

3rd IEEE International Information Assurance Workshop

College Park, Maryland, USA

March 23-24, 2005

Program



in cooperation with



Program Committee

Blaine Burnham (University of Nebraska Omaha, USA)
Yves Deswarte (LAAS-CNRS, France)
Tim Gibson (DARPA, USA)
Dieter Gollmann (University of Hamburg-Harburg, Germany)
Sushil Jajodia (George Mason University, USA)
John James (United States Military Academy, USA)
Paul Karger (IBM T.J. Watson Labs, USA)
Carl Landwehr (National Science Foundation, USA)
Emil Lupu (Imperial College London, UK)
John McDermott (U.S. Naval Research Laboratory, USA)
Henry L. Owen (Georgia Institute of Technology, USA)
Peter G. Neumann (SRI International Computer Science Laboratory, USA)
Gene Spafford (Purdue University, USA)
Shambhu Upadhyaya (SUNY Buffalo, USA)
John Zachary (IEM Inc., USA)
Yuliang Zheng (University of North Carolina Charlotte, USA)

General Chair

John L. Cole (US Army Research Laboratory, USA)

Program Chair

Stephen D. Wolthusen (Fraunhofer-IGD, Germany)

The workshop is sponsored by the IEEE Computer Society Task Force on Information Assurance. For information on the IEEE TFIA and related activities please refer to <http://www.ieee-tfia.org>

The workshop is held in cooperation with the ACM Special Interest Group on Security, Audit, and Control. For information on the ACM SIGSAC please refer to <http://www.acm.org/sigsac>



3rd IEEE International Information Assurance Workshop

Workshop Program

March 23–24, 2005

0800 — 0845 **Registration / Breakfast**

0845 — 0900 Welcome and Introduction

Session I: Malware Defense

0900 — 0930 A Methodology for Designing Countermeasures against Current and Future Code Injection Attacks
Y. Younan, W. Joosen, and F. Piessens

0930 — 1000 Making the Kernel Responsible: A New Approach to Detecting & Preventing Buffer Overflows
W. Speirs

1000 — 1030 Evaluation of Worm Containment Algorithms and Their Effect on Legitimate Traffic
M. Abdelhafez and G. Riley

1030 — 1100 Malware Defense Using Network Security Authentication
J. Antrosio and E. Fulp

1100 — 1120 **Break**

Session II: MANET Security

1120 — 1150 A General Cooperative Intrusion Detection Architecture for MANETs
D. Sterne, P. Balasubramanyam, D. Carman, B. Wilson, R. Talpade, C. Ko, R. Balupari, C.-Y. Tseng, T. Bowen, K. Levitt, and J. Rowe

1150 — 1220 SAWAN: A Survivable Architecture for Wireless LANs
M. Virendra, S. Upadhyaya, V. Kumar, and V. Anand

1220 — 1400 **Lunch**

1400 — 1500 Keynote Talk

Roger Schell

1500 — 1520 Break

Session III: Intrusion Detection I

1520 — 1550 Meta IDS Environments: An Event Message Anomaly Detection Approach

J. Tölle, M. Jahnke, M. Bussmann, and S. Henkel

1550 — 1620 An Alert Fusion Framework for Situation Awareness of Coordinated Multistage Attacks

S. Mathew, C. Shah, and S. Upadhyaya

1620 — 1650 Stellar: A Fusion System for Scenario Construction and Security Risk Assessment

S. Boyer, O. Dain, and R. Cunningham

1650 — 1710 Break

Panel Session

1710 — 1800 To be confirmed.

To be confirmed.

March 24, 2005

Session IV: Modeling and Policies

0900 — 0930 Attack-Potential-Based Survivability Modeling for High-Consequence Systems

J. McDermott

0930 — 1000 Enforcing Messaging Security Policies

J. Likavec and S. Wolthusen

1000 — 1030 Cross Domain Controlled Interface and Labeling (CDCIL) Services

K. Goertzel

1030 — 1100 Break

Session V: Intrusion Detection II

1100 — 1130 The Design of VisFlowConnect-IP: A Link Analysis System for IP Security Situational Awareness

X. Yin, W. Yurcik, and A. Slagell

1130 — 1200 Forensic Analysis of File System Intrusions Using Improved Backtracking

S. Sitaraman and S. Venkatesan

1200 — 1230 Combining Static Analysis and Dynamic Learning to Build Accurate Intrusion Detection Models

Z. Liu, S. Bridges, and R. Vaughn

1230— 1245 Closing Remarks

J. Cole