS); 2. no-performance-impact testing; and, 3. smart backups. Implementation of online self-test for uncore components of the open-source OpenSPARC T2 multi-core SoC, using a combination of these three techniques, achieve high test coverage at < 1% area impact, < 1% power impact, and < 3% system-level performance impact. These results demonstrate the effectiveness and practicality of our techniques. Enabling service guarantees in on-chip-network based multi-cores cost-efficiently (ISCA 2011): Today's chip-level multiprocessors (CMPs) feature up to a hundred discrete cores, and with increasing levels of integration, CMPs with hundreds of cores, cache tiles, and specialized accelerators are anticipated in the near future. In this paper, we propose and evaluate technologies to enable networks-on-chip (NOCs) to support a thousand connected components (Kilo-NOC) with high area and energy efficiency, good performance, and strong quality-of-service (QOS) guarantees. Our analysis shows that QOS support burdens the network with high area and energy costs. In response, we propose a new lightweight topology-aware QOS architecture that provides service guarantees for applications such as consolidated servers on CMPs and real-time SOCs. Unlike prior NOC quality-of-service proposals, which require QOS support at every network node, our scheme restricts the extent of hardware support to portions of the die, reducing router complexity in the rest of the chip. We further improve network area- and energy-efficiency through a novel flow control mechanism that enables a single-network, low-cost elastic buffer implementation. Together, these techniques yield a heterogeneous Kilo-NOC architecture that consumes 45% less area and 29% less power than a state-of-the-art QOSenabled NOC without these features. Providing fair performance in the presence of prefetching in future many-core systems (ISCA 2011): Chip multiprocessors (CMPs) share a large portion of the memory subsystem among multiple cores. Recent proposals have addressed high-performance and fair management of these shared resources; however, none of them take into account prefetch requests. Without prefetching, significant performance is lost, which is why existing systems prefetch. By not taking into account prefetch requests, recent shared-resource management proposals often significantly degrade both performance and fairness, rather than improve them in the presence of prefetching. This paper is the first to propose mechanisms that both manage the shared resources of a multi-core chip to obtain highperformance and fairness, and also exploit prefetching. We apply our proposed mechanisms to two resource-based management techniques for memory scheduling and one source-throttling-based management technique for the entire shared memory system. We show that our mechanisms improve the performance of a 4-core system that uses network fair queuing, parallelism-aware batch scheduling, and fairness via source throttling by 11.0%, 10.9%, and 11.3% respectively, while also significantly improving fairness.

Re: Security Patters: Assurance for Secure Concurrent and Distributed Computing, Jonathan Aldrich and William Scherlis reports: Proved the soundness of our CyLab-funded architecture assurance technology, and carried out a case study applying the tool to verify secure information flow and find seeded defects in an application of moderate size. Carried out experiments with typestate verification at scale, and explored a wider application of the technology in the context of a novel programming language with a permission-based type system. Developed and published a new technique for assuring compliance with complex, security-relevant framework constraints.

Re: Robust, Secure, Efficient Cyber-Physical Systems, Bruno Sinopli reports: As sensing, computing and communication capabilities become increasingly faster and cheaper, they will be embedded in interconnected devices placed in complex physical environments. Applications with enormous societal impact and economic benefit will harness these capabilities, changing the way humans interact with the physical world. My research addresses the joint modeling, analysis and design of Cyber-Physical Systems (CPS), large-scale physical systems that employ a networking and computing infrastructure for monitoring and control, with particular focus on energy efficiency, robustness and security. In these areas my research group has made fundamental contributions and opened new research directions. Cyber-Physical Systems raise significant engineering challenges because of their scale, their need to bridge the physical, information and communication technology

domains and their need to operate efficiently, securely and reliably. The close interplay among these fields renders independent design of the control, communication, and computing subsystems a risky approach, as separation of concerns does not constitute a realistic assumption in real world scenarios. It is therefore imperative to derive new models and methodologies to allow analysis and design of robust and secure CPS. A major thrust of my research aims at developing the theoretical foundations of cyber-physical systems by looking at the tight coupling between the available information and communication technologies (ICT) and the physical systems in which these technologies are embedded. The application perspective is fundamental to my approach, as it provides invaluable insights to help discern the relevant from the superfluous, the impactful from the sterile. I am focusing on smart power grids and server farms. In my research I propose to develop analytical and computational techniques in the following directions: Networked Control Systems. This research focuses on control and estimation problems where sensor and actuator signals are transmitted to various subsystems over a network. In contrast to traditional control and estimation problems, here the observation and control packets may be lost or delayed. The unreliability of the underlying communication network is modeled stochastically by assigning probabilities to the successful transmission of packets. This requires a novel approach to generalize classical control/estimation paradigms. In “Kalman Filtering with Intermittent Observations¿” (IEEE TAC 2004), I proposed a linear system model that ¿takes into account sensor packet loss and I investigated the performance of the Kalman Filter, proving the existence of a critical packet arrival probability below which the average error covariance of the filter goes unbounded for unstable processes. The model has been widely adopted and results extended in several directions by the control community. In “Kalman Filtering with Intermittent Observations: Weak Convergence to a Stationary Distribution” (IEEE TAC, in press) we use Random Dynamical Systems theory to show that for arrival rates above the critical one, not only the mean is bounded, but also the error covariance of the estimation error converges in distribution. Using Ergodicity we can empirically approximate the asymptotic distribution, thus providing important practical insights. In “Kalman Filtering with Intermittent Observations: Tail Distribution and Critical Value” (IEEE TAC, in press) we show that the trace of the Kalman estimation error covariance under intermittent observations follows a power decay law. Moreover we are able to compute the exact decay rate for non-degenerate systems. Finally we derive the critical value for non-degenerate systems based on the decay rate. In “LQG Control For Distributed Systems Over TCP-like Erasure Channels (IEEE TAC, in press) we extend the results in “Foundations of Control and Estimation over Lossy Networks” (Proceedings of the IEEE, 2007) to the multi channel case. Sensor Scheduling for Networked Estimation and Detection. The ability to parse the potentially enormous amount of data is a key requirement for large scale CPS. Sensor Networks will often rely on battery power to operate. In order to guarantee long lifetime and low maintenance costs, sensors need to sense and communicate frugally to save energy. In the context of state estimation and event detection my research group has extensively investigated the problem of dynamically selecting a subset of the available sensors to save energy while satisfying the design specification on estimation error and detection probability. In “Sensor Selection for Event Detection in Wireless Sensor Networks” (IEEE TSP, Oct ‘11) we address the problem of selecting the subset of sensors that achieve the best detection performance. In “Sensor Selection Strategies for State Estimation in Energy Constrained Wireless Sensor Networks” (Automatica, July ‘11), and “Stochastic Sensor Scheduling and Topology Control for Energy Constrained Estimation in Multi-Hop Wireless Sensor Networks” (IEEE TAC, in press) we address the problem of sensor selection for estimation over sensor networks, where we consider both deterministic and stochastic approaches and several configurations from star topologies to arbitrary meshes. Cyber-Physical Modeling and Control of Data Centers. The growth in scale and number of data centers is raising concerns about their power consumption. Through an NSF GOALI Bruce Krogh and I have investigated the problem by developing a CPS model of a data center, which couples the computational dynamics, i.e. the network of workload queues, with the ones describing the temperature evolution at the servers. We designed a hierarchical control that jointly provides inputs to the cooling system (Physical) and to the networks of servers (Cyber). The approach is summarized in “Cyber-Physical-System Approach to Data Center Modeling and Control for Energy Efficiency” (IEEE Proc., special issue on Cyber-Physical Systems, in press). Security of Cyber-Physical Systems. The increasing use of open networking allows malicious agents to execute attacks on CPS remotely. Next generation infrastructures like the smart grid, intelligent buildings and transportation systems will be particularly susceptible to security threats if this concern is not addressed at design time. CPS have to be able to detect malicious attacks and guarantee continuity of operations through graceful rather than abrupt degradation. They also need to be able to reconfigure to eradicate attacks and restore full functionality. In order to achieve this goal I propose to combine system theory and cyber security to ultimately build a science of cyber-physical security. Toward this goal, I have developed cyber-physical security models capable of integrating dynamic systems and threat models within a unified framework. I believe that cyber-physical security will not only address problems that cannot be currently solved but provide new improved solutions for detection, response, reconfiguration, and restoration of system functionalities while keeping the system operating. My research group is strongly committed to it. In “Secure Control against Replay Attack” (Allerton Conference 2009), we predated the strategy then used by Stuxnet and provided a countermeasure based on the concept of physical authentication. In “False Data Injection Attacks in Control Systems” (Workshop on Secure Control Systems, CPS Week, April 2010) and “False data injection attacks against state estimation in wireless sensor networks” (IEEE CDC 2010) we analyze the effect on stealthy integrity attacks on sensors, providing results on the resilience of a linear control system to such attacks. In “Malicious Data Attacks in Power Market Operations” (IEEE Transactions on Smart Grid, in press) we show how an attacker can affect to his advantage the real time nodal pricing via virtually undetectable integrity attack on power flow measurements. In “Intrusion Detection in Distributed Control Systems” (IEEE CDC 2010) we provide insights on the detectability of integrity attacks on local controllers as a function of the communication topology.

Re: Adaptive Strategies for Cross-Layer Jamming and Anti-Jamming, Patrick Tague reports: The following describes our research progress over the past year while funded by CyLab using ARO funds. Our research comprises the following three

projects: 1. Adaptive jamming attacks based on event observation and inference, 2. Dynamic anti-jamming techniques using performance-based inference, 3. Modeling interactions between jamming attackers and defenders. In project 1, we have established a preliminary model for adaptive jamming attacks by modeling the interplay between the attacker and target communication link as a feedback control system. We implemented a proof-of-concept jamming attacker that can observe the impact of its own attacks, adapt its attack parameters, and quickly converge to a highly efficient state with no prior knowledge of specific parameters used by the communicating parties (e.g., topology, transmit power, etc.). We are now making significant efforts to generalize and broaden the scope of the model and develop additional capabilities needed to fully understand such attacks. Preliminary versions of submitted and in-progress papers and technical reports can be made available upon request. We also have a working demo (live or video) of the current implementation that can be made available. In project 2, we have demonstrated that sub-channel filtering in software radios can be used to remove narrow-band jamming signals at a receiver in the case of highly-efficient jamming attacks that minimize the attack energy by using jamming signals that use narrower bandwidth than the target signal. We implemented a simple proof-of-concept with a fixed sub-channel filter tuned to the center frequency of the channel, assuming that this is where the jammer is tuned. We are currently developing an adaptive technique that attempts to find the jamming signal by observing performance statistics and cycling through several candidate frequencies. This technique thus provides an all-signal-processing approach to detect and mitigate highly efficient, narrow-band jamming attacks. A preliminary version of this anti-jamming capability appeared at the IEEE ICCCN 2011 conference, and preliminary versions of in-progress papers and technical reports can be made available upon request. We also have a working demo (live or video) of the current implementation that can be made available. In project 3, we are working to establish a model to capture interactive behaviors between attacking and defending teams using multi-agent systems. We are incorporating aspects of game theory, control system theory, and probabilistic methods in order to characterize features such as stability, convergence, oscillation, etc.

Re: Probablistic Verification of Security Properties in Self-Adaptive Systems, David Garlan reports: Demonstrated the feasibility of applying probabilistic model checking to the problem of determining whether a system is vulnerable to security attack scenarios based on their representation as “attack graphs’. Showed that the Prism model checker can be used to effectively evaluate the likelihood of an attack succeeding given estimates about the likely behavior of various components in the system and countermeasures (such as intrusion detection systems). Key contributions are efficient encodings of architectural structures in Prism, and automated translation of attack graphs to properties that can be checked over those structures. Demonstrated that formal software architecture models can be used to effectively analyze a system for violation of information flow policies using a combination of architecture and code-based analysis techniques. Developed a tool that can analyze service-oriented architecture workflows to detect patterns representing potential privacy policy violations. Integrated this tool into a ONR-funded platform used by intelligence analysts.

Re: Security Issues in Information Naming, Srinivasan Seshan: Over the past year, we have been developing the concept of information bound references (IBRs). The motivation for IBRs is that while publishing multimedia content on the Web has become simple, the URLs we use to reference this content are fragile because of their tight coupling to specific protocols, hosts and filenames. Past efforts have made important advances toward mak- ing content references more robust by allowing users to fetch content from anywhere using any transfer protocol (e.g., se- mantic free references, DOT and DONA). Unfortunately, they don't go far enough, especially for multimedia content. The key observation that allows us to push the design space further is that human users are often the final consumers of content. Users primarily wish that the content they retrieve and view matches the information conveyed by the referenced link. Here, “information” refers to a perceptual entity that is invariant across different presentation formats, encodings, resolutions, etc. of an object. In contrast, “data” refers to information coupled with a specific presentation format. Thus, we argue that multimedia references should be bound directly to the information and not to details such as protocols, hosts, filenames, or data: instead of using URLs like www.foo.com/video.mpg that tightly couple both the location (i.e.,foo.com) and the content format (i.e., mpg), we believe that references should be based on what the video actually contains. We call such references Information-Bound References (IBR). The key challenge that we have been addressing over this past year is the generation of robust IBRs. To ensure contention-freeness, IBRs must be algorithmically generated from the content (as opposed to say human-input labels such as “Charlie bit my finger”. The main challenge is to ensure that they are presentation invariant and bound to the information. Because the data-level representations of different variants of the same content could be vastly different, this requires a new way to think about naming content that is significantly different from data-centric architectures. Our insight is that it is possible to borrow from the literature on fingerprinting algorithms used for similarity identification in image and video processing. We have found suitable algorithms that can generate the fingerprints that satisfy the above requirements to serve as IBRs. One concern, however, is that the fingerprinting algorithms may not be robust to determined attackers who craft malicious or inappropriate content. To alleviate this concern, we have developed mechanisms that content providers and/or consumers can employ to provide additional integrity checks. Specifically, we have designed hierarchical IBRs in which small-sized IBRs are used for lookup and longer IBRs are used for integrity checks. We have also developed a human-assisted reputation system that leverages reCaptcha-like techniques to identify content the erroneously matches an IBR.

Re: Accountable Mobile Computing Framework Based on User Behavior Modeling, Joy Zhang reports: We have demonstrated the feasibility of using mobile sensors to build users’ behavior model for casual authentication and anomaly detection. In particular, we have been using accelerometer readings to identify user’s activity, accelerometer/gyroscope/magnetometer to identify user’s indoor location, and using WiFi access points’ RSS signature to derive users’ pseudo location trace. We have

developed a novel “behavior text” representation to discretize sensor readings and convert them to symbols. The behavior text representation enables us to reuse all algorithms developed for statistical natural language processing to process sensor readings, including information retrieval, classification, summarization, novelty detection etc. We are developing a novel unsupervised grammar induction algorithm called HELIX to derive the underlying grammar of human activity. With the learned grammar, we are able to derive the high-level meaning of human activities which in turn, helps to build up the behavior model for casual authentication and other security applications.

Re: Secure Distributed Logic Programming, Frank Pfenning reports: We developed a compilation technique for distributed logic programs from high level specifications, speaking about the knowledge of the principles, to distributed implementation following certain communications protocols to exchange this knowledge. The principal theoretical advance was to formalize this compilation and to prove several versions correct. The STM’11 publication describes a significant experimentally evaluated case study, but is not yet connected to the new theoretical underpinnings. Building this connection is planned for the coming year.

Re: Semantic Geotagging for Situational Awareness During Disaster Response, Ray Bareiss reports: We developed a robust prototype of an Android-based hypermedia application for collaboratively constructing situational awareness in the event of a disaster. As noted above, the system has also been integrated with the Golden Gate Safety Network’s common operating picture software as well as a standalone web map-based interface. We conducted usability tests with firefighters and are revising the interface in accordance with the results. We have also developed an extensive roadmap for future work.

Re: Efficient Trojan Detection in Field Programmable Gate Arrays, Shawn Blanton reports: Globalization of the semiconductor industry has raised new concerns regarding the integrity of integrated circuits (ICs). The concern is that an adversary can maliciously introduce a design alteration (typically referred to as a Trojan) that compromises IC operation while remaining undetected. A well-accepted model of a Trojan consists of two major circuit components, a trigger and a payload. The trigger captures the activation conditions of the Trojan, and is likely controlled by design signals in close proximity to the trigger circuitry. The other part of the Trojan, the payload, performs the malicious action. It is assumed that an adversary would choose infrequent but guaranteed-to-occur conditions for the trigger in order to avoid detection by manufacturing test. Extrapolation of conventional testing techniques therefore would be of little use in detecting Trojans. Detection is possible however by using side-channel signals to detect Trojan circuitry. For this approach to work however, it is essential to differentiate the noise in a side-channel measurement due to manufacturing variations, and the additional disturbance resulting from the presence of an actual Trojan. The integrity of field-programmable gate arrays (FPGAs) has received special attention recently due to their use in critical applications involving communication, health, defense, security, etc. Trojan detection in an FPGA poses unique problems due to its reconfigurable characteristics. But this inherent property of FPGAs can also be exploited to perform side-channel detection of a Trojan. In this project, a Trojan, via FPGA configuration, is included in an arbiter circuit (Fig. 1) in order to detect its presence. The Trojan is revealed by detecting the path-delay increase caused by its payload. Trojan detection is limited however by the inherent and varying delay of FPGA routing and the circuitry of the arbiter. In Fig. 2, the detectable Trojan delay, in terms of double-line delay, is reported for an actual Spartan-3 FPGA. Current work is focused on ensuring that every possible Trojan location is efficiently tested using the minimum number of FPGA configurations as well as statistically characterizing the detection capability of the arbiter. This is a novel, and cost-effective approach for detecting Trojans within FPGAs. It is a technique that all end customers (military, commercial, etc.) can easily employ to ensure that the FPGAs used in critical systems are free from malicious tampering. Also, unlike many other approaches, this technique has been demonstrated using real hardware (Figure 2). Fig. 1: Trojan detection circuit that uses a configured SR-latch as an arbiter. Fig 2: Trojan detection resolution for a Digilent Spartan-3 FPGA. Most Trojans that impose delay greater than 6 double lines can be detected using the SR-latch arbiter; others must impose a delay greater than 8 double lines.

