

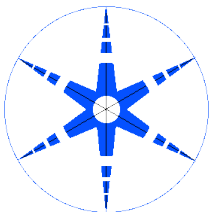
Fourth Annual Cyber Security and Information Intelligence Research Workshop

May 12-14, 2008

DEVELOPING
STRATEGIES TO
MEET THE CYBER
SECURITY AND
INFORMATION
INTELLIGENCE
CHALLENGES AHEAD



Frederick Sheldon, Axel Krings, Robert Abercrombie, and
Ali Mili (Editors)



OAK RIDGE NATIONAL LABORATORY

MANAGED BY UT-BATTELLE FOR THE DEPARTMENT OF ENERGY



CSIIRW08: Cyber Security and Information Intelligence Research Workshop

May 12-14, 2008

Oak Ridge National Laboratory, Oak Ridge, Tennessee, USA

Frederick Sheldon, Axel Krings, Robert Abercrombie, and Ali Mili (Editors)

Developing strategies to meet the cyber security and information intelligence challenges ahead

As our dependence on the cyber infrastructure grows ever larger, more complex and more distributed, the systems that compose it become more prone to failures and/or exploitation. Intelligence is information valued for its currency and relevance rather than its detail or accuracy. Information explosion describes the pervasive abundance of (public/private) information and the effects of such. Gathering, analyzing, and making use of information constitutes a business- / sociopolitical- / military-intelligence gathering activity and ultimately poses significant advantages and liabilities to the survivability of "our" society. The combination of increased vulnerability, increased stakes and increased threats make cyber security and information intelligence (CSII) one of the most important emerging challenges in the evolution of modern cyberspace "mechanization."

The goal of the workshop was to challenge, establish and debate a far-reaching agenda that broadly and comprehensively outlined a strategy for cyber security and information intelligence that is founded on sound principles and technologies. We aimed to discuss novel theoretical and applied research focused on different aspects of software security/dependability, as software is at the heart of the cyber infrastructure.

The workshop scope covered a wide range of methodologies, techniques, and tools to (1) assure, measure, estimate and predict software security/dependability and (2) analyze and evaluate the impact of such applications on software security/dependability. We encouraged researchers and practitioners from a wide swath of professional areas (not only the programmers, designers, testers, and methodologists but also the users and risk managers) to participate. In this way, we can all understand the needs, stakes and context of the ever-evolving cyber world. We looked to software engineering to help provide us the products and methods to accomplish these goals including:

- Better precision in understanding existing and emerging vulnerabilities and threats (e.g., insider threat).
- Advances in insider threat detection, deterrence, mitigation and elimination.
- Game-changing ventures, innovations and conundrums (e.g., quantum computing, QKD, phishing, malware market, botnet/DOS).
- Assuring security, survivability and dependability of our critical infrastructures.
- Assuring the availability of time-critical scalably secure systems, information provenance and security with privacy.
- Observable/ measurable/ certifiable security claims, rather than hypothesized causes.
- Methods that enable us to specify security requirements, formulate security claims, and certify security properties.
- Assurance against known and unknown (though perhaps pre-modeled) threats.
- Mission fulfillment, whether or not security violations have taken place (rather than chasing all violations indiscriminately).

A principle goal of the workshop was to foster discussions and dialog among the 95 attendees from 21 countries. This goal was initiated and facilitated by multiple (daily) keynote speakers and a panel entitled "From Application to Network Security Engineering: Theory and Practice" with panelists John Abeles (System1), Michael Franz (UCI), Steve Lines (SAIC), Patrick Arnold (Microsoft) and Brian Witten (Symantec). A total of 38 papers are included in the proceedings, 6 in the Formal Methods track, 8 in the Intrusion Detection / Insider Threat track, 9 in the Next Generation Security track, 5 in the Security Frameworks track, 5 in the Learning/Optimization track, and 5 in the Metric track.

Table of Contents for the Proceedings of CSIRW 2008

Oak Ridge National Laboratory, Oak Ridge, TN 37831

Plenary Session

1. Richard M. (Dick) Kemmerer, Security Group, UC Santa Barbara, "Electronic Voting Systems: Are Your Votes Really Counted"
2. Patrick Arnold, Federal CTO, Microsoft, "End to End Trust"
3. Steve Lines, Director, Business Continuity and Information Assurance, SAIC, "Best Practices on Information Sharing of Threats and Warnings between the USG and Industry"
4. Michael Franz, Secure Systems and Software Laboratory, UC Irvine, "Eliminating the Insider Threat in Software Development by Combining Parallelism, Randomization and Checkpointing"
5. Mike McDuffie, VP, Public Sector Services, Microsoft "Computing and the Future"
6. Brian Witten, Director of Government Research, Symantec, "Internet Security Threat Landscape: Current Changes in Targets & Methods"
7. Jeff Voas, Director of System Assurance, SAIC, "Thirteen Rules for Trust"

