

2007 Third International Conference on Security and Privacy in Communication Networks and Workshops

**Nice, France
17-21 September 2007**



IEEE Catalog Number:
ISBN 13:

CFP07SPN-PRT
978-1-4244-0974-7

Table of Contents

NetTRUST: mixed NETworks Trust infrastrUcture baSed on Threshold cryptography	2
<i>Mawloud Omar, Yacine Challal, Abdelmadjid Bouabdallah</i>	
Temporal Factors to evaluate trustworthiness of virtual identities.....	11
<i>Luca Longo, Pierpaolo Dondio, Stephen Barrett</i>	
Trustworthiness of Collaborative Open Source Software Quality Assessment.....	20
<i>Jean-Marc Seigneur</i>	
An Entropy based method for Measuring Anonymity	28
<i>Michele Bezzi</i>	
Flexible and High-Performance Anonymization of NetFlow Records using Anontool	33
<i>Michalis Foukarakis , Demetres Antoniadis , Spiros Antonatos , Evangelos P. Markatos</i>	
Practical Anonymous Communication on the Mobile Internet using Tor.....	39
<i>Christer Andersson, Andriy Panchenko</i>	
SCRUB-tcpdump: A Multi-Level Packet Anonymizer Demonstrating Privacy/Analysis Tradeoffs	49
<i>William Yurcik, Clay Woolam, Greg Hellings, Latifur Khan and Bhavani Thuraisingham</i>	
Secure Computation for Data Privacy	58
<i>Meena Singh and Ashutosh Saxena</i>	
An Efficient and Scalable Security Protocol for Protecting Fixed-Content Objects in Content Addressable Storage Architectures.....	63
<i>Wassim Itani, Ayman Kayssi, Ali Chehab</i>	
Scalable discovery of private resources	73
<i>Spyros Kotoulas and Ronny Siebes</i>	
A Context Service for Multimodal Pervasive Environments.....	84
<i>Antonio Coronato and Giuseppe De Pietro</i>	
Beyond Web 2.0: enabling multimodal web interactions using VoIP and Ajax.....	89
<i>Giovanni Frattini, Pierpaolo Petriccione, Giuseppe Leone, Gianluca Supino, Fabio Corvino</i>	
iToken: a Wireless Smart Card Reader which Provides Handhelds with Desk Top Equivalent Security	98
<i>G. Cattaneo, L. Catuogno, F. Petagna, G. Di Matteo, L. Romano</i>	
Web Services Workflow Reliability Estimation Through Reliability Patterns.....	107
<i>Luigi Coppolino, Luigi Romano, Nicola Mazzocca, Sergio Salvi</i>	
The CONNECT Platform: An Architecture for Context-Aware Privacy in Pervasive Environments.....	117
<i>Susana Alcalde Bagues, Jelena Mitic, and Elisabeth-Anna Emberger</i>	
Privacy-preserving Authentication with Low Computational Overhead for RFID Systems.....	127
<i>Fen Liu, Lei Hu, Li Lu, and Weijia Wang</i>	
A Study on Secure RFID Authentication Protocol in Insecure Communication	133
<i>Jang-Su Park, Soo-Young Kang and Im-Yeong Lee</i>	
Optimizing Secure Web Services with MAWeS: a Case Study	144
<i>Massimiliano Rak, Valentina Casola, Nicola Mazzocca, Emilio Pasquale Mancini, Umberto Villano</i>	
Verification Method of Network Simulation for Pervasive Environments.....	155
<i>Kyuhyung Cho, Jongsung Lee, Jongin Lim, Jongsub Moon</i>	
A secure and efficient key management scheme for wireless sensor networks	162
<i>Yong Ho Kim, Hwaseong Lee, and Dong Hoon Lee</i>	
A Model for Usage Control in GRID Systems.....	169
<i>Fabio Martinelli, Paolo Mori</i>	