Re: Differentially-Private Synthetic Dataset Release for Machine Learning and Clustering, Avril Blum reports: This project has focused on the two related problems of (a) how to release privacy-preserving “sanitized” information about a social network or data set that can still be useful for analysis, and (b) how to design data-analysis algorithms that can best use such noisy information. Problem (a) is especially difficult because certain networks have the property that one provably cannot release accurate information while satisfying the demanding requirements of the gold-standard differential privacy definition. Thus, progress here has been on developing methods that will allow for releasing information that will be accurate in typical cases, while preserving privacy in all instances. Progress on (b) has been on development of new clustering algorithms that are especially suited to “stable” networks and datasets, which are the kind of cases for which more accurate information can in principle be released.

Re: A Static Approach to Operating System Security IV, Karl Crary reports: We have designed the interface for the runtime layer (including, especially, a garbage collector) of an operating system based on static checking. We also devised the necessary algorithms to implement the layer. This required new advances in low-level memory management as existing parallel, concurrent, real-time garbage collection algorithms do not support uncooperative threads.

Re: Data Confidentiality, Privacy, and Security, Stephen Fienberg reports: We have made major progress on three different aspects of work on data confidentiality and privacy protection. (1) Through collaborations with colleagues as other institutions, such as Microsoft Research, Pennsylvania University, Microsoft Research, and now the Technion and the University of Haifa in

Israel,

Avrim Blum: This project has been focused on the following problem: how to publish a "sanitized version" of a sensitive social network in a way that both (a) preserves privacy and yet (b) still resembles the original network in important ways. Or, barring that, what are good ways of at least answering individual queries that researchers may have about such a network in ways that preserve both privacy and utility? To date, we have made progress in both directions, using the challenging and appealing criterion of "differential privacy". In the first direction, we have developed an algorithm that given as input a "sensitive" graph G, publishes a sanitized (weighted) graph G' that resembles the original in the sense of approximately preserving cut-queries. That is, suppose you have a collection of sets of nodes you are interested in: S_1, S_2, ..., and you want to know how many edges there are between each S_i and its complement V - S_i. Then with high probability, G' will give approximately the same answer as G does for all these queries. Furthermore, the notion of "approximately" is better than achieved by previous approaches to this problem. One caveat (of this work and also previous work on this problem): the notion of differential privacy here is with respect to single edge changes. That is, a person (node) can hide any single friendship link, but he couldn't necessarily pretend to be friends with everyone if really he's friends with no-one (i.e., an adversary with prior knowledge that one of the two events is true might be able to distinguish those cases since they differ in n-1 edges). This work recently appeared in the IEEE FOCS 2012 conference. In the second direction, we have developed algorithmic techniques for interactively answering questions about local structures in a social network (such as "how many people know at least two doctors"?) One of the key challenges here is that these kinds of questions can have very high sensitivity in some networks (e. g., if some celebrity is known by many people and decides to change her hair color, then the answer to "how many people know someone who has green hair?" might change a lot). Our approach is to allow the querier to posit a hypothesis about the structure of the network (e.g., perhaps that no node has more than k links) and then the system will guarantee that if indeed the graph satisfies this condition, then the answer given will be close to the truth (but the system cannot confirm or deny if the hypothesis is actually true). This work was just accepted to the ITCS 2013 conference.

Fienberg: We completed a series of papers on the uses of differential privacy for protecting the privacy of statistical databases, and on the use of secure multiparty computation for jointly carrying out regression and logistic regression analyses.

Pfenning: Developed proof theory and semantics to reason about security properties of distributed systems specified using advanced logical formalisms and type theory.

Joy Ying Zhang: Significant achievements have been made in 2012 on mobile sensing and its implication on security. We have investigated the impacts of mobile sensing on security from two directions: 1) how does mobile sensing reveals users' private information such as his/her location (without GPS) and the password the user is typing on the mobile device. These findings (Han et al., 2012, Owusu et al., 2012) lead us to argue that there are huge risks on smart phones if sensors are activated without users' knowledge. 2) we leverage the mobile sensing to build users' behavior model and proposed the idea of using behavior-metric to authenticate the user in a passive manner. This work (Zhu et al., 2012) has led to the development of a the research software called CMU SenSec that is now available on Android Market. We have studied how different sensor modalities and their combinations best identify a user and compared the effectiveness vs. response time.

Christin: Provided the first (and only, to date) comprehensive technical and economic measurement analysis of the online anonymous market "Silk Road." The resulting technical report has been extensively covered in the press (Forbes, The Economist, …). A revised version is in preparation for submission. Proposed metrics to quantify the level of ISP "badness."

Tague: The following describes our research progress over the past year while funded by CyLab using ARO funds. Our research comprises the following three tasks:
Adaptive jamming attacks based on event observation and inference,
Dynamic anti-jamming techniques using performance-based inference,
Modeling interactions between jamming attackers and defenders.
Task 1 was the primary focus of the previous year of the project, but we elaborated on the prior results and published a paper in MASS 2012 on an adaptive jamming attack model. In this attack, the jammer observes interactions between a wireless transmitter and receiver and modifies a set of signal parameters in response, similar to a feedback control system. We consider an attacker not only interested in the impact of the attack on the target system, but also in the amount of energy required to mount the attack and the potential for attack detection. As such, the attacker can specify a set of requirements (e.g., bounds on energy efficiency or probability of detection) that feed into an optimization problem to determine signal parameters. The feedback provided by observing the target system under attack provides the basis for characterization of the effect of the attack, so the attacker does not need a precise physical layer model. In fact, in our results, we showed that the feedback provides the valuable capability for the attacker to fit a seemingly weak system model to the observed performance. We implemented the adaptive jamming attack both as a software package in MATLAB Simulink and as a GNURadio module for use in USRP2 software-defined radios. A working demo (live or video) of the current implementation can be made available upon request.
Task 2 was also a major focus of the previous year of the project, and we vastly elaborated the prior capabilities and published a paper in PECCS 2012 on an adaptive filtering technique to detect and eliminate the effect of a certain form of narrow-band jamming in a direct-sequence spread spectrum communication system. In our previous work (ICCCN 2011), we showed that relatively simple digital filters could be used to isolate and eliminate the jamming signal, but the approach only worked if the

receiving radio knew of the existence of and parameters for the jamming signal. Our expanded work included a learning and feedback model that allows the radio to find the signal and take action. Upon sensing a sub-standard level of performance (for example, when the packet decoding rate falls below a predetermined threshold), the radio can initialize a search by partitioning the channel bandwidth into sub-bands and testing the resulting performance with a digital filter eliminating each sub-band in turn. If a particular sub-band filter yields a significant boost in performance (e.g., returning the packet decoding rate above the threshold), then the radio has successfully mitigated the narrow-band jamming attack. Because this detection and mitigation strategy is triggered based on performance, it can also adapt to changes in the attacker's strategy. For example, if the attacker moves the jamming signal randomly in the frequency domain, the responsive sub-band filtering technique will activate whenever the jamming signal moves away from the currently-filtered sub-band. However, the limitation of this work is that the responsive adaptive filtering technique is only effective if the attacker changes frequency slower than the interference signal can be detected and mitigated. We implemented the adaptive jamming attack as a GNURadio module for use in USRP2 software-defined radios. A working demo (live or video) of the current implementation can be made available upon request.
Our primary focus of this academic year has been on Task 3, studying the interactions between adaptive jamming attackers and adaptive anti-jamming defenders. We have developed a preliminary game-theoretic model with a learning aspect to describe the interactions at a high level, and the result was published at D-SPAN 2012. In the model, each player in the game (whether attacker or defender) observes its opponent and builds knowledge about the system, the effects of different parameter choices, and what strategies its opponents may be using. Based on the collected knowledge (and the level of uncertainty therein), the player decides on a particular strategy, which may include the type of attack of defense to use as well as a collection of corresponding parameters. While we have yet to characterize important qualities such as convergence or stability, we have observed the emergence of interesting (and quite unexpected) behaviors. For example, in one implementation, the jammer would eventually reach a point where the strategy with the highest payoff was to not attack, meaning that the defender found a strategy that effectively disincentivized the attack. Our current implementation is based on the GNURadio implementations of the attack and defense models in Tasks 1 and 2, but both are enhanced to include the necessary inference capabilities. A working demo of the interactive attack-defense game can also be made available upon request.
This project has now been awarded funding from NSF, so we are continuing our work on all of the above Tasks. We are working in parallel on the theoretical foundations of the work as well as the implementation details, to ensure that the directions taken on the theoretical side remain well-informed by practical limitations that we encounter.

Bauer, Cranor, Ganger (Home Storage): As a result of the study that we conducted on tag-based policies, we fund the following:
Tags created for organizational purposes (e.g., to make files easier to find or to remind users of their content) can be re-purposed to create efficient and reasonably accurate access-control rules. In our experiment, even a first iteration of expressing policy through tag-based rules achieved 95+% accuracy. Users who tag content with access control in mind develop coherent strategies that led to tag-based rules becoming significantly more accurate then when using organizational tags alone. Participants can easily understand and actively engage with the concept of tag-based access control.Given a few example policies for specific files, machine-learning algorithms can automatically create rules that closely match a user's policy preferences.
Cumulatively, these findings imply that tag-based rules are a promising approach for conveniently and effectively specifying access-control policy, and that machine learning could be used to enable users to specify policy without requiring them to manually specify the rules that describe their policy. A paper describing these findings was presented at ACM CHI in May 2012. In our work on device-to-device exchange protocols, we found the following:The popular Bump protocol is vulnerable to even unsophisticated attackers. We showed that an attacker who controls the WiFi or mobile access point to which a phone is connected can easily launch a man-in-the-middle attack on Bump. Under some circumstances, the attack will succeed 75% of the time.We developed a secure device-to-device exchange protocol in which two devices exchange information via a third-party server (as with Bump) and authenticate the information by transmitting a digital signature via the vibrator-to-accelerometer channel (one phone vibrates to send; the other uses its accelerometer to sense vibrations). We showed that this new protocol has similar usability properties to Bump, but guarantees that even a powerful attacker cannot mount a successful man-in-the-middle attack.These findings were described in a paper published at ACSAC in December 2011.

(Bauer, Grey): Our work year adds to the body of research on Android security in two main ways: first, by developing a formal framework for analyzing Android-style security mechanisms, including defining properties desired of those, and verifying whether these properties hold; and, second, by designing and implementing an enforcement system that provides application developers with simple language constructs to specify flexible secrecy and integrity policies, and provably exhibits desirable security properties. To remain practically relevant, we constrain our enforcement system, which we call Sorbet, to be easily retrofittable into Android's current architecture. The design and implementation of Sorbet improves existing Android permission system in the following aspects: (1) we formally state the properties that we wish our new mechanisms to achieve, and formally prove that our system design supports them; (2) we enhance Android's permission system to support coarse-grained secrecy and integrity policies; and (3) we provide more flexible support for fine-grained and scope-limited delegation of permissions.
Formal analysis: One of our main goals was to improve our understanding of the security properties that we desire of Android-like permission systems, and to verify that specific systems are capable of specifying and enforcing desired properties. We pursue this goal by building a generalized, abstract model of the Android permission system, and stating a set of desirable properties in terms of the model. We then develop instantiations of this model both for the current Android permission system and for Sorbet. Based on this formal account, we study the properties of the current system; our investigation reveals both

design and implementation flaws, which guide the design of Sorbet. We also prove that Sorbet's design is sufficient to support the properties that we have defined.Coarse-grained secrecy and integrity policies: Sorbet's key innovation is coarse-grained mechanisms that allow developers to protect their applications against privilege escalation and undesired information flows. Android's permission system only prevents applications that do not have the correct permissions from directly calling a protected component. This is inadequate to protect against a malicious application that reaches a protected component indirectly, via a chain of calls to innocent applications. To protect against such attacks, we enrich Android's permission system with the ability to specify information-flow constraints and explicit declassification permissions, and implement a light-weight calling-context tracking and checking mechanism. A key challenge here was to support *local* specification of *global* properties. Flexible and fine-grained delegation: Run-time delegation of URI permissions is a key feature in Android, and allows applications to use third-party components (e.g., a viewer activity) to manipulate content that those components normally would not be permitted to access. On examination, we discovered that Android's implementation of permission delegation is plagued by a number of flaws and questionable design decisions. Sorbet supports more flexible and principled permission delegation and revocation, and allows developers to specify constraints that limit the lifespan and redelegation scope of the delegated permissions. Developing a mechanism that correctly enforces lifetime and scope constraints turns out to be unexpectedly tricky, due to redelegation and the dynamic nature of Android applications and components, including application installation and uninstallation, and instantiation and termination of components. Prototype system: We implemented Sorbet on top of Android 2.3.7, tested it on a Nexus S phone, and demonstrated several new scenarios that it enables. These findings have been described in a paper that appeared at ESORICS in September 2012.

(Cranor, Passwords):Text-based passwords remain the dominant authentication method in computer systems, despite significant advancement in attackers' capabilities to perform password cracking. In response to this threat, password composition policies have grown increasingly complex. However, there is insufficient research defining metrics to characterize password strength and evaluating password-composition policies using these metrics. We analyzed 12,000 passwords collected under seven composition policies via an online study. We developed an efficient distributed method for calculating how effectively several heuristic password-guessing algorithms guess passwords. Leveraging this method, we investigated (a) the resistance of passwords created under different conditions to password guessing; (b) the performance of guessing algorithms under different training sets; (c) the relationship between passwords explicitly created under a given composition policy and other passwords that happen to meet the same requirements; and (d) the relationship between guessability, as measured with password-cracking algorithms, and entropy estimates. Our findings advance understanding of both password-composition policies and metrics for quantifying password security.
To help users create stronger text-based passwords, many web sites have deployed password meters that provide visual feedback on password strength. Although these meters are in wide use, their effects on the security and usability of passwords have not been well studied. We conducted a 2,931-subject study of password creation in the presence of 14 password meters. We found that meters with a variety of visual appearances led users to create longer passwords. However, significant increases in resistance to a password-cracking algorithm were only achieved using meters that scored passwords stringently. These stringent meters also led participants to include more digits, symbols, and uppercase letters. Password meters also affected the act of password creation. Participants who saw stringent meters spent longer creating their password and were more likely to change their password while entering it, yet they were also more likely to find the password meter annoying. However, the most stringent meter and those without visual bars caused participants to place less importance on satisfying the meter. Participants who saw more lenient meters tried to fill the meter and were averse to choosing passwords a meter deemed "bad" or "poor." Our findings can serve as guidelines for administrators seeking to nudge users towards stronger passwords. Users tend to create passwords that are easy to guess, while system-assigned passwords tend to be hard to remember. Passphrases, space-delimited sets of natural language words, have been suggested as both secure and usable for decades. In a 1,476-participant online study, we explored the usability of 3- and 4-word system-assigned passphrases in comparison to system-assigned passwords composed of 5 to 6 random characters, and 8-character system- assigned pronounceable passwords. Contrary to expectations, system-assigned passphrases performed similarly to system-assigned passwords of similar entropy across the usability metrics we examined. Passphrases and passwords were forgotten at similar rates, led to similar levels of user difficulty and annoyance, and were both written down by a majority of participants. However, passphrases took significantly longer for participants to enter, and appear to require error-correction to counteract entry mistakes. Passphrase usability did not seem to increase when we shrunk the dictionary from which words were chosen, reduced the number of words in a passphrase, or allowed users to change the order of words.

Acqisti: "The Impact of Online Social Networks on Firms' Hiring Practices": We successfully completed the survey-experiment version of the study, using a sample of over 5,000 online subjects. The results of that experiment highlight a relationship between online social media profiles and discriminatory bias, and are about to be submitted to a premiere economics journal. The second experiment (a field experiment) is ongoing and preliminary positive results are being gathered.
"The Evolutionary Roots of Privacy and Security Concerns": We have completed the pilot phase of the experiment with CMU subjects, and we are gathering data from the actual experiment. In the meanwhile, we have received additional NSF funding for the continuation of this experiment.

Brumley: Main accomplishments and advancements are towards a sound framework for performing program analysis on x86 code. Please see published paper above for specifics.

Sadeh: In 2011-2012, we continued to make significant progress on user-oriented machine learning techniques with a particular focus on developing understandable privacy personas for location sharing. We were able to show how personas derived using novel user-oriented clustering techniques were able to increase policy accuracy and how these techniques complement machine learning techniques used to generate suggestions for how to improve one's current privacy policies. We were also able to deploy and evaluate the benefits of a wizard implementing privacy personas derived using our clustering techniques. Experiments conducted with 35 users over a period of 3 weeks showed clear benefits of using privacy personas in the context of location privacy.

Zhang, Pei: PANDAA uses relative ambient sound to obtain relative topology of the network. Our experiments show indoor relative device localization up to 10cm accuracy. Using this relative localization, CoughLoc can detect and locate sound events with self-organizing deployments.

B.V.K. Vijaya Kumar: Many scenarios require that face recognition be performed at conditions that are not optimal. Traditional face recognition algorithms are not best suited for matching images captured at a low-resolution to a set of high-resolution gallery images. To perform matching between images of different resolutions, we have developed a method of learning two sets of projections, one for high-resolution images and one for low- resolution images, based on local relationships in the data. Subsequent matching is done in a common subspace. This method is called coupled marginal Fisher analysis (CMFA).

Experiments show that CMFA yields higher recognition rates than other similar methods. We compare CMFA to simultaneous discriminant analysis (SDA) and marginal fisher analysis (MFA). SDA is a coupled mapping and learns projections for HR and LR probe images at the same time. On the other hand, MFA must be learned at a single dimension. Results labeled `MFA' is a baseline using high resolution (HR) gallery and probe images. `MFA-LR' uses low resolution (LR) gallery and probe images. Results for `MFA-BL' use HR gallery images and learn HR projections, and then use LR probe images that are upsampled to the HR dimensionality using bilinear interpolation.

