REPORT DOCUMENTATION PAGE

AFRL-SR-AR-TR-04-

0454

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED (From - To)
04-09-2004	Final	1-9-2001 to 28-2-2004

4. TITLE AND SUBTITLE
CIPIA Fellow in Survivable Information Systems

5a. CONTRACT NUMBER
F49620-01-1-0340

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
61103D

6. AUTHOR(S)
PI: Pradeep K. Khosla, co-PI: Gregory R. Ganger

5d. PROJECT NUMBER
3484I

5e. TASK NUMBER
S

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Carnegie Mellon University

Office of Research Contracts
5000 Forbes Avenue
Pittsburgh, PA 15213-3890

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Air Force Office of

4015 Wilson Blvd.
Arlington, VA 22203-1954

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

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution unlimited.

20040910 060

13. SUPPLEMENTARY NOTES

14. ABSTRACT
This project leveraged ongoing IA/survivability research and a critical mass of collaborators to train, mentor, and develop three post-PhD Fellows into top-notch IA researchers/faculty. These researchers all now lead IA research efforts at Carnegie Mellon. Dr. Chenxi Wang joined CMU as a CIPIA Fellow, and the support helped her frame and launch her research program; she is now a research faculty at CMU. Dr. Chris Long joined CMU as a CIPIA fellow to shift his previous human-computer interaction research experience to a new focus: security-centric design for human-computer interfaces; he currently leads two such efforts at CMU and expects to soon take a job at the National Security Agency in this area. Dr. James Hoe became a CIPIA Fellow to augment his computer architecture expertise with computer security knowledge to initiate new research in hardware support for secure/trusted computing; as an Assistant Professor, he now leads research in this space. In summary, this CIPIA Fellows project has been extremely successful at meeting its original goals.

15. SUBJECT TERMS
Information Assurance, Survivable Systems, Intrusion Tolerance, Computer Security

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Dr. Pradeep Khosla
UNCLAS	UNCLAS	UNCLAS	UNCLAS	7	19b. TELEPHONE NUMBER *(include area code)*

Final Report for Project AFOSR-Critical Infrastructure Protection Information Assurance Fellowship

PI: Pradeep Khosla
Carnegie Mellon University

The Critical Infrastructure Protection Information Assurance Fellowship awarded to CMU from AROSR started from September 2001 and lasted till December 2003. The fellowship supported three CIPIA fellows: Dr. Chenxi Wang, Dr. Chris Long, and Dr. James Hoe. This report details the achievements of the fellows as a result of the support.

1 Fellow—Dr. Chenxi Wang

Dr. Chenxi Wang joined CMU as a CIPIA fellow in September, 2001. She was supported by the CIPIA fellowship from September 2001 to November 2003. The fellowship support has kickstarted her research program in CMU. Since she came to CMU, Dr. Wang started three major research thrusts. They are:

Security and Privacy for large scale information dissemination systems: In this project, the research focus is to add security and privacy mechanisms on top of information dissemination in a wide area network. The specific purposes of this project is to add security and fault tolerance to publish/subscribe systems and to study privacy concerns for communication systems. The privacy concerns are designed against powerful adversaries that can compromise large amounts of network resources. This project currently has two focuses. The first is to study attacks against mix-based private communication systems. This work has uncovered previously unknown timing attacks: we showed in our study that mix-based privacy communication systems are particularly vulnerable to traffic injection/deletion attacks. The second focus is using Peer-to-peer information systems to provide secure content-based services. To this end, the project has yielded an innovative design of an information dissemination system that combines the benefits of efficient routing in P2P and expressive subscription languages in publish/subscribe systems.

This project produced a conference publication in 2004 Financial Cryptology, and a workshop publication in 2004 Workshop for Distributed Event-based Systems. The fellow is currently advising two students on this project. She plans to extend this work into the domain of censorship resistance for P2P networks.

- *The Coral Project: Automatic defense against viruses and worms on the Internet*: Virus and worm attacks are a prevalent threat against today's computer networks and systems. The voracity of the recent high profile attacks such as Slammer and Blaster means that the traditional "patch-them-n-go" approach simply does not work—we need automated detection and defense mechanisms. The coral project at CMU focuses on developing a comprehensive detection and defense architecture against widespread virus and worm attacks. The first phase of this project focused on modeling and understanding the fundamental characteristics of malicious spread. On that front, the research yielded three major results: a)we developed a new topology-independent mathematical model for malicious spread, b)we developed a universal epidemic threshold condition which predicts exactly whether a particular infection will attain widespread, and c)we developed analytic models for viral spread that incorporates external human-induced factors such as user vigilance. These new models are proven to be more accurate than previous proposals. In addition, they work on arbitrary network topology—previous models are constructed for special-case graphs. In summary, the models we developed enhanced our fundamental understanding of the ways in which malicious code spreads on the Internet and helped to shed new light on potential defense mechanisms.

