REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
10-01-2018	Final Report	31-May-2013 - 30-Aug-2017

4. TITLE AND SUBTITLE
Final Report: A Statistical Framework for Analyzing Cyber Threats

5a. CONTRACT NUMBER
W911NF-13-1-0141

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
206022

6. AUTHORS

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
University of Texas at San Antonio
One UTSA Circle

San Antonio, TX 78249 -1644

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)
62846-CS-REP.22

12. DISTRIBUTION AVAILIBILITY STATEMENT
Approved for public release; distribution is 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

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			Shouhuai Xu
UU	UU	UU	UU		19b. TELEPHONE NUMBER 210-458-5739

RPPR Final Report
as of 27-Mar-2018

Agency Code:

Proposal Number: 62846CSREP **Agreement Number: W911NF-13-1-0141**
INVESTIGATOR(S):

Name: Maochao Xu
Email: mxu2@ilstu.edu
Phone Number: 3014387674
Principal: N

Name: Shouhuai Xu
Email: shxu@cs.utsa.edu
Phone Number: 2104585739
Principal: Y

Organization: **University of Texas at San Antonio**
Address: One UTSA Circle, San Antonio, TX 782491644
Country: USA

DUNS Number: 800189185 EIN: 741717115
Report Date: 30-Nov-2017 Date Received: 10-Jan-2018
Final Report for Period Beginning 31-May-2013 and Ending 30-Aug-2017
Title: A Statistical Framework for Analyzing Cyber Threats
Begin Performance Period: 31-May-2013 **End Performance Period:** 30-Aug-2017
Report Term: 0-Other

Submitted By: Shouhuai Xu Email: shxu@cs.utsa.edu
Phone: (210) 458-5739

STEM Degrees: 4 **STEM Participants:** 8

Major Goals: The project consists of a main project (3 years) and an add-on project (1 year).

The research objective of the main project is centered on addressing the following fundamental questions:

----How can we "decode" the useful information about cyber threats that is "encoded" in the cyber attack data collected by various cyber defense instruments?

----To what extent, or at what levels of abstraction, can cyber attacks be predicted with a good/useful enough accuracy?

----What are the limits of prediction?

----How can we quantify the cyber defense (e.g., early-warning) utilities of cyber attack data collected by cyber defense instruments?

Adequately addressing these questions not only will deepen our understanding of cyber security, but also will offer insights for proactive cyber defense based on the prediction of incoming dynamic cyber threats.

Our technical approach is centered on an innovative "Grey-Box" Statistical Framework. This framework is centered on investigating a new kind of mathematical objects, which we introduce and call Stochastic Cyber Attack Processes. These processes describe cyber threats at multiple resolutions, such as: network-level (e.g., considering all attacks against a network as a whole), computer-level (e.g., considering all attacks against a computer or IP address as a whole), port-level (e.g.,
the defender cares most about the attacks against certain ports or services).

The "grey-box" statistical framework formulates a new methodology of Cybersecurity Data Analytics as follows: The analyst should extract the statistical properties exhibited by real-world data, and then use these properties to guide the design of prediction models. Our research showed that the ``grey-box" framework is effective in predicting

cybersecurity situational awareness. For example, our research showed that the framework can predict cyber attack rates, which reflect on aspect of cybersecurity situational awareness, at a 88\% prediction accuracy 1-hour ahead of time, while noting that 93\% is the prediction upper bound (i.e., the limit of prediction).
An initial study also showed that the framework could be further enhanced to predict the emergence of zero-day attacks, which will be further investigated in the future.

The ``grey-box'' statistical framework has been invited to present at a DoD meeting.

The research objective of the add-on project is centered at systematizing the knowledge and understanding of security metrics and identifying future research directions towards ultimately tackling this hard problem of high importance.

Accomplishments: Please refer to the 182-page PDF document entitled "ARO Project Final Report: A Statistical Framework for Analyzing Cyber Threats".

Training Opportunities: Nothing to Report

Results Dissemination: Research results are disseminated via scientific and academic venues, including journal and conference publications. Some research results are also disseminated through presentations at other institutes, including USAF RATPAC Working Group (April 6, 2016), Army Research Lab (December 13, 2016), and ARO Invitational Workshop on Foundations and Challenges for Proactive and Dynamic Network Defense (Nov. 30-Dec. 1, 2017). Some research results are incorporated into the graduate courses the PI taught.

Honors and Awards: The PI received UTSA College of Sciences Dean's Research Achievement Awards in 2015 and 2016.

Protocol Activity Status:

Technology Transfer: 1. The PI delivered the following presentations at the following DOD institutes:

---US Air Force Research Lab (August 26, 2014)

---US Air Force Research Lab (June 9, 2015)

---USAF RATPAC Working Group (April 6, 2016)

---Army Research Lab (December 13, 2016)

---ARO Invitational Workshop on Foundations and Challenges for Proactive and Dynamic Network Defense (Nov. 30-Dec. 1, 2017).

2. The PI has the following joint publications with DOD researchers:

---J. Mireles, E. Ficke, J. Cho, P. Hurley, and S. Xu. Metrics Towards Measuring Cyber Agility. Paper under journal review.

---P. Du, Z. Sun, H. Chen, J. Cho, and S. Xu. Statistical Estimation of Malware Detection Metrics in the Absence of Ground Truth. Paper under journal review.

---J. Cho, S. Xu, P. Hurley, M. Mackay, T. Benjamin, and M. Beaumont. STRAM: Measuring the Trustworthiness of Computer-based Systems. Paper under journal review.

---M. Pendleton, R. Garcia-Lebron, J. Cho, and S. Xu. A Survey on Systems Security Metrics, ACM Computing Survey, 49(4): 62:1-62:35 (2017).

---M. Saleh, P. Ratazzi, and S. Xu. A Control Flow Graph-based Signature for Packer Identification. Proceedings of Milcom'2017.

---J. Mireles, J. Cho, and S. Xu. Extracting Attack Narratives from Traffic Datasets. The 1st International Conference on Cyber Conflict in the U.S. (CyCon U.S. '2016).

---J. Cho, P. Hurley, and S. Xu. Metrics and Measurement of Trustworthy Systems. Milcom'2016.