For testing we use the CMU Pose, Illumination, and Expression (PIE) database, and the CMU Multi-PIE database. We take a part of the PIE dataset containing frontal images of 66 subjects with varying illumination, such that each subject has 21 images taken in one session. Multi-PIE addresses some concerns of the PIE dataset, and includes 337 subjects, with multiple sessions (up to 5) for most subjects. Again, frontal images with a neutral expression are used. Each of the 337 subjects has between 20 and 100 images (20 per session). Images in both datasets are registered based on eye locations. For all tests, HR images are 48x48, and in lieu of genuine LR images, they are generated by downsampling and blurring the HR images to 12x12. Example HR and LR images are shown above.

The data is split such that each subject has an equal number of images in the gallery and the remaining images become the probe set. The gallery images are then used for training. Table below shows rank-1 Identification rates when training on a set of gallery images, and testing on LR and HR probe images. The number in parentheses for Data is the number of gallery images per subject. The number in parentheses for each reported performance level is the standard deviation over 20 runs.

Above Table shows that CMFA and MFA both outperform SDA on the PIE dataset, and CMFA is the best performing algorithm on the Multi-PIE dataset. The table shows similar trends when testing HR probe images, but it is interesting to note that CMFA and MFA-LR both outperform the baseline MFA in some cases. CMFA's better performance compared to SDA indicates that CMFA does a better job discriminating between classes it trains on.

Technology Transfer

SoS Lablet

Kathleen Carley - Learned Resiliency in Multi-Level Systems

1) CASOS Summer Institute, June 2013 - This is technology transfer through education. We trained over 45 individuals in a) the new metrics, b) the process of assessing organizational-level impacts of cyber events, and c) use of the multi-level simulation technology developed for this project. Trainees included individuals from universities, government and industries. Due to sequestration there were no active duty military participants this year.

2) STRATCOM - We engaged in discussions with members of STRATCOM about this research with the aim of providing them with material needed for their design review process.

3) USMA - Michael Lanham has returned to USMA and will be teaching Cadets using the materials and models developed herein. He is part of the cyber group.

Kathleen Carley - Geo-Temporal Characterizations

1) CASOS Summer Institute, June 2013 - This is technology transfer through education. We trained over 45 individuals in a) procedure for assessing global cyber network, b) over time analytics and MRQAP needed to assess global cyber network, and c) result of global cyber network assessment.

2) STRATCOM - We engaged in discussions with members of STRATCOM about this research with the aim of providing them with material requested on global cyber networks.

3) Discussions with NATO about possible international issues related to cyber security. We expect to be invited to a conference in Belgium on this issue in October 2013.

4) Other NAS projects – results from this study were leveraged to validate model developed under the Learned Resiliency project.

David Garlan, Jonathan Aldrich, Bradley Schmerl - Secure Frameworks

1) We have successfully transferred the Rainbow framework to our partners at GMU.

2) An open-source prototype of the system described in the GlobalDSL paper is available at https://github.com/wyvernlang

Perpetually Available and Secure Information Systems

Re: Soft Biometrics from Emerging Media, Yang Cai reports:
We transferred our technology to DIA, USSS and CERT for video and imagery forensics analytics projects. We delivered our prototypes to DIA, USSS and CERT. Also, we delivered demos to AFRL Rome, NY in 2010 for UAV based video encoder and visualization.

Re: Security Patters: Assurance for Secure Concurrent and Distributed Computing, William Scherlis and Jonathan Aldrich report:
Invention disclosure from Dean Sutherland and William Scherlis, with subsequent license given to SureLogic, Inc (a CMU spinoff) Talked
with two entrepreneurs about commercializing our CyLab-funded secure architecture/information flow technology. Interest has been expressed and we are following up.

Re: Reconciling Privacy and Usability by Learning Default, Norman Sadeh reports:
Wombat Security Technologies, which is a CyLab spinoff, co-founded by Norman Sadeh, Jason Hong and Lorrie Cranor in June 2008, to commercialize their work on combating phishing attacks has now licensed it products for use by several million users world-wide. This includes end-user organizations coming from a broad cross section of sectors, including government, finance, insurance, health care, telecommunications, energy, transportation, IT, e-tailing, entertainment and education. In September 2010, Wombat Security Technologies was awarded a SBIR Phase II grant by the US Air Force to develop a

Platform for Micro Games for Cyber Threat Awareness In February 2011, Wombat Security Technologies was awarded a SBIR Phase I grant by OSD/Army to develop high-accuracy, zero-hour anti-phishing filtering techniques Results from our research in location privacy have been referenced in Congressional Hearings Norman Sadeh was also invited to present his results at the Digital Privacy Forum (featured on C-SPAN) as well as other events. In October 2010, the MIT Technology Review published an article titled “Locaccino Shows How Facebook Places Should Work” (http://www.technologyreview.com/blog/mimssbits/25832/?p1=Blogs

Re: Adaptive Strategies for Cross-Layer Jamming and Anti-Jamming, Patrick Tague reports:
Initial interaction with Northrop Grumman through the Cybersecurity Research Consortium, but no explicit transfer of information to date

Re: Efficient and Effective High Speed Network Logging for Digital Forensics, David Andersen reports:
We have been interacting with researchers from Symantec and Lockheed-Martin to discuss opportunities for technology transfer. We have launched a project in collaboration with a major solid-state-drive manufacturer to integrate some of the key-value storage and retrieval techniques into their products. We have also met several times with researchers from a DoD organization that performs extensive data analysis to inform them about our techniques and results, and have made our source code available to them.

Re: Exploring reactive access control, Lujo Bauer reports:
We had extensive technical discussions with a number of industry partners, some of which, e.g., Cisco, can readily transition some of research ideas into products.

Re: Semantic Geotagging for Situational Awareness During Disaster Response, Ray Bareiss reports: We have integrated the system with the Golden Gate Safety Network’s common operating picture software.
Re: Cloud Computing and CyLab: Establishing a Shared Utility and Informing Assured Cloud Computing Research, Greg Ganger reports: The biggest success was this effort contributed significantly to the development of a large new multi-institution research center focused on cloud computing. Funded by Intel at over $3M/year, the Intel Science and Technology Center for Cloud Computing has a broad research agenda targeted at creating the underlying technologies for future cloud computing to be more efficient, more ubiquitous, and a greater boon to productivity. In addition, the research team reaches out regularly to industry providers of information systems, which is critical to
transfer of survivable and secure infrastructure technologies to COTS systems. In addition to the broad CyLab Partner’s Conference, we have two annual industry affiliates meetings that are more focused on our underlying technology activities like cloud computing infrastructures. In the Spring, we have a one-day on-campus event during which 20-25 representatives from 17 companies (APC, EMC, Facebook, Google, Hitachi, HP, IBM, Intel, LSI, Microsoft, NEC, NetApp, Oracle, Samsung, Seagate, Symantec, VMware) interact with the researchers over demos and posters. Our most extensive annual technology transfer activity, for the infrastructure research, is an annual
3-day PDL Retreat. Attended by over 30 storage and information systems leaders from the companies listed above, this retreat/workshop consists of presentations from most of the researchers and lots of interaction/feedback from the visitors. Regular in-depth interactions, like these, are the backbone of our technology transfer activity, leading to understanding and appreciation of the technologies and deployment issues by everyone involved. In addition to these structured events, we frequently visit with or host visits by key technical personnel from the above companies and others.

Re: Soft Biometrics from Emerging Media, Yang Cai reports: We transferred our technology to DIA, USSS and CERT for video and imagery forensics analytics projects. We delivered our prototypes to DIA, USSS and CERT. Also, we delivered demos to AFRL Rome, NY in 2010 for UAV based video encoder and visualization.

Re: Security Patters: Assurance for Secure Concurrent and Distributed Computing, William Scherlis and Jonathan Aldrich report: Invention disclosure from Dean Sutherland and William Scherlis, with subsequent license given to SureLogic, Inc (a CMU spinoff) Talked with two entrepreneurs about commercializing our CyLab-funded secure architecture/information flow technology. Interest has been expressed and we are following up.

Re: Reconciling Privacy and Usability by Learning Default, Norman Sadeh reports: Wombat Security Technologies, which is a CyLab spinoff, co-founded by Norman Sadeh, Jason Hong and Lorrie Cranor in June 2008, to commercialize their work on combating phishing attacks has now licensed it products for use by several million users world-wide. This includes end-user organizations coming from a broad cross section of sectors, including government, finance, insurance, health care, telecommunications, energy, transportation, IT, e-tailing, entertainment and education. In September 2010, Wombat Security Technologies was awarded a SBIR Phase II grant by the US Air Force to develop a Platform for Micro Games for Cyber Threat Awareness In February 2011, Wombat Security Technologies was awarded a SBIR Phase I grant by OSD/Army to develop high-accuracy, zero-hour anti-phishing
filtering techniques Results from our research in location privacy have been referenced in Congressional Hearings Norman Sadeh was also invited to present his results at the Digital Privacy Forum (featured on C-SPAN) as well as other events. In October 2010, the MIT Technology Review published an article titled “Locaccino Shows How Facebook Places Should Work”

(http://www.technologyreview.com/blog/mimssbits/25832/?p1=Blogs

Re: Adaptive Strategies for Cross-Layer Jamming and Anti-Jamming, Patrick Tague reports: Initial interaction with Northrop Grumman through the Cybersecurity Research Consortium, but no explicit transfer of information to date

Re: Efficient and Effective High Speed Network Logging for Digital Forensics, David Andersen reports:
We have been interacting with researchers from Symantec and Lockheed-Martin to discuss opportunities for technology transfer. We have launched a project in collaboration with a major solid-state-drive manufacturer to integrate some of the key-value storage and retrieval techniques into their products. We have also met several times with researchers from a DoD organization that performs extensive data analysis to inform them about our techniques and results, and have made our source code available to them.

Re: Exploring reactive access control, Lujo Bauer reports: We had extensive technical discussions with a number of industry partners, some of which, e.g., Cisco, can readily transition some of research ideas into products.

Re: Semantic Geotagging for Situational Awareness During Disaster Response, Ray Bareiss reports: We have integrated the system with the Golden Gate Safety Network's common operating picture software.

Re: Cloud Computing and CyLab: Establishing a Shared Utility and Informing Assured Cloud Computing Research, Greg Ganger reports: The biggest success was this effort contributed significantly to the development of a large new multi-institution research center focused on cloud computing. Funded by Intel at over $3M/year, the Intel Science and Technology Center for Cloud Computing has a broad research agenda targeted at creating the underlying technologies for future cloud computing to be more efficient, more ubiquitous, and a greater boon to productivity. In addition, the research team reaches out regularly to industry providers of information systems, which is critical to
transfer of survivable and secure infrastructure technologies to COTS systems. In addition to the broad CyLab Partner's Conference, we have two annual industry affiliates meetings that are more focused on our underlying technology activities like cloud computing infrastructures. In the Spring, we have a one-day on-campus event during which 20-25 representatives from 17 companies (APC, EMC, Facebook, Google, Hitachi, HP, IBM, Intel, LSI, Microsoft, NEC, NetApp, Oracle, Samsung, Seagate, Symantec, VMware) interact with the researchers over demos and posters. Our most extensive annual technology transfer activity, for the infrastructure research, is an annual
3-day PDL Retreat. Attended by over 30 storage and information systems leaders from the companies listed above, this retreat/workshop consists of presentations from most of the researchers and lots of interaction/feedback from the visitors. Regular in-depth interactions, like these, are the backbone of our technology transfer activity, leading to understanding and appreciation of the technologies and deployment issues by everyone involved. In addition to these structured events, we frequently visit with or host visits by key technical personnel from the above companies and others.

Geo-Temp Characterization - 29983.1O

Kathleen M. Carley

Introduction

Objective

The objective of this project is to empirically characterize the nature of the current threat environment and to test a series of existing hypotheses about that threat environment using Symantec data. Our focus is global. The basic theory is that the potential severity of the threat is a function of the political environment rather than the technology. Questions to be addressed empirically include:

1. What is the likelihood of a catastrophic threat? Hypothesis: Most attacks are small.
2. How does the likelihood differ by type of threat? Hypothesis: there are no differences by type of threat.
3. Do these answers differ by country? Hypothesis A: Once GDP, internet penetration, and the number of attacks are accounted for there are no differences by country. Hypothesis B: The likelihood of a company being attacked depends on their position in the alliance/enmity network.

Background

In their 2011 survey Symantec found that the number one cyber risk business concern was external cyber-attacks, followed by concerns about both unintentional insider error (2nd risk) and intentional insider error (3rd risk) (Symantec, 2011, pg 9). Analysis by Verizon's cyber forensics team indicates that the massive increase in external threats overshadows insider attacks (Verizon, 2012b, pg 21). See also Richardson (2008). Despite the increase in external threats little is known about the source of such threats; or the global implications this evolving threat environment.

Wynne (2010) notes that the need to do attribution and forensics is critical to stem the tide of cyber-attacks. To meet this need, an understanding of the threat environment at the global level is needed. Cyber security, at the global level, is critical on a number of fronts including countering terrorism (Westby, 2007). At the global level, cyber security requires not only attribution and forensics, but harmonized laws and effective information sharing. In spite of this growing consensus there is still little empirical understanding of the global cyber threat environment, an understanding that is critical for forensics. We have found that most global information sharing is done through security providers and the data is only now becoming available and in restricted form given the dual privacy and security needs that must be met.

We note that reliance on anecdotal evidence can be damaging for the Science of Security. As empirical findings come to light, assumptions about the nature of cyber threat are changing. For example, in 2004, Byre and Lowe showed that process control and SCADA systems were not immune to attack using incidence data. Further basic assumptions are falling as new empirical evidence comes to light. This is creating a new baseline against which forensics can operate. While there are an increasing body of findings focused on specific threats and empirical

assessments of key incidents; there is less understanding of the human socio-behavioral factors, particularly at the global level.

At the global level, multiple conceptual frameworks abound. For example, Kshetri (2005) argues that country level differences in the regulative, normative and cognitive legitimacy of different types of web attacks lead to differences in the extent to which organized crime can use the internet in those countries. BSA (2010) provides guiding principles for global cyber security. Broadhurst (2006) argues that cyber-attacks are traditional crimes in a new venue which makes traditional forensic methods obsolete. And so on. Despite the recognition of the global nature of the cyber threat there is little characterization of that threat.

Approach

The basic approach used was to develop code for extracting country level indicators of attacks and attack paths from the Symantec data. The analysis is based on the Symantec WINE telemetry data set. WINE is a platform through which external researchers can access data sets used within Symantec Research labs. To the best of our knowledge, Symantec is currently the only security company that makes such platform available to external researchers. The telemetry data set consists of attack reports from more than 10 million Symantec customer computers worldwide.

This was then combined with other open-source data to create a global threat profile. An example of such additional open source data is the ICT index cira 2010 for all countries. The ICT index is a combined measure based on 11 indicators including adult literacy, internet access and so on. The data was fused to create a global indicators data set and was then assessed using network analytics and standard statistical procedures. Based on this data a network based model of the impact of hostilities and other factors on geo-cyber-attack-network was developed.

Summary of Key Results

There are two key aspects to this research. The first is the characterization of the threat profile. The second is the assessment of the over-all global threat with respect to cyber attacks.

In terms of the general threat profile, our results led to an empirical characterization of the change in cyber-threat over the past several years. This work indicated that web attacks account for the vast majority of attacks in the IPS catalog. Around 2003, worms and viruses were the most dominant threat types. At that time, the main malware distribution technique was infection propagation among computers. The main goal of attacks was to cause damage or to "show off". Since then, we have seen the emergence of new attack types that reflect either new distribution techniques (e.g. web attacks) or that mainly have monetary goal (fake anti-viruses, adware/spyware). 61% of attacks are transmitted from an exploiting machine, 37% of attacks are transmitted from malicious websites, 2% are from other sources not specified.

The results confirmed the hypothesis that most attacks are small, and so low severity threats. This result informed other research in the lablet. It Is important to recognize though that Symantec (as an example of key anti-virus vendor) prioritizes releasing attack signatures for fast propagating threats, but not necessarily for threats that might cause high damage.

We conducted a global assessment of the extent to which countries were threatened, threatening, or utilized for sending cyber-attacks. It was hypothesized that once GDP, internet penetration, and the number of attacks are accounted for there are no differences by country. This hypothesis was disconfirmed. While these factors do mitigate the effect, there are still country effects.

Developed countries are more likely to encounter web attacks and fake applications (such as fake anti-viruses) – see Figure 1. High ICT countries, e.g., US, are more likely to encounter fake applications and web attacks; whereas, mid ICT countries are more likely to encounter threats. Mid ICT countries are most likely to transmit attacks, e.g., Romania, Moldovia, Bosnia. And in general, the USA is exposed to more fake applications than other countries. It is possible that attackers target these countries because such attacks are likely to be more lucrative. From a statistical perspective - monetary and computing resources are the main factor that attracts attacks at the country level.

Further, we find that the global threat profile is complicated and does not match the standard view from political science of the US and one or two other countries mostly fighting with each other. This means that our results are counter to the standard wisdom which is case based. A general social-influence model is a better predictor than the traditional great-powers model.

How attacking computers' hosting varies across countries was analyzed and factors that explain such variation were identified. We found that many countries in Eastern Europe and Central America extensively host attacking computers. Such countries have a combination of good computing infrastructure and high levels of corruption. The high levels of corruption facilitates conducting cyber criminal activities such as registering malicious websites through the complicity of ISPs and law officials.

The international cyber attack network was analyzed. For web attacks and fake applications, most attacks are from Eastern Europe and Central America to developed countries in Western Europe and North America. See for example, the network of dominant attacks from the Ukraine in Figure 2. Exploits have a tendency to spread to geographically nearby countries.

