2010 Sixth International Conference on Information Assurance and Security

(IAS 2010)

Atlanta, Georgia, USA
23 – 25 August 2010
Program

<table>
<thead>
<tr>
<th>Time</th>
<th>324</th>
<th>433</th>
<th>Foyer Area</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Monday, August 23</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10:50</td>
<td></td>
<td>P1: Plenary Session 1: Kwok-L. Tsui</td>
<td></td>
</tr>
<tr>
<td>11:30</td>
<td></td>
<td>P2: Plenary Session 2: Václav Snášel</td>
<td></td>
</tr>
<tr>
<td>12:30</td>
<td></td>
<td>P3: Plenary Session 3: Amy Neustein</td>
<td></td>
</tr>
<tr>
<td>13:00</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14:00</td>
<td>SSA: Secure System Architectures</td>
<td>ID: Intrusion Detection</td>
<td>PP: Poster Presentation</td>
</tr>
<tr>
<td>15:00</td>
<td></td>
<td>15:30 AUP: Anonymity and User Privacy</td>
<td></td>
</tr>
<tr>
<td><strong>Tuesday, August 24</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>09:00</td>
<td>SPEDA 2010: Security and Performance in Emerging Distributed Architectures (SPEDA2010)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11:15</td>
<td>AIS: Authentication and Identity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14:00</td>
<td>MS: Multimedia Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16:15</td>
<td>ITCTS: International Workshop on Intelligent Technologies for Counter Terrorism and Security</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Monday, August 23**

**10:50 - 11:30**

**P1: Plenary Session 1: Kwok-L. Tsui**

Recent Research in System Informatics, Prognostics, and Health Management

Recent research in system informatics, prognostics, and health management (PHM) is driven by (i) concerns in public health safety, product reliability, system safety and failure prevention, and (ii) latest advancement in data collection technologies and modelling tools. There are tremendous opportunities in quantitative modelling research in system informatics (SI) as well as system prognostics and health management (PHM). First, we will present our view on research in system informatics, including data mining, surveillance, simulation, and system integration in healthcare and public health applications. In health surveillance, we will review and classify the various types of health surveillance research problems. In simulation, we review the latest research in disease spread simulation models and hospital operation simulation models. In system integration, we explore the opportunities for integrating surveillance, simulation, diagnostics, prognostics, data mining, and bioinformatics for personalized health management. Second, we will then discuss the recent research in system diagnostics and health management and how they are connected to research in system informatics and human health management. In particular, we will explain the characteristics of PHM and how they are different from traditional reliability modelling research.

**11:30 - 12:00**

**P2: Plenary Session 2: Václav Snášel**

Sequence Package Analysis: A New Speaker Biometric for Performing Speaker Verification of Terror Suspects in Stressed Environments

Sequence Package Analysis (SPA) identifies another kind of speaker trait: the unique conversational sequence patterns that are associated with each speaker. In stressed environments where extraction features, acoustic vectors, and classifications, and other classical speaker biometric features are compromised by noisy texts, which include speakers who deliberately alter their voices when colluding on crimes and terrorist acts, SPA finds the speaker traits which are not obscured by such conditions. What this means is that when there is a mismatch, a non match or a low confidence match between a suspects normal speech sample and the speech sample obtained by law enforcement during a high stressed situation (for example, the unidentified speaker is making a threat and is naturally agitated) SPA identifies the conversational sequence patterns that remain constant and identifiable notwithstanding the stressed environment. As such, SPA may be seen as a complementary biometric measure to improve accuracy of speaker verification in stressed environments. For
future study is a determination of whether conversation sequence patterns (because they are not subject to the acoustic compromises of stressed environments) outperform standard biometrics or, at least, serve as a complementary biometric to improve accuracy of speaker verification in stressed environments.