  The coral project is now entering it's second year and we are focusing on defense strategies. We are currently collecting traffic traces from our local network, and also from our industry partners, Symantec and Akamai. We are studying these traces to uncover unique traffic patterns during worm attacks. Some preliminary findings of this study will be reported in an uncoming paper in WORM'04. In this paper, we reported our study of two mass-mailing worms: SoBig, and MyDoom. Our study showed that distinct IP traffic patterns do emerge during the time of attack. More specifically, we identified anomalous traffic behavior with respect to destination IP addresses and the patterns of DNS queries. These patterns can be used in engineering behavior blocking mechanisms, which is the topic of our current research.

  Dr. Wang has partnered with CERT and Symantec on this effort and has procured an NSF medium ITR award for follow-up efforts. She also has

produced three publications in top conferences in the first year of this project.

- *Survivable Storage Systems*: This is a collaborative effort between Dr. Wang and the PASIS project (funded by DARPA). This effort focused on developing secure and reliable storage system for long-lived data. The problem of storage solutions for long-lived data with security implications is an unexplored area. In this project, we based our solution on a well-known cryptographic primitive: secret sharing. We developed a storage scheme that secret-shares the secret data and periodically redistributes the secret shares to different machines so as to maintain the reliability and security assurance of the scheme. This work is novel because it is one of the very few dynamic secret sharing schemes exist today that allows dynamic redistribution of the secrets to arbitrary machines. To the best of our knowledge, it is the only implementation of dynamic secret sharing application. This work produced a design and prototype implementation of the storage scheme. The research also produced a Ph.D. dissertation and a workshop publication.

For each of these research directions, Dr. Wang has collaborated with researchers in academia as well as in industry. She is currently advising three Ph.D. students and two Master's students who are conducting research in the above areas.

Dr. Chenxi Wang and her students published the following papers as a result of the CIPIA support fellowship support.

1. "A Study of Mass-mailing Worms", C. Wong, S. Bielski, J. McCune, and C. Wang. To appear in the proceedings of the 2004 Workshop of Rapid Malcode (WORM'04). October, 2004. Washington D.C. To be held in conjunction with the 2004 ACM's Computer and Communications Security Conference.

2. "Dynamic Quarantine of Internet Worms". C. Wong, C. Wang, D. Song, S. Bielski, and G. Ganger. In the proceedings of the 2004 IEEEIFIP Dependable Systems and Networks, (DSN 04), June 29—July 2nd. Florence, Italy.

3. "Providing content-based services in a Peer-to-peer Environment". G. Perng, C. Wang, and M. Reiter. In the proceedings of the 2004 workshop of Distributed Event-based Systems (DEBS 04). May 20—22nd. Edingbrough. Scotland.

4. "Modeling Timing Parameters of Virus Propagation on the Internet". Y. Wang and C. Wang. In the proceedings of the 1 st Workshop of Rapid Malcode (WORM 03), held in conjunction with 2003 ACMś Computer and Communications Security, October 27—30th,2003. Washington D.C.

5. "On Timing Attacks for Low-latency Mix-based Systems", B. Levine, M. Reiter, C. Wang, and M. Wright. In the proceedings of the 2004 Financial Cryptology. Feb. 12—14th, Florida.

6. "Epidemic Spreading: An Eigenvalue Viewpoint", Y. Wang, D. Charkarbarti, C. Wang, and C. Faloutsos. In the proceedings of the 2003 Symposium of Reliable and Distributed Systems (SRDS 03). October 4—6th, 2003. Florence. Italy.

7. "The Design and Implementation of A JCA-compliant Capture Protection Infrastructure", M. Reiter, A. Samar, and C. Wa ng. In the proceedings of the 2003 Symposium of Reliable and Distributed Systems (SRDS 03). October 4—6th, 2003. Florence. Italy.

8. "Verifiable Secret Sharing for Archival Storage Systems", T. Wong, C. Wang, and J. Wing. In the proceedings of the 1st Security in Storage Workshop. December, 2002. Greenbelt, Maryland.

During the period of 2001-2003, Dr. Wang applied and successfully procured four federal research grants.

- NSF Trusted Computing award CCR-0208853. "Privacy and Security of Publish/subscribe Systems". PI: Mike Reiter. Co-PI: Chenxi Wang. September 2002 to August 2005. Amount: $562,000.

- NSF medium ITR award ANI-0326472 "Defending against Virus Propagation on the Internet". PI: Chenxi Wang. September 2003 to August 2008. Amount: $1,500,000.

- NIST award: "Secure and Dynamic Network". PI: Chenxi Wang. October 2002 to August 2004. Amount: $200,000.