The country-level specificity of the results means that diplomatic and soft-power solutions may be valuable in mitigating cyber-attacks. Many countries are cyber-crime friendly environments – see Figure 3. Some of these countries serve as wayports – and so are "usable" by others to send attacks. Globally – countries with weak cyber policies or poor enforcement or unsophisticated approach to cyber attacks are most "used" or serve as the "source" to spread attacks. Thus, countries in Eastern Europe and Central America host most cyber-attack infrastructure (such as malicious web sites and botnets). A combination of good computing infrastructure and lax policies makes the above countries attractive for hosting attack infrastructure. It is interesting to note that the Ukraine and several countries that were part of the USSR fall into this category. We note that Russia is about to require all blogs to register and to add more control over the web. Based on this research and other research we have done on social media we expect this to a) impact the potential for state instability, and b) to alter the flow of web-based attacks that flow through the related countries. A possible future study might look specifically at the Russia/China/US cyber environment in more detail.

Bibliography

Broadhurst, Roderic, 2006, "Developments in the global law enforcement of cyber-crime", Policing: An International Journal of Police Strategies & Management, 29(3): 408 – 433

BSA, 2010, Global Cyber-Security Framework. Accessed from: http://www.bsa.org/country/Public%20Policy/~/media/Files/Policy/Security/CyberSecure/Cybersecurity_Framework.ashx

Byres, Eric and Justin Lowe, 2004, The Myths and Facts behind Cyber Security Risks for Industrial Control Systems, Proceedings of the VDE Kongress, 2004.

Kshetri, Nir, 2005, Pattern of Globalcyber War and Crime: A Conceptual Framework, Journal of International Management, 11(4): 541–562.

Richardson, R., 2008, 2008 CSI Computer Crime and Security Survey. Accessed from: http://gocsi.com/sites/default/files/uploads/CSIsurvey2008.pdf

Symantec, 2011, 2011 State of Security Survey. Accessed from: http://www.symantec.com/content/en/us/about/media/pdfs/symc_state_of_security_2011.pdf

Verizon, 2012b, 2012 Data Breach Investigations Report. Accessed from: http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

Wynne, Michael W., 2010, Report from the Stevens Institute Cybersecurity Policy Conference, January 19-20 Reagan Building Washington DC.

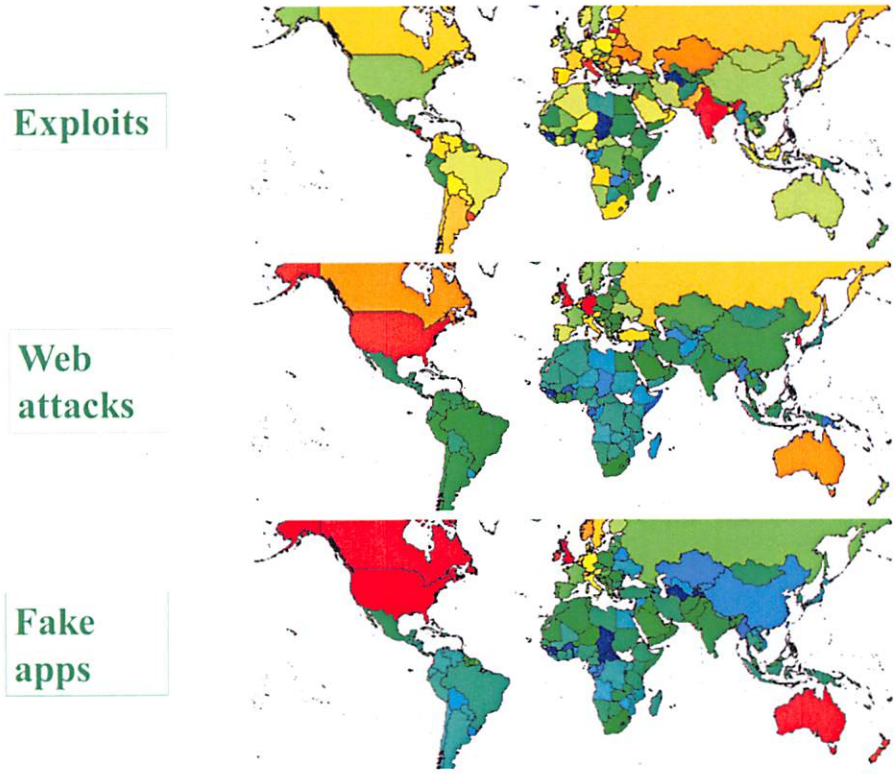


Figure 1. Threatened countries. Red is high, blue is low

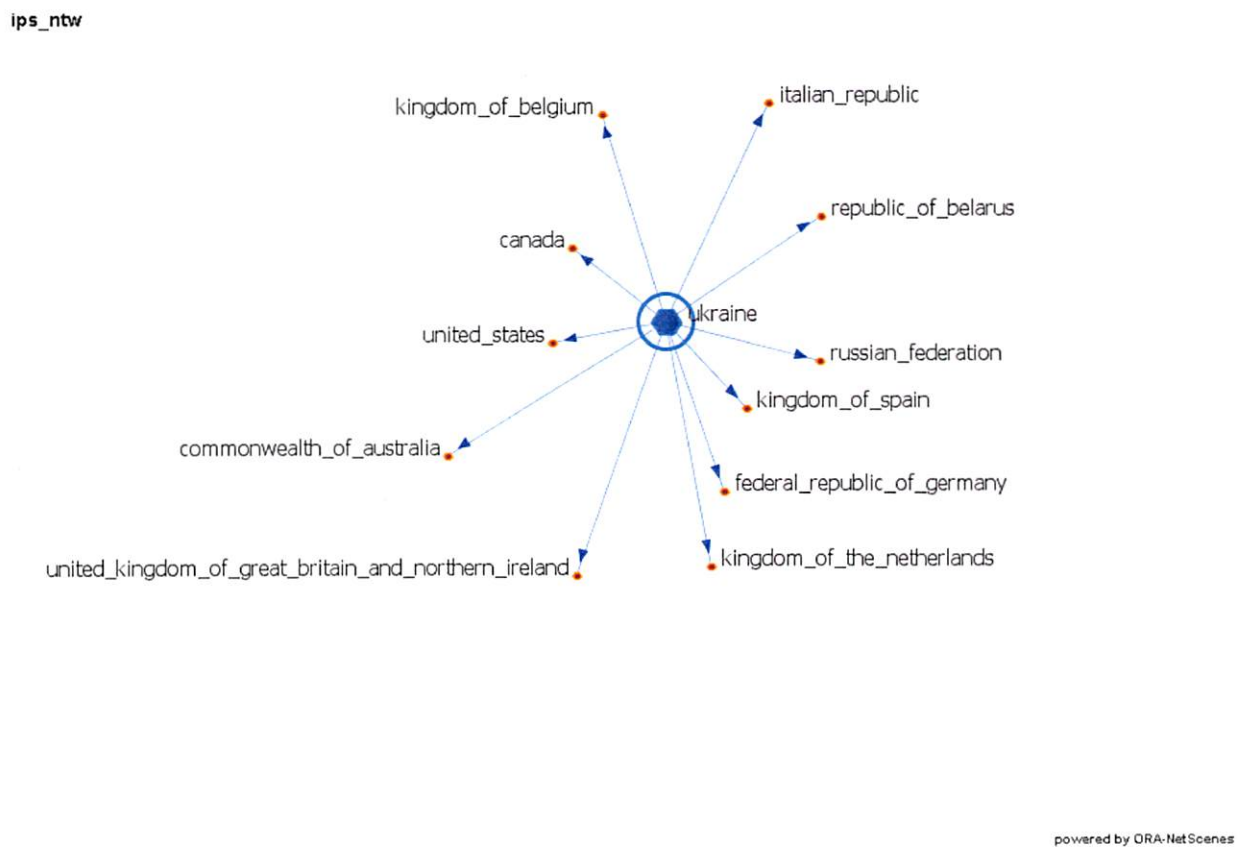


Figure 3. Those countries receiving many web-attacks from the Ukraine. These countries receive almost 2 standard deviations more attacks from the Ukraine, than the the average number of attacks from one country to another.

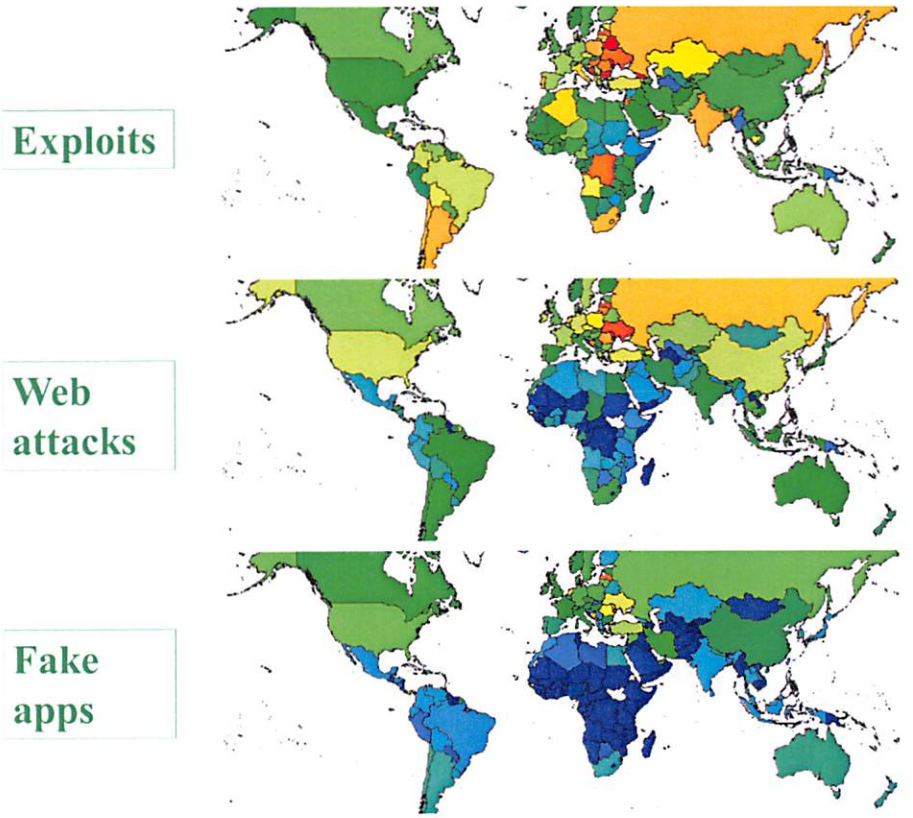


Figure 2. Countries with cyber-crime friendly environment. Red is high, blue is low.

Learned Resiliency in Multi-Level Systems – 26803.1I

Kathleen M. Carley

Introduction

Increasingly organizations are under cyber-attack. These attacks may take many forms, with denial of service, data stealing or sabotage, being simple examples. These attacks have the potential to impede mission planning, reduce performance, and cause information to "leak" or "be-discovered" where inappropriate. The question arises, how can organizations be structured to mitigate these cyber-induced risks, to be resilient in the face of these cyber-threats? Using agent-based simulation thee questions are addressed. The results provide guidance for how to design for cyber-security resilience. In addition to the organizational design guidance, this work led to a novel agent-based technology, new metrics of resilience, and new visualization capabilities for simulation data.

Statement of the problem studied

Organization's face security risks from both human and computer (hardware or software) errors. These errors can compound, and grow worse as more individuals are connected to more people and more information technology (IT) in more ways (e.g., VoIP, direct interaction, email, social media ...). Identifying the source of the errors, and responding to errors in a rapid and effective manner is often made more difficult when the organization is operating simultaneously at multiple levels of security – an example is the unclassified, classified secret and classified above-secret levels employed by many governments. The multi-level security impacts IT system, information and human segmentation due to controls on who can relay and access what information using what systems. The need to operate with multi-level security places added constraints on what organizational design solutions are possible to achieve high levels of resiliency in the face of cyber threats and events and increases the need to be resilient in the face of security risks. We ask, is it possible to design organizations that are operating at multiple levels of security to be resilient to cyber threats?

Objective

The objective of this project is to develop a theory of system resiliency for complex adaptive socio-technical systems. A secondary objective is to develop the modeling framework and associated metrics for examining the resiliency of complex socio-technical systems in the face of various cyber- and non-cyber-attacks, such that the methodology can be used to support both basic level simulation based experimentation and assessment of actual socio-technical systems. To meet these objectives multi-modeling is used to examine how to design and impact complex organizational systems in which information is segmented to multiple levels of security with all the attending issues for personnel access and IT usage.

Background

Much of the recent research on threatened complex socio-technical systems, in the security area, has focused on tracking (Lipson, 2002; Gao & Ansari, 2005), investigating (Nilson & Larson, 2008), characterizing (Kotapati et al, 2005), or measuring the damage caused by (Lala & Panda,

2001) cyber attacks. Such work, while providing a context for this research, does not address the issue of system resiliency in the face of such threats. Current approaches seeking to mitigate these threats, in complex socio-technical systems tend to either model cyber attacks at the IT level or provide guidelines to managers about how to handle the human side of the equation. For example, on the IT side, the CAML approach to modeling cyber attacks focuses on data streams and features of the IT system (e.g., Cheung, Lindqvist & Fong, 2003), and the DDoS attack detection models focus on network usage characteristics (Li, Li and Jiang, 2008). For example, on the organizational side, efforts have been made to provide managers with exercises for improving reaction to threat events (Andersen et al., 2004). One exception to this trend is the cyber command and control model (Scherrer & Grund, 2009) which is a conceptual model laying out processes and lines of authority for the DOD and which cannot be used for empirical assessment of resiliency, nor is it generally applicable beyond the DoD. We seek to develop a model that considers both the human and the IT side, such that the model supports empirical analysis of both hypothetical and real complex socio-technical systems. The other key exception is the service restoration model (Lee, Mitchell & Wallace, 2007) which uses highly theoretical and stylized organizations subject to generic attacks and assesses resilience along seven dimensions. Ws build on these dimensions but recast them, and formalize them, using network metrics.

In the area of cyber threat, relatively less is known about the human than the IT side of the equation (Stytz & Banks, 2008). In general, more work is needed on how humans and so organizations respond to varying cyber threats and events – especially those of significant impact and duration. Drawing on the work in high-reliability organizations, there are models of mitigation based on assumptions of human error and organizational design (LaPorte & Consolini, 1991; Bigley & Roberts, 2001). Admittedly the high reliability research was focused on types of threat other than cyber; nevertheless, this research speaks to the need for specialized organizational structures and norms when the socio-technical system must exhibit high reliability in the face of a highly volatile and potentially hostile environment. Organizations faced with high security needs are in a similar environmental situations and so too would need specialized structures and norms. In complex socio-technical systems, where security is a premium, a comprehensive model must account for both these IT and organizational issues. The proposed work is a step toward creating a joint human-IT framework for assessing the impact of cyber threat and the resiliency of the socio-technical system.

Current approaches to understanding the impact of threats and vulnerabilities on these systems tend to focus on the system as it was planned with some flexibility for how it was built – rarely do cyber or organizational security attempt to identify how the system(s) may evolve. However, the nature of the threat evolves, the threatened organization, its operating environment and its operating dependencies are changing, and the individuals in the organization are learning. While a full explication of these co-evolutionary processes is beyond this proposal we do focus in on the extent to which individual learning results in the evolution of trust, norms, and coordination practices that may support or be detrimental to overall system resiliency. For this we employ agent-based models of learning. The impact of learning on system behavior has been extensively studied. Key finding of relevance here are that: the type of learning employed impacts outcomes (Lant & Mezias, 1992); learning at the individual

and group level can conflict resulting in a decrease in resiliency (Carley & Svaboda, 1996); organizational-complexity and the organizational structure impacts the leaning of norms (Harrison & Carroll, 1991) and so would impact the development of a security culture; in contrast to novices, experts models of complex phenomena are richer (Chi, Feltovich & Glaser, 1981), contain more detailed relations among factors (Klein & Hoffman, 1993) informed by experience (Klein, 1998) and so the experts should be less likely to under or over-react than novices; high personnel turnover in conjunction with a volatile and perhaps hostile environment can mitigate the impact of learning and decrease resilience (Lin & Carley, 2003).

Approach

To address these issues, an approach combining agent-based simulation and dynamic network analysis is used. The specific agent-based model that we extended is Construct (Carley 1990; Carley, Martin & Hirshman, 2009). The result was a new system that supports reasoning about both individuals and groups and can be used to assess multi-level security systems at the organizational level. Resiliency metrics based on a high-dimensional dynamic network representation of organizations were constructed. This representation is referred to as a meta-network representation of the socio-technical organization. A series of scenario driven virtual experiments were then used to assess the relative resiliency of organizations with different designs in either or both the lines of personnel authority and interaction or IT/data access. Over 2 million simulation runs were conducted generating over 900GB of simulated data. A response-surface visualizer was developed for visualizing the results, a set of compression and aggregation techniques were developed for data management. A new system for running the models through condor was developed.

Summary of Key Results

These simulations show that most organizations are reasonably resilient to small and medium cyber attacks. The attack must be large and fairly pervasive to have a major impact on performance and the ability to engage in and complete mission planning. We find this result to be consistent with the data findings from Symantec. Our results further indicate that hierarchies, overall, are among the top performers and exhibit high resilience when operating a multi-level security environment. When under cyber-attack resiliency is enhanced by organizations resort to direct human communication; however, that increases the chances of inadvertent information leaks. Results of these simulations further suggest that inadvertent information leaks are more likely to occur when the organization is under cyber-attack and are likely to occur in all organizations, regardless of their design. These can be thought of as "normal" accidents. However, such leaks, are most likely in mesh organizations and least likely in hierarchies – see Figure 1.

At one level, these results suggest that organizations to be resilient in the face of cyber-attacks should operate as a high-reliability organization (Weick & Roberts, 1993; Shulman, 2004; Roberts, 1990). Such organizations are ones that utilize management and design practices that enable them to avoid failure despite operating in high risk environments were errors can be expected due to both the complexity of the system and the level of external risk. High-tech multi-level security systems are inherently complex and the potential cost of errors

due to cyber threats creates a high risk environment. In these simulations, those organizational designs that rely on personal expertise, and that support change in the face of attacks (commitment to resilience) operate at higher reliability.