13:00 - 18:00

PP: Poster Presentation

A Comparison of the Standardized Versions of ECIES
Victor Gayoso (Spanish National Research Council (CSIC), Spain); Fernando Hernandez (Spanish National Research Council (CSIC), Spain); Luis Hernandez (Spanish National Research Council (CSIC), Spain); Carmen Sanchez (Polytechnic University of Madrid, Spain)
pp. 1-4

Discriminative Multinomial Naïve Bayes for Network Intrusion Detection
Mrutyunjaya Panda (Gandhi Institute of Engineering and Technology, Gunupur, India); Ajith Abraham (Machine Intelligence Research Labs (MIR Labs), USA); Manas Patra (Berhampur University, India)
pp. 5-10

Secure Universal Plug and Play Network
Vesa Pehkonen (VTT Technical Research Centre of Finland, Finland); Juha Koivisto (VTT, Finland)
pp. 11-14

A Case Analysis of a Contextual Model Of Trust for Digital Identities Using UML 2.0 and Context Graph Algorithms
Sean Thorpe (University of Technology, Jamaica)
pp. 15-20

Safeguarding Malaysia's Critical National Information Infrastructure (CNII) Against Cyber Terrorism: Towards Development of a Policy Framework
Zahri Yunus (CyberSecurity Malaysia, Malaysia); Syahrul Hafidz Suid (CyberSecurity Malaysia, Malaysia)
pp. 21-27

The Five Modes AES Applications in Sounds and Images
Chien-Lun Yen (National Taiwan Normal University, Taiwan)
pp. 28-31

Vincent Hu (NIST, USA)
pp. 32-35

A Hybrid Authentication and Authorization Process for Control System Networks
David Manz (Pacific Northwest National Laboratory, USA); Thomas Edgar (Pacific Northwest National Laboratory, USA); Glenn Allen Fink (Virginia Polytechnic and State University, USA)
pp. 36-39

Security Preferences Specification and Implementation in a Service-Based Workflow
Wendpanga Francis Ouedraogo (INSA - Lyon, France); Frederique Biennier (INSA-Lyon, France); Nicolas Salatge (eBM Websourcing, France)
pp. 40-43

Resource-Efficient Implementation of BLUE MIDNIGHT WISH-256 Hash Function on Xilinx FPGA Platform
Mohamed Aly (UMASS Lowell university, USA); Martin Margala (University of Rochester, USA); Danilo Gligoroski (Norwegian University of Science and Technology, Norway)
pp. 44-47

Novel Technique for Steganography in Fingerprints Images: Design and Implementation
Hanan Mahmoud (Center of Excellence in Information Assurance, Saudi Arabia)
pp. 48-51