PARTICIPANTS:

Participant Type: Co PD/PI
Participant: Maochao Xu
Person Months Worked: 3.00 **Funding Support:**
Project Contribution:
International Collaboration:
International Travel:
National Academy Member: N
Other Collaborators:

Participant Type: Graduate Student (research assistant)
Participant: Zhenxin Zhan
Person Months Worked: 12.00 **Funding Support:**
Project Contribution:
International Collaboration:
International Travel:
National Academy Member: N
Other Collaborators:

Participant Type: Graduate Student (research assistant)
Participant: Marcus Pendleton

RPPR Final Report
as of 27-Mar-2018

Person Months Worked: 6.00 **Funding Support:**
Project Contribution:
International Collaboration:
International Travel:
National Academy Member: N
Other Collaborators:

Participant Type: PD/PI
Participant: Shouhuai Xu
Person Months Worked: 2.00 **Funding Support:**
Project Contribution:
International Collaboration:
International Travel:
National Academy Member: N
Other Collaborators:

Participant Type: Graduate Student (research assistant)
Participant: Li Xu
Person Months Worked: 12.00 **Funding Support:**
Project Contribution:
International Collaboration:
International Travel:
National Academy Member: N
Other Collaborators:

ARTICLES:

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
Journal: IEEE Transactions on Information Forensics and Security
Publication Identifier Type: DOI Publication Identifier: 10.1109/TIFS.2013.2279800
Volume: 8 Issue: 11 First Page #: 0
Date Submitted: Date Published:
Publication Location:
Article Title: Characterizing Honeypot-Captured Cyber Attacks: Statistical Framework and Case Study
Authors:
Keywords: Cyber security, cyber attacks, stochastic cyberattack process, statistical properties, long-range dependence(LRD), cyber attack prediction
Abstract: Rigorously characterizing the statistical properties of cyber attacks is an important problem. In this paper, we propose the first statistical framework for rigorously analyzing honeypot-captured cyber attack data. The framework is built on the novel concept of stochastic cyber attack process, a new kind of mathematical objects for describing cyber attacks. To demonstrate use of the framework, we apply it to analyze a lowinteraction honeypot dataset, while noting that the framework can be equally applied to analyze high-interaction honeypot data that contains richer information about the attacks. The case study finds, for the first time, that Long-Range Dependence (LRD) is exhibited by honeypot-captured cyber attacks. The case study confirms that by exploiting the statistical properties (LRD in this case), it is feasible to predict cyber attacks (at least in terms of attack rate) with good accuracy. This kind of prediction capability would provide sufficient early-warning time for defe
Distribution Statement: 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support:

RPPR Final Report
as of 27-Mar-2018

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
Journal: IEEE TIFS
Publication Identifier Type: Publication Identifier:
Volume: 0 Issue: 0 First Page #: 0
Date Submitted: 11/3/2017 12:00:00AM Date Published:
Publication Location:
Article Title: Analyzing the Extreme-Value PhenomenonExhibited by Honeypot-Captured Cyber Attacks
Authors: Zhenxin Zhan, Maochao Xu, and Shouhuai Xu
Keywords: Cyber attack analytics, extreme value phenomenon,extreme value theory, prediction, intense attacks
Abstract: It is important to understand and characterize the statistical phenomena/propeties of cyber attacks. In this paper, we rigorously characterize the extreme-value phenomenon exhibited by honeypot-captured cyber attacks, namely the outlier attack rates (per unit time) that are above certain thresholds. To the best of our knowledge, we are the first to study the extreme-value phenomenon in the domain of cyber security analytics. Our study is based on a novel methodology, which aims to integrate two complementary statistical approaches that analyze the same data but from different perspectives: the Extreme Value Theory (EVT) and the Time Series Theory (TST). We investigate an interesting connection between the two approaches, when applying them to predict extreme attack rates. Besides the methodological novelty, we propose a novel family of time-series FARIMA+GARCH models, which can accommodate both the extreme-value phenomenon and the Long-Range Dependence (LRD) phenomenon that are exhibit
Distribution Statement: 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support: **Y**

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
Journal: PLoS ONE
Publication Identifier Type: Publication Identifier:
Volume: 1.0E+001 Issue: 5.0E+000 First Page #: 0
Date Submitted: Date Published:
Publication Location:
Article Title: Spatiotemporal patterns and predictability of cyberattacks
Authors:
Keywords: Prediction, Cybersecurity Data Analytics, Cyber Threats
Abstract: A relatively unexplored issue in cybersecurity science and engineering is whether there exist intrinsic patterns of cyberattacks. Conventional wisdom favors absence of such patterns due to the overwhelming complexity of the modern cyberspace. Surprisingly, through a detailed analysis of an extensive data set that records the time-dependent frequencies of attacks over a relatively wide range of consecutive IP addresses, we successfully uncover intrinsic spatiotemporal patterns underlying cyberattacks, where the term “spatio” refers to the IP address space. In particular, we focus on analyzing macroscopic properties of the attack traffic flows and identify two main patterns with distinct spatiotemporal characteristics: deterministic and stochastic. Strikingly, there are very few sets of major attackers committing almost all the attacks, since their attack “fingerprints” and target selection scheme can be unequivocally identified according to the very limited number of unique spatiotempor
Distribution Statement: 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support:

RPPR Final Report
as of 27-Mar-2018

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
Journal: IEEE Transactions on Information Forensics and Security
Publication Identifier Type: Publication Identifier:
Volume: 1.0E+001 Issue: 8.0E+000 First Page #: 1666
Date Submitted: Date Published:
Publication Location:
Article Title: Predicting Cyber Attack Rates WithExtreme Values
Authors:
Keywords: Extreme values, extreme value theory,prediction, gray-box models, time series.
Abstract: It is important to understand to what extent, and in what perspectives, cyber attacks can be predicted. Despite its evident importance, this problem was not investigated until very recently, when we proposed using the innovative methodology of gray-box prediction. This methodology advocates the use of gray-box models, which accommodate the statistical properties/phenomena exhibited by the data. Specifically, we showed that gray-box models that accommodate the long-range dependence phenomenon can predict the attack rate (i.e., the number of attacks per unit time) 1-h ahead-of-time with an accuracy of 70.2%–82.1%. To the best of our knowledge, this is the first result showing the feasibility of prediction in this domain. We observe that the prediction errors are partly caused by the models' incapability in predicting the large attack rates, which are called extreme values in statistics. This motivates us to analyze the extreme-value phenomenon, using two complementary approaches: 1) the
Distribution Statement: 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support:

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
Journal: INTERNET MATH
Publication Identifier Type: Publication Identifier:
Volume: 1.1E+001 Issue: 1.0E+000 First Page #: 62
Date Submitted: Date Published:
Publication Location:
Article Title: Cyber Epidemic Models with Dependencies
Authors:
Keywords: Dependence, Cybersecurity Dynamics, Stochastic Processes
Abstract: Studyingmodels of cyber epidemics over arbitrary complex networks can deepen our understanding of cyber security from a whole-system perspective. In this work, we initiate the investigation of cyber epidemic models that accommodate the dependences between the cyber attack events. Due to the notorious difficulty in dealing with such dependences, essentially all existing cyber epidemic models have disregarded them. Specifically, we introduce the idea of copulas into cyber epidemic models for accommodating the dependences between the cyber attack events. We investigate the epidemic equilibrium thresholds as well as the bounds for both equilibrium and nonequilibrium infection probabilities. We further characterize the side effects of disregarding the due dependences between the cyber attack events by showing that the results thereof are unnecessarily restrictive or even incorrect.
Distribution Statement: 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support:

RPPR Final Report
as of 27-Mar-2018

Publication Type: Journal Article Peer Reviewed: N **Publication Status:** 5-Submitted
Journal: Annuals of applied statistics
Publication Identifier Type: Publication Identifier:
Volume: 0 Issue: 0 First Page #: 0
Date Submitted: Date Published:
Publication Location:
Article Title: VINE COPULA MODELS FOR CHARACTERIZING AND PREDICTING THE EFFECTIVENESS OF EARLY-WARNING IN CYBER DEFENSE
Authors:
Keywords: Dependence, Prediction, Earlywaring, Secuity Metrics
Abstract: Internet-based computer information systems play critical roles in many aspects of the modern society. However, these systems are constantly under cyber attacks that can cause catastrophic consequences. In order to defend these systems, it is necessary to predict the effectiveness of cyber defense mechanisms. In this paper, we investigate how to predict the effectiveness of an important cyber defense mechanism that is known as early-warning. This turns out to be a challenge because we must accommodate the dependence between time series. This motivates us to introduce an innovative Vine Copula model. We show that the model offers accurate predictions on the effectiveness of early-warning.
Distribution Statement: 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support:

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
Journal: Journal of Applied Statistics
Publication Identifier Type: Publication Identifier:
Volume: Issue: First Page #:
Date Submitted: 11/3/2017 12:00:00AM Date Published: 9/1/2016 3:58:58AM
Publication Location:
Article Title: Modeling and Predicting Extreme Cyber Attack Rates via Marked Point Processes
Authors: Peng Chen, Maochao Xu, Shouhuai Xu, Taizhong Hu
Keywords: Autoregressive conditional duration; Extreme value theory; Generalized Pareto distribution; Intensity
Abstract: Cyber attacks have become a problem that is threatening the economy, human privacy, and even national security. Before we can adequately address the problem, we need to have a crystal clear understanding about cyber attacks from various perspectives. This is a challenge because the Internet is a large-scale complex system with humans in the loop. In this paper, we investigate a particularperspective of the problem, namely the extreme value phenomenon that is exhibited by cyber attack rates, which are the numbers of attacks against a system of interest per time unit. It is important to explore this perspective because understanding the statistical properties of extreme cyber attack rates will pave the way for cost-effective, if not optimal, allocation of resources in real-life cyber defense operations. Specifically, we propose modeling and predicting extreme cyber attack rates via marked point processes, while using the Value-at-Risk (VaR) as a natural measure of intense cyber attacks.
Distribution Statement: 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support: **Y**

RPPR Final Report
as of 27-Mar-2018

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
Journal: ACM Computing Surveys
Publication Identifier Type: DOI Publication Identifier: 10.1145/3005714
Volume: 49 Issue: 4 First Page #: 1
Date Submitted: 11/3/2017 12:00:00AM Date Published: 12/1/2016 12:00:00PM
Publication Location:
Article Title: A Survey on Systems Security Metrics
Authors: Marcus Pendleton, Richard Garcia-Lebron, Jin-Hee Cho, Shouhuai Xu
Keywords: Security metrics, security measurement, security foundation, quantitative security
Abstract: Security metrics have received significant attention. However, they have not been systematically explored based on the understanding of attack-defense interactions, which are affected by various factors, includingthe degree of system vulnerabilities, the power of system defense mechanisms, attack (or threat) severity, and situations a system at risk faces. This survey particularly focuses on how a system security state can evolve as an outcome of cyber attack-defense interactions. This survey concerns how to measure system-level security by proposing a security metrics framework based on the following four sub-metrics: (1) metrics of system vulnerabilities, (2)metrics of defense power, (3)metrics of attack or threat severity, and (4) metrics of situations. To investigate the relationships among these four sub-metrics, we propose a hierarchical ontology with four sub-ontologies corresponding to the four sub-metrics and discuss how they are related to each other.
Distribution Statement: 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support: **Y**

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
Journal: Physica A: Statistical Mechanics and its Applications
Publication Identifier Type: DOI Publication Identifier: 10.1016/j.physa.2017.04.078
Volume: 482 Issue: First Page #: 713
Date Submitted: 11/3/2017 12:00:00AM Date Published: 9/1/2017 5:00:00AM
Publication Location:
Article Title: Robustness of non-interdependent and interdependent networks against dependent and adaptive attacks
Authors: Adam Tyra, Jingtao Li, Yilun Shang, Shuo Jiang, Yanjun Zhao, Shouhuai Xu
Keywords: Complex networks, Robustness, Percolation, Randomattacks, Dependent attacks, Adaptive attacks, Cybersecurity
Abstract: Robustness of complex networks has been extensively studied via the notion of site percolation, which typically models {\em independent} and {\em non-adaptive} attacks (or disruptions). However, real-life attacks are often {\em dependent} and/or {\em adaptive}. This motivates us to characterize the robustness of complex networks, including non-interdependent and interdependent ones, against dependent and adaptive attacks. For this purpose, dependent attacks are accommodated by L-hop percolation where the nodes within some L-hop ($L\geq 0$) distance of a chosen node are all deleted during one attack (with $L=0$ degenerating to site percolation). Whereas, adaptive attacks are launched by attackers who can make node-selection decisions based on the network state in the beginning of each attack. The resulting characterization enriches the body of knowledge with new insights.
Distribution Statement: 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support: **Y**

RPPR Final Report
as of 27-Mar-2018

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 3-Accepted
Journal: Technometrics
Publication Identifier Type: DOI Publication Identifier: 10.1080/00401706.2016.1256841
Volume: Issue: First Page #: 1
Date Submitted: 11/3/2017 12:00:00AM Date Published: 11/1/2016 5:00:00AM
Publication Location:
Article Title: A Vine Copula Model for Predicting the Effectiveness of Cyber Defense Early-Warning
Authors: Maochao Xu, Lei Hua, Shouhuai Xu
Keywords: Copula-GARCH, Cybersecurity, Prediction
Abstract: Internet-based computer information systems play critical roles in many aspects of the modern society. However, these systems are constantly under cyber attacks that can cause catastrophic consequences. In order to defend these systems effectively, it is necessary to measure and predict the effectiveness of cyber defense mechanisms. In this paper, we investigate how to measure and predict the effectiveness of an important cyber defense mechanism that is known as early-warning. This turns out to be a challenging problem because we must accommodate the dependence among certain 4-dimensional time series. In the course of using a dataset to demonstrate the prediction methodology, we discover a new non-exchangeable and rotationally symmetric dependence structure, which may be of independent value. We propose a new vine copula model to accommodate the newly discovered dependence structure, and show that the new model can predict the effectiveness of early-warning accurately.
Distribution Statement: 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support: **Y**

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 3-Accepted
Journal: Journal of Computer Virology and Hacking Techniques
Publication Identifier Type: DOI Publication Identifier: 10.1007/s11416-017-0304-8
Volume: Issue: First Page #:
Date Submitted: 11/3/2017 12:00:00AM Date Published: 8/1/2017 5:00:00AM
Publication Location:
Article Title: Multi-context features for detecting malicious programs
Authors: Moustafa Saleh, Tao Li, Shouhuai Xu
Keywords: Malware Detection, Machine Learning, Code Obfuscation
Abstract: Malware detection is still an open problem. There are numerous attacks that take place every day where malware is used to steal private information, disrupt services, or sabotage industrial systems. In this paper, we combine three kinds of contextual information, namely static, dynamic, and instruction-based, for malware detection. This leads to the definition of more than thirty thousand features, which is a large features set that covers a wide range of a sample characteristics. Through experiments with one million files, we show that this features set leads to machine learning based models that can detect both malware seen roughly at the time when the models are built, and malware first seen even months after the models were built (i.e., the detection models remain effective months ahead of time). This may be due to the comprehensiveness of the features set.
Distribution Statement: 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support: **Y**