At another level, these results refine the notion of what it takes to be a high reliability organization by providing explicit guidance for how to design for resiliency. In particular, our results indicate that:

- Redundancy leads to improved performance and resiliency but at the cost of increased opportunities for information leakage.
- Hierarchies are more impacted initially by a reliability attack, but are barely impacted by an integrity attack. Scale Free organizations are the opposite. In the absence of an attack, the Scale Free organizations have superior task performance.
- Although leadership may be relatively insulated from attacks, specific sub-populations of interest within the organization will be more impacted. IT and Human IT changes tend to improve the ability of the hierarchical organization to support these sub-populations, while such changes in the scale-free organizations are detrimental.
- Low magnitude attacks are unlikely to be noticed by leadership unless leadership is looking for them. To maintain high reliability, leadership needs to be vigilant to these attacks.
- Organizations with IT dependencies are able to shrug off minor attacks because information is not optimally distributed for efficiency.
- Increasing the number of information classification levels and distribution protocols, degrades robustness.
- Combinations of attacks are more harmful than single attacks.
- Cloud topologies suffer more in the short-term, but are more robust in the long.
- Hierarchical organizations with cloud IT are the most robust tested organization in the long-term.
- Stove-piped IT systems, where each system is maintained separately, tend to retain bad information longer and so are less resilient in the face of integrity attacks.
- Matrix Organizations, with their cross-functional teams, may be able to overcome knowledge gaps caused by cyber-attacks; but, are often to coherently finish any tasking once the attack has begun.

At a technical level, a key finding is that agent-based simulation modeling that employs "social" reasoning and so agents at both the individual and group level is a significant win as it enables increased accuracy, increased predictive capability in general, and increased speed/ number of actors modelable. Traditionally in agent-based modeling as you improve the model by making the agents more cognitively accurate, or by making the networks more realistic the number of agents that could be modeled or the speed of the model runs decreased. Our results demonstrate that adding social cognition to the model and the associated multi-level actions actually increased the number of agents modelable or the speed for the same number of agents, in the cyber-security domain.

At a measurement level, this research led to a temporal approach and a set of network of metrics for assessing organizational resiliency to cyber attacks and other organizational issues – see Figure 2. The basic idea is that a metric of interest can be used to assess immediate impact, persistent impact and recovery by varying the time period of interest. These metrics take the into account the lines of authority and communication among personnel, access to data and IT systems, mode of communication, and direct IT to IT connections. Both static and dynamic metrics were developed. In general, we find that the dynamic metrics are more effective for assessing resiliency than the static.

Bibliography

Andersen, David, Dawn M. Cappelli, Jose J. Gonzalez, Mohammad Mojtahedzadeh, Andrew P. Moore, Eliot Rich, Jose Maria Sarriegui, Timothy J. Shimeall, Jeffrey M. Stanton, Elise A. Weaver, and Aldo Zagonel. 2004. Preliminary System Dynamics Maps of the Insider Cyber-threat Problem. Paper read at System Dynamics Modeling for Information Security: An Invitational Group Modeling Workshop, 16-20 February, at Pittsburgh, PA, USA.

Bigley, Gregory A. and Karlene H. Roberts. 2001. The incident command system: High-reliability organization for complex and volatile task environments. Academy of Management Journal, 44, 6, 1281-1300.

Carley & Svoboda, 1996. Kathleen M. Carley & David M. Svoboda, 1996, Modeling Organizational Adaptation as a Simulated Annealing Process. Sociological Methods and Research, 25(1): 138-168

Carley, Kathleen M., 1990, "Group Stability: A Socio-Cognitive Approach," Advances in Group Processes: Theory and Research. Edited by Lawler E., Markovsky B., Ridgeway C. and Walker H. (Eds.), Vol. VII. Greenwhich, CN: JAI Press, 7: 1-44.

Carley, Kathleen M., Michael K. Martin and Brian Hirshman, 2009, "The Etiology of Social Change," Topics in Cognitive Science, 1.4:621-650.Zhiang Lin and Kathleen M. Carley, 2003, Designing Stress Resistant Organizations: Computational Theorizing and Crisis Applications, Boston, MA: Kluwer.

Cheung, S.; Lindqvist, U.; Fong, M.W.; , "Modeling multistep cyber attacks for scenario recognition," DARPA Information Survivability Conference and Exposition, 2003. Proceedings , vol.1, no., pp. 284-292 vol.1, 22-24 April 2003

Chi, M.T.H., Feltovich, P.J., & Glaser, R. , 1981. Categorization and representation of physics problems by experts and novices. Cognitive Science, 5, 121-152.

Dennis K. Nilsson and Ulf E. Larson. 2008. Conducting forensic investigations of cyber attacks on automobile in-vehicle networks. In Proceedings of the 1st international conference on Forensic applications and techniques in telecommunications, information, and multimedia and workshop (e-Forensics '08). ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), ICST, Brussels, Belgium

Gao, Zhiqiang and Ansari, N., 2005 , "Tracing cyber attacks from the practical perspective," Communications Magazine, IEEE , vol.43, no.5, pp. 123- 131, May 2005

Harrison, J.R. and G.R. Carroll. 1991. Keeping the Faith: A Model of Cultural Transmission in Formal Organizations. Administrative Science Quarterly, 36, 552-582.

Kameswari Kotapati, Peng Liu, Yan Sun and Thomas F. LaPorta, 2005, A Taxonomy of Cyber Attacks on 3G Networks Intelligence and Security Informatics Lecture Notes in Computer Science, Volume 3495/2005, 129-138

Klein, G. A., & Hoffman, R. R., 1993. Seeing the invisible: Perceptual-cognitive aspects of expertise. In Rabinowitz, M. (ed.),Cognitive science foundations of instruction. Hillsdale, NJ: Erlbaum. 203-226.

Klein, Gary A. 1998, "Sources of Power: How People Make Decisions", MIT Press, Cambridge, Mass, pp. 1-30.

La Porte, Todd R. and Paula M. Consolini. 1991. Working in Practice But Not in Theory: Theoretical Challengers of 'High-Reliability Organizations'. Journal of Public Administrative Research and Theory, 1, 1, 19-47.

Lala, C. and B. Panda, 2001, Evaluating damage from cyber attacks: a model and analysis, IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans, 31(4):300-310.

Lant, T.L. and S.J. Mezias, 1992, "An Organizational Learning Model of Convergence and Reorientation," Organization Science, 3(1): 47-71.

Lee, Earl E. II, John E. Mitchell, and William A. Wallace. 2007. Restoration of Services in Interdependent Infrastructure Systems: A Network Flows Approach. Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on 37 (6):1303-1317.

Li, Muhai, Ming Li and Xiuying Jiang, 2008, DDoS attacks detection model and its application, WSEAS Transactions on Computers, 7(8).

Lipson, Howard F., 2002, Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues, Technical Report, Software Engineering Institute, Carnegie Mellon University

Roberts, K. H. (1990). Some Characteristics of High-Reliability Organizations. Organization Science, 1, 160-177.

Scherrer, Joseph H., and William C. Grund. 2009. A Cyberspace Command and Control Model. edited by U. A. Force. Maxwell AFB, AL: Air War College.

Schulman, P. R. (2004). General attributes of safe organizations. Quality and Safety in Health Care. 13, Supplement II, ii39-ii44.

Stytz, Martin & Sheila Banks, 2008, Advancing Cyber Warfare Simulation System Capabilities, SimTecT 2008 Simulation Conference: Simulation - Maximising Organisational Benefits (SimTecT 2008) Melbourne, Australia, May 12 – 15 , 2008

Weick, K. E., & Roberts, K. H. (1993). Collective Mind in Organizations: Heedful Interrelating on Flight Decks. Administrative Science Quarterly, 38, 357-381.

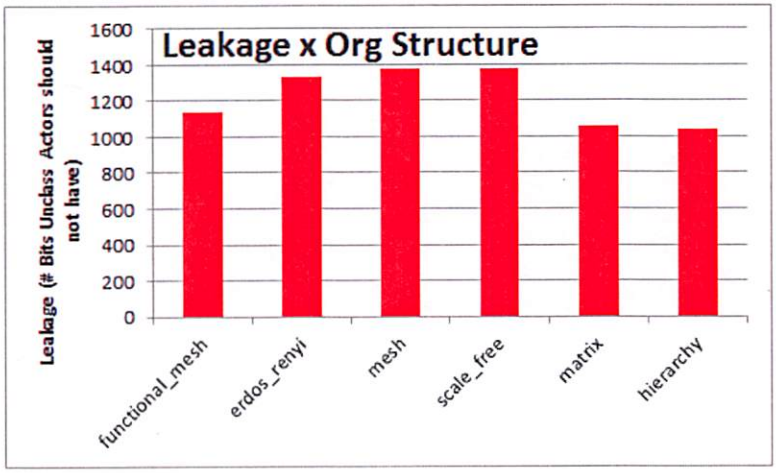
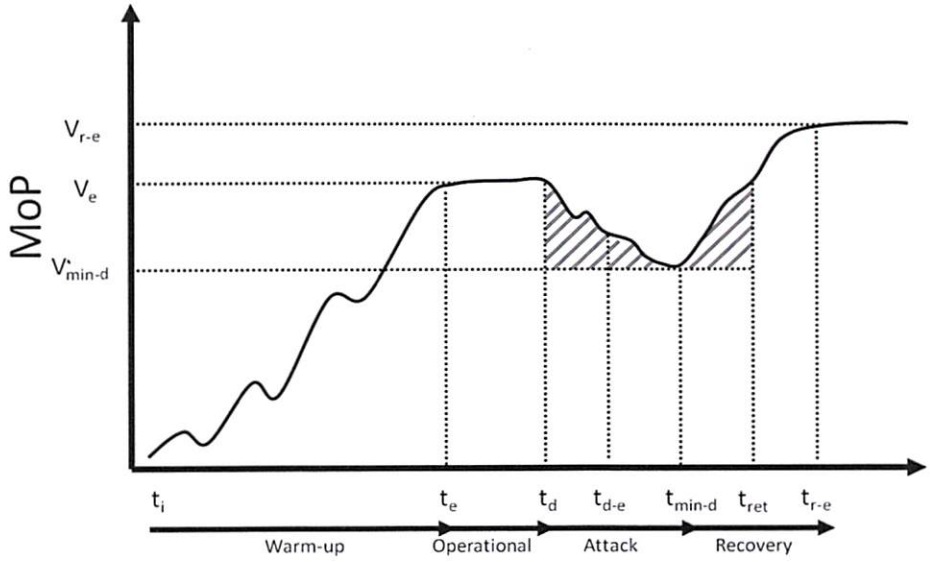


Figure 1. Inadvertent Leaks under cyber-attack.



Impact:

Immediate Impact: $I_m = V_e - V_{min\text{-}d}$

Persistent Impact: $I_p = V_e - V_{r\text{-}e}$

Recovery:

Recovery Time: $t_{r\text{-}e} - t_{min\text{-}d}$

Figure 2. Measuring resilience from a temporal perspective

Security Behavior Observatory: Infrastructure for Long-term Monitoring of Client Machines

Alain Forget, Saranga Komanduri, Alessandro Acquisti,
Nicolas Christin, Lorrie Faith Cranor, and Rahul Telang

July 14, 2014

CMU-CyLab-14-009

CyLab
Carnegie Mellon University
Pittsburgh, PA 15213

Security Behavior Observatory: Infrastructure for Long-term Monitoring of Client Machines

Alain Forget[a], Saranga Komanduri[b],
Alessandro Acquisti[c], Nicolas Christin[d], Lorrie Faith Cranor[e], Rahul Telang[f]
Carnegie Mellon University
[a]aforget@cmu.edu, [b]sarangak@cs.cmu.edu,
[c]acquisti@andrew.cmu.edu, [d]nicolasc@cmu.edu, [e]lorrie@cmu.edu, [f]rtelang@andrew.cmu.edu

***Abstract*—Much of the data researchers usually collect about users' privacy and security behavior comes from short-term studies and focuses on specific, narrow activities. We present a design architecture for the Security Behavior Observatory (SBO), a client-server infrastructure designed to collect a wide array of data on user and computer behavior from a panel of hundreds of participants over several years. The SBO infrastructure had to be carefully designed to fulfill several requirements. First, the SBO must scale with the desired length, breadth, and depth of data collection. Second, we must take extraordinary care to ensure the security and privacy of the collected data, which will inevitably include intimate details about our participants' behavior. Third, the SBO must serve our research interests, which will inevitably change over the course of the study, as collected data is analyzed, interpreted, and suggest further lines of inquiry. We describe in detail the SBO infrastructure, its secure data collection methods, the benefits of our design and implementation, as well as the hurdles and tradeoffs to consider when designing such a data collection system.**

I. Introduction

Our understanding of the security and privacy challenges users face has grown substantially since some seminal usable security papers were first published [1], [2]. Much of the empirical data relating to topics such as authentication [3], [4], computer warnings [5], phishing [6], [7], identity theft [8], has been collected through either in-lab or online controlled experiments, or with surveys and interviews. Controlled lab and online studies allow researchers to isolate variables to observe and measure specific phenomena and effects. Survey and interview data have given us a better understanding of users' perceptions and perspectives, which are invaluable if we are to make security and privacy systems more usable. However, lab studies often lack ecological validity, since users may behave differently in the real world than in an artificial experimental setting [9]. Furthermore, self-reported data may not match users' actual behavior [10], [11].

Thus, the research community has begun focusing on more ecologically-valid data collection. Most published field studies to date have concentrated on specific sub-areas in the usable security and privacy field (e.g., text passwords [12], [13], ATM usage [11], malware infection [14], [15], mobile locking [16], social networks [17]). Most of these studies have short-term focus and monitor only a specific aspect of user or machine behavior. If we are to discover the ground truth of users' most pressing security and privacy challenges, it seems important to collect data on users' and their computers' overall naturalistic behavior in the wild over an extended period of time.

In this paper, we present and describe the Security Behavior Observatory (SBO) we designed to help researchers collect more ecologically-valid data of the widest possible scope over several years. The SBO is a client-server infrastructure for collecting data from a panel of several hundred household computers. Our software will allow us to deploy modular and independent sensors to monitor many security and privacy aspects of home computer use. Observing comprehensive and real-time decision-making of a large panel of users over an extended period of time in a real world setting, in itself, is invaluable. This information can provide a variety of practical and powerful insights into improving security and privacy policies and technologies. However, designing and building the SBO requires attention to factors less frequently considered in shorter-term, more focused studies. The infrastructure must be sufficiently scalable, reliable, and robust to collect the required size, breadth, and depth of data over the study's lengthy duration. In addition, we must carefully consider how best to maintain the security and privacy of participants' data, given the sheer amount and detail of behavioral data we will collect. We also require the flexibility to adjust the types of data we collect throughout the study, since research needs will invariably change as earlier data analysis leads to further lines of inquiry.

This paper is organized as follows. Section II describes how this project contributes to the science of security. Section III introduces the SBO and provides examples of the data we intend to begin collecting. Section IV elaborates on the SBO's architecture from two perspectives. First, we use a data flow model (Figure 1) to describe how data is collected from participants' client machines and sent to our server, and describe the specific benefits of our design decisions. Second, we use a deployment model (Figure 2) to describe our server configuration and how it securely and reliably handles the data encryption, transfer, and storage procedures. We briefly describe how participants enroll in our study in Section V. Section VI discusses some challenges, trade-offs, and limitations to consider when designing and deploying such an SBO system. Finally, we describe related work of similar data collection endeavors in Section VII and offer some concluding remarks in Section VIII.

II. The Science

Our understanding of computer and user behavior, with respect to security and privacy, has largely been based on studies of short duration and narrow focus. These studies have helped guide research over the past 20 years. However, a large-scale field study permits the measurement of users' security and privacy challenges and behaviors with much greater ecological validity than in the lab, where the experimental setting might not reflect users' actual behavior in their natural environment [?]. Furthermore, a long-term longitudinal study would provide data on the frequencies at which users encounter various security and privacy issues. These frequencies would represent risk probabilities, which are a key element of any risk assessment or risk management strategy. Thus, data from such a field study could be used to both inform and prioritize future research agendas.

To fill this need for more ecologically-valid data, we have built the Security Behavior Observatory (SBO): a framework for collecting data from a large panel of end-users whose online behavior will be monitored and analyzed over an extended period of time. This project is now possible thanks to widespread access to broadband Internet connections with reasonable upload speeds. The SBO offers an unprecedented window on real-time, real-life security and privacy behavior in the wild. Through the SBO, we aim to contribute to the evolution of a data-driven science of information security, with immediate applications in usability, economics, and secure system design. We hope this project will encourage discussions on collecting ecologically-valid data in current research practices, and serve as a template for future field studies.

III. Security Behavior Observatory

The Security Behavior Observatory (SBO) is a client-server architecture where participants' client computers are monitored over an extended period of time and upload collected user and computer behavior data to our servers. The initial launch of the SBO will monitor computers running Windows Vista, 7, and 8. We currently focus on these operating systems because their underlying architectures are almost identical (at least for the purposes of data collection), Windows has been the most popular operating system for the past 5 years [18], and desktop usage remains dominant over mobile computing [19]. However, the high-level infrastructure design and our own implementation (both described throughout this paper) can easily be applied to other operating systems (see Section IV-A7). Examples of the data we intend to monitor from hundreds of client machines over several years, with IRB approval and under strict security and privacy safeguards, include those described in the following subsections.

Our architecture is designed to provide data covering as much of the security and privacy space as possible. Some example research questions we intend to examine include:

- How up-to-date are operating systems?
- How long before a clean machine is infected, and how does infection actually occur in the wild?
- What are users' online social network privacy settings? Do they ever change, and why?
- What warning dialog messages do users encounter most often, and how do users respond?

As of this writing, we are performing final tests on most the implemented data collection sensors (see Sections III-A to III-E) while the others are under development (see Sections III-F to III-H). We intend to invite participants to complete questionnaires and interviews to elicit their perspectives on issues and events we observe throughout the study. We are beginning a pilot study on the main client-server SBO infrastructure (see Sections III-I to IV-A) and user study methodology (see Section V). We have purchased the server deployment configuration (see Section IV-B) and hope to begin data collection no later than this summer.