Novel Algorithmic Countermeasures for Differential Power Analysis Attacks on Smart Cards
Hanan Mahmoud (Center of Excellence in Information Assurance, Saudi Arabia)
pp. 52-55
<table>
<thead>
<tr>
<th>Title</th>
<th>Authors</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Insider Threat Discovery Using Automatic Detection of Mission Critical Data Based On Content</strong></td>
<td>Jonathan White (University of Arkansas, USA); Brajendra Panda (University of Arkansas, USA)</td>
<td>56-61</td>
</tr>
<tr>
<td><strong>Benchmarking IP Blacklists For Financial Botnet Detection</strong></td>
<td>David Oro (Barcelona Digital Technology Centre, Spain); Jesus Luna (Barcelona Digital CT, Spain); Serna Jetzabel (Technical University of Catalonia, Spain); Pelguera Toni (Barcelona Digital CT, Spain); Vilanova Marc (La Caixa, Spain)</td>
<td>62-67</td>
</tr>
<tr>
<td><strong>Using Vulnerability Information and Attack Graphs for Intrusion Detection</strong></td>
<td>Sebastian Roschke (Hasso-Plattner-Institute, University of Potsdam, Germany); Feng Cheng (University of Potsdam, Germany); Christoph Meinel (Hasso-Plattner-Institut für Softwaresystemtechnik GmbH, Germany)</td>
<td>68-73</td>
</tr>
<tr>
<td><strong>Detect Multi-Hop Stepping-Stone Pairs with Clock Skew</strong></td>
<td>Ying-Wei Kuo (University of Houston, USA); Stephen Huang (University of Houston, USA)</td>
<td>74-79</td>
</tr>
<tr>
<td><strong>Efficient Defense Strategies to Minimize Attackers' Success Probabilities in Honeynet</strong></td>
<td>Frank Yeong-Sung Lin (National Taiwan University, Taiwan); Yu-Shun Wang (National Taiwan University, Taiwan); Po-Hao Tsang (National Taiwan University, Taiwan)</td>
<td>80-85</td>
</tr>
<tr>
<td><strong>Scaling IDS Construction Based on Non-Negative Matrix Factorization Using GPU Computing</strong></td>
<td>Jan Platos (VSB-Technical University of Ostrava, FEECS, Czech Republic); Pavel Kromer (VSB-Technical University of Ostrava, FEECS, Czech Republic); Vaclav Snasel (VSB-Technical University of Ostrava, FEECS, Czech Republic); Ajith Abraham (Machine Intelligence Research Labs (MIR Labs), USA)</td>
<td>86-91</td>
</tr>
<tr>
<td><strong>A Structured Approach to Anomaly Detection for In-Vehicle Networks</strong></td>
<td>Michael Mütter (Daimler AG, Germany); André Gröll (University of Siegen, Germany); Felix C Freiling (University of Mannheim, Germany)</td>
<td>92-98</td>
</tr>
<tr>
<td><strong>Intelligent Response System to Mitigate the Success Likelihood of Ongoing Attacks</strong></td>
<td>Wael Kanoun (Bell Labs, France); Nora Cuppens-Boulahia (IT TELECOM Bretagne, France); Frédéric Cuppens (TELECOM Bretagne, France); Samuel Dubus (Bell Labs, France); Antony Martin (Bell Labs, France)</td>
<td>99-105</td>
</tr>
<tr>
<td><strong>Fast Intrusion Detection System Based on Flexible Neural Tree</strong></td>
<td>Tomas Novoád (VSB-Technical University of Ostrava, FEECS, Czech Republic); Jan Platos (VSB-Technical University of Ostrava, FEECS, Czech Republic); Vaclav Snasel (VSB-Technical University of Ostrava, FEECS, Czech Republic); Ajith Abraham (Machine Intelligence Research Labs (MIR Labs), USA)</td>
<td>106-111</td>
</tr>
<tr>
<td><strong>Towards Intrusion Detection by Information Retrieval and Genetic Programming</strong></td>
<td>Pavel Kromer (VSB-Technical University of Ostrava, FEECS, Czech Republic); Jan Platos (VSB-Technical University of Ostrava, FEECS, Czech Republic); Vaclav Snasel (VSB-Technical University of Ostrava, FEECS, Czech Republic); Ajith Abraham (Machine Intelligence Research Labs (MIR Labs), USA)</td>
<td>112-117</td>
</tr>
<tr>
<td><strong>RAPID: Reputation Based Approach for Improving Intrusion Detection Effectiveness</strong></td>
<td>Ashley Thomas (Secureworks Inc, USA)</td>
<td>118-124</td>
</tr>
</tbody>
</table>

**SSA: Secure System Architectures**

<table>
<thead>
<tr>
<th>Title</th>
<th>Authors</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Detecting Memory Spoofing in Secure Embedded Systems Using Cache-Aware FPGA Guards</strong></td>
<td>Eugen Leontie (George Washington University, USA); Olga Gelbart (The George Washington University)</td>
<td>118-124</td>
</tr>
</tbody>
</table>
15:00 - 15:45

C: Cryptography

The Number of the Isomorphism Classes of Hyperelliptic Curves of Genus Four Over Finite Fields
Lin You (Hangzhou Dianzi University, China, USA)
pp. 161-166

Fault Attack on AES with Single-Bit Induced Faults
Alessandro Barenghi (Politecnico di Milano, Italy); Guido Bertoni (ST Microelectronics, Italy); Luca Breveglieri (Politecnico di Milano, Italy); Mauro Pellicioli (Politecnico di Milano, Italy); Gerardo Pelosi (Politecnico di Milano, Italy)
pp. 167-172

15:30 - 16:30

AUP: Anonymity and User Privacy

Anonymous Service Access for Vehicular Ad Hoc Networks
Hesiri Weerasinghe (Oakland University, USA); Huirong Fu (Oakland University, USA); Supeng Leng (University of Electronic Science and Technology of China, P.R. China)
pp. 173-178

