

2007 IEEE Information Assurance Workshop

**West Point, NY
20-22 June 2007**



IEEE Catalog Number:
ISBN:

07EX1816
1-4244-1303-6

Table of Contents

Best Practices

A Global Look at Authentication	1
<i>Stephen S. Hamilton, Martin C. Carlisle and John A. Hamilton, Jr.</i>	
Recovering from Database Recovery: Case Studies and the Lessons they Teach	9
<i>Mary J. Hoferek and Susan C. Wilson</i>	
Do Word Clues Suffice in Detecting Spam and Phishing?	14
<i>Neil C. Rowe, David S. Barnes, Michael McVicker, Melissa Egan, Richard Betancourt, Rommel Toledo, Douglas P. Horner, Duane T. Davis, Louis Guitierrez and Craig H. Martell</i>	

IA Education

Experiences and Lessons Learned in the Design and Implementation of an Information Assurance Curriculum	22
<i>Sreekanth Malladi, Omar El-Gayar and Kevin Streff</i>	
Mapping Information Security Curricula to Professional Accreditation Standards	30
<i>Colin J. Armstrong and Helen L. Armstrong</i>	
Evaluating an IA Virtual Network Education Program	36
<i>Helen L. Armstrong, Nimal Jayaratna and Ronald C. Dodge</i>	

Security Considerations

Protocol of Secure Mutual Authentication	43
<i>Natalia Miloslavskaya, Alexander Tolstoy and Dmitriy Ushakov</i>	
Building Security into an IEEE FIPA Compliant Multiagent System	49
<i>Jidé B. Odubiyi and Abdur Rahim Choudhary</i>	

Computer Forensics I

A Framework for Redacting Digital Information from Electronic Devices	56
<i>Gavin W. Manes, Lance Watson, Elizabeth Downing, Alex Barclay, David Greer and John Hale</i>	
The Observability Calibration Test Development Framework	61
<i>Barbara E. Endicott-Popovsky and Deborah A. Frincke</i>	
Volleystore: A Parasitic Storage Framework	67
<i>Kurt Rosenfeld, Husrev Taha Sencar and Nasir Memon</i>	

Wireless Security I

A Family of Efficient Key Predistribution Schemes for Pairwise Authentication	76
<i>Mahalingam Ramkumar</i>	
Efficient Distribution of Trust Authority Functions in Tactical Networks	84
<i>Steffen Reidt and Stephen D. Wolthusen</i>	

Honeynet I

Detection of Virtual Environments and Low Interaction Honeypots	92
<i>S. Mukkamala, K. Yendrapalli, R. Basnet, M.K. Shankarapani and A.H. Sung</i>	
Improving Honeynet Data Analysis	99
<i>Camilo Viecco</i>	
Deception in Honeynets: A Game-Theoretic Analysis	107
<i>Nandan Garg and Daniel Grosu</i>	

Computer Forensics II

TimeKeeper: A Metadata Archiving Method for Honeypot Forensics	114
<i>Kevin D. Fairbanks, Christopher P. Lee, Ying H. Xia and Henry L. Owen III</i>	
Stego Scrubbing – A New Direction for Image Steganography	119
<i>Ira S. Moskowitz, Patricia A. Lafferty and Farid Ahmed</i>	

Wireless Security II

Scalable, Cluster-based Anti-replay Protection for Wireless Sensor Networks	127
<i>David R. Raymond, Randy C. Marchany and Scott F. Midkiff</i>	
Battery Polling and Trace Determination for Bluetooth Attack Detection in Mobile Devices	135
<i>Timothy K. Buennemeyer, Theresa M. Nelson, Michael A. Gora, Randy C. Marchany and Joseph G. Tront</i>	
Keyless Jam Resistance	143
<i>Leemon C. Baird III, William L. Bahn, Michael D. Collins, Martin C. Carlisle and Sean C. Butler</i>	

Honeynet II

Thwarting Cyber-Attack Reconnaissance with Inconsistency and Deception	151
<i>Neil C. Rowe and Han C. Goh</i>	
Rationale for and Capabilities of IT Security Assessment	159
<i>Niklas Hallberg, Jonas Hallberg and Amund Hunstad</i>	

Privacy

Protecting Privacy Credentials from Phishing and Spyware Attacks	167
<i>Sean M. Price</i>	

