

# *Proceedings*

---

## **The Fourth International Symposium on Information Assurance and Security**

September 8-10, 2008  
Napoli, Italy

### **Technically Sponsored by:**



Dipartimento di Ingegneria dell'informazione – Seconda Università degli Studi di Napoli, Italy



ICST (International Communication Sciences and Technology Association)



Create-Net (Center of REsearch And Telecommunication Experimentations for NETworked communities)



Los Alamitos, California  
Washington • Tokyo



# Table of Contents

IAS 2008

The Fourth International Symposium  
on Information Assurance and Security

<b>Welcome Message</b> .....	ix
<b>IAS 2008 Organisation</b> .....	xi
<b>Plenary Talk Abstracts</b> .....	xiii

---

## Authentication and Access Control

A Formal Comparison of the Bell & LaPadula and RBAC Models .....	3
<i>Lionel Habib, Mathieu Jaume, and Charles Morisset</i>	
Threshold Proxy Signature Scheme with Strong Real-Time Efficiency.....	9
<i>Xiaoming Wang and Huoyan Chen</i>	
A Purchase Protocol with Live Cardholder Authentication for Online Credit Card Payment.....	15
<i>Hannan Xiao, Bruce Christianson, and Ying Zhang</i>	
Comparison and Evaluation of Identity Management in Three Architectures for Virtual Organizations .....	21
<i>Ali N. Haidar and Ali E. Abdallah</i>	
Speaker Identification by Multi-Frame Generative Models .....	27
<i>Donato Impedovo and Mario Refice</i>	

## Short Papers

Integrating Delegation with the Formal Core RBAC Model.....	33
<i>Ali E. Abdallah and Hassan Takabi</i>	
Security Analysis of Temporal-RBAC Using Timed Automata.....	37
<i>Samrat Mondal and Shamik Sural</i>	

## Cryptographic Schemes and Applications

Secure Hybrid Group Key Management for Hierarchical Self-Organizing Sensor Network .....	43
<i>Shu Yun Lim, Meng-Hui Lim, Sang Gon Lee, and Hoon Jae Lee</i>	
PHAL-256 – Parameterized Hash Algorithm .....	50
<i>Przemyslaw Rodwald and Janusz Stokłosa</i>	
Steganography in Textiles .....	56
<i>Sajad Shirali-Shahreza and Mohammad Shirali-Shahreza</i>	

Persian/Arabic Unicode Text Steganography .....	62
<i>Mohammad Shirali-Shahreza and Sajad Shirali-Shahreza</i>	
Efficient Hierarchical Group-Oriented Key Establishment and Decryption .....	67
<i>Sigurd Eskeland and Vladimir Oleshchuk</i>	
Forward-Secure Proxy Signature Scheme for Multiple Proxy Signers Using Bellare-Miner Scheme with Proxy Revocation .....	73
<i>N.R. Sunitha and B.B. Amberker</i>	
Data Hiding in Non-Expansion Visual Cryptography Based on Edge Enhancement Multitoning.....	79
<i>Hao Luo, Faxin Yu, and Jeng-Shyang Pan</i>	
Skin Segmentation Using Color Distance Map and Water-Flow Property.....	83
<i>M. Abdullah-Al-Wadud and Oksam Chae</i>	
An Implementation Infrastructure for Server-Passive Timed-Release Cryptography .....	89
<i>Konstantinos Chalkias, Foteini Baldimtsi, Dimitrios Hristu-Varsakelis, and George Stephanides</i>	

### Short Papers

A Group Key Agreement Scheme Revisited .....	95
<i>Zhengjun Cao and Lihua Liu</i>	
Secure E-Passport Protocol Using Elliptic Curve Diffie-Hellman Key Agreement Protocol.....	99
<i>Mohamed Abid and Hossam Afifi</i>	
A Server Based ASR Approach to Automated Cryptanalysis of Two Time Pads in Case of Speech .....	103
<i>Liaqat Ali Khan and Muhammad Shamim Baig</i>	
Dynamic Substitution Model.....	108
<i>Mohamed Abo El-Fotouh and Klaus Diepold</i>	

## Data Security and Privacy

Data Fusion Assurance for the Kalman Filter in Uncertain Networks .....	115
<i>Bonnie Zhu and Shankar Sastry</i>	
A Time and Storage Efficient Solution to Remote File Integrity Check .....	120
<i>Sarad AV, Sankar K, and Vipin M</i>	
A New Narrow Block Mode of Operations for Disk Encryption .....	126
<i>Mohamed Abo El-Fotouh and Klaus Diepold</i>	
Provenance Tracking with Bit Vectors.....	132
<i>Siddharta S. Gadang, Brajendra Panda, and Joseph E. Hoag</i>	

## Intrusion Detection, Intrusion Prevention, Threat Modeling, and Analysis

Impact of Cheating and Non-Cooperation on the Stability and the Performances of Application-Level Multicast Sessions.....	141
<i>Mothanna Alkubeyli, Hatem Bettahar, and Abdelmadjid Bouabdallah</i>	
ACML: Capability Based Attack Modeling Language.....	147
<i>Navneet Kumar Pandey, S.K. Gupta, Shaveta Leekha, and Jingmin Zhou</i>	
Realistic Threats to Self-Enforcing Privacy .....	155
<i>Giampaolo Bella, Francesco Librizzi, and Salvatore Riccobene</i>	
Operator-Centric and Adaptive Intrusion Detection.....	161
<i>Ulf E. Larson, Stefan Lindskog, Dennis K. Nilsson, and Erland Jonsson</i>	