Patient’s Perception of Health Information Security: The Case of Selected Public and Private Hospitals in Addis Ababa
Tibebe Tesema (Addis Ababa University, Ethiopia); Ajith Abraham (Machine Intelligence Research Labs (MIR Labs), USA); Dawn Medlin (Appalachian State University, USA)
pp. 179-184

Ganthan Narayana Samy (Universiti Teknologi Malaysia (UTM), Malaysia); Rabiah Ahmad (Universiti Teknologi Malaysia, Malaysia); Zuraini Ismail (University Teknologi Malaysia, Malaysia)
pp. 185-190

Extending the Definition of Guesswork
Reine Lundin (Karlstad University, Sweden); Stefan Lindskog (Karlstad University, Sweden)
pp. 191-196
Reconciling IHE-ATNA Profile with a Posteriori Contextual Access and Usage Control Policy in Healthcare Environment
Hanieh Azkia (IT-Telecom Bretagne, France); Nora Cuppens-Boulahia (IT TELECOM Bretagne, France); Frédéric Cuppens (TELECOM Bretagne, France); Gouenou Coatrieux (INSTITUT TELECOM - TELECOM Bretagne, France)
pp. 197-203

Inconsistency Detection Method for Access Control Policies
Riaz Ahmed Shaikh (Université du Québec en Outaouais (UQO), Canada); Kamel Adi (University of Quebec in Outaouais, Canada); Luigi Logrippo (Universite de Quebec a l'Outaouais, Canada); Serge Mankovski (CA Inc, Canada)
pp. 204-209

Anonymous Communication System Using Probabilistic Choice of Actions and Multiple Loopbacks
Kazuhiko Kono (Kansai University, Japan); Yoshimichi Ito (Osaka University, Japan); Noboru Babaguchi (Osaka University, Japan)
pp. 210-215

Assurance in Identity Management Systems
Maya Chehab (E-Security Research Centre, United Kingdom); Ali E. Abdallah (London South Bank University, United Kingdom)
pp. 216-221

Tuesday, August 24
09:00 - 11:00

SPEDA 2010: Security and Performance in Emerging Distributed Architectures (SPEDA2010)

Audited Credential Delegation - A User-Centric Identity Management Solution for Computational Grid Environments
Ali Nasrat Haidar (University College London, United Kingdom); Stefan Zasada (University College London, United Kingdom); Ali E. Abdallah (London South Bank University, United Kingdom); Bruce Beckles (University of Cambridge Computing Service, United Kingdom); Peter Coveney (University College London, United Kingdom)
pp. 222-227

Cooperative Access Control for the Grid
Alessio Merlo (University of Genoa, Italy); Alessandro Armando (University of Genoa, Italy)
pp. 228-233

CARMA: Composable-Adaptive Resource Management Authorization for Ubiquitous Environments
Roberto Morales (Universitat Politècnica de Catalunya, Spain); Sema Jetzabel (Technical University of Catalonia, Spain); Manel Medina (Technical University of Catalonia, Spain); Jesus Luna (Barcelona Digital CT, Spain)
pp. 234-239

A Semantic Based Methodology to Classify and Protect Sensitive Data in Medical Records
Valentina Casola (Università degli Studi di Napoli "Federico II", Italy); Flora Amato (Università degli Studi di Napoli Federico II, Italy); Antonino Mazzeo (Università degli Studi di Napoli Federico II, Italy); Sara Romano (Università degli Studi di Napoli "Federico II", Italy)
pp. 240-246

A Naming System Applied to a RESERVOIR Cloud
Antonio Celesti (University of Messina, Italy); Massimo Villari (University of Messina, Italy); Antonio Puliafito (University of Messina, Italy)
pp. 247-252

Identity Federation in Cloud Computing
Massimiliano Rak (Second University of Naples, Italy); Valentina Casola (Università degli Studi di Napoli "Federico II", Italy); Umberto Villano (University of Sannio, Italy)
pp. 253-259

