

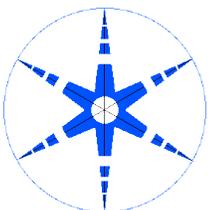
Sixth Annual Cyber Security and Information Intelligence Research Workshop

April 21-23, 2010

CYBER SECURITY
AND INFORMATION
INTELLIGENCE
CHALLENGES
AND STRATEGIES



Frederick Sheldon, Stacy Prowell,
Axel Krings, and Robert Abercrombie (Editors)



OAK RIDGE NATIONAL LABORATORY

MANAGED BY UT-BATTELLE FOR THE DEPARTMENT OF ENERGY



CSIRW10: Cyber Security and Information Intelligence Research Workshop

April 21-23, 2010

Oak Ridge National Laboratory, Oak Ridge, Tennessee, USA

Frederick Sheldon, Stacy Prowell, Axel Krings, and Robert Abercrombie (Editors)

Cyber security and information intelligence challenges and strategies

As our dependence on the cyber infrastructure grows more complex and more distributed, the systems that compose it become more prone to failures and exploitation. Intelligence refers to discrete or private information, which possess currency and relevance. The ability to abstract, evaluate, and understand such information underlies its accuracy and true value. The collection, analysis and utilization of information constitutes a business-, sociopolitical-, military-intelligence activity that ultimately poses significant advantages and liabilities to the survivability of "our" society.

The aim of this workshop (www.csiir.ornl.gov/csiirw) was to discuss (and publish) novel theoretical and empirical research focused on the many different aspects of cyber security and information intelligence. The scope will vary from methodologies and tools to systems and applications to more precise definition of the various problems and impacts. Topics include:

- Scalable trustworthy systems
- Enterprise-level metrics
- Coping with insider and life-cycle threats
- Coping with malware and polymorphism
- Phishing/whaling, spam and cyber crime
- High assurance system survivability
- Cyber security for the Smart Grid
- Digital provenance and data integrity
- Privacy-aware security and usable security
- Social networking models for managing trust and security

A principle goal of the workshop was to foster discussions and dialog among the 150 registered attendees from North America, Europe, Asia, and Africa. This goal was initiated and facilitated by 14 plenary keynote addresses including a banquet presentation and the CIO / CTO perspectives panel. A total of 98 papers (i.e., extended abstracts [EAs]) were submitted and 54 EAs were accepted plus 11 posters were invited. All of the abstracts and either presentation materials or posters are included in the proceedings. The subject areas span the topics above and were organized into eight tracks: Trust, Design, Malware, Network, Privacy and Metrics, Enterprise, Survivability and Formal Methods. Nearly all of the keynote presentations were video recorded and can be reviewed at <https://share.ornl.gov/sites/csiirw-videos/> (SharePoint registration is required).

Table of Contents for the Proceedings of CSIIRW 2010

Oak Ridge National Laboratory, Oak Ridge, TN 37831

Plenary and Panel Sessions[†]:

1. Susan Alexander, Senior Advisor and Chief, Initiative Integration, Joint Interagency Cyber Task Force, Office of the Director of National Intelligence, Keynote (Wed. 8:00 AM), Presentation Title: Change the game or win the war: The metaphor matters (s, v)
2. Hart Rossman, Vice President, CTO Cyber Security Solutions, SAIC, Schedule: Keynote (Wed. 8:45 PM) & CIO/CTO Perspectives Panel (Thu. 12:15), Presentation Title: Gov 2.0 and Collaborative Security Models: Security Platforms and Architectures of Participation Are the Foundations of a Winning Strategy (s, v)
3. Sean McGurk, Director, Control Systems Security Program, National Cyber Security Division, Department of Homeland Security, Keynote (Wed. 12:15 PM), Presentation Title: Coordinating and Guiding Federal, State and Private Sector Cybersecurity Initiatives (v)
4. Professor Nabil Adam, Fellow, Infrastructure & Geophysical Division, Science & Technology Directorate, US Department of Homeland Security, and Professor of Computers and Information Systems, Rutgers University, Schedule: Keynote (Wed. 1:00 PM), Presentation Title: Cyber Physical Systems R&D at DHS Science and Technology Directorate (v)
5. Jim Stikeleather, Chief Technology Officer, Dell Services, Schedule: Keynote (Wed. 4:15 PM) & CIO/CTO Perspectives Panel (Thu. 12:15), Presentation Title: Next Generation Computing: The Rise of the Utility in a Future that is Cloudy with Scattered Security (s, v))
6. Gareth J. Moravec, Director, Cyber and Information Assurance, Lockheed Martin Aeronautics Corporation, Schedule: Banquet (Wed. PM) & CIO/CTO Perspectives Panel (Thu.), Presentation Title: Holistic Cyber Approach (s, v))
7. Professor David Nicol, Department of Electrical and Computer Engineering (ECE) and Information Trust Institute, University of Illinois at Urbana-Champaign, and Director of the Center for Assured Critical Applications and Infrastructure Security (CACAIS), Schedule: Keynote (Thu. 8:00 AM), Presentation Title: Securing the Perimeter : Challenges in Enforcing Global Access Control (s, v)
8. Dr. James Whittaker, Director of Test Engineering, Google, Schedule: Keynote (Thu. 8:45 AM), Presentation Title: How Google Tests Software (s, v)
9. Scott Augenbaum, Supervisory Special Agent, Federal Bureau of Investigation, Schedule: Keynote (Thu. 3:30 PM), Presentation Title: A Break Down in Trust, the Emerging Threat of Cyber Crime in Connection with Our Dependence on Web 2.0 Technologies
10. Dr. Tom Longstaff, Senior Information Assurance (IA) Advisor, Information Warfare Systems Branch, Applied Information Science Department of the Applied Physics Laboratory (APL), The Johns Hopkins University, Schedule: Keynote (Thu 4:15 PM), Presentation Title: Cyber Science – Moving from the Toes to the Shoulders of Giants (s, v)
11. Melissa Hathaway, President, Hathaway Global Strategies, and Senior Advisor at Harvard Kennedy School's Belfer Center for Science and International Affairs, Harvard University,

[†] S – indicates slides are available, V – indicates video is available online www.csiiirw.gov/csiiirw

- Schedule: Keynote (Fri. 8:00 AM) & CIO/CTO Perspectives Panel (Thu. 12:15 PM),
Presentation Title: Cyberspace Policy Review and Blueprint for Research Priorities (v)
12. Rich Pethia, Director, Community Emergency Response Teams (CERT) Program at Carnegie Mellon University's Software Engineering Institute (SEI), Schedule: Keynote (Fri. 8:45 AM) & CIO/CTO Perspectives Panel (Thu. 12:15 PM), Presentation Title: 20+ Years of Cyber (in)Security: What have we seen? What have we learned? What might we do? (s, v)
 13. Dawn Cappelli, Senior Member of Technical Staff, Software Engineering Institute, Schedule: Keynote (Fri. 12:15 PM), Presentation Title: Risk Mitigation Strategies: Lessons Learned from Actual Insider Attacks (s, v)
 14. Professor Michael R. Grimaila, Department of Systems and Engineering Management, Air Force Institute of Technology, Air Force Research Laboratory, Schedule: Keynote (Fri. 3:30 PM), Presentation Title: Mission Assurance: Challenges and Opportunities (s, v)
 15. Thomas Overman, Chief Architect, Energy Solutions Cyber Security, Boeing Defense, Space & Security, Schedule: CIO/CTO Perspectives Panel (Thu. 12:15 PM Panelist) (v)
 16. Michael E. Bartell, Chief Information Officer, Oak Ridge National Laboratory, Schedule: CIO/CTO Perspectives Panel (Thu. 12:15 PM Panelist) (v)

Panel Discussions:

1. "Keynote CIO/CTO Perspectives Panel" with panelists (v)
 - a. Melissa Hathaway (President, Hathaway Global Strategies, and Senior Advisor at Harvard Kennedy School's Belfer Center for Science and International Affairs, Harvard University Harvard University),
 - b. Garett J. Moravec (Director, Cyber and Information Assurance, Lockheed Martin Aeronautics Corporation),
 - c. Thomas Overman (Chief Architect, Energy Solutions Cyber Security Boeing Defense, Space & Security),
 - d. Rich Pethia (Director, CERT Program at Carnegie Mellon University's SEI),
 - e. Hart Rossman (Vice President, CTO Cyber Security Solutions, SAIC),
 - f. Jim Stikeleather (Chief Technology Officer, Dell Services) and
 - g. Michael E. Bartell (Chief Information Officer, Oak Ridge National Laboratory)

Track1: Design

1. "Cuckoo Bags for Exploring Multikey Data" John McHugh, Teryl Taylor and Jeff Janies
2. "PUF ROKs: Generating Read-Once Keys from Physically Unclonable Functions", Michael Kirkpatrick, Elisa Bertino and Sam Kerr
3. "Towards Safe and Productive Development of Secure Software: FADES and Model- Based Software Engineering Riham Hassan, Shawn Bohner and Mohamed Eltoweissy

4. "Implementation of the PowerCyber SCADA Cyber Security Testbed", Adam Hahn and Manimaran Govindarasu
5. "Forensic Implications of Ext4", Kevin Fairbanks, Christopher Lee and Henry Owen
6. "Data Diodes in Support of Trustworthy Cyber Infrastructure", Hamed Okhravi and Frederick Sheldon
7. "Software Process Control for Secure Program Execution", John Munson, Jack Meador and Rick Hoover
8. "Graph Based Strategies to Role Engineering", Dana Zhang, Kotagiri Ramamohanarao, StevenVersteeg and Rui Zhang
9. "A Java Based Component Identification Tool for Measuring the Strength of Circuit Protections", James Parham, J. Todd McDonald, Michael Grimaila and Yong Kim
10. "SecureMyDroid: Enforcing Security in the Mobile Devices Lifecycle", Alessandro Distefano, Antonio Grillo, Alessandro Lentini and Giuseppe Francesco Italiano

Track 2: Malware

1. "Cyber Security Analysis using Attack Countermeasure Trees", Arpan Roy, Dong-Seong Kim and Kishor Trivedi
2. "Vulnerability Categorization Using Bayesian Networks", Andy Wang and Minzhe Guo
3. "Concordia: A Google for Malware", Timothy Daly and Luanne Burns
4. "Towards an Empirical Measure for Assessing Public Attitudes Regarding Government Cybercrime Countermeasures", Stan Bowie, Brenda Lenard and Craig Shue
5. "Adding Value to Log Event Correlation Using Distributed Techniques", Justin Myers, Michael Grimaila and Robert Mills
6. "A Reference Based Analysis Framework for Analyzing System Call Traces", Varun Chandola, Shyam Boriah, and Vipin Kumar
7. "Game Theory for Cyber Security", Sajjan Shiva, Sankardas Roy and Dipankar Dasgupta
8. "The Handicap Principle, Strategic Information Warfare and the Paradox of Asymmetry", Zhanshan (Sam) Ma, Frederick Sheldon and Axel Krings
9. "Computing the Behavior of Malware", Rick Linger, Mark Pleszkoch and Kirk Sayre
10. "A Data Security Protocol for the Trusted Truck® System", Srinivasa Anuradha Bulusu, Itamar Arel, Benjamin Arazi, Andrew Davis and George Bitar
11. "Multi-Variant Program Execution for Vulnerability Detection and Analysis", Todd Jackson, Christian Wimmer and Michael Franz
12. "Local Binary Patterns for Face Recognition under Varying Variations", Yang Zhang, Taolun Chai and Chih-Cheng Hung