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 4-Under Review
Journal: ACM computing Surveys
Publication Identifier Type: DOI Publication Identifier:
Volume: Issue: First Page #:
Date Submitted: 3/27/2018 12:00:00AM Date Published:
Publication Location:
Article Title: STRAM: Measuring the Trustworthiness of Computer-based Systems
Authors: Hin-Hee Cho, Shouhuai Xu, Patrick M. Hurley, Matthew Mackay, Trevor Benjamin, Mark Beaumont
Keywords: Security, Trust, Resilience, Agility Metrics
Abstract: Various system metrics have been proposed for measuring the quality of computer-based systems, such as dependability and security metrics for estimating their performance and security characteristics. As computer-based systems grow in complexity with many sub-systems or components, measuring their quality in multiple dimensions is a challenging task. In this work, we tackle the problem of measuring the quality of computer-based systems based on the four key attributes of trustworthiness we developed, namely security, trust, resilience and agility. In addition to conducting a systematic survey on metrics, measurements, attributes of metrics and associated ontologies, we propose a system-level trustworthiness metric framework that accommodates four submetrics, called STRAM (Security, Trust, Resilience, and Agility Metrics). The proposed STRAM framework offers a hierarchical ontology structure where each submetric is defined as a sub-ontology. Moreover, this work proposes develop...
Distribution Statement: 3-Distribution authorized to U.S. Government Agencies and their contractors
Acknowledged Federal Support: **Y**

CONFERENCE PAPERS:

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: Proceedings of the 6th international conference ontrustworthy systems (InTrust'2014)
Date Received: 03-Nov-2017 Conference Date: 16-Dec-2014 Date Published:
Conference Location: Beijing
Paper Title: A Characterization of Cybersecurity Pos-ture from Network Telescope Data
Authors: Z. Zhan, M. Xu, and S. Xu
Acknowledged Federal Support: **Y**

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: Proceedings of IEEE 2014 Conference on Com-munications and Network Security (IEEE CNS'14)
Date Received: 03-Nov-2017 Conference Date: 28-Sep-2014 Date Published:
Conference Location: San Francisco
Paper Title: An Evasion and Counter-Evasion Study in Malicious Websites Detection
Authors: L. Xu, Z. Zhan, S. Xu, and K. Ye
Acknowledged Federal Support: **Y**

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: MILCOM 2016 - 2016 IEEE Military Communications Conference (MILCOM)
Date Received: 03-Nov-2017 Conference Date: 01-Nov-2016 Date Published:
Conference Location: Baltimore, MD, USA
Paper Title: Metrics and measurement of trustworthy systems
Authors: J. Cho, P. Hurley, and S. Xu
Acknowledged Federal Support: **Y**

RPPR Final Report
as of 27-Mar-2018

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: 2016 International Conference on Cyber Conflict (CyCon U.S.)
Date Received: 03-Nov-2017 Conference Date: 21-Oct-2016 Date Published:
Conference Location: Washington, DC, USA
Paper Title: Extracting attack narratives from traffic datasets
Authors: J. Mireles, J. Cho, and S. Xu
Acknowledged Federal Support: **Y**

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: IEEE Milcom
Date Received: 03-Nov-2017 Conference Date: 23-Oct-2017 Date Published:
Conference Location: Baltimore
Paper Title: A Dataset Generator for Next Generation System Call Host Intrusion Detection Systems
Authors: Marcus Pendleton, Shouhuai Xu
Acknowledged Federal Support: **Y**

DISSERTATIONS:

Publication Type: Thesis or Dissertation
Institution:
Date Received: 21-Aug-2014 Completion Date:
Title: A Statistical Framework for Analyzing Cyber Attacks
Authors:
Acknowledged Federal Support:

ARO Project Final Report

A Statistical Framework for Analyzing Cyber Threats

Grant number: W911NF-13-1-0141

PI: Prof. Shouhuai Xu
Department of Computer Science
University of Texas at San Antonio
email: shxu@cs.utsa.edu
web: www.cs.utsa.edu/~shxu
phone: 210-458-5739
fax: 210-458-4437

Program Manager: Dr. Cliff Wang

Report date: November 3, 2017
Report period: 2013—2017

Contents

1 Executive Summary

This 4-year project consists of a 3-year main project on building a statistical framework for analyzing cyber threats, called the *main* project thereafter, and a 1-year add-on project on investigating security metrics, call the *add-on* project thereafter.

The research objective of the *main* project is centered on addressing the following fundamental questions:

- How can we **"decode" the useful information** about cyber threats that is "encoded" in the cyber attack data collected by various cyber defense instruments?
- To what extent, or at what levels of abstraction, can cyber attacks be **predicted** with a good/useful enough accuracy?
- What are the limits of prediction?
- How can we quantify the cyber defense (e.g., **earlywarning**) utilities of cyber attack data collected by cyber defense instruments?

Adequately addressing these questions not only will deepen our understanding of cyber security, but also will offer insights for proactive cyber defense based on the prediction of incoming dynamic cyber threats.

Our technical approach is centered on an innovative **"Grey-Box" Statistical Framework**. This framework is centered on investigating a new kind of mathematical objects, which we introduce and call **Stochastic Cyber Attack Processes**. These processes describe cyber threats at multiple resolutions, such as: network-level (e.g., considering all attacks against a network as a whole), computer-level (e.g., considering all attacks against a computer or IP address as a whole), port-level (e.g., the defender cares most about the attacks against certain ports or services).

The "grey-box" statistical framework formulates a new methodology of **Cybersecurity Data Analytics** as follows: The analyst should extract the statistical properties exhibited by real-world data, and then use these properties to guide the design of prediction models. Our research showed that the "grey-box" framework is effective in predicting cybersecurity situational awareness. For example, our research showed that the framework can predict cyber attack rates, which reflect on aspect of cybersecurity situational awareness, at a 88% prediction accuracy 1-hour ahead of time, while noting that 93% is the prediction upper bound (i.e., the limit of prediction). An initial study also showed that the framework could be further enhanced to predict the emergence of zero-day attacks, which will be further investigated in the future.

The "grey-box" statistical framework has been invited to present at a DoD meeting [1].

The research objective of the *add-on* project is centered at systematizing the knowledge and understanding of security metrics and identifying future research directions towards ultimately tackling this hard problem of high importance.