Securing a Tiered Re-Taskable Sensing System
Alessandra De Benedictis (University of Naples Federico II, Italy); Andrea Gaglione (University of Naples Federico II, Italy); Nicola Mazzocca (University of Naples "Federico II", Italy)
Integrating a Network IDS Into an Open Source Cloud Computing Environment
Claudio Mazzariello (Federico II University of Napoli, Italy); Roberto Bifulco (University of Napoli Federico II, Italy); Roberto Canonico (University of Napoli Federico II, Italy)
pp. 260-264

11:15 - 13:00

AIS: Authentication and Identity

A Two-Tiered Authentication and Encryption Scheme in Secure Healthcare Sensor Networks
Mohammed Raza Kanjee (University of Massachusetts Dartmouth, Canada); Kalyani Divi (University of Massachusetts Dartmouth, USA); Hong Liu (University of Massachusetts Dartmouth, USA)
pp. 271-276

UDT - Authentication Option Field: an Approach
Danilo Bernardo (University of Technology, Australia)
pp. 277-279

Data Aggregation for Information Authentication in VANETs
Jezabel Molina-Gil (University of La Laguna, Spain); Pino Caballero-Gil (University of La Laguna, Spain); Candelaria Hernández-Goya (University of La Laguna, Spain); Cándido Caballero-Gil (University of La Laguna, Spain)
pp. 282-287

Secure Protocol for Ad Hoc Transportation System
Johnson Thomas (Oklahoma State University, USA); Matthew Thomas (, ?)
pp. 288-293

A Hierarchical Access Authentication in Network
He Liu (University of BJTU, P.R. China); Mangui Liang (Beijing Jiaotong University, P.R. China); Liang Qi (University of Beijing Jiaotong, P.R. China); Wei Chen (University of Beijing Jiaotong, P.R. China)
pp. 294-297

Quantifying Authentication Levels of Assurance in Grid Environments
Li Yao (University of Manchester, United Kingdom); Ning Zhang (University of Manchester, United Kingdom)
pp. 298-303

14:00 - 15:00

MS: Multimedia Security

Optimum Fusion of Visual and Thermal Face Images for Recognition
Mrinal Kanti Bhowmik (Tripura University (A Central University), India)
pp. 311-316

Automatic Semantic Annotation of Images Based on Web Data
Guiguang Ding (University of Tsinghua, P.R. China)
pp. 317-322

Comparison of Real-Time DSP-Based Edge Detection Techniques for License Plate Detection
Zuwena Musoromy (University of hertfordshire, United Kingdom); Faycal Bensaali (University of Hertfordshire, United Kingdom); Soodamani Ramalingam (University of Hertfordshire, United Kingdom); Georgios Pissanidis (University of Hertfordshire, United Kingdom)
pp. 323-328
### Integrated Security Risk Management for IT-Intensive Organizations
Jeffrey Mounzer (Stanford University, USA); Tansu Alpcan (Technical University Berlin, Germany); Nicholas Bambos (Stanford University, USA)
pp. 329-334

### Link Suggestions in Terrorists Networks Using Semi Discrete Decomposition
Vaclav Snasel (VSB-Technical University of Ostrava, FEECS, Czech Republic); Zdenek Horak (VSB Technical University Ostrava, Czech Republic, Czech Republic); Ajith Abraham (Machine Intelligence Research Labs (MIR Labs), USA)
pp. 335-337

### Fuzzified Aho-Corasick Search Automata
Zdenek Horak (VSB Technical University Ostrava, Czech Republic, Czech Republic); Vaclav Snasel (VSB-Technical University of Ostrava, FEECS, Czech Republic); Ajith Abraham (Machine Intelligence Research Labs (MIR Labs), USA); Aboul Ella Otifey Hassanien (University of Cairo, Egypt)
pp. 338-342

### A Framework for Cyber Surveillance of Unlawful Activities for Critical Infrastructure Using Computational Grids
Vaclav Snasel (VSB-Technical University of Ostrava, FEECS, Czech Republic); Ajith Abraham (Machine Intelligence Research Labs (MIR Labs), USA); Khalid Saeed (Bialystok Technical University, Poland); Hameed Al-Qaheri (Kuwait university, Kuwait)
pp. 343-348