Track 3: Network

1. "Neighborhood Monitoring in Ad Hoc Networks", Axel Krings and Stephan Muehlbacher-Karrer
2. "Alerts Visualization and Clustering in Network-based Intrusion Detection", Swetha Dasireddy, Wade Gasior, Yang Li and Xiaohui Cui
3. "Towards A Secure Frequency Monitoring Network (FNET) System", Joseph McDaniel and Ambareen Siraj
4. "Towards Trustworthy Shared Sensor-Actuator Networks", Ramy Eltarras, Mohamed Eltoweissy, Stephan Olariu and Ing-Ray Chen
5. "Extracting Security Control Requirements", John Hosey and Rose Gamble
6. "Fast Malware Classification by Automated Behavioral Graph Matching", Younghee Park and Douglas S. Reeves
7. "A Security Ontology for Incident Analysis", Clive Blackwell
8. "NgViz: Detecting DNS Tunnels through N-Gram Visualization and Quantitative Analysis", Kenton Born and David Gustafson
9. "Propagation Modeling and Analysis of Network Work Attack", Ossama A. Toutonji, Seong-Moo Yoo, and Moongyu Park
10. "Plug & Execute Framework for Network Traffic Generation", Uta Ziegler, Youssif Al-Nashif and Salim Hariri
11. "A Service Model for Network Security Applications", Livio Ricciulli
12. "Multi stage attack Detection System for Network Administrators using Data Mining" Rajeshwar Katipally, Wade Gasior, Xiaohui Cui and Yang Li
13. "The Privacy Implications of Stateless IPv6 Addressing", Stephen Groat, Matthew Dunlop, Randy Marchany and Joseph Tront
14. "The Need to Consider Both Object Identity and Behavior in Establishing the Trustworthiness of Network Devices within a Smart Grid", Owen Mccusker, Benjamin Gittins, Joel Glanfield, Scott Brunza and Stephen Brooks
15. "Vulnerabilities Leading to Denial of Services Attacks in Grid Computing Systems: a Survey", Wonjun Lee, Anna Squicciarini and Elisa Bertino

Track 4: Privacy and Metrics

1. "Modeling Stakeholder/Value Dependency Through Mean Failure Cost", Anis Ben Aissa, Robert Abercrombie, Frederick Sheldon, and Ali Mili
2. "Threat Agents: a Necessary Component of Threat Analysis", Claire Vishik, Timothy Casey and Patrick Koeberl
3. "Orwell Was an Optimist", RyanCraven, Christopher Abbott, Harikrishnan Bhanu, Juan Deng and Richard Brooks

Track 5: Enterprise

1. "Ontologies for Modeling Enterprise Level Security Metrics", Anoop Singhal and Duminda Wijesekera
2. "Lies and the Lying Liars that Tell Them: A Fair and Balance Look at TLS", Richard Brooks
3. "Overview of SLL's Proposal in Response to NIST's Call for New Global IdM/CKM Designs Without Public Keys", Benjamin Gittins
4. "High Assurance Smart Grid - Architecture for Cyber Security and Reliability", Thomas Overman, Ronald Sackman and Terry Davis
5. "Power, Performance and Security optimized Hardware Design for H.264", Mahadevan Gomathisankaran, Gayatri Mehta and Kamesh Namuduri
6. "Reasoning about Policy Noncompliance", Robert Baird and Rose Gamble

Track 6: Survivability

1. "Decentralized Information Flow Control on a Bare-Metal JVM", Karthikeyan Manivannan, Christian Wimmer and Michael Franz
2. "Building a Trusted Image for Embedded Communication Systems", Jack Harris and Raquel Hill
3. "An Organic Model for Detecting Cyber-Events", Christopher Oehmen, Scott Dowson and Elena Peterson

Track 7: Formal Methods

1. "Using Formal Methods for Security in the Xenon Project", John McDermott
2. "Discovery of C++ Data Structures From Binaries", Daniel Quinlan and Cory Cohen
3. "On Generalization Performance of Classifiers for Steganalysis", Josef Allen, Xiuwen Liu, Liam Mayron and Washington Mio