A. Filesystem

As currently designed, the SBO tracks changes to the filesystem, including the added, modified, or deleted file's size, last date modified, permissions, and other related information. [1] This data will help determine, for instance, if malware exists on the system and if so, how it affects machines' file systems, and whether or not users are likely to have noticed its presence.

B. Installed software and operating system updates

The SBO maintains a list of installed applications, their version numbers, and other related data, to determine what privacy or security software (e.g., anti-virus, firewall, adblockers, anonymizers) are installed, and whether they are up to date. The SBO also tracks which (and how soon after their release) operating system updates and patches have been installed. This allows us to measure the duration and severity of client machines' vulnerability to security threats.

C. Processes

The SBO monitors which processes (e.g., programs, applications) are running on clients' machines. It captures when all processes start and terminate, and can provide additional process status information at regular intervals. Primarily, this data will assist with the detection of malware. The SBO also collects general computer usage statistics that may help prioritize future security and privacy work, such as towards frequently-used applications.

D. Security-related events

The SBO also notes general security-related events, such as account-related events (e.g., logins, settings changes, password changes), registry modifications, wireless network authentications, firewall changes, and potential attacks detected by the operating system. This will provide valuable insights on multiple usable security topics, including the security measures users' employ on their computers, potentially dangerous program behavior, and the types and frequency of attacks that occur on home users' machines.

[1] However, we do not collect file or network packet contents since this may be too invasive and bandwidth intensive.

E. Network traffic

The SBO captures all network packet headers sent and received to clients' computers. [1] This data would allow us to detect various network traffic types that may be risky (e.g., peer-to-peer file transfers, dangerous websites) or suspicious (e.g., malware, intrusion attacks). We could thereby verify whether risky Internet behavior is correlated with a higher probability of an attack or infection.

F. Internet browsing behavior

We intend to further monitor users' web browsing behavior by collecting data from Microsoft Internet Explorer, Mozilla Firefox, and Google Chrome. We intend to capture search queries, online social network activity, browsers' and some online accounts' privacy and security settings, as well as other behavior of particular research interest (e.g., social networks, behavioral advertising). One example of possible analyses includes: what are users' privacy settings and behaviors on online social networks, do said settings adequately preserve users privacy, and if not, how could the website be better designed to empower users to more easily and accurately express their desired privacy settings. Another example of planned analysis consists of measuring how often users' actually make purchases derived from behavioral advertising links. This would reveal insights on the actual utility users gain from behavioral advertising, with respect to the privacy cost.

G. Configuration of software and online accounts

We also intend to track the security and privacy settings of users' software (see Section III-B) and online accounts (e.g., Facebook, Twitter). This would provide data regarding users' security and privacy practices. Should users change any such settings during the course of the study, it will be particularly interesting to understand users' motivation for initiating the change. If this could not be inferred with our data (i.e., if we did not detect any particular event preceding the setting modifications), we may send participants a survey or request an interview to inquire further.

H. Warnings

We intend to capture the content of and users' response to warning dialogs that request users make a security- or privacy-related decision. Past research has shown that users frequently do not understand these warnings, let alone know how to respond [5], [20]. This data would bring insights into the warnings users must cope with most frequently and what security and privacy decisions users make when prompted.

I. Security, Privacy, Usability, and Research Requirements

To capture such a wide array of data types over a long period of time, it is crucial we design and build an infrastructure that satisfies several requirements. First, we should minimize the impact of our data collection software on participants' computing and network performance. Thus, since the amount of data we can gather and transmit from clients is limited, we need the ability to be selective with and vary the types of data we collect over time. Second, as we collect and analyze data, we expect our research questions will evolve and require different types of data to be answered. For these reasons, our data collection architecture must be flexible enough to accommodate our changing needs. Third, unlike most experimental software which is typically used for only a short time for specific targeted purposes and environments, any problems caused by our client software could profoundly impact participants' computing experience, due to the breadth, depth, and duration of our data collection. Thus, our system requires a much higher degree of stability and reliability than typical experimental software. With these requirements in mind, we have designed and implemented the following architecture for the SBO.

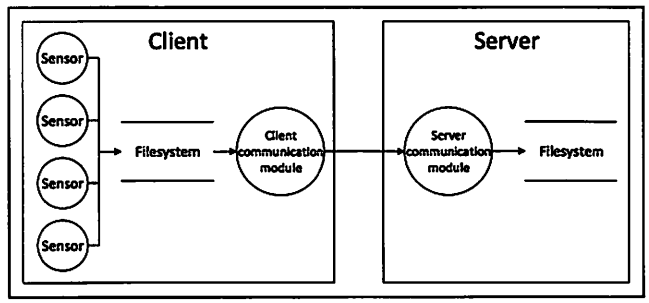


Fig. 1. Data flow between our SBO client and server software.

IV. Architecture

In this section we describe our design and implementation of the SBO architecture from two perspectives. We first illustrate how the data flows from initial collection on the client to storage on our server. Second, we discuss our deployment of servers and each of their roles. For both of these perspectives, we highlight the specific benefits of our design.

A. Data Collection and Flow

Figure 1 shows a data flow diagram of the client-server architecture. Each type of data is collected by a *sensor*, which outputs the data into a common directory. The *client communication module* periodically checks this directory for data files, and compresses, encrypts, and sends them over an SSL-encrypted channel to the *server communication module*. This architecture provides a number of beneficial design features.

1) Silent updates: We use Windows Installer [21] to package all the client software components into a single executable. Windows Installer provides functionality for cleanly installing and uninstalling the software, as well as upgrading. When the client communication module establishes a connection to the server, it first verifies that client software is up to date. If the server determines that it is not, the server provides a link to the current version's installation executable (hosted on our server) to the client. The client then disconnects from the server, downloads the current version of the client software, and checks the file's integrity with an MD5 hash. If the file is intact, the client shuts itself down after silently running

the installer executable in the background. Windows Installer then performs a "major upgrade" whereby the previous version is completely uninstalled before installing the new version. This clean-install approach avoids potential complex problems that can occur with minor upgrades and patches, which can result in an unstable software state. Should the update fail for some reason, Windows Installer will roll back to the previous software version, and the data collection can continue until the client attempts the update again. The entire update process is completely invisible to the user, and does not affect their normal computer usage in any way.

2) Independent sensors: Each type of data of interest (see Section III) is collected by a software *sensor* we have designed and implemented. Each sensor is independent of the rest of the data collection system. This sensor independence provides the following robustness and adaptability benefits. Firstly, if a sensor fails, the other sensors will continue to collect data, which the client communication module will continue to upload to the server. Secondly, if the client communication module fails or the server is unavailable, the client sensors will continue to collect and store data locally, and upload the data once the client communication module has finished restarting and/or the server becomes available. Thirdly, as the data interests for the study change over time, sensors can be silently (see Section IV-A1) and independently added, enabled, configured, disabled, or removed by the experimenters at any time without impacting any other aspect of the client system or our software. Finally, sensors can be implemented in whichever language is best for collecting the desired data. In Windows, this is most often a .NET language (e.g., C#, PowerShell), a command-line batch script, or Java.

3) Least privilege: To ensure clients' security and privacy, the principle of least privilege should be followed whenever possible. However, some data we seek to collect is likely to require administrator access to the client system. Fortunately, our architecture's sensors are independent, so higher privileges can be given only to sensors that require them.

4) Minimal footprint: Since the study's primary goal is to *observe* computer users' typical behavior, we must take care to avoid experimental effects that may influence this behavior. Thus, users should not notice a decrease in computer or network performance during the study. We achieve this in two ways. First, we take care to avoid intensive processing or blocking access to system resources as much as possible. Second, we throttle our client software's data upload speed to at most 192 kilobits per second (kbps), which is half of the slowest upload speed of the least expensive home Internet service plan available (excluding dial-up) in our initial area of participant recruitment (see Section VI-D). A data transfer rate of 192 kbps is equivalent to about 1.44 megabytes per minute, which is not much bandwidth for on-going data collection. This further enforces a minimal footprint by requiring the experimenters to be selective about what types and richness of data we collect. Although necessary, prioritizing what data to collect can be challenging (see Section VI).

5) Minimal user interaction: The use of passive observation to avoid experimental effects also implies we must minimize any user interaction. Our sensors and client communication module execute as Windows *services* [22], which implicitly provides this benefit. A Windows service is an executable program that runs in the background. Similar to Unix daemons, services (or any process or thread they spawn) cannot display any form of user interface (since Windows Vista). Thus, should a program running as a service attempt to display anything to the user, it will not be shown. This acts as a safeguard to ensure that we do not influence the user's normal computing tasks. However, this can be a challenge should the experimenters purposefully desire to interact with the user. This may be desirable should the experimenters wish to test participants' behavior to some stimuli. If future research questions require this, the application containing the stimuli would run as a standard program, not as a service, and would be designed so that any disruption to the user is minimized. However, the stimuli, and any effects it may have on all data being collected, should be carefully considered.

6) Multiple user accounts: Participants' computers may have multiple accounts. The computer's owner may have a separate account for guests, or each member of a household may have a separate account on a common machine. It is crucial that our data collection software run regardless of which user account may be logged in. Fortunately, Windows services can be set to always run when the system starts, independently of which user(s) logs in or logs out. Since our sensors and client communication module run as services, they are assured to run irrespective of which users login. Standard (non-service) applications can also be executed at startup, regardless of which user logs in, by adding a value to the registry [23].

7) Portability: Although we are currently targeting only Windows machines, we may desire the flexibility to collect data from other operating systems (OSes). To do so, we would almost certainly need to write new sensors, since the Windows underlying architecture is completely different from Unix-based operating systems. However, the client and server communication modules are written in Java, and thus should be easily-portable to any OS.

B. Deployment

There are several high-level requirements the SBO must meet. It is crucial that the data is securely and efficiently collected from participants. The data must must also be as securely and reliably stored as possible. Finally, researchers must be able to access and work with the data with as little inconvenience as possible. Figure 2 illustrates the deployment of our server architecture we believe best meets these requirements. We describe below each physical server's role, how data flows from the clients to the various server machines, and the security precautions that are in effect throughout.

1) Data collection server: The data collection server's role is solely to receive data from clients, and periodically send said

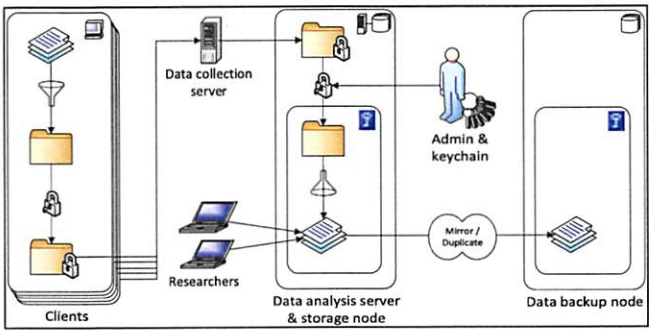


Fig. 2. Our SBO high-level hardware architecture and data flow.

data to the data analysis server when requested. The data flow from clients to the data collection server proceeds as follows:

1) Data is continuously generated on client machines (see Section IV-A).
2) At regular intervals, each client establishes an SSL connection to the data collection server.
3) The client and server mutually authenticate each other by encrypting random numbers with a shared symmetric authentication key [24].
4) When the server is ready to receive data, the client compresses the data, encrypts the compressed data with its symmetric encryption key (which is distinct from the authentication key and unknown to the data collection server), and sends it to the server.
5) The server stores the data locally, still encrypted with the client's encryption key.

2) Data analysis server: The purpose of the data analysis server is to periodically retrieve the encrypted data from the data collection server (and thereafter delete is from the data collection server), store all collected data in the data storage node(s), and provide access to researchers to perform work with the data. To ensure the data's security, it must remain solely on the data analysis server and be accessible only to project administrators and researchers. Thus, the data analysis server can be accessed only through a secure shell (SSH) tunnel originating from the specific IP addresses of the researchers' and administrators' work machines. To remotely access the data analysis server, researchers and administrators must first remotely connect to their work machine and, through said machine, establish an SSH tunnel into the data analysis server. Since the data must never exist anywhere other than our servers, all work with the data must be performed through this SSH tunnel.

As previously mentioned, the data analysis server periodically requests clients' encrypted data from the data collection server. This data transmission occurs over a mutually-authenticated SSL connection [24], and is scheduled to occur at a time of day when the data collection server is least likely to be busy receiving data from clients (e.g. 4:00 AM). The received data is still be encrypted with the corresponding clients' symmetric encryption key (see Section IV-B1). Clearly, the data cannot be analyzed while it is encrypted, but we also cannot risk storing it on the server unencrypted. Section VI-C discusses how we handle the decryption of the data for analysis.

3) Data node(s): Participants' encrypted data is ultimately stored in two places; in the data storage node(s) and data backup node(s). The backup node(s) are located in a physically-separate building from the storage nodes. These nodes are accessible only through the data analysis server, which represents the storage and backup nodes each as a network-attached storage (NAS) ZFS volume [25], [26]. Some key features of ZFS include snapshots (i.e., simple revision control), error detection, protections against data corruption, and storage pools, which allow the single logical ZFS volume to dynamically expand to include additional physical volumes. Thus, as our needs for additional storage grow and we add storage nodes, the additional storage space can simply be added to the existing logical ZFS volume, rather than being represented as a new volume (which would require additional researcher effort to manage and organize the data among multiple logical volumes).

An alternative filesystem could be the Hadoop Distributed File System (HDFS) [27], [28]. With similar benefits as ZFS, HDFS also allows data processing and analysis to be parallelized by distributing the data and computations among the nodes to more quickly process the data. However, HDFS cannot be treated as a traditional logical volume; it must be accessed through a special interface (i.e., API). Furthermore, programs must be written in a particular way to leverage the parallelism benefits of HDFS. Thus, Hadoop may require significant investment costs of time and effort. Furthermore, Hadoop would be beneficial when there are several data storage nodes which can perform computations in parallel. However, we currently need only a single storage node with an 8-core CPU to begin data collection, so the parallelism gains are not worth the time and effort investment. As the size of our panel and collected data grows to require several storage nodes, we will consider using Hadoop or another data storage and management technology instead of ZFS.

V. User Study Methodology

With the aforementioned infrastructure in place and having already obtained approval from our institutional review board for these procedures, we can solicit users to participate in our panel. Our primary method of finding participants is through a recruitment service for which people have asked to be notified about experiments. Potential participants will be asked a number of pre-screening questions. Participants must be over 18 and own a Windows Vista, 7, or 8 personal computer. We send interested persons an e-mail with a link to where they can complete the following initial enrollment tasks:

1) Reading and completing a consent form, which clearly informs users that we may monitor all activity on their computer and collect any data except for the contents of personal files, e-mails sent or received, content of documents on Google Docs, and bank card numbers.

2) Providing the names and e-mail addresses of others who also use the computer to be instrumented, so we can obtain their consent.
3) Completing an initial questionnaire
4) Download and install our data collection client software

Once these steps are complete, and all the other users of the computer have provided their consent, the participant is awarded a $30 Amazon.com gift card, since we can now collect data from the participant's machine. Participants thereafter receive a $10 gift card for every month our client software continues to upload data from their computer. This data transmission occurs silently in the background without requiring any action from participants. We also send periodic e-mails informing participants that either everything is working fine, which of the above enrollment tasks still need to be completed, or if we are not receiving data from their machine. If we do not receive data from users for 3 months, we may cease their participation.

VI. Discussion

There are a number of issues warranting careful consideration when collecting data from hundreds of participants' personal machines.

A. Participant IDs

It is necessary for our server to be able to identify which client belongs to which participant for several reasons. Primarily, every client machine must locally store its unique encryption and authentication keys to encrypt its data and securely communicate with our server (see Section IV-B1). We also need to verify users' continued participation (i.e. uploading data), so we can compensate them or remind them that they need to keep their computer on and connected to the Internet to continue participating. Additionally, we wish to be able to perform participant-specific data analyses to evaluate whether particular demographics are correlated with certain behaviors. We also wish to perform longitudinal analyses across specific machines' lifetimes (e.g. time before a malware infection).

The easiest way to identify client machines is to prompt the user for their assigned ID when they first install our client software. However, because our software runs as a Windows service (see Section IV-A5), it cannot display any user interface elements, and thus cannot interact with the participant. We solved this problem by creating an independent program that verifies that the stored participant ID and keys are valid, and if they are not, the program prompts the user. This program is run as a standard process, independently of any of our services, which allows it to interact with users if necessary. However, since the program does not run as a service, it does not execute within the same workspace or with the same privileges as the rest of the client software. Thus, we had to resolve various challenges regarding program-service communication, differing access control privileges, and synchronization.

B. Ethics & participant privacy

Although true for all user studies, it is critical that an institutional review board (IRB) approve the study's methodologies and procedures to ensure participants' are treated ethically and their data is kept confidential and secure. We spent considerable time iterating over our consent procedures with our IRB before their approval. However, many review boards do not have the expertise to understand the specific security and privacy challenges that may arise. Thus, the burden lies on the experimenters to consider carefully which data they are willing to collect and hold in trust, and to weigh the risk of a compromise with the value of such data to the advancement of the community's knowledge. Regarding de-identification, participants are assigned a random ID, which decouples their uploaded data from their provided personal information. We are also considering additional anonymization strategies and weighing their costs (e.g., loss of data richness, client-side computational loads) against possible threat models (e.g., client, network, server attacks).

C. Data Security

Given the potential sensitivity of the data our infrastructure collects and transmits from client machines across the Internet and stores on our servers, the data's security and confidentiality must be carefully considered and strictly enforced. In our implementation, we employ reliable end-to-end data encryption. Every client is assigned a unique encryption key. Client-side keys are stored in a permission-secured file on the client. To obtain the keyfile, an attacker would need access to the client with elevated privileges. The value of a participant's keys is unclear in this scenario, since this attacker could install malware to collect more sensitive information (e.g., passwords, bank account numbers) than we do.