- DARPA SRS Award: "Genesis: A framework for achieving component diversity". PI: John C. Knight. Subaward to CMU, Subcontractor: Chenxi Wang. September 2004 to March 2005. Sub-award amount: $150,000

Dr. Chenxi Wang has applied for the following award (decision pending)

- NSF CyberTrust Center: "Security Through Interaction Modeling". PI: Mike Reiter, Co-PI: Jennette Wing, Chenxi Wang, Dena Tsamitis, and Bruce Maggs. Duration: September 2004 to August 2009, Amount: $9,500,000.

2 Fellow—Dr. Chris Long

Dr. Chris Long joined CMU as a CIPIA fellow in August 2002. Dr. Long's training was in Human Computer Interface, and the fellowship grant allowed him to bring a new focus to his research—security-centric design for Human-computer interfaces. Dr. Long started the follwing research projects while in CMU.

- *Castellan: A Management Tool for Distributed Intrusion Detection.* Many organizations use intrusion detection systems (IDSs) to protect themselves against threats such as viruses and attacks. We are developing new self-securing devices (e.g., self-securing storage and NIC-based firewalls), to provide increased security by creating separate, smaller security domains. However, this distribution of security raises significant administrative challenges.

  To display and manage security alerts, we are developing Castellan, a software tool for managing distributed intrusion detection systems. Castellan will support network administrators in configuration, detection, diagnosis, and recovery.

  We are investigating how to correlate security alerts from different types of self-securing devices to reduce the incidence of false alarms and to increase the specificity of information presented to the security administrator. We believe this approach will allow our system to scale to allow self-securing devices on every desktop.

- *Chameleon: Towards Improved Desktop Security.* Current security software available to and usable by typical home computer users, such as anti-virus software, is helpful but inadequate to the growing threat of malicious software (viruses, trojan horses, etc.). Commonly available access control mechanisms, such as file permissions or access control lists (e.g., in Microsoft Windows), could provide more security in theory, but they are too fine-grained and cumbersome; as a result, they are not used. Chameleon seeks to simplify security management for desktop computers to reduce the impact of malicious software. The Chameleon security model uses coarse-grained partitioning of applications and data, based on roles, and its user interface is designed for easy management of a role-based desktop. Partitioning reduces the impact of a virus, for example, because if a virus infects a role, only the data in the infected role will be vulnerable rather than the whole computer as is common today. In Chameleon, users can trade off security and convenience by choosing how many roles to use and deciding how to assign data and applications to them.

Chameleon is inspired by previous work on sandboxing, partitioning, and role-based access control, however, it starts not with security mechanisms but with making the security features intelligible, convenient, and usable to a broad group of users. We believe it is possible to create a role-based desktop that provides another layer of protection from malicious software and is usable by typical home computer owners. Preliminary user studies with a prototype of the user interface support this belief.

We also plan to use Chameleon to explore larger issues in human-computer interaction and security, such as how much control over and awaress of security is optimal, and in what software layer security should be implemented.

Dr. Long and his colleagues published the following paper:

1. A. Chris Long, Courtney Moskowitz, and Greg Ganger. "A Prototype User Interface for Coarse-Grained Desktop Access Control." Technical Report CMU-CS-03-200, Carnegie Mellon University, 2003. Available at http://reports-archive.adm.cs.cmu.edu/cs2003.html.

3 Fellow—Dr. James Hoe

Dr. James Hoe became a CIPIA fellow in summer 2002. Dr. Hoe has an appointment as an Assistant Professor in the Department of Electrical and Computer Engineering. The fellowship provided part time support for Dr. Hoe, and it allowed him to kickstart the following research efforts:

- Secure Architecture: This joint effort with Prof. Greg Ganger and Prof. Adrian Perrig combines three disjoint areas of expertiseoperating systems, computer security and computer architectureto explore new processor protection primitives that enable the development and execution of intrusion tolerant software. We look to hardware to provide simple but effective security enforcements that could not be violated regardless of accidental or intentional software misbehavior. The project is currently focused on new processor memory protection to allow fine-grain compartmentalized protection of modules within with a single (kernel) process.

- Fault-Tolerant Architecture: This research investigates the impact of soft-error tolerance in future deep-submicron microprocessor designs. The study proposes and investigates different options to achieve the desired level of protection against soft errors. Currently, we propose a fault-tolerant extension to modern superscalar out-of-order datapath that can be supported by only modest additional hardware. This research is also related to the TRUSS

project (http://www.ece.cmu.edu/ truss/) to develop a reliable, available, and serviceable (RAS) hardware platform based on a distributed cluster of commodity blade servers. The TRUSS project is a joint project with Prof. Babak Falsafi and Prof. Andreas Nowatzyk.

- DSP Hardware Synthesis: This research develops a domain-specific hardware synthesis framework for digital signal processing (DSP) computations. By incorporating domain-specific knowledge of mathematics and algebra into a synthesis tool, the proposed framework can manipulate a math-level transform description to optimize a DSP transform implementation at the algorithmic and architectural design level. This research is a part of the SPIRAL DSP compiler project (www.spiral.net).

The fellows plan to pursue their respective research agenda further after the end of the fellowship support.