Track 8: Trust

1. "A Learning-Based Approach for SELinux Policy Optimization with Type Mining", Said Marouf and Mohamed Shehab
2. "ReDS: Reputation for Directory Services in P2P Systems", Matthew Wright, Apu Kapadia, Mohan Kumar and Apurv Dhadphale
3. "Augmenting Trust Mechanisms with Social Networks", Brent Lagesse, Mohan Kumar, Mihai Lazarescu and Svetha Venkatesh

Track 9: Posters

1. "Software Requirements for a System to Compute Mean Failure Cost", Anis Ben Aissa, Robert K. Abercrombie, Frederick T. Sheldon and Ali Mili
2. "Developing Cyberspace Data Understanding: Using CRISP-DM for Host-based IDS Feature Mining", Joseph R. Erskine, Gilbert L. Peterson, Barry E. Mullins, Michael R. Grimaila

3. "The Impact of Predicting Attacker Tools in Security Risk Assessments", Ezequiel Gutesman and Ariel Waissbein
4. "Evaluating Confidence Levels for Security Scenarios in Attribute Architectures", Tacksoo Im and John D. McGregor
5. "Safety and Security in Industrial Control", Andrew J. Kornecki and Janusz Zalewski
6. "Positing Social and Justice Models for Cyber Security", Michael Losavio, J. Eagle Shutt and Deborah Keeling
7. "Building Ontology of Cybersecurity Operational Information", Takeshi Takahashi, Hiroyuki Fujiwara and Youki Kadobayashi
8. "Degrees of Anonymity in Today's Computing Environments: Decomposing Complex Processes for Anonymity Analysis", Giusella Finocchiaro and Claire Vishik
9. "Behavioral Model for Secure Group Communication in Wireless Mesh Networks", Qian Wei, Jingsha He and Xing Zhang
10. "Protecting Senior Citizens from Cyber Security Attacks in the e-Health Scenario: An International Perspective", Haricharan Rengamani, Shambhu Upadhyaya, H. Raghav Rao and Ponnurangam Kumaraguru
11. "A Conceptual Model of Self-Monitoring Multi-Core Systems", Dipankar Dasgupta, Harkeerat Bedi and Deon Garrett

Acknowledgements:

The CSIRW 2010 program committee consisted of Frederick T. Sheldon, Stacy Prowell, and Robert K. Abercrombie (Oak Ridge National Laboratory), Professor Elisa Bertino, Director of CERIAS, Department of Electrical and Computer Engineering, Purdue University, and Professor Axel Krings, Department of Computer Science, University of Idaho.

The CSIRW 2010 program committee wishes to recognize the contributions of the CSIRW 2010 review committee which consisted of Ali Mili, Richard Brooks, Craig Shue, Michael Kirkpatrick, James Nutaro, Clive Blackwell, Erik Ferragut, Akaninyene Udoeyop, Brent Lagesse, Christopher Rathgeb, Krishna Kavi, Gregory Peterson, Lee Hively, Dipankar Dasgupta, Li Liu, Matthew Wright, Stephen Kelly, Xiaohui Cui, Dave Richardson, Steven Fernandez, Nathanael Paul, Anna Squicciarini, Wonjun Lee, Sankardas Roy, Zhanshan Ma, Seong-Moo Yoo, Rick Linger, Tim Daley, Luann Burns, Hamed Okharavi, Qun Ni, Lawrence MacIntyre, Xukai Zou, Murat Kantarcioglu, Mohamed Shehab, Louis Wilder, James Joshi Akaninyene Udoeyop and John Munson as well as the other half whom will remain anonymous. Thirty two percent of the ninety-eight papers that were submitted received 2 reviews while all of the rest of the papers received three or more. We received papers from sixteen countries including Argentina, Australia, Canada, China, Egypt, India, Ireland, Israel, Italy, Japan, Malta, New Zealand, Tunisia, United Kingdom, United States and Viet Nam.