Before transmitting the data, the client communication module compresses and encrypts the data with 128-bit AES [29] using Cipher Block Chaining mode [30] and PKCS5 Padding [31]. This encrypted data is sent to the server through an SSL connection and stored, still encrypted with the client's unique key. Once the encrypted data is received by the server, the client-side copy is deleted.

Although methods for computing on encrypted data exist (e.g., homomorphic encryption), our analyses across multiple sensors' data longitudinally across time are likely to be complex enough that they would not be practically feasible with such solutions. Instead, one researcher with access to all the clients' keys (stored in an isolated and secured MySQL database owned by a separate, dedicated, and tightly-secured user account) will decrypt and decompress each client's data into a TrueCrypt volume, to which all project researchers will have the key to analyze the data. Unencrypted data may temporarily exist in memory while and after working with it. However, the data must remain on the data storage nodes, which can be accessed only through a secure shell to the data analysis server from the specific IP addresses of the researchers' own campus machines. No other connections to this server are permitted. We feel that this is the best solution

for offering sufficient data security without overburdening researchers with complex, time-consuming procedures to access the data.

D. Client upload bandwidth

Given the wide breadth and depth of data we ideally wish to collect, the limit on how much data we can realistically collect is the clients' upload data rate. We must restrict the amount of data we upload from participants' machines to avoid a noticeable reduction of their Internet connection bandwidth.

To calculate this maximum upload rate, we first found the lowest data upload rate of Internet plans in our area, which is 384 kbps (kilobits per second). To avoid a noticeable impact on participants' network performance, we should use only a fraction of this total upload rate. By using only half, the actual data rate our software should be allowed to use is 192 kbps, or 24 KBps (kilobytes per second).

To ensure we do not surpass our desired bandwidth usable, we throttle clients' data upload speed by interleaving data transmission and sleep commands. For example, to achieve an upload rate of 24 KBps, the client process could alternate between uploading 6 KB and then sleeping for 250 ms until all the data is transferred. Sleeping between data transmissions should cause the OS to flush the uploaded data stream (i.e., actually send the data to our server rather than leave it in the client's network buffer in case our process adds more data to be sent) and free the network bandwidth and processing cycles for other applications until our application resumes. We hope to add adaptive throttling functionality to upload either more data when the network and computer are idle or less when the machine and Internet are in heavy use. However, this risks biasing the lower-priority types of data that would be collected only for clients with more computing capability and network bandwidth, which might be higher-income participants.

Given the massive amount of data this infrastructure can collect about client machine behavior (see Section III), it is important to employ techniques to minimize the physical size of the data transferred and stored. One such technique involves sensors that perform periodic snapshots, which should only log differences between the previously-recorded and current state, rather than always logging the complete current state. This is particularly important for snapshot sensors that gather large amounts of data for every snapshot. For example, when monitoring the filesystem, we may want to know all files' permissions, size, date first created and last modified, and potentially an MD5 hash. Such a complete list could easily be at least several hundred megabytes in size, which is an unreasonable amount of data to regularly transfer and store. However, only logging differences between the previous and current snapshot would likely be a realistically manageable size.

Another technique we use to reduce our data logs' footprint is the Binary JSON (BSON) data format [32]. The BSON data format is ideal for our infrastructure's purpose, since BSON is specifically designed to minimize spatial overhead in data transfers and storage, be easily traversable, and be efficient to encode and decode. We use BSON to log data that is either hierarchical in nature or may contain variable data elements (i.e., where there could be many null values if the data were logged in a flat table structure).

Even with data minimization techniques such as these, we anticipate having to make difficult decisions about which types of data to prioritize. However, while performing our preliminary data analysis, we may observe phenomena that we wish to further explore, but may be unable to because we had previously chosen not to enable the relevant sensors. To illustrate, suppose we initially choose to focus on malware infection. Thus, the minimum data we would need to collect appears to be network packet traffic, filesystem changes, and the executing processes. However, there are a number of scenarios where we would be missing data. For example, the network packet sensor would be unable to detect malware downloaded through SSL. Without the warning dialog sensor, we would not know if the user was ever warned from visiting a website, or prompted to download or install the malware. Without tracking security-related events, we may be unable to detect changes to the Windows firewall or other computer security settings. Admittedly, it may be possible to make some inferences from the sensors we did enable, but our understanding of the malware-infection events would certainly be incomplete. However, since we cannot possibly collect all the data, it is clear that there will be some limitations to the analysis we will be able to perform. Still, the choices of which data to collect in tandem will need to be made carefully, since poor decisions could pose unnecessary additional challenges when analyzing the data.

E. Server specifications & other cost considerations

There are a number of significant costs involved in conducting such a long-term data collection study. First and foremost, as discussed in Section IV-B, at least four physical server machines are required to begin the study; data collection, analysis, storage, and backup. Each of these machines have different specification requirements which should be carefully considered before committing to a purchase. The importance we place on each server's components are noted in Table I. Our reasoning for these priorities is as follows. The data collection server would benefit from several processor cores for receiving data from multiple clients at once, but these do not necessarily need to be the highest-possible clock speed (hence the *medium* rating). Our server software does not require much memory. This server's storage requirements are also relatively little, since it needs to retain only data collected over a few days, in case the data analysis server is temporarily delayed from removing the data (see Section IV-B2). The data analysis server itself also requires relatively little storage space for the operating system, data transfer, manipulation, and analysis applications and scripts. However, the data analysis server does require significant memory and processing power for its namesake purpose. The data storage nodes require at least a reasonably powerful processor and memory for data transfers to occur rapidly (and to quickly perform data processing tasks

TABLE I
IMPORTANCE OF EACH COMPONENT FOR EACH SERVER (SEE SECTION IV-B).

Server	Processor	Memory	Storage
Data Collection	Medium	Low	Low
Data Analysis	High	High	Low
Data Storage & Backup	Medium	Medium	High

if HDFS is in use). Of course, the storage nodes must have sufficient space to hold all the data to be collected. We use the following calculation to estimate our long-term storage needs. Assuming each participant uploads approximately 24 KBps (kilobytes per second) to our server (see Section VI-D), this equates to 377.4 gigabytes (GB) per year per participant. In our study's first year, we intend to have 100 users participating in our study. Thus, 100 participants each generating 377.4 GB per a year results in about 37.74 terabytes (TB) of data. We have obtained a minimum hardware configuration that satisfies the above requirements, and can be expanded for further data collection beyond one year, for around $35,000 (USD).

In addition to the server configuration costs, there are also on-going costs to be budgeted. Primarily, the participants require compensation. We are currently offering $30 for completing the necessary initial tasks to begin participating in the study (see Section V), and $10 for every month they continue to participate (e.g. we continue to regularly receive data from their machine). These costs add up quickly, since each participant costs $150 per year, so 100 participants cost $15,000 for a single year. Furthermore, if we cannot initially attract enough participants, we may need to consider increasing this stipend, which would further increase costs. Other on-going costs that should be considered include the technical administration and maintenance of the server hardware as well at least one dedicated project leader (and ideally a support team) to build and continuously refine the software and sensors, oversee the smooth execution of the study, and lead the data management (see Section VI-C) and analysis.

F. Study Limitations

Despite the wide scope of this infrastructure and study, there are some limitations which must be noted. Firstly, we are currently targeting only participants using Windows Vista, 7, or 8. Our focus on modern Microsoft operating systems (OS) means that we may not observe phenomena that occur on Unix-based OSes. Furthermore, mobile devices and tablets are growing in popularity [19]. Users' behavior and risk with respect to privacy and security with these devices may differ significantly than with traditional desktops or laptops. For future work, we could build sensors to collect data on Unix-based systems' usage, as well as mobile devices and tablets. Fortunately, our client communication module (see Section IV-A) can run on any system that supports Java (which includes most modern operating systems, see Section IV-A7).

In our user study, we ask users to install our software only on their one main Windows computer, because we are interested in observing the breadth of behaviors of multiple independent machines. However, people often have multiple devices through which they may have privacy and security challenges, including mobile devices and tablets. Thus, a complete in-depth examination of participants' behavior would require instrumenting all of a user's devices. This would be particularly challenging, given the multiple OS architectures participants may use. It is also unclear whether or not a participant's work machines should be instrumented. This would be required for a truly complete understanding of users' computing experience and behavior, but it would require participants' employers' consent, since data collection software on these machines may unintentionally capture the employers' intellectual property or other sensitive data. In any case, as our user study is currently designed, even though we capture a wider breadth of data than previous studies, we still risk missing some behaviors that occur on participants' non-instrumented devices. In future work, we hope to also collect data from mobile devices and tablets. We hope to reuse our client communication module to collect data from devices that support Java (see Section IV-A7).

As previously mentioned (see Section V), we offer participants $30 to complete the initial enrollment, and $10 per month of continued participation. This may bias our sample towards lower-income and privacy unaware or unconcerned participants. We will be able to confirm the former by asking participants to self-disclose their income in our enrollment questionnaire. However, it is unclear if any affordable level of compensation could attract higher-income participants. Additional compensation may also fail to attract privacy-concerned users, since users willing to be monitored are likely to do so for relatively small immediate short-term gains [33], [34].

VII. RELATED WORK

Lalonde Lévesque et al. [14] performed a 50-subject 4-month study of the effectiveness of an anti-virus software (AV) with respect users' computer behavior. Participants were given a Windows 7 laptop with Trend Micro's premium home anti-virus software and various monitoring software and scripts pre-installed. Every month, participants were required to meet with the experimenters to complete a survey about their computer usage and for the data to be collected from the machines. The AV detected 95 distinct threats on 38% of machines during the study, the vast majority of which were trojans, which is comparable with publicly-available statistics [14]. The authors' found 18 threats (e.g., 7 unwanted software, 9 adware, one malware, and another suspected as malware) that the AV failed to detect on 20% of machines. Participants with a greater computer expertise were more at risk of being exposed to threats than less computer-knowledgeable users. Furthermore, the authors reported that visiting sports and Internet infrastructure sites were more associated with a higher rate of infection, while visiting sites with pornographic or questionable content was less so. Although their methodology bares some resemblance to ours, there are several important differences between this and our study. Most obviously, our target sample size and study duration will both be several times

greater (i.e., hundreds of participants over several years). A more fundamental difference lies in our respective experimental models. Their study follows a "clinical trials" experimental model from medical research, whereby subjects are given a *treatment* (i.e., AV) and its effects are monitored over time. In contrast, our study's primary purpose is to passively observe our participants' and their machines' behavior by collecting a very wide array of security- and privacy-related data (see Section III) without any form of experimental intervention whatsoever.

Van Bruggen et al. [16] instrumented 149 student participants' Android smartphones with software that collected two types of data over two weeks; usage statistics (e.g., data usage, text messages, screen lock) and participant responses to weekly surveys on various topics. They found that 65% of their participants used a phone locking mechanism; 51% used the Android pattern lock and 14% chose a text password or PIN. They found no correlations for this choice with gender, previous phone type, text message frequency, data usage, or personality traits. Upon being surveyed about their password sharing behavior, 19% responded that they shared the password to their phone, while 63% shared passwords for other devices or services. The authors suggested that participants may place greater value the security of the mobile device over other devices or services. The authors later employed intervention messages based on incentives, morality, and deterrence to encourage users to either adopt a screen lock or upgrade to a more secure lock (e.g., from the pattern lock to a text password). The interventions did not appear result in many conversions. The authors concluded that the cost associated with targeting the users and implementing the interventions may not be worth the limited results. Our study does not currently target smartphones or attempt to modify users' normal computing behavior, we may consider testing attempts to assist, inform, and persuade users to take security precautions, should our data suggest that many users leave their computers dangerously vulnerable or otherwise behave insecurely. We also hope to expand our study in the future to include a broader range of devices, including smartphones and tablets.

Florêncio and Herley [12] collected Internet password data from over a half-million people over 85 days. This data was collected voluntarily from users of the Windows Live Toolbar. Their component hashed and stored passwords users' entered in web pages' password input fields, as well as the related URL, the passwords' bit strength, and other data. The authors also tracked incidents of password re-use as follows. Every time a character was typed into the web browser, their system hashed and compared each sequence of the last 7 to 16 typed characters to each of the stored password hashes that had been collected thus far. If a match was found and the current website's URL did not match the stored password hash's URL, then a password re-use event was logged. The authors reported many interesting findings of users' real-world password use, including the following highlights. Users had an average of 25 different online accounts, and typed 8 passwords on an average day. Users maintained an average of 6.5 distinct passwords, each across 3.9 separate websites. Users predominately chose lowercase-only passwords unless required otherwise. Finally, based on their study's results, the authors estimated that 0.4% of Internet users enter passwords on known phishing sites every year. Clearly, this study provided the research community with great insight into live user behavior, despite having only collected data for 3 months. However, unlike this study, we currently do not intend to collect data on participants' passwords (see Section VI-B), given the risks (despite our security precautions) of storing such data for a study spanning several years.

De Luca et al. [11] observed 360 people's interactions with automated teller machines (ATMs). A single experimenter personally monitored 60 people without their knowledge at each of 6 different banks' ATMs at varied times of day. The goal of the study was to better understand the context of ATM usage without capturing users' actual PINs. The data collected from each ATM interaction included the location, gender, time of day, interaction time, queue length, security measures taken by the user, and repeated PIN entry. The authors found that users were distracted in 11% of interactions, and that 65% of users made no effort to protect their PINs from observation attacks, either out of negligence, inability (e.g. carrying bags), or social context (e.g., did not want to imply mistrust in a nearby friend or family member). These and other results (including from interviews) led the authors to conclude that security should not rely on the user whenever possible, should be compatible with the social context, and PIN memorability is not a problem for most people, but it is severe when it occurs, since forgetting led to unsafe practices. The authors also shared lessons learned from the field observation study, including the utility of conducting pilot studies to test and refine the types and methods of data collection, abiding by strict codes of conduct to ensure ethical and consistent data collection, and importance of field studies in measuring users' actual behavior, which can differ from users' stated behavior in surveys and interviews.

VIII. Conclusion

Research to date has brought to light many usable security and privacy challenges computer users face, but there remain many unknowns, particularly with respect to home computer usages. Capturing data on these challenges in the wild as they occur naturally is essential if we are to conduct research and foster innovations with the greatest impact in improving the security and privacy of users and their machines. The Security Behavior Observatory (SBO) aims to collect said highly ecologically valid data on multiple security and privacy topics from hundreds of users' home computers over several years. This paper has specified the SBO client-server architecture, the benefits of our design decisions, and the challenges and trade-offs involved in building a system with the reliability, robustness, and flexibility required for a study of this lengthy duration and grand scope. We hope the data collected will yield insights on a wide variety of security and

privacy challenges, and guide future research efforts towards solving the challenges users actually face in the wild.

REFERENCES

[1] A. Adams and M. Sasse, "Users are not the enemy," *Communications of the ACM*, vol. 42, no. 12, 1999.

[2] A. Whitten and J. Tygar, "Why Johnny can't encrypt: A usability evaluation of PGP 5.0," in *USENIX Security Symposium*, 1999.

[3] R. Biddle, S. Chiasson, and P.C. van Oorschot, "Graphical passwords: Learning from the first twelve years," *ACM Computing Surveys*, vol. 44, no. 4, 2012.

[4] A. Forget, "A world with many authentication schemes," Ph.D. dissertation, School of Computer Science, Carleton University, 2012.

[5] C. Bravo-Lillo, L. Cranor, J. Downs, and S. Komanduri, "Bridging the gap in computer security warnings: A mental model approach," *Security & Privacy*, vol. 9, no. 2, 2011.

[6] J. Hong, "The state of phishing attacks," *Communications of the ACM*, vol. 55, no. 1, 2012.

[7] M. Jakobsson, "The human factor in phishing," *Privacy & Security of Consumer Information*, 2007.

[8] I. T. L. Review, "G.r. newman and m.m. mcnally," US Department of Justice, Tech. Rep. 210459, July 2005.

[9] M. Brewer, "Research design and issues of validity," *Handbook of research methods in social and personality psychology*, pp. 3–16, 2000.

[10] B. Berendt, O. Günther, and S. Spiekermann, "Privacy in e-commerce: Stated preferences vs. actual behavior," *Communications of the ACM*, vol. 48, no. 4, April 2005.

[11] A. De Luca, M. Langheinrich, and H. Hussmann, "Towards understanding ATM security – a field study of real world ATM use," in *Symposium on Usable Privacy and Security (SOUPS)*. ACM, 2010.

[12] D. Florêncio and C. Herley, "A large-scale study of WWW password habits," in *International World Wide Web Conference (WWW)*. ACM, May 2007.

[13] M. Mazurek, S. Komanduri, T. Vidas, L. Bauer, N. Christin, L. Cranor, P. Kelley, R. Shay, and B. Ur, "Measuring password guessability for an entire university," in *Conference on Computer and Communications Security (CCS)*. ACM, 2012.

[14] F. Lalonde Lévesque, J. Nsiempba, J. Fernandez, S. Chiasson, and A. Somayaji, "A clinical study of risk factors related to malware infections," in *Conference on Computer and Communications Security (CCS)*. ACM, 2013.

[15] N. Christin, S. Egelman, T. Vidas, and J. Grossklags, "It's all about the benjamins: An empirical study on incentivizing users to ignore security advice," in *International Conference on Financial Cryptography and Data Security (FC)*. Springer, 2011.

[16] D. Van Bruggen, S. Liu, M. Kajzer, A. Striegel, C. Crowell, and J. D'Arcy, "Modifying smartphone user locking behavior," in *Symposium on Usable Privacy and Security (SOUPS)*. ACM, 2013.

[17] G. Friedland, G. Maier, R. Sommer, and N. Weaver, "Sherlock holmes' evil twin: On the impact of global inference for online privacy," in *New Security Paradigms Workshop (NSPW)*. ACM, 2011.

[18] StatCounter.com, "Top 7 operating systems from july 2008 to nov 2013," October 2013, http://gs.statcounter.com/#os-ww-monthly-200807-201311.

[19] ——, "Mobile vs. desktop from july 2008 to oct 2013," accessed October 2013 2013, http://gs.statcounter.com/#mobile_vs_desktop-ww-monthly-200807-201311.