2 The Main Project: The "Grey-Box" Statistical Framework and Its Applications

We aim to systematically analyze various cyber attack data collected by cyber defense instruments, including (client) honeypots and network telescopes (also known as blackhole, darknet, or network sink). At the same time, we want to assure that the resulting methodologies are equally applicable to analyze cyber attack data that would contain much richer information (e.g., the data that would be collected in production networks).

2.1 The "Grey-Box" Statistical Framework

The research objective of the project is centered on addressing the following fundamental questions:

- How can we **"decode" the useful information** about cyber threats that is "encoded" in the cyber attack data collected by various cyber defense instruments?
- To what extent, or at what levels of abstraction, can cyber attacks be **predicted** with a good/useful enough accuracy?
- What are the limits of prediction?
- How can we quantify the cyber defense (e.g., **earlywarning**) utilities of cyber attack data collected by cyber defense instruments?

Adequately addressing these questions not only will deepen our understanding of cyber security, but also will offer insights for proactive cyber defense based on the prediction of incoming dynamic cyber threats.

Our technical approach is centered on an innovative **"Grey-Box" Statistical Framework**. This framework is centered on investigating a new kind of mathematical objects, which we introduce and call **Stochastic Cyber Attack Processes**. These processes describe cyber threats at multiple resolutions, such as: network-level (e.g., considering all attacks against a network as a whole), computer-level (e.g., considering all attacks against a computer or IP address as a whole), port-level (e.g., the defender cares most about the attacks against certain ports or services).

As highlighted in Figure 1, the "grey-box" statistical framework first extracts the statistical properties exhibited by real-world data, and then uses these properties to guide the design of prediction models. Our research showed that the "grey-box" framework is effective in predicting cybersecurity situational awareness. For example, our research showed that the framework can predict cyber attack rates, which reflect on aspect of cybersecurity situational awareness, at a 88% prediction accuracy 1-hour ahead of time, while noting that 93% is the prediction upper bound (i.e., the limit of prediction). An initial study also showed that the framework could be further enhanced to predict the emergence of zero-day attacks, which will be further investigated in the future.

The "grey-box" statistical framework has been invited to present at an AF/DoD meeting [1].

Figure 1: The "grey-box" statistical framework, where the statistical properties that we have investigated include Long Range Dependence, Extreme value, and Dependence. These properties are used to guide the design of statistical models for predicting cybersecurity situational awareness from various aspects (e.g., cyber attack rates). "Grey-box" means that the prediction models are devised to accommodate the statistical properties exhibited by real-world data.

2.2 Using the Framework to Predict Cyber Threats

Statistical prediction models accommodating the Long-Range Dependence property. In [2, 3], we propose the first statistical framework for systematically analyzing and exploiting honeypot-captured cyber attack data. The framework is centered on a novel concept and abstraction, which we introduce and call Stochastic Cyber Attack Processes — a new kind of mathematical objects that can naturally model cyber attacks. Based on some real data, we find that stochastic cyber attack processes are not Poisson, but instead can exhibit **Long-Range Dependence** (LRD), which is not known to be relevant in the cyber security domain until now. This finding has profound implications for modeling cyber attacks. In particular, we show that LRD can be exploited to **predict the incoming attacks** at least in terms of attack rate (i.e., number of attacks per time unit). This demonstrates the power of **"grey-box" prediction**, where prediction models can accommodate the relevant statistical properties. We find that the cause of the LRD that is exhibited by cyber attacks might be different from the cause of the LRD that is exhibited by the benign traffic. In [2], we show that based on the "grey-box" methodology, we can predict attack rates one hour ahead with an accuracy about 80%.

Statistical prediction models accommodating the Long-Range Dependence property and the Extreme-Value Property. In [4], we initiate the investigation of the *extreme-value* phenomenon exhibited by honeypot-captured cyber attacks. The extreme-value phenomenon refers to the many outliers above certain thresholds, such as the large attack rates (per unit time) against a target of interest. We propose the first methodology for investigating the extreme-value phenomenon exhibited by cyber attacks. The methodology aims to integrate two complementary statistical approaches: the Extreme Value Theory (EVT) and the Time Series Theory (TST). We find that **these two predictive approaches should be used together** in practice, because EVT-based methods are more appropriate for long-term predictions and TST-based methods are more appropriate for short-term predictions. For example, we propose a family of time-series **FARIMA+GARCH** models, where GARCH (Generalized AutoRegressive Conditional Heteroskedasticity) accommodates the extreme-value phenomenon, and FARIMA (Fractional AutoRegressive Integrated Moving Average) accommodates the LRD phenomenon. We show that FARIMA+GARCH can

indeed better predict the attack rates with good accuracy. Specifically, we can use the "grey-box" methodology to predict attack rates one hour ahead with an accuracy about 88% [4].

Characterizing the spatiotemporal predictability of cyber attack rates. The aforementioned studies essentially focus on the temporal properties of cyber attacks. In [5], we discover the existence of intrinsic **spatiotemporal patterns** underlying cyber attacks. We show, for the first time, that robust macroscopic spatialtemporal patterns exist in the seemingly random cyberspace. More specifically, we find that majority of the attacks are governed by a few very limited number of patterns, indicating that cyber attacks are mainly committed by a few types of major attackers, each with unique spatiotemporal characteristics. Moreover, the patterns can be divided into two types: deterministic and stochastic attack patterns. The emergence of deterministic patterns implies predictability. The stochastic patterns can be quantitatively characterized by the flux-fluctuation laws in statistical and nonlinear physics. Our study suggests an upper bound of about 93% accuracy when predicting attack rates. This hints future research directions to further improve the "grey-box" prediction models mentioned above.

Predicting extreme cyber attack rates via marked point processes. In [6], we investigate a new approach to predicting extreme cyber attack rates. Specifically, we propose modeling and predicting extreme cyber attack rates via *marked point processes*, while using the Value-at-Risk (VaR) as a natural measure of intense cyber attacks. The approach is featured by its capability of simultaneously accommodating the magnitudes of extreme values (i.e., extreme attack rates in the context of the present paper), the inter-exceedance times between extreme values, and the dependence between the inter-arrival times of extreme values. Our empirical analysis, which is based on two real-world datasets that are collected by network telescope and honeypot, shows that the approach can accurately describe and predict extreme cyber attack rates. The approach is interesting on its own from a theoretical perspective, and useful in practice because it enables the defender to dynamically allocate defense resources based on the predicted extreme attack rates.

2.3 Using the Framework to Characterize Situational Awareness

Characterizing cybersecurity posture. In [7], we characterize the cybersecurity posture based on a dataset collected by CAIDA's /8 network telescope (i.e., 2^{24} IP addresses) during the month of March 2013. We describe **cybersecurity posture** by using three time series: the number of victims, the number of attackers, and the number of attacks. We define the notion of **sweep-time**, namely the time it takes for (e.g.) at least 85% telescope IP addresses to be attacked at least once. We find that sweep-time cannot be described by a probabilistic distribution, despite that a proper subset of the large sweep-times follows the power-law distribution; instead, we show that an appropriate stochastic process can describe the sweep-time. This means that when incorporating sweep-time into first-principle cybersecurity models, it cannot be always treated as a random variable and may need to be treated as a stochastic process. We investigate whether or not substantially smaller network

telescopes would give approximately the same statistics as what would be offered by a single, large network telescope. This question is interesting on its own and, if answered affirmatively, could lead to more cost-effective operation of network telescopes. Unfortunately, our analysis shows that substantially smaller telescopes might not be as useful a single, large telescope (of 2^{24} IP addresses).