Preserving User Location Privacy based on Web Queries and LBS Responses	175
<i>Calvert L. Bowen III and Thomas L. Martin</i>	
Privacy Preserving Reputation Inquiry in a Peer-to-Peer Communication Environment	183
<i>Bon K. Sy</i>	
Wireless Security II	
SWAP: Shared Wireless Access Protocol (using Reciprocity)	191
<i>Matthew W. Dunlop, Ginger Perng and David G. Andersen</i>	
On the Effort to Create Smartphone Worms in Windows Mobile	199
<i>Michael Becher, Felix C. Freiling and Boris Leidner</i>	
Intrusion I	
Fuzzy Belief k-Nearest Neighbors Anomaly Detection of User to Root and Remote to Local Attacks	207
<i>Te-Shun Chou and Kang K. Yen</i>	
Arachne: Integrated Enterprise Security Management	214
<i>Matthew Burnside and Angelos D. Keromytis</i>	
An Efficient Network Anomaly Detection Scheme based on TCM-KNN Algorithm and Data Reduction Mechanism	221
<i>Yang Li and Li Guo</i>	
Data Protection I	
An Exploration on Security and Privacy Issues of Biometric Smart ID Cards	228
<i>Qinghan Xiao and Mario Savastano</i>	
An Elementary Electronic Voting Protocol using RFID	234
<i>Xiangdong Li, Michael Carlisle, Andis C. Kwan, Lin Leung, Amara Enemuo and Michael Anshel</i>	
A Knowledge-Base Model for Insider Threat Prediction	239
<i>Qutaibah Althebyan and Brajendra Panda</i>	
Information Warfare I	
Analysis and Statistical Properties of Critical Infrastructure Interdependency Multiflow Models	247
<i>Nils K. Svendsen and Stephen D. Wolthusen</i>	
Identifying Image Spam based on Header and File Properties using C4.5 Decision Trees and Support Vector Machine Learning	255
<i>Sven Krasser, Yuchun Tang, Jeremy Gould, Dmitri Alperovitch and Paul Judge</i>	
Guiding Threat Analysis with Threat Source Models	262
<i>K. Clark, C. Lee, S. Tyree and J. Hale</i>	

Intrusion II

GUI Usage Analysis for Masquerade Detection	270
<i>Eric S. Imsand and John A. Hamilton, Jr.</i>	
MSP-system: Mobile Secure Passport System to detect Malicious Users	277
<i>Shinya Tahara, Nobutaka Kawaguchi, Taro Inaba, Hidekazu Shiozawa, Hiroshi Shigeno and Ken-ichi Okada</i>	
PANEMOTO: Network Visualization of Security Situational Awareness through Passive Analysis	284
<i>William Streilein, Kendra Kratkiewicz, Michael Sikorski, Keith Piwowarski and Seth Webster</i>	

Data Protection II

Memoization Attacks and Copy Protection in Partitioned Applications	291
<i>Charles W. O'Donnell, G. Edward Suh, Marten van Dijk and Srinivas Devadas</i>	
H.264/AVC Stream Authentication at the Network Abstraction Layer	302
<i>Shintaro Ueda, Yasutaka Shinzaki, Hiroshi Shigeno and Ken-ichi Okada</i>	
A Linux Implementation of Temporal Access Controls	309
<i>Ken Chiang, Thuy D. Nguyen, Cynthia E. Irvine</i>	

Information Warfare II

Enhancing Internet Domain Name System Availability by Building Rings of Cooperation among Cache Resolvers	317
<i>Nayot Poolsappasit and Indrajit Ray</i>	
Traffic Flow Confidentiality in a Future Network Enabled Capability Environment	325
<i>Geir Hallingstad and Lasse Øverlier</i>	

Secure Software Technology

An Evaluation of Naïve Bayesian Anti-Spam Filtering Techniques	333
<i>Vikas P. Deshpande, Robert F. Erbacher and Chris Harris</i>	
Vulnerability Analysis of SCADA Protocol Binaries through Detection of Memory Access Taintedness	341
<i>Carlo Bellettini and Julian L. Rrushi</i>	
Design and use of a Secure Testing Environment on Untrusted Hardware	349
<i>Martin C. Carlisle and Leemon C. Baird III</i>	

Poster Session

Automated Retrieval of Security Statistics from the World Wide Web	355
<i>Michael McVicker, Paul Avellino and Neil C. Rowe</i>	
Automated Tracing and Integration of Security Functionality via Requirement Taxonomies, Annotations and Aspects	357
<i>Thomas Llansó and George Barrett</i>	