[20] S. Egelman, L. Cranor, and J. Hong, "You've been warned: an empirical study of the effectiveness of web browser phishing warnings," in *Conference on Human Factors in Computing Systems (CHI)*. ACM, 2008.

[21] Microsoft Corporation, "Windows Installer (Windows)," November 2013, http://msdn.microsoft.com/en-us/library/cc185688.aspx.

[22] ——, "Services (Windows)," October 2013, http://msdn.microsoft.com/en-us/library/windows/desktop/ms685141.aspx.

[23] ——, "INFO: Run, RunOnce, RunServices, RunServicesOnce and Startup," November 2013, http://support.microsoft.com/kb/179365.

[24] A. Menezes, P.C. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*. CRC Press, 1996, ch. 10, p. 402, http://cacr.uwaterloo.ca/hac/.

[25] S. Watanabe, *Solaris 10 ZFS Essentials*, 1st ed. Prentice Hall, 2010.

[26] "OpenZFS," accessed November 2013, http://open-zfs.org.

[27] T. White, *Hadoop: The Definitive Guide*, 3rd ed. O'Reilly, 2012.

[28] Apache Software Foundation, "Welcome to apache hadoop," https://hadoop.apache.org/, accessed November 2013.

[29] Federal Information Processing Standards (FIPS), "Advanced encryption standard," National Institute of Standards and Technology (NIST), Tech. Rep. 197, November 2001, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

[30] ——, "Des modes of operations," National Institute of Standards and Technology (NIST), Tech. Rep. 81, December 1980, http://www.itl.nist.gov/fipspubs/fip81.htm.

[31] R. Laboratories, "Pkcs #5: Password-based cryptography standard," accessed November 2013, http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/pkcs-5-password-based-cryptography-standard.htm.

[32] "Bson - binary json," accessed November 2013, http://bsonspec.org/.

[33] A. Acquisti, "Privacy in electronic commerce and the economics of immediate gratification," in *Conference on Electronic Commerce*. ACM, 2004.

[34] A. Shostack and P. Syverson, "What price privacy?" in *The Economics of Information Security*. Kluwer Academic Publishers, 2004.

PI: CRANOR

ARO Annual Progress Report
D) Scientific progress and accomplishments

I. Statement of the Problem Studied

So far, the research community has been relying on specific experiments or surveys to understand how users respond to specific security threats. Lab experiments and ad-hoc field experiments have offered insights into, for instance, how users fall to phishing or malware scams [1], [4], [5] or how users ignore security and privacy alerts [2], [6], [7]. These experiments offer a useful but narrow slice of user behavior under particular experimental settings. Developing scientific models of user behavior in response to security threats in a natural, real-world setting, is ultimately what we need to design sound security defenses.

Our ability to design appropriate information security mechanisms and sound security policies depends on our understanding of how end-users actually behave: End-users are not only the victims of cyber-threats, but also the passive participants in cyber-attacks originating from their own resources or exploiting their limitations. Models of users' behavior require extensive data collection; without that data, there cannot be a science of information security. To fill this gap, we are establishing the Security Behavior Observatory (SBO); a repository of data from a large panel of end-users whose online computing behavior will be captured, monitored, and analyzed over an extended period of time. This panel will offer an unprecedented window on real-time, real-life security and privacy behavior "in the wild." Through it, we aim at contributing to the evolution of a data-driven science of information security, with immediate applications in usability, economics, and secure system design.

The SBO will collect data about users' installation of and interactions with security products (e.g., anti-virus products, firewalls), their response to security-related alerts offered by browsers and operating systems, the websites they visits and the files they download that may expose them to malware and other security threats, as well as other security- and privacy-related behaviors. The SBO is currently targeting Windows computer users, but we plan to expand our methodology to other operating systems as well as mobile devices. Researchers will have opportunities to survey and interview panel members periodically to gain insights into why users behave in particular ways. In addition, researchers can use the observatory's infrastructure to not only collect data, but also to push stimuli (e.g, a simulated phishing email) and interventions (e.g. an alert about a new threat) out to panel members in order to collect data on subsequent changes in behavior. The data we will collect will provide a foundation on which sound models of user and attacker behavior. These models will eventually lead to the scientific design of intervention policies and technical countermeasures against security threats.

The SBO has multiple scientific objectives. First, our panel will provide fertile grounds for multi-disciplinary research in computer science, human-computer interaction, behavioral sciences, and economics focused on understanding both end-user and attacker behaviors and strategies. This will lead to the creation of tools and products that can help users better protect themselves, and to tools and policies that better protect critical infrastructure. Thus, the SBO will not only lead to ground-breaking academic research, but it would also lead to actionable recommendations for policy makers and firms. Second, our work to develop the SBO provides insights into the design of sound measurement methodologies of end-user security behavior. Users' response to security and privacy threats remains largely unknown, in large part due to the significant difficulties in recruiting and monitoring users while addressing privacy concerns.

II. Summary of the Most Important Results

By the very nature of this project, which requires building infrastructure to collect data, then collecting, and eventually analyzing the data, there is a long setup phase. As a result, the project will be much more publication-centered toward the second half of its projected duration. However, we are confident that the more secure, reliable, and robust infrastructure as well as the greater number and quality of data collection sensors we have built and are refining will provide more and better data, resulting in more and stronger publications. Towards this end, we report the following accomplishments.

A. Dedicated Server Infrastructure

Designing and building the SBO requires attention to factors less frequently considered in shorter-term, more focused studies. The infrastructure must be sufficiently scalable, reliable, and robust to collect the required size, breadth, and depth of data over the study's lengthy duration. In addition, given the sheer amount and detail of behavioral data we will collect, we must carefully consider how best to maintain the security and privacy of participants' data while inconveniencing as little as possible researchers' working with the data. We also require the flexibility to adjust the types of data we collect throughout the study, since research needs will invariably change as earlier data analysis leads to further lines of inquiry.

Thus, we have designed, purchased, and deployed a dedicated server architecture that we believe best meets these requirements (see Figure 1). We summarize below each physical server's role, how data flows from the clients to the various

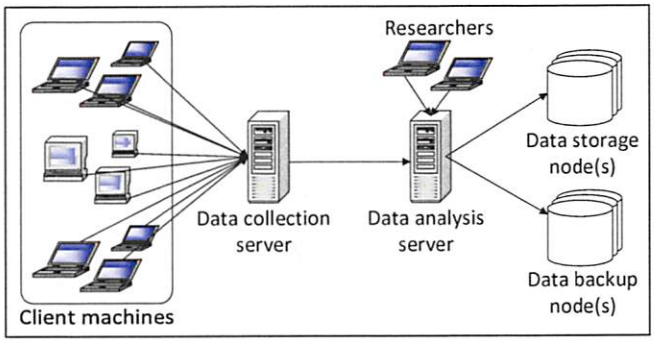


Fig. 1. Our SBO high-level hardware architecture and data flow.

server machines, and the security precautions that are in effect throughout. For more details on our client-server architecture and data security procedures, see our technical report [3].

1) Data collection server: The data collection server's role is solely to receive data from the panel's client machines, and periodically send said data to the data analysis server when requested. Data is encrypted before it is sent from the client to the data collection server (through an SSL secured tunnel). This server then stores the data locally, still encrypted with the client's encryption key.

2) Data analysis server: The data analysis server periodically retrieves the encrypted data from the data collection server (and thereafter deletes it from the data collection server), and stores it in the data storage node(s). To maintain data security, it must remain solely on the data analysis server and be accessible only to project administrators and researchers. Thus, the data analysis server can be accessed only through a secure shell (SSH) tunnel originating from the specific IP addresses of the researchers' and administrators' work machines. To remotely access the data analysis server, researchers and administrators must first remotely connect to their work machine and, through said machine, establish an SSH tunnel into the data analysis server. Since the data must never exist anywhere other than our servers, all work with the data must be performed through this SSH tunnel.

3) Data node(s): Participants' encrypted data is ultimately stored in two places; in the data storage node(s) and data backup node(s). The backup node(s) are located in a physically-separate building from the storage nodes, both for security reasons and as a contingency for catastrophic events.

B. Data Collection Sensors

To best understand the nature of users' security and privacy challenges in computing, we must capture many types and depths of data. To capture such a wide array of data types over a long period of time, it is crucial we design and build an infrastructure that satisfies several requirements. First, we should minimize the impact of our data collection software on participants' computing and network performance. Thus, since the amount of data we can gather and transmit from clients is limited, we need the ability to be selective with and vary the types of data we collect over time. Second, as we collect and analyze data, we expect our research questions will evolve and require different types of data to be answered. For these reasons, our data collection architecture must be flexible enough to accommodate our changing needs. Third, unlike most experimental software which is typically used for only a short time for specific targeted purposes and environments, any problems caused by our client software could profoundly impact participants' computing experience, due to the breadth, depth, and duration of our data collection. Thus, our system requires a much higher degree of stability and reliability than typical experimental software.

Thus, we have carefully designed our client data collection software to support many features necessary to provide us with the aforementioned requirements. These features are discussed in detail in our technical report [3]. One feature is support for data collection sensors that run independently of each other. This sensor independence provides the following robustness and adaptability benefits. Firstly, if a sensor fails, the other sensors will continue to collect data. Secondly, as the data interests for the study change over time, sensors can be silently and independently added, enabled, configured, disabled, or removed by the experimenters at any time without impacting any other aspect of the client system or our software. Finally, sensors can be implemented in whichever language is best for collecting the desired data.

We have been developing numerous sensors to collect many types of data, of which the following are ready for deployment in our pilot study (see Section II-C).

1) Filesystem: As currently designed, the SBO tracks changes to the filesystem, including the added, modified, or deleted file's size, last date modified, permissions, and other related information. [1] This data will help determine, for instance, if malware exists on the system and if so, how it affects machines' file systems, and whether or not users are likely to have noticed its presence.

2) Installed software and operating system updates: The SBO maintains a list of installed applications, their version numbers, and other related data, to determine what privacy or security software (e.g., anti-virus, firewall, ad-blockers, anonymizers) are installed, and whether they are up to date. The SBO also tracks which (and how soon after their release) operating system updates and patches have been installed. This allows us to measure the duration and severity of client machines' vulnerability to security threats.

3) Processes: The SBO monitors which processes (e.g., programs, applications) are running on clients' machines. It captures when all processes start and terminate, and can provide additional process status information at regular intervals. Primarily, this data will assist with the detection of malware. The SBO also collects general computer usage statistics that may help prioritize future security and privacy work, such as towards frequently-used applications.

4) Security-related events: The SBO also notes general security-related events, such as account-related events (e.g.,

[1] However, we do not collect file or network packet contents since this may be too invasive and bandwidth intensive.

logins, settings changes, password changes), registry modifications, wireless network authentications, firewall changes, and potential attacks detected by the operating system. This will provide valuable insights on multiple usable security topics, including the security measures users' employ on their computers, potentially dangerous program behavior, and the types and frequency of attacks that occur on home users' machines.

5) Network traffic: The SBO captures all network packet headers sent and received to clients' computers. [1] This data would allow us to detect various network traffic types that may be risky (e.g., peer-to-peer file transfers, dangerous websites) or suspicious (e.g., malware, intrusion attacks). We could thereby verify whether risky Internet behavior is correlated with a higher probability of an attack or infection.

6) Internet browsing behavior: We intend to further monitor users' web browsing behavior by collecting data from Microsoft Internet Explorer, Mozilla Firefox, and Google Chrome. We intend to capture search queries, online social network activity, browsers' and some online accounts' privacy and security settings, as well as other behavior of particular research interest (e.g., social networks, behavioral advertising). One example of possible analyses includes: what are users' privacy settings and behaviors on online social networks, do said settings adequately preserve users privacy, and if not, how could the website be better designed to empower users to more easily and accurately express their desired privacy settings. Another example of planned analysis consists of measuring how often users' actually make purchases derived from behavioral advertising links. This would reveal insights on the actual utility users gain from behavioral advertising, with respect to the privacy cost.

C. Pilot Study

Now that we have a secure, reliable, and scalable dedicated server infrastructure (see Section II-A) on which to store and manage the massive amount of data the SBO clients' data sensors (see Section II-B) will collect, we are now launching a pilot study with a small number of participants from the general population to test our data collection infrastructure. The pilot study will be the ideal beta test for our SBO study participant recruitment and enrollment process, as well as for our data collection systems to ensure they will have a minimal impact on the performance of clients' machines while providing us with sample data to test our data collection and analysis methodologies. While we cannot predict the number and severity of problems that may arise, we hope that there will be few such problems and that we will be ready to begin full data collection from 50-100 client machines soon. In the meantime, we hope to compile the lessons learned about building and launching such a large-scale field study into an early publication. We also hope the pilot will go smoothly enough that we could submit a paper with early results from the short-term data collected.

REFERENCES

[1] N. Christin, S. Egelman, T. Vidas, and J. Grossklags. It's all about the benjamins: An empirical study on incentivizing users to ignore security advice. In *International Conference on Financial Cryptography and Data Security (FC)*. Springer, 2011.

[2] S. Egelman, L. Cranor, and J. Hong. You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In *Conference on Human Factors in Computing Systems (CHI)*. ACM, 2008.

[3] A. Forget, S. Komanduri, A. Acquisti, N. Christin, L. Cranor, and R. Telang. Security behavior observatory: Infrastructure for long-term monitoring of client machines. Technical Report CMU-CyLab-14-009, CyLab, Carnegie Mellon University, 2014.

[4] S. Y. N. Christin and K. Kamataki. Dissecting one click frauds. In *Conference on Computer and Communications Security (CCS)*. ACM, 2010.

[5] S. Sheng, M. Holbrook, P. Kumaraguru, L. Cranor, and J. Downs. Who falls for phish? a demographic analysis of phishing susceptibility and effectiveness of interventions. In *Conference on Human Factors in Computing Systems (CHI)*. ACM, 2010.

[6] J. Sunshine, S. Egelman, H. Almuhimedi, N. Atri, and L. Cranor. Crying wolf: an empirical study of ssl warning effectiveness. In *USENIX Security Symposium*, 2009.

[7] M. Wu, R. Miller, and S. Garfinkel. Do security toolbars actually prevent phishing attacks? ACM, 2006.

Composability of Big Data and Algorithms for Social Networks Analysis Metrics

PI(s): Jürgen Pfeffer

Scientific progress and accomplishments

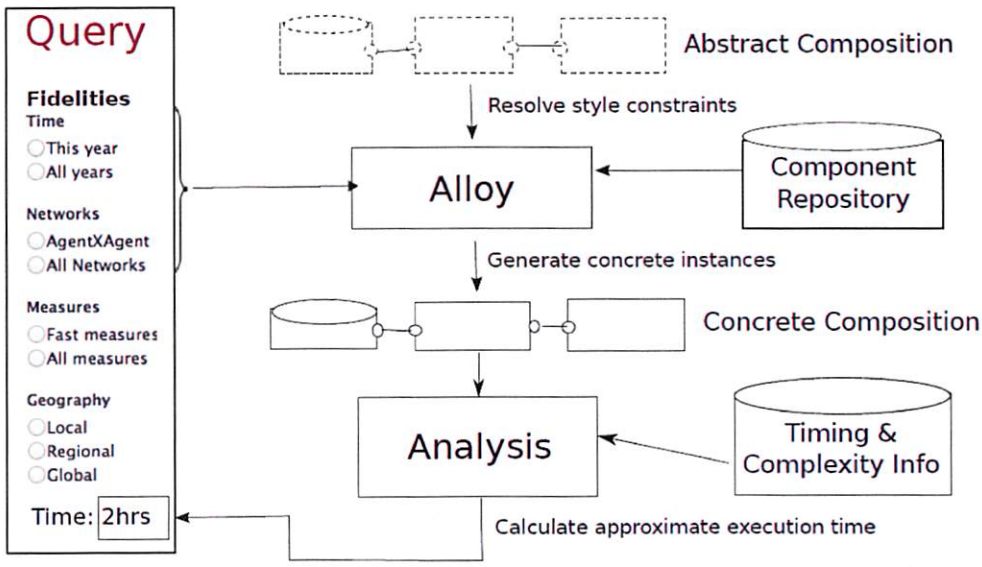
- Although, network metrics are not necessarily robust for sampled data, we could show that estimating the goodness of fit of the metrics estimation is possible. Non-linear fit is superior to linear fit.

Nonlinear least squares (NLS): $r(C_y, C_y^S) = \beta_0 + \beta_1 n + \beta_2 e + [\beta_3 n_S^{\alpha_1}] + \beta_4(1 - e_S^{\alpha_2})$

Covariate	Description
n	original network size. $\|V\|$
e	original network edge communication count. $\|E\|$
n_s	sampled node count
e_s	sampled edge communication count

	Degree Centrality		Betweenness Centrality	
Predictor	Email	Message	Email	Message
Intercept	− 1.305 ***	− 0.354 **	− 0.653 ***	0.230 ***
n	− 0.146 ***	− 0.323 ***	− 0.226 ***	− 0.300 ***
e	− 0.504 *	33.133 ***	1.613 ***	30.414 ***
$n_s^{\alpha_1}$	0.000	0.136 ***		
α_1	2.296 ***	0.490 ***		
$1 - e_s^{\alpha_2}$	2.587 ***	1.249 ***	3.184 ***	2.556 ***
α_2	0.359 ***	0.560 ***	0.107 ***	0.056 ***
AIC	− 16970	− 29993	− 11766	− 19219
BIC	− 16918	− 29937	− 11727	− 19177
Adj-R^2	0.783	0.736	0.794	0.631

- In collaboration with David Garlan, Bradley Schmerl, and Vishal Dwivedi (Ph.D. student) we studied the integration of metrics optimization in software architectures. Results of this collaboration are a publication (Dwivedi et al, 2014) as well as a new project for the 2014+ Lablet.



- The PI ran a "big data" session at the last Sunbelt 2013 conference for social network analysis. In our presentation we introduced the metrics optimization problem from a software architecture perspective including several layers for possible optimizations.