Table of Contents

Intrusion Detection and Tolerance in Grid-based Applications	177
<i>Jun Wang, Luigi Lo Iacono</i>	
Secure token passing at application level	187
<i>Augusto Ciuffoletti</i>	
Gaining Users' Trust by Publishing Failure Probabilities	193
<i>Dominic Battre, Karim Djemame, Odej Kao, Kerstin Voss</i>	
Platform to enforce multiple access control policy in grid hosting environment	199
<i>Leonardo Mattes, Leonardo C. Militelli, João Antonio Zuffo</i>	
Design patterns for Secure Virtual Organization Management Architecture	207
<i>Angelo Gaeta, Matteo Gaeta, Alan Smith, Ivan Djordjevic, Theo Dimitrakos, Maurizio Colombo, Sergio Miranda</i>	
An Analysis of the Chinese Wall Pattern for Guaranteeing Confidentiality in Grid-based Virtual Organisations	217
<i>G. Dallons, P. Massonet, J.-F. Molderez, C. Ponsard, A. Arenas</i>	
OpenFire: Using Deception to Reduce Network Attacks	224
<i>Kevin Borders, Laura Falk, and Atul Prakash</i>	
Modeling and Detection of Complex Attacks	234
<i>Seyit Ahmet Camtepe and Bulent Yener</i>	
Intrusion Detection Technology based on CEGA-SVM	244
<i>Yuxin Wei, Muqing Wu</i>	
Misleading and Defeating Importance-Scanning Malware Propagation	250
<i>Guofei Gu, Zesheng Chen, Phillip Porras, Wenke Lee</i>	
A BitTorrent-Driven Distributed Denial-of-Service Attack	261
<i>Jerome Harrington, Corey Kuwanoe, Cliff C. Zou</i>	
Parameterizing Access Control for Heterogeneous Peer-to-Peer Applications	269
<i>Ashish Gehani, Surendar Chandra</i>	
Securing Pseudo Identities in an Anonymous Peer-to-Peer File-Sharing Network	279
<i>Tom Chothia</i>	
Using Recurring Costs for Reputation Management in Peer-To-Peer Streaming Systems	283
<i>Michael Rossberg, Guenter Schaefer, Thorsten Strufe</i>	
A Feedback Reputation Mechanism to Secure the Optimized Link State Routing Protocol	294
<i>Joao P. Vilela, Joao Barros</i>	
Enhancing Frequency-based Wormhole Attack Detection with Novel Jitter Waveforms	304
<i>Maria A. Gorlatova, Marc Kelly, Ramiro Liscano, and Peter C. Mason</i>	
Mitigating Denial-of-Service Attacks in MANET by Incentive-based Packet Filtering: A Game-theoretic Approach	310
<i>Xiaoxin Wu, David K. Y. Yau</i>	
Securing Personal Network clusters	320
<i>Assed Jehangir, Sonia M. Heemstra de Groot</i>	
Implications of Radio Fingerprinting on the Security of Sensor Networks	331
<i>Kasper Bonne Rasmussen, Srdjan Capkun</i>	
SET: Detecting node clones in Sensor Networks	341
<i>Heesook Choi, Sencun Zhu, Thomas F. La Porta</i>	
RoK: A Robust Key Pre-distribution Protocol for Multi-Phase Wireless Sensor Networks	351
<i>Claude Castelluccia, Angelo Spognardi</i>	

Table of Contents

Deception Framework for Sensor Networks	361
<i>Ruiyi Zhang, Johnson Thomas and Venkata Manoj Mulpuru</i>	
An Assessment of VoIP Covert Channel Threats	371
<i>Takehiro Takahashi, Wenke Lee</i>	
Detecting Bogus BGP Route Information: Going Beyond Prefix Hijacking	381
<i>Jian Qiu and Lixin Gao, Supranamaya Ranjan and Antonio Nucci</i>	
Securing Network Location Awareness with Authenticated DHCP	391
<i>Tuomas Aura, Michael Roe, Steven J. Murdoch</i>	
Global Interoperability of National Security and Emergency Preparedness (NS/EP) Telecommunications Services	403
<i>Arye, Frank J. Suraci, Arye R. Ephrath, John R. Wullert</i>	
Detecting Worms via Mining Dynamic Program Execution.....	412
<i>Xun Wang, Wei Yu, Adam Champion, Xinwen Fu and Dong Xuan</i>	
Efficient Mechanisms to Provide Convoy Member and Vehicle Sequence Authentication in VANETs	422
<i>Ahren Studer, Mark Luk, Adrian Perrig</i>	
PWC: A Proactive Worm Containment Solution for Enterprise Networks.....	433
<i>Yoon-Chan Jhi, Peng Liu, Lunquan Li, Qijun Gu, Jiwu Jing and George Kesidis</i>	
Secure Crash Reporting in Vehicular Ad hoc Networks.....	443
<i>Sumair Ur Rahman and Urs Hengartner</i>	
A Layout-Similarity-Based Approach for Detecting Phishing Pages.....	454
<i>Angelo P. E. Rosiello, Engin Kirda, Christopher Kruegel, and Fabrizio Ferrandi</i>	
Simple Cross-Site Attack Prevention	464
<i>Florian Kerschbaum</i>	
Simple Authentication for the Web.....	473
<i>Timothy W. van der Horst and Kent E. Seamons</i>	
Secure Lightweight Tunnel for Monitoring Transport Containers	484
<i>Jens Ove Lauf, Harald Sauff</i>	
Sybil Attack Detection in a Hierarchical Sensor Network.....	494
<i>Jian Yin and Sanjay Kumar Madria</i>	
Anonymity and Security in Delay Tolerant Networks.....	504
<i>Aniket Kate, Gregory M. Zaverucha, and Urs Hengartner</i>	
Breaking EMAP.....	514
<i>Mihaly Barasz, Balazs Boros, Peter Ligeti, Krisztina Loja, Daniel A. Nagy</i>	