A Queuing Theory Based Model for Studying Intrusion Evolution and Elimination in Computer Networks.....	167
<i>Pantelis Kammas, Thodoros Komninos, and Yannis C. Stamatiou</i>	
Matrix Factorization Approach for Feature Deduction and Design of Intrusion Detection Systems .....	172
<i>Václav Snášel, Jan Platoš, Pavel Krömer, and Ajith Abraham</i>	
Ensemble of One-Class Classifiers for Network Intrusion Detection System.....	180
<i>Anazida Zainal, Mohd Aizaini Maarof, Siti Mariyam Shamsuddin, and Ajith Abraham</i>	
Web Application Attack Prevention for Tiered Internet Services .....	186
<i>Susanta Nanda, Lap-chung Lam, and Tzi-cker Chiueh</i>	
LoSS Detection Approach Based on ESOS and ASOSS Models.....	192
<i>Mohd Fo'ad Rohani, Mohd Aizaini Maarof, Ali Selamat, and Houssein Kettani</i>	
COTraSE: Connection Oriented Traceback in Switched Ethernet .....	198
<i>Marios S. Andreou and Aad van Moorsel</i>	

### *Short Papers*

Improving the Efficiency of Misuse Detection by Means of the $q$ -gram Distance.....	205
<i>Slobodan Petrović and Sverre Bakke</i>	
An Efficient Approach to Minimum-Cost Network Hardening Using Attack Graphs .....	209
<i>Feng Chen, Lingyu Wang, and Jinshu Su</i>	

## **Security Tools Design**

Developing a Security Typed Java Servlet .....	215
<i>Doaa Hassan, Sherif El-Kassas, and Ibrahim Ziedan</i>	
Designing a DRM System .....	221
<i>Franco Frattolillo and Federica Landolfi</i>	

### *Short Papers*

Challenges for Security Typed Web Scripting Languages Design .....	227
<i>Doaa Hassan, Sherif El-Kassas, and Ibrahim Ziedan</i>	
Systematic Website Verification for Privacy Protection .....	231
<i>Ji-Hee Jeoung, Eun-Ji Shin, Seng-Phil Hong, Sung-Hoon Kim, In-Ho Kim, and Min-Woo Lee</i>	

## **Network Security and Sensor, Mobile and “ad hoc”**

### **Network Security**

Abusing SIP Authentication .....	237
<i>Humberto Abdelmur, Tigran Avanesov, Michael Rusinowitch, and Radu State</i>	
A Friend Mechanism for Mobile Ad Hoc Networks .....	243
<i>Shukor Abd Razak, Normalia Samian, and Mohd Aizaini Maarof</i>	
A Composite Network Security Assessment .....	249
<i>Suleyman Kondakci</i>	
Managing Reputation over MANETs.....	255
<i>Giampaolo Bella, Gianpiero Costantino, and Salvatore Riccobene</i>	
Network Level Privacy for Wireless Sensor Networks .....	261
<i>Riaz Ahmed Shaikh, Hassan Jameel, Brian J. d'Auriol, Sungyoung Lee, Young-Jae Song, and Heejo Lee</i>	

A Device Management Framework for Secure Ubiquitous Service Delivery .....	267
<i>Adrian Leung and Chris J. Mitchell</i>	
Automatic Verification of Simulatability in Security Protocols .....	275
<i>Tadashi Araragi and Olivier Pereira</i>	
A New Secure Binding Management Protocol for Mobile IPv6 Networks .....	281
<i>Osama Elshakankiry, Andy Carpenter, and Ning Zhang</i>	
 <i>Short Papers</i>	
Geolocation-Based Trust for Vanet’s Privacy .....	287
<i>Jetzabel Serna, Jesus Luna, and Manel Medina</i>	
An Automated Validation Method for Security Policies: The Firewall Case .....	291
<i>Ryma Abassi and Sihem Guemara El Fatmi</i>	
Adaptive Dynamic Reaction to Automotive IT Security Incidents Using Multimedia Car Environment.....	295
<i>Tobias Hoppe, Stefan Kiltz, and Jana Dittmann</i>	
Semantics-Driven Introspection in a Virtual Environment.....	299
<i>Francesco Tamberi, Dario Maggiari, Daniele Sgandurra, and Fabrizio Baiardi</i>	
 <b>Special Session on Security in Critical Infrastructure</b>	
Information Assurance in Critical Infrastructures via Wireless Sensor Networks .....	305
<i>Michele Albano, Stefano Chessa, and Roberto Di Pietro</i>	
A Model for the Study of Privacy Issues in Secure Shell Connections .....	311
<i>Maurizio Dusi, Francesco Gringoli, and Luca Salgarelli</i>	
IRC Traffic Analysis for Botnet Detection .....	318
<i>Claudio Mazzariello</i>	
 <b>Special Session on Quantum Cryptography</b>	
Key Distribution Using Dual Quantum Channels .....	327
<i>Di Jin, Pramode Verma, and Stamatios Kartalopoulos</i>	
Quantum Key Distribution Based on Multi-qubit Hadamard Matrices .....	333
<i>Dazu Huang and Zhigang Chen</i>	
Chaotic Quantum Cryptography.....	338
<i>Stamatios V. Kartalopoulos</i>	
 <b>Author Index</b> .....	 343