

**2006 IEEE Information Assurance Workshop**

**21 – 23 June 2006**

**West Point, NY**

**Copyright © 2006 Institute of Electrical and Electronics Engineers, Inc.**

**Copyright and Reprint Permission:**

Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923. For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Operations Center, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331. All rights reserved.

**IEEE Catalog Number:** 06EX1287

**ISBN:** 1-4244-0129-1

**Library of Congress Number:** 2006920138

# Table of Contents

---

## Information Assurance Professional Development and Best Practices

<b>Service Oriented Modeling of Communication Infrastructure for Assurance</b> .....	1
<i>Albin Zuccato, Bertrand Marquet, Serge Papillon, Magnus Aldén</i>	
<b>Developing a Threat Model for Enterprise Storage Area Networks</b> .....	9
<i>Casimer DeCusatis</i>	
<b>Creating a Balanced Scorecard for Computer Security</b> .....	15
<i>Lori L. DeLooze</i>	

## Data Protection

<b>Toward a Boot Odometer</b> .....	19
<i>Richard C. Vernon, Cynthia E. Irvine, Timothy E. Levin</i>	
<b>Design and Implementation of a File Transfer and Web Services Guard Employing Cryptographically Secured XML Security Labels</b> .....	26
<i>Andreas Thümmel, Knut Eckstein</i>	

## Usage/User Focused Security

<b>The Usage-Centric Security Requirements Engineering (USEr) Method</b> .....	34
<i>Niklas Hallberg, Jonas Hallberg</i>	
<b>Liveness Detection based on Fine Movements of the Fingertip Surface</b> .....	42
<i>Martin Drahanský, Ralf Nötzel, Wolfgang Funk</i>	
<b>Profiling Users in GUI Based Systems for Masquerade Detection</b> .....	48
<i>Ashish Garg, Ragini Rahalkar, Shambhu Upadhyaya, Kevin Kwiat</i>	

## Information Assurance Education

<b>The CyberDefense Laboratory: A Framework for Information Security Education</b> .....	55
<i>Mohamed S. Aboutabl</i>	
<b>The CERT® Survivability and Information Assurance Curriculum: Building Enterprise Networks on a Firm Educational Foundation</b> .....	61
<i>Lawrence R. Rogers</i>	
<b>The Design and Use of Interactive Visualization Applets for Teaching Ciphers</b> .....	69
<i>Dino Schweitzer, Leemon Baird</i>	

## Privacy I

<b>P3ARM: Privacy-Preserving Protocol for Association Rule Mining</b> .....	76
<i>Iman Saleh, Alaa Mokhtar, Amin Shoukry, Mohamed Eltoweissy</i>	
<b>Cascaded Authorization with Anonymous-Signer Aggregate Signatures</b> .....	84
<i>Danfeng Yao, Roberto Tamassia</i>	
<b>Allowing Finer Control Over Privacy Using Trust as a Benchmark</b> .....	92
<i>Sudip Chakraborty, Indrajit Ray</i>	

## Innovative Intrusion Detection and Response Methodologies I

<b>Applying Data Mining of Fuzzy Association Rules to Network Intrusion Detection</b> .....	100
<i>Aly El-Semary, Janica Edmonds, Jesús González-Pino, Mauricio Papa</i>	
<b>Attack Characterization and Intrusion Detection using an Ensemble of Self-Organizing Maps</b> .....	108
<i>Lori L. DeLooze</i>	
<b>Analyzing Attack Trees using Generalized Stochastic Petri Nets</b> .....	116
<i>George C. Dalton II, Robert F. Mills, John M. Colombi, Richard A. Raines</i>	

## Forensics

<b>The Need for a Technical Approach to Digital Forensic Evidence Collection for Wireless Technologies</b> .....	124
<i>Jill Slay, Benjamin Turnbull</i>	
<b>Embedding Forensic Capabilities into Networks: Addressing Inefficiencies in Digital Forensics Investigations</b> .....	133
<i>Barbara E. Endicott-Popovsky, Deborah A. Frincke</i>	
<b>File Type Identification of Data Fragments by Their Binary Structure</b> .....	140
<i>Martin Karresand, Nahid Shahmehri</i>	

## Privacy II

<b>Compound Identity Measure: A New Concept for Information Assurance</b> .....	148
<i>Abdur Rahim Choudhary</i>	
<b>Aspects of Personal Information Theory</b> .....	155
<i>Sabah S. Al-Fedaghi</i>	
<b>Quantitative Analysis of Efficient Antispam Techniques</b> .....	163
<i>Anders Wiehe, Erik Hjelmås, Stephen D. Wolthusen</i>	

## Innovative Intrusion Detection and Response Methodologies II

<b>PalProtect: A Collaborative Security Approach to Comment Spam</b> .....	170
<i>Benny Wong, Michael E. Locasto, Angelos D. Keromytis</i>	