Characterizing the effectiveness of cyber defense earlywarning. In [8], we investigate how to predict the effectiveness of cyber defense earlywarning, which is to filter (some of) the attackers that are observed at monitoring instruments such as network telescope or honeypot. The study is centered on predicting a set of cyber security metrics we introduce, such as *cyber attack pressure*, *victim defense pressure reduction rate*, and *cyber attack pressure reduction rate*. In the course of pursuing accurate prediction of these cyber security metrics, we encounter a particular challenge imposed by the *dependence* between time series. The technical research is therefore to adequately deal with the dependence, which is one of the inherent barriers that must be overcome before we can deeply understand and assure cyber security [9]. We discover a new type of non-exchangeable and approximately rotational symmetric dependence structure among the before- and after- earlywarning time series, which can be adequately described by a mixed copula structure we introduce. We show that the model offers accurate predictions on the effectiveness of earlywarning.

Characterizing the effectiveness of preventive and reactive cyber defense. Preventive and reactive defense dynamics, where the defender only employs preventive and reactive defenses, is one type of Cybersecurity Dynamics [9]. Recently, we proved that preventive and reactive dynamics is globally stable [10], meaning that the global cybersecurity state always converges to a unique equilibrium regardless of the initial global cybersecurity state. However, the theoretical result does not give the location of the unique equilibrium. In [11], we propose a novel method for constructing upper bounds of the equilibrium global cybersecurity state. This represents a significant step towards ultimately predicting the equilibrium global cybersecurity state.

2.4 Applying the Framework in Other Cybersecurity Settings

We believe that the "grey-box" statistical framework can be extended to predict other kinds of threats, such as the emergence of zero-day vulnerabilities and attacks. In what follows we report our initial work towards the ultimate goal of predicting zero-day vulnerabilities and attacks.

Automating the detection of software vulnerabilities. In [12], we investigate the automated detection of software vulnerabilities using real-world data. The problem is important because software vulnerabilities are the root cause of many attacks. The problem remains relevant despite the employment of rapid vulnerability patching because, for example, instances of the same vulnerability may exist in multiple software copies that are difficult to track in real life (e.g., different versions of libraries and applications). This calls for methods by which we can automatically detect and predict software vulnerabilities. In

this paper [12], we move a step forward in this direction by presenting Vulnerability Pecker (VulPecker), a system for automatically detecting whether or not the software source code contains a given vulnerability. The key insight underlying VulPecker is to leverage (i) a set of features that we define to characterize patches, and (ii) code-similarity algorithms that have been proposed for various purposes. Experiments show that VulPecker detected 40 vulnerabilities that were not published in the National Vulnerability Database (NVD). Among these vulnerabilities, 18 are not known for their existence and the other 22 vulnerabilities have been "silently" patched by vendors. We believe this first-step exhibits the high promise in detecting and predicting zero-day vulnerabilities and attacks.

Characterizing the robustness of non-interdependent and interdependent networks against dependent and adaptive attacks. Robustness of complex networks has been extensively studied via the notion of site percolation, which typically models *independent* and *non-adaptive* attacks (or disruptions). However, real-life attacks are often *dependent* and/or *adaptive*. This motivates us to characterize the robustness of complex networks, including non-interdependent and interdependent ones, against dependent and adaptive attacks. For this purpose, dependent attacks are accommodated by L-hop percolation where the nodes within some L-hop ($L \geq 0$) distance of a chosen node are all deleted during one attack (with $L = 0$ degenerating to site percolation). Whereas, adaptive attacks are launched by attackers who can make node-selection decisions based on the network state in the beginning of each attack. The resulting characterization enriches the body of knowledge with new insights, such as [13]: (i) the Achilles' Heel phenomenon is only valid for independent attacks, but not for dependent attacks; (ii) powerful attack strategies (e.g., targeted attacks and dependent attacks, dependent attacks and adaptive attacks) are not compatible and cannot help the attacker when used collectively. Our results shed some light on the design of robust complex networks.

Characterizing multiple cyber attacks against a target with observation errors and dependent outcomes. In [14] we investigate a cybersecurity model: An attacker can launch multiple attacks against a target with a termination strategy that says that the attacker will stop after observing a number of successful attacks or when the attacker is out of attack resources. However, the attacker's observation of the attack outcomes (i.e., random variables indicating whether the target is compromised or not) has an observation error that is specified by both a false-negative and a false-positive probability. The novelty of the model we study is the accommodation of the dependence between the attack outcomes, because the dependence was assumed away in the literature. In this model, we characterize the monotonicity and bounds of the compromise probability (i.e., the probability that the target is compromised). In addition to extensively showing the impact of dependence on quantities such as compromise probability and attack cost, we give methods for finding the optimal strategy that leads to maximum compromise probability or minimum attack cost. This study highlights that the dependence between random variables cannot be assumed away, because the results will be misleading.

Extracting attack narratives from traffic datasets. Parsing through large amounts of network traffic to extract attack signatures is a complex and time consuming process. It is an even harder process to piece together those signatures to formulate an attack narrative. An attack narrative can be defined as the set of attack signatures, that when combined provides an overview of the attack and the attacker themselves. In [15], we propose a framework for extracting attack narratives from traffic datasets. Within this framework, we propose the re-examination of packet grepping for attack signatures in network traffic as a viable, fast, and effective means to extract attack narratives from large amounts of network traffic. By combining attack signature packet grepping with Mandiant's Attack Lifecycle Model, we increase the effectiveness of packet grepping and create a methodology that is simple and powerful for constructing attack narratives. In order to show the effectiveness of the framework, we conduct a case study by using the 2015 National Collegiate Cyber Defense Competition (NCCDC) network traffic. Our preliminary results show that the framework is promising.

2.5 Future Research Directions

Our research has opened the door for exciting future research opportunities:

- Building a full-fledged statistical framework to predict the holistic cybersecurity situational awareness, including the the emergence of zero-day vulnerabilities and attacks. Our study already showed the capabilities of predicting cyber threats [2, 3, 4, 5, 6, 7, 8], while our initial study [12] has demonstrated the great potential of predicting the emergence of zero-day vulnerabilities and attacks.

- Investigating prediction models that accommodate the **dependence between cyber attacks** exhibited by high-dimensional data: In principle, cyber attacks are not independent; rather, they are dependent. Accommodating the due dependence into first-principle cyber defense dynamics models is an important, although difficult, problem. Our result in [16] can accommodate some classes of dependence between cyber attacks via the idea of **Copulas**. It is important to systematically investigate what kinds of dependence are exhibited by real-world cyber attack data.

