

# **2011 5th International Conference on Network and System Security**

**(NSS 2011)**

**Milan, Italy  
6 – 8 September 2011**



**IEEE Catalog Number: CFP11NES-PRT  
ISBN: 978-1-4577-0458-1**

# Table of Contents

<b>Foreword from the Conference Chairs</b> .....	VIII
<b>Conference Committee</b> .....	IX
<b>Program Committee</b> .....	X
<b>Additional Reviewers</b> .....	XI
 <b>Intrusion Detection</b>	
A Misuse-Based Network Intrusion Detection System Using Temporal Logic and Stream Processing .....	1
<i>Abdulbasit Ahmed, Alexei Lisitsa, and Clare Dixon</i>	
A Holistic Methodology for Evaluating Wireless Intrusion Detection Systems .....	9
<i>Khalid Nasr, Anas Abou El Kalam, and Christian Fraboul</i>	
A Grid-Based Clustering for Low-Overhead Anomaly Intrusion Detection .....	17
<i>Yang Zhong, Hirohumi Yamaki, and Hiroki Takakura</i>	
Towards Ground Truthing Observations in Gray-Box Anomaly Detection .....	25
<i>Jiang Ming, Haibin Zhang, and Debin Gao</i>	
 <b>Client-side Vulnerabilities</b>	
Defeating Pharming Attacks at the Client-side .....	33
<i>Sophie Gastellier-Prevost, and Maryline Laurent</i>	
Automated Extraction of Polymorphic Virus Signatures Using Abstract Interpretation .....	41
<i>Serge Chaumette, Olivier Ly, and Renaud Tabary</i>	
Modeling Worms Propagation on Probability .....	49
<i>Yini Wang, Sheng Wen, and Yang Xiang</i>	
Detecting Infection Onset with Behavior-Based Policies .....	57
<i>Kui Xu, Danfeng Yao, Qiang Ma, and Alexander Crowell</i>	
 <b>Authentication and Watermarking Systems</b>	
KL-F: Karhunen-Loève Based Fragile Watermarking .....	65
<i>Marco Botta, Davide Cavagnino, and Victor Pomponiu</i>	
Designing Secure RFID Authentication Protocols is (still) a Non-Trivial Task .....	73
<i>Panagiotis Rizomiliotis, Evangelos Rekleitis, and Stefanos Gritzalis</i>	
Make Mine a Quadruple: Strengthening the Security of Graphical One-Time PIN Authentication .....	81
<i>Ravi Jhavar, Philip Inglesant, Nicolas Courtois, and M. Angela Sasse</i>	

## Web Security

Privacy-enhanced Identity via Browser Extensions and Linking Services .....	89
<i>Renato Accornero, Daniele Rispoli, and Francesco Bergadano</i>	
Reactive Non-Interference for a Browser Model .....	97
<i>Nataliia Bielova, Dominique Devriese, Fabio Massacci, and Frank Piessens</i>	
Tracking End-Users in Web Databases .....	105
<i>Boris Rozenberg, Yaron Gonen, Ehud Gudes, Erez Shmueli, and Nurit Gal-Oz</i>	

## Security in Cloud and Peer to Peer Systems

CloudSec: A Security Monitoring Appliance for Virtual Machines in the IaaS Cloud Model .....	113
<i>Amani S. Ibrahim, James Hamlyn-Harris, John Grundy, and Mohamed Almorsy</i>	
An Efficient VM-based Software Protection .....	121
<i>Amir Averbuch, Michael Kiperberg, and Nezer Jacob Zidenberg</i>	
Removing the Blinders: Using Information to Mitigate Adversaries in Adaptive Overlays .....	129
<i>David Zage, Charles Killian, and Cristina Nita-Rotaru</i>	
Improving P2P IPTV Random Peers Search Through User Similarity .....	137
<i>Alessio Bonti, Ming Li, and Wen Shi</i>	

## Network Security

A Distributed Client-Puzzle Mechanism to Mitigate Bandwidth Attacks .....	145
<i>Mazdak Alimadadi and Mehran S. Fallah</i>	
Towards Safe and Optimal Filtering Rule Reordering for Complex Packet Filters .....	153
<i>Nizar Ben Neji and Adel Bouhoula</i>	
DANAK: Finding the Odd! .....	161
<i>Cynthia Wagner, Jérôme François, Radu State, and Thomas Engel</i>	
A Novel Semi-Supervised Approach for Network Traffic Clustering .....	169
<i>Yu Wang, Yang Xiang, Jun Zhang, and Shunzheng Yu</i>	

## Hardware-based Security

Scalable Consistency-based Hardware Trojan Detection and Diagnosis .....	176
<i>Sheng Wei and Miodrag Potkonjak</i>	
FORTUNA – A Probabilistic Framework for Early Design Stages of Hardware-Based Secure Systems .....	184
<i>Roberto Gallo, Henrique Kawakami, and Ricardo Dahab</i>	
Attack-resilient Compliance Monitoring for Large Distributed Infrastructure Systems .....	192
<i>Mirko Montanari and Roy Campbell</i>	