<b>Battery-Sensing Intrusion Protection System</b> .....	176
<i>Timothy K. Buennemeyer, Grant A. Jacoby, Wayne G. Chiang, Randolph C. Marchany, Joseph G. Tront</i>	
<b>Evaluation of Run-Time Detection of Self-Replication in Binary Executable Malware</b> .....	184
<i>Alexander Volynkin, Victor A. Skormin, Douglas H. Summerville, James Moronski</i>	
<b>Visualization I</b>	
<b>Foundations for Visual Forensic Analysis</b> .....	192
<i>Sheldon Teerlink, Robert F. Erbacher</i>	
<b>Secure Visualization of GIS Data</b> .....	200
<i>Stephen D. Wolthusen</i>	
<b>Rendering the Elephant: Characterizing Sensitive Networks for an Uncleared Audience</b> .....	208
<i>Ross Stapleton-Gray, Sam Gorton</i>	
<b>Honeynet I</b>	
<b>Towards High Level Attack Scenario Graph through Honeynet Data Correlation Analysis</b> .....	215
<i>Jianwei Zhuge, Xinhui Han, Yu Chen, Zhiyuan Ye, Wei Zou</i>	
<b>Fake Honeypots: A Defensive Tactic for Cyberspace</b> .....	223
<i>Neil C. Rowe, Binh T. Duong, E. John Custy</i>	
<b>Design and Implementation of the Honey-DVD</b> .....	231
<i>Maximillian Dornseif, Felix C. Freiling, Nils Gedicke, Thorsten Holz</i>	
<b>Wireless Security I</b>	
<b>Using Active Scanning to Identify Wireless NICs</b> .....	239
<i>Cherita L. Corbett, Raheem A. Beyah, John A. Copeland</i>	
<b>Location-Based Pairwise Key Establishment and Data Authentication for Wireless Sensor Networks</b> .....	247
<i>Cungang Yang, Jie Xiao</i>	
<b>Smart Handling of Colluding Black Hole Attacks in MANETs and Wireless Sensor Networks using Multipath Routing</b> .....	253
<i>Satish Salem Ramaswami, Shambhu Upadhyaya</i>	
<b>Visualization II</b>	
<b>Grid Based Network Address Space Browsing for Network Traffic Visualization</b> .....	261
<i>Erwan Le Malécot, Masayoshi Kohara, Yoshiaki Hori, Kouichi Sakurai</i>	
<b>An Integrated Visualisation Framework for Intrusion Detection</b> .....	268
<i>Huw Read, Andrew Blyth</i>	

## Honeynet II

- A Dynamic Filtering Technique for Sebek System Monitoring** ..... 275  
*Edward Balas, Gregory Travis, Camilo Viecco*
- Network Based Detection of Virtual Environments and Low Interaction Honeypots** ..... 283  
*P. Defibaugh-Chavez, R. Veeraghattam, M. Kannappa, S. Mukkamala, A.H. Sung*

## Wireless Security II

- Securing Ad Hoc Networks with "Asymmetric" Probabilistic Key Predistribution Schemes** ..... 290  
*Mahalingam Ramkumar*
- Effects of Denial of Sleep Attacks on Wireless Sensor Network MAC Protocols** ..... 297  
*David Raymond, Randy Marchany, Michael Brownfield, Scott Midkiff*

## Information Warfare

- Visual Reverse Turing Tests: A False Sense of Security** ..... 305  
*Miroslav Ponec*
- Investigating the Effect of an Attack on a Distributed Database** ..... 312  
*Rami Samara, Brajendra Panda*
- Test Bed for Assessment of CNO and EW Against Emulated Wireless Ad Hoc Networks** ..... 318  
*Erika Johansson, Mats Persson*

## Secure Software Technologies

- Safely Redistributing Untrusted Code using .NET** ..... 326  
*Martin C. Carlisle, Jeffrey W. Humphries, John A. Hamilton, Jr.*
- LibsafeXP: A Practical and Transparent Tool for Run-time Buffer Overflow Preventions** ..... 332  
*Zhiqiang Lin, Bing Mao, Li Xie*
- A Dynamically Modified Privilege Control Policy** ..... 340  
*Sihan Qing, Qingni Shen, Qingguang Ji, Yeping He*

## Flow, Scheduling, Fault Tolerance

- A Control Theoretical Approach for Flow Control to Mitigate Bandwidth Attacks** ..... 348  
*Sui Song, C.N. Manikopoulos*
- Covert Timing Channel Analysis of Rate Monotonic Real-Time Scheduling Algorithm in MLS Systems** ..... 361  
*Joon Son, Jim Alves-Foss*
- Fault-Tolerant Overlay Protocol Network** ..... 369  
*Nicholas J. Shelly, Nathan A. Jensen, Leemon C. Baird, Jason A. Moore*

## Poster Session

<b>Automatically Building an Information-Security Vulnerability Database</b> .....	376
<i>Adrian D. Arnold, Bret M. Hyla, Neil C. Rowe</i>	
<b>A Methodology for Evaluation of Host-Based Intrusion Prevention Systems and Its Application</b> .....	378
<i>Keith G. Labbe, Neil C. Rowe, J.D. Fulp</i>	
<b>Secure State Processing</b> .....	380
<i>Sean M. Price</i>	
<b>Post-Quantum Diffie-Hellman and Symmetric Key Exchange Protocols</b> .....	382
<i>Xiangdong Li, Lin Leung, Andis Chi-Tung Kwan, Xiaowen Zhang, Damikka Kahanda, Michael Anshel</i>	
<b>Design of a Micro-kernel Based Secure System Architecture</b> .....	384
<i>Jianjun Shen, Sihan Qing, Qingni Shen</i>	
<b>Cryptography Software System using Galois Field Arithmetic</b> .....	386
<i>Ahmed H. Desoky, Aleksey Y. Ashikhmin</i>	
<b>Analysis and Defensive Tools for Social-Engineering Attacks on Computer Systems</b> .....	388
<i>Lena Larabee, David S. Barnes, Neil C. Rowe, Craig H. Martell</i>	
<b>Visualization in Interrogator using Graphviz</b> .....	390
<i>Charles Fox, Duane Wilson</i>	
<b>A Multi-step Method for Speaker Identification</b> .....	393
<i>M. Savastano, A. Luciano, A. Pagano, B. Peticone, L. Riccardi</i>	