- Predicting the evolution of malicious websites: In [17, 18], we show that sophisticated attacks can evade the defense against malicious websites, which are often exploited to launch drive-by download attacks. Our investigation hints that current attacks are already evolving. This motivates us to systematically characterize the **attack evolution process**. Moreover, this further inspires us to study *resilient predictions against evasive attacks*, where the attacker knows the defender's predictions models and therefore can adjust its attacker to disrupt the defender's predictions (e.g., attack rate).

3 The Add-On Project: Security Metrics

How to develop security metrics has been identified as one of the hard problems by many key organizations including the US INFOSEC Research Council and the US National Science and

Technology Council. However, the gaps or limitations between the state-of-the-art security metrics and the desirable ultimate goals, and how to fill these gaps, have not been discussed in the literature. This 1-year add-on project aims to deepen our understanding of the problem, systematizing the knowledge that has been presented in the literature, and shedding a light on future research directions.

3.1 Systematization of Security Metrics Knowledge

Systematizing systems security metrics. Security metrics have not been systematically explored based on the understanding of attack-defense interactions, which are affected by various factors, including the degree of system vulnerabilities, the power of system defense mechanisms, attack (or threat) severity, and situations a system at risk faces. This survey particularly focuses on how a system security state can evolve as an outcome of cyber attack-defense interactions. In [19], we discuss how to measure system-level security by proposing a security metrics framework based on the following four sub-metrics: (1) metrics of *system vulnerabilities*; (2) metrics of *defense power*; (3) metrics of *attack or threat severity*; (4) metrics of *situations*. To investigate the relationships between these four sub-metrics, we propose a hierarchical ontology with four sub-ontologies corresponding to the four sub-metrics and discuss how they are related to each other. Using the four sub-metrics, we discuss the state-of-art existing security metrics and their advantages and disadvantages (or limitations) to obtain lessons and insight in order to achieve an ideal goal in developing security metrics. Finally we discuss open research questions in the security metrics research domain and we suggest key factors to enhance security metrics from a system security perspective.

Systematizing systems trustworthiness metrics. Various system metrics have been proposed for measuring the quality of computer-based systems, such as dependability and security metrics for estimating their performance and security characteristics. As computer-based systems grow in complexity with many sub-systems or components, measuring their quality in multiple dimensions is a challenging task. In [20, 21], we tackle the problem of measuring the quality of computer-based systems based on the four key attributes of trustworthiness we developed, namely security, trust, resilience and agility. In addition to conducting a systematic survey on metrics, measurements, attributes of metrics and associated ontologies, we propose a system-level trustwothiness metric framework that accommodates four submetrics, called STRAM (Security, Trust, Resilience, and Agility Metrics). The proposed STRAM framework offers a hierarchical ontology structure where each submetric is defined as a sub-ontology. Moreover, this work proposes developing and incorporating metrics describing key assessment tools, including Vulnerability Assessment, Risk Assessment and Red Teaming, to provide additional evidence into the measurement and quality of trustworthy systems. We further discuss how assessment tools are related to measuring the quality of computer-based systems and the limitations of the state-of-the-art metrics and measurements. Finally, we suggest future research directions for system-level metrics research towards measuring fundamental attributes of the quality of computer-based systems and improving the current metric and measurement methodologies.

3.2 Defining and Measuring Novel Security Metrics

Defining metrics to measure cyber agility. In cyberspace, adaptive strategies are commonly used by both attackers and defenders. For example, an attacker's new strategy often triggers a defender's countermeasures to deal with the new attacks, and vice versa. It is therefore important to have a set of quantitative metrics by which we can characterize and understand the effectiveness of attackers' and defenders' adaptation strategies as an outcome of their interplay. Despite its clear importance, there are no systematic metrics that quantify the effectiveness of cyber attack and defense adaptations. In [22], we propose the first security metric framework with the aim of measuring system agility in terms of the effectiveness of dynamic adaptations by cyber attackers and defenders. The proposed framework is generic and applicable to transform any relevant, quantitative, and/or conventional security metric (e.g., static metrics such as false-positives and false-negatives) into dynamic metrics to capture dynamics of system behaviors. To validate the usefulness of the proposed framework, we conducted a case study that measures the adaptations by cyber attackers and defenders using two real datasets. Through defining a set of adaptation metrics to measure system agility and conducting case studies using real datasets, we discuss the limitations of the current work as well as identify the future work directions that can further enhance the efforts made by this work.

Estimating malware detection metrics in the absence of ground truth. The accurate measurement of security metrics is a critical research problem because an improper or inaccurate measurement process can ruin the usefulness of the metrics, no matter how well they are defined. This is a highly challenging problem particularly when the ground truth is unknown or noisy. In contrast to the well perceived importance of defining security metrics, the measurement of security metrics has been little understood in the literature. In [23], we measure five malware detection metrics in the *absence* of ground truth, which is a realistic setting that imposes many technical challenges. The ultimate goal is to develop principled, automated methods for measuring these metrics at the maximum accuracy possible. The problem naturally calls for investigations into statistical estimators by casting the measurement problem as a *statistical estimation* problem. We propose statistical estimators for these five malware detection metrics. By investigating the statistical properties of these estimators, we are able to characterize when the estimators are accurate, and what adjustments can be made to improve them under what circumstances. We use synthetic data with known ground truth to validate these statistical estimators. Then, we employ these estimators to measure five metrics with respect to a large dataset collected from VirusTotal. We believe our study touches upon a vital problem that has not been paid due attention and will inspire many future investigations.

3.3 Future Directions

We suggest the following action items:

- Security publications should specify explicit definitions of security metrics they use. This effort can be made in terms of both *bottom-up* and *top-down* approaches. For the

bottom-up approach, each publication should define specific security metrics and their attributes. For the top-down approach, the security metrics used should achieve security goals in a broad sense such as five security goals including availability, integrity, confidentiality, non-repudiation, and authentication. One may consider a security metric in terms of its *temporal* characteristics, its *spatial* characteristics, and connect them with the above high-level security goals.

- Security curriculum should include substantial materials for educating and training future generations of security researchers and practitioners with a systematic body of knowledge in security metrics. This has been largely hindered by the lack of systematic treatment. We hope to see more curriculum materials on security metrics.

- Security metrics research should be proceeded based on productive collaboration between the government, industry, and academia. Only leading by one party, either the government or industry/academia, cannot achieve developing a generic security metric framework which can be widely accepted and used by research community. In particular, while academic researchers tend to be obligated to propose *what to measure*, they often encounter the lack of real data for verification and validation of their proposed metrics. The industry may have datasets, but is often prohibited from sharing them with academic researchers because of legitimate concerns (e.g., privacy). Although the government has already incentivized data sharing through projects such as `PREDICT` (www.predict.org), our research experience hints that semantically richer data is imperative for tackling the problem of security metrics. Thus, the productive collaboration between these three parties is the first step for security metrics research to be fruitful in a meaningful way.

References

[1] Shouhuai Xu. *"Grey-Box" Cybersecurity Data Analytics*. Invited presentation at the USAF RATPAC Working Group, Tampa, FL, April 6, 2016.