## Access Control

A Secure, Constraint-Aware Role-Based Access Control Interoperation Framework .....	200
<i>Nathalie Baracaldo, Amirreza Masoumzadeh, and James Joshi</i>	
Model-based Safety Analysis of SELinux Security Policies .....	208
<i>Peter Amthor, Winfried E. Kühnhauser, and Anja Pölck</i>	
Exploring Twisted Paths: Analyzing Authorization Processes in Organizations.....	216
<i>Steffen Bartsch</i>	

## Authentication

SMS Linguistic Profiling Authentication on Mobile Device .....	224
<i>Hataichanok Saevanee, Nathan L. Clarke, and Steven M. Furnell</i>	
User-Representative Feature Selection for Keystroke Dynamics .....	229
<i>Eesa AlSolami, Colin Boyd, Andrew Clark, and Irfan Ahmed</i>	
STORK e-Privacy and Security .....	234
<i>Vasilis Koulolias, Athanasios Kountzeris, Alberto Crespo, Herbert Leitold, Bernd Zwattendorfer, and Marc Stern</i>	
Towards a Metric for Recognition-Based Graphical Password Security.....	239
<i>Rosanne English and Ron Poet</i>	
RCHB: Light-Weight, Provably-Secure Variants of the HB Protocol Using Rotation and Complementation .....	244
<i>Samia A. Ali, Refaat M. Mohamed, and Mahmoud H. Fahim</i>	

## Key Managements

A Trustful Authentication and Key Exchange Scheme (TAKES) for Ad Hoc Networks .....	249
<i>Tony Cheneau, Andrei Vlad Sambra, and Maryline Laurent</i>	
Automatic Security Verification for 3-Party Authentication and Key Exchange Protocols .....	254
<i>Haruki Ota, Shinsaku Kiyomoto, and Yutaka Miyake</i>	
On the Security of the ECKE-1N and EECKE-1N Elliptic-Curve Key Agreement Protocols.....	259
<i>Maurizio Adriano Strangio</i>	
Channel State Information based Key Generation vs. Side-Channel Analysis Key Information Leakage .....	264
<i>Huiyun Li, Qi Zhang, and Hai Yuan</i>	
A Microcontroller SRAM-PUF .....	269
<i>Christoph Boehm, Maximilian Hofer, and Wolfgang Pribyl</i>	

## Emerging Scenarios and e-Services

Data Control in Social Networks.....	274
<i>Robert Koch, Dominik Holzappel, and Gabi Dreo Rodosek</i>	

Trustable Outsourcing of Business Processes to Cloud Computing Environments .....	280
<i>Sami Alsouri, Stefan Katzenbeisser, and Sebastian Biedermann</i>	
Secure Conjunctive Keyword Searches for Unstructured Text .....	285
<i>Florian Kerschbaum</i>	
The Power of Credit Card Numbers and Long CVVs .....	290
<i>Valentim Oliveira and Tito Silva</i>	
A Privacy-Preserving eID Based Single Sign-On Solution .....	295
<i>Bernd Zwattendorfer, Arne Tauber, and Thomas Zefferer</i>	

## **Wi-Fi and Network Security**

Enhancement of ZigBee and Wi-Fi Security by a Robust and Fast Chaotic Algorithm .....	300
<i>Bassem Bakhache, Joseph Ghazal, and Safwan El-Assad</i>	
Flooding Attacks Against Network Coding and Countermeasures .....	305
<i>Yuanyuan Zhang, Wassim Znaidi, Cédric Lauradoux, and Marine Minier</i>	
Avoiding DDoS with Active Management of Backlog Queues .....	310
<i>Martine Bellaïche and Jean-Charles Grégoire</i>	
$R^5N$ : Randomized Recursive Routing for Restricted-Route Networks .....	316
<i>Nathan S. Evans and Christian Grothoff</i>	
Analysis of Prefix Hijacking Based on AS Hierarchical Model .....	322
<i>Bo-Feng Zhang, Yuan Li, Yu-Jing Liu, and Jin-Shu Su</i>	

## **Risk Assessment and Usability**

Modelling Self-protected Networks and Dynamic Systems .....	327
<i>Marta Fernández-Diego and Julián Marcelo-Cocho</i>	
A Conceptual Framework for Evaluating Usable Security in Authentication Mechanisms - Usability Perspectives .....	332
<i>Martin Mihajlov, Borka Jerman-Blazic, and Saso Josimovski</i>	
Usability of Internet Security Software: Have They Got It Right? .....	337
<i>Patryk Szewczyk</i>	

## **Malicious Code and Security Analysis**

Semi-supervised Learning for Packed Executable Detection .....	342
<i>Xabier Ugarte-Pedrero, Igor Santos, Pablo G. Bringas, Mikel Gastesi, and José Miguel Esparza</i>	
A Propagation Model of A Vulnerability Mitigation Computer Worm - Seawave .....	347
<i>Ziyad Al-Salloum and Stephen Wolthusen</i>	
Towards Improving Security Testability of AADL Architecture Models .....	353

*Ayda Saidane and Nicolas Guelfi*

Reconstructing Security Types for Automated Policy Enforcement in FABLE ..... 358  
*Arash Afshar and Mehran S. Fallah*

Measuring the Revised Guessability of Graphical Passwords ..... 364  
*Rosanne English and Ron Poet*

**Author Index** ..... 369