# Program

## 2nd IEEE International Information Assurance Workshop

Charlotte, North Carolina, April 8-9, 2004

**Program Committee**

Mario Barbacci
Tim Gibson
Jim Hughes
John James
Emil Lupu
John McDermott
James Bret Michael
Henry L. Owen
Peter Ryan

**General Chairs**

Jack Cole
Yuliang Zheng

**Program Chair**

Stephen D. Wolthusen

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`

# 2nd IEEE International Information Assurance Workshop

## Workshop Program

### April 8, 2004

0800 — 0845 **Registration / Breakfast**

0845 — 0900 Welcome and Introduction

---

**Session I: Network Security Metrics and Tools**

**0900 — 0930** Packet Filtering for Congestion Control under DoS Attacks
*Yenhung Hu, Hongsik Choi, and Hyeong-Ah Choi*

**0930 — 1000** Architecture and Performance of a Secure Wireless Agent-Based Testbed
*Gustave Anderson, Leonardo Urbano, Gaurav Naik, David Dorsey, Andrew Mroczkowski, Donovan Artz, Nicholas Morizio Andrew Burnheimer, Kris Malfetone, Dan Lapadat, Evan Sultanik, Saturnino Garcia Max Peysakhov, William Regli, and Moshe Kam*

**1000 — 1030** Survivable Monitoring in Dynamic Networks
*Giuseppe Ateniese, Chris Riley, and Christian Scheideler*

**1030 — 1100** A Systematic Approach to Multi-Stage Network Attack Analysis
*Jerald Dawkins, John Hale*

**1100 — 1120 Break**

---

**Session II: Works In Progress**

**1120 — 1150** A Multi-level Multi-Hop Overlay Method for Messaging in Secure Wireless Networks
*Jeff Janies, John Zachary*

**1150 — 1220** Embedded Firewall Defense
*George Stewart III, Ronald Dodge, Daniel Ragsdale*

**1220 — 1400 Lunch**

---

**1400 — 1445 Invited Talk**
Information Assurance Practices at Financial Companies — What Works (and What Didn't)
*Jeff Jancula, Vice President and Senior Security Advisor Information Technology, Wachovia Bank*

**1445 — 1500 Break**

---

**Session III: Intrusion Detection**

**1500 — 1530** Conversation Exchange Dynamics for Real-Time Network Monitoring and Anomaly Detection
*John Zachary, John McEachen, Dan Ettlich*

**1530 — 1600** Methods for Cluster-Based Incident Detection
*Brian Carrier, Blake Matheny*

**1600 — 1630** A Testbed for Quantitative Assessment of Intrusion Detection Systems using Fuzzy Logic
*Gautam Singaraju, Lawrence Teo and Yuliang Zheng*

**1630 — 1700 Break**

---

**Invited Talk**

**1700 — 1730** Information Assurance for the US Army
*Cliff Wang, United States Army Research Office*

**Panel Session**

**1730 — 1800** Information Assurance Standardization
*Gary Stoneburner, TBA, TBA, TBA*

---

**Evening Social Event**

# April 9, 2004

**Session IV: Host Security**

**0930 — 1000** Protection against Indirect Overflow Attacks on Pointers
*Ge Zhu, Akhilesh Tyagi*

**1000 — 1030** A Methodology to Detect and Characterize Kernel Level Rootkit Exploits Involving Redirection of the System Call Table
*John Levine, Julian Grizzard, and Henry Owen*

**1030 — 1045 Break**

**Invited Talk**

**1045 — 1115** TBD
*Tony Pressley, United States Army Research Laboratories*

**1115 — 1130 Break**

**Session V: Modeling and Evaluation**

**1130 — 1200** Increased Information Flow Needs for High-Assurance Composite Evaluations
*Paul A. Karger, Helmut Kurth*

**1200 — 1230** A Role-Based Trust Model for Peer-to-Peer Communities and Dynamic Coalitions
*Mujtaba Khambatti, Partha Dasgupta, and Kyung Dong Ryu*

**1230 — 1300** Defeating Internet Attacks Using Risk Awareness and Active Honeypots
*Lawrence Teo, Yu-An Sun, and Gail-Joon Ahn*

**1300— 1315** Closing Remarks