[2] Zhenxin Zhan, Maochao Xu, Shouhuai Xu. *Characterizing Honeypot-Captured Cyber Attacks: Statistical Framework and Case Study*. IEEE Transactions on Information Forensics and Security 8(11): 1775-1789 (2013).

[3] Zhenxin Zhan. *A Statistical Framework for Analyzing Cyber Attacks*. PhD Thesis. Department of Computer Science, University of Texas at San Antonio, May 2014.

[4] Zhenxin Zhan, Maochao Xu, and Shouhuai Xu. *Predicting Cyber Attack Rates With Extreme Values*. IEEE Transactions on Information Forensics and Security 10(8): 1666-1677 (2015).

[5] Yu-Zhong Chen, Zi-Gang Huang, Shouhuai Xu, and Ying-Cheng Lai. *Spatiotemporal patterns and predictability of cyberattacks*. PLoS ONE 10(5): e0124472. doi: 10.1371/journal.pone.0124472. pmid:25992837. Published: June 22, 2015.

[6] Chen Peng, Maochao Xu, Shouhuai Xu, and Taizhong Hu. *Modeling and Predicting Extreme Cyber Attack Rates via Marked Point Processes*. Journal of Applied Statistics, Vol. 44, Issue 14, pp 2534-2563, 2017.

[7] Zhenxin Zhan, Maochao Xu, Shouhuai Xu. *A Characterization of Cybersecurity Posture from Network Telescope Data*. Proceedings of the 6th international conference on trustworthy systems (InTrust'2014), Springer.

[8] Maochao Xu, Lei Hua and Shouhuai Xu. *Vine Compula Models for Characterizing and Predicting the Effectiveness of Early-Warning in Cyber Defense*. Technometrics, accepted for publication, 2016.

[9] Shouhuai Xu. *Cybersecurity Dynamics*. Proceedings of the 2014 Symposium and Bootcamp on the Science of Security (HotSoS14).

[10] Ren Zheng, Wenlian Lu, and Shouhuai Xu. *Preventive and Reactive Cyber Defense Dynamics Is Globally Stable*. `http://arxiv.org/pdf/1602.06807.pdf`, Accepted to IEEE Transactions on Network Science and Engineering, 2017.

[11] Gaofeng Da, Maochao Xu, and Shouhuai Xu. *On the Quasi-Stationary Distribution of SIS Models*. Probability in the Engineering and Informational Sciences, Volume 30, Issue 4, pages 622-639, 2016.

[12] Zhen Li, Hai Jin, Deqing Zou, and Shouhuai Xu. *VulPecker: An Automated Vulnerability Detection System Based on Code Similarity Analysis*. Proceedings of the 2016 Annual Computer Security Applications Conference (ACSAC'2016), pp 201-213.

[13] A. Tyra, Jingtao Li, Y. Shang, S. Jiang, Y. Zhao, and S. Xu. *Robustness of non-interdependent and interdependent networks against dependent and adaptive attacks*. Physica A 482 (2017) 713-727.

[14] Xiaoxiao Hu, Maochao Xu, Shouhuai Xu, and Peng Zhao. *Multiple cyber attacks against a target with observation errors and dependent outcomes: Characterization and optimization*. Rel. Eng. & Sys. Safety 159: 119-133 (2017).

[15] J. Mireles, J. Cho, and S. Xu. *Extracting Attack Narratives from Traffic Datasets*. The 1st International Conference on Cyber Conflict in the U.S. (CyCon U.S. '2016).

[16] Maochao Xu, Gaofeng Da, and Shouhuai Xu. *Cyber Epidemic Models with Dependencies*. Internet Mathematics, DOI:10.1080/15427951.2014.902407, 11:1, pages 62-92, 2015.

[17] Li Xu. *Characterizing and Detecting Malicious Websites*. PhD Thesis. Department of Computer Science, University of Texas at San Antonio, May 2014.

[18] Li Xu, Zhenxin Zhan, Shouhuai Xu, and Keying Ye. *An Evasion and Counter-Evasion Study in Malicious Websites Detection*. Proceedings of IEEE 2014 Conference on Communications and Network Security (IEEE CNS'14), pp 265-273.

[19] Marcus Pendleton, Richard Garcia-Lebron, Jin-Hee Cho, Shouhuai Xu: *A Survey on Systems Security Metrics*. ACM Computing Survey 49(4): 62:1-62:35 (2017)

[20] JIN-HEE CHO, SHOUHUAI XU, PATRICK M. HURLEY, MATTHEW MACKAY, TREVOR BENJAMIN, and MARK BEAUMONT. *STRAM: Measuring the Trustworthiness of Computer-based Systems*, in submission, 2017.

[21] Jin-Hee Cho, Patrick M. Hurley, and Shouhuai Xu. *Metrics and measurement of trustworthy systems*. MILCOM 2016: 1237-1242

[22] Jose David Mireles, Eric Ficke, Jin-Hee Cho, Patrick Hurley, and Shouhuai Xu. *Metrics Towards Measuring Cyber Agility*, in submission, 2017.

[23] Pang Du, Zheyuan Sun, Huashan Chen, Jin-Hee Cho, and Shouhuai Xu. *Statistical Estimation of Malware Detection Metrics in the Absence of Ground Truth*, in submission, 2017.

4 Appendix: Listing of Publications

1. Zhenxin Zhan, Maochao Xu, Shouhuai Xu. *Characterizing Honeypot-Captured Cyber Attacks: Statistical Framework and Case Study*. IEEE Transactions on Information Forensics and Security 8(11): 1775-1789 (2013).

2. Zhenxin Zhan, Maochao Xu, and Shouhuai Xu. *Predicting Cyber Attack Rates With Extreme Values*. IEEE Transactions on Information Forensics and Security 10(8): 1666-1677 (2015).

3. Yu-Zhong Chen, Zi-Gang Huang, Shouhuai Xu, and Ying-Cheng Lai. *Spatiotemporal patterns and predictability of cyberattacks*. PLoS ONE 10(5): e0124472. doi: 10.1371/journal.pone.0124472. pmid:25992837. Published: June 22, 2015.

4. Maochao Xu, Lei Hua and Shouhuai Xu. *Vine Compula Models for Characterizing and Predicting the Effectiveness of Early-Warning in Cyber Defense*. Technometrics, accepted for publication, 2016.

5. *An Evasion and Counter-Evasion Study in Malicious Websites Detection*. Proceedings of IEEE 2014 Conference on Communications and Network Security (IEEE CNS'14), pp 265-273.

6. Marcus Pendleton, Richard Garcia-Lebron, Jin-Hee Cho, Shouhuai Xu: *A Survey on Systems Security Metrics*. ACM Computing Survey 49(4): 62:1-62:35 (2017)

7. JIN-HEE CHO, SHOUHUAI XU, PATRICK M. HURLEY, MATTHEW MACKAY, TREVOR BENJAMIN, and MARK BEAUMONT. *STRAM: Measuring the Trustworthiness of Computer-based Systems*, in submission, 2017.