Track: Formal Methods

1. "Secure and Reliable Covert Channel" by B. Ray and S. Mishra
2. "Noisy Defenses: Subverting Malware's OODA Loop" by D. Bilal
3. "Formal Derivation of Security Design Specifications from Security Requirements" by R. Hassan, S. Bohner and S. El-Kassas
4. "Semantics for a Domain-Specific Language for the Digital Forensics Domain" by D. Ray and P. Bradford
5. "Design for Survivability: A Tradeoff Space" by A. Krings
6. "A Rigorous Methodology for Security Architectural Modeling" by Y. Ali and S. El-Kassas

Track: Intrusion Detection/ Insider Threat

1. "Cyber Security and Information Intelligence Research Overview" by J. Trien, R.K. Abercrombie and F.T. Sheldon
2. "Defining the Insider Threat" by M. Bishop and C. Gates
3. "Detecting Sensitive Data Exfiltration by an Insider Attack" by Y. Liu, C. Corbett, K. Chiang, R. Archibald, B. Mukherjee and D. Ghosal
4. "Log-Based Distributed Intrusion Detection for Hybrid Networks" by F. Sailhan and J. Bourgeois

5. "Dynamic Instruction Sequences Monitor for Virus Detection" by J. Dai, R. Guha, and J. Lee
6. "Towards Practical Intrusion Tolerant Systems" by W. Zhao
7. "ULISSE, A Network Intrusion Detection System" by S. Zanero
8. "Real-World Polymorphic Attack Detection using Network-Level Emulation" by M. Polychronakis, K. Anagnostakis and E. Markatos

Track: Next Generation Security

1. "Emergence of Antiforensics in Cyber Security" by B. Schlicher
2. "Extending Hardware Based Mandatory Access Controls for Memory to Multicore Architectures" by B. Sharp, G. Peterson and L. Yan
3. "Active Semantically Aware Hard Real-Time Security Hypervisors" by V. Yodaiken and C. Dougan
4. "Accessing and Manipulating Meaning of Textual and Data Information for Information Assurance and Security and Intelligence Information" by V. Raskin, B. Buck, A. Keen, C. Hempelmann, and K. Triezenberg
5. "Automotive Systems Security: Challenges and State of the Art" by R. R. Brooks, S. Sander, J. Deng and J. Taiber
6. "Quantum Information Opportunities and Challenges" by R. Bennink
7. "Security in a Peer-to-Peer Data Grid Storage System" by L. Xiao and I.L. Yen
8. "End-to-End Accountability in Grid Computing Systems for Coalition Information Sharing" by E. Bertino, W. Lee, A. C. Squicciarini and B. Thuraisingham
9. "Securing Vehicles Against Cyber Attacks" by U. Larson and D. Nilsson

Track: Security Frameworks

1. "NIST PRISMA Enhancement" by J. Abeles
2. "Improving the Cyber Incident Mission Impact Assessment (CIMIA) Process" by R. Grimaila, R. Mills, and L. Fortson
3. "Creating the Secure Software Testing Target List" by R. Martin and S. Barnum
4. "Comprehensive Security in Constrained Environments" by B. Arazi
5. "A Multi-Layered Security Architecture for Modeling Complex Systems" C. Blackwell

Track: Learning/ Optimization

1. "Optimizing Quality of Service (QoS) for Wireless Mobile Ad-Hoc Networks (MANETs) Using Evolutionary Computation" by T. Sapienza

2. "An Abstract Interface for Cyber-Defense Mechanisms" by F. Webber, P. Pal, P. Rubel and M. Atighetchi
3. "Markov Models for Application Behavior Analysis" by G. Mazeroff, J. Gregor and M. Thomason
4. "Peer to Peer Botnet Detection for Cyber-Security: A Data Mining Approach" by M. Masud, J. Gao, L. Khan, J. Han, and B. Thuraisingham
5. "Improving Self Defense Learning from Limited Experience" by K. Haigh and S. Harp

Track: Metrics

1. "Evaluating Security Controls Based on Key Performance Indicators and Stakeholder Mission" by F. Sheldon and R. Abercrombie
2. "A Comprehensive Objective Network Security Metric Framework for Proactive Security Configuration" by M. Ahmed, E. Al-Shaer and L. Khan
3. " Cyber-Vulnerability of Power Grid Monitoring and Control Systems" by C. W. Ten, C. C. Liu and M. Govindarasu
4. "Temporal Metrics for Software Vulnerabilities" by J. Wang, F. Zhang, and M. Xia "Measuring Security Risk of Networks Using Attack Graphs" by A. Singhal, L. Wang, and S. Jajodia