2008 2nd International Conference on Emerging Security Information, Systems and Technologies

(SECURWARE 2008)

Cap Esterel, France
25 – 31 August 2008

IEEE Catalog Number: CFP0889C-PRT
ISBN: 978-0-7695-3512-8

The Second International Conference on Emerging Security Information, Systems and Technologies

SECURWARE 2008

Table of Contents

Preface

Committees

SECURWARE 1: Frameworks, Architectures and Protocols I

Enhancing Trusted Platform Modules with Hardware-Based Virtualization Techniques 1
Frederic Stumpf and Claudia Eckert

A Secure Task Delegation Model for Workflows 10
Khaled Gaaloul, Andreas Schaad, Ulrich Flegel, and François Charoy

Formal Modeling of Authentication in SIP Registration 16
Anders Moen Hagalisletto and Lars Strand

Controlling Access to Location-Based Services in Vehicular Mobile Pervasive Environments 22
Sameerchand Pudaruth, Nevin Vunka Jungum, Soulakshmee D. Ghurbhurrun, and Leckraj Nagowah

SECURWARE 2: Frameworks, Architectures and Protocols II

A New Approach for Secure and Portable OS 28
H. Rezaei Ghaleh and M. A. Doustari

Distack – A Framework for Anomaly-Based Large-Scale Attack Detection 34
Thomas Gamer, Christoph P. Mayer, and Martina Zitterbart

Team--Based MAC Policy over Security--Enhanced Linux 41
J. Briffaut, J.-F. Lalande, and Waleed W. Smari
Prototyping a New Identity Authentication Framework for IP Telephony 47
Shu-Lin Chen, Stanley Chow, Christophe Gustave, and Dmitri Vinokurov
Polynomial Heuristic Algorithms for Inconsistency Characterization in Firewall Rule Sets 53
S. Pozo, R. Ceballos, R. M. Gasca, and A. J. Varela-Vaca

SECURWARE 3: Frameworks, Architectures and Protocols III

Security Patterns for Capturing Encryption-Based Access Control to Sensor Data 62
Angel Cuevas, Paul El Khoury, Laurent Gomez, and Annett Laube
Security Policy Management for Peer Group Meetings 68
Fuwen Liu and Hartmut Koenig
FEEPVR: First End-to-End Protocol to Secure Ad Hoc Networks with Variable Ranges against Wormhole Attacks 74
Sandhya Khurana and Neelima Gupta
Proving Trust Locally 80
Anders Moen Hagalisletto
A Security Framework for Input Validation 88
Rafael Bosse Brinhosa, Carlos Becker Westphall, and Carla Merkle Westphall

SECURWARE 4: System Security

Defending E-Banking Services: Antiphishing Approach 93
Antonio San Martino and Xavier Perramon
Preventing Insider Information Leakage for Enterprises 99
Imad M. Abbadi and Muntaha Alawneh
Analysis of the Impact of Intensive Attacks on the Self-Similarity Degree of the Network Traffic 107
Pedro R. M. Inácio, Mário M. Freire, Manuela Pereira, and Paulo P. Monteiro
Scalable Detection of SIP Fuzzing Attacks 114
Eric Y. Chen and Mitsutaka Itoh
Authentication Mechanisms for Mobile Ad-Hoc Networks and Resistance to Sybil Attack 120
Sarosh Hashmi and John Brooke

SECURWARE 5: Malware & Security

The Automatic Discovery, Identification and Measurement of Botnets 127
Ian Castle and Eimear Buckley
A Protection Scheme against the Attacks Deployed by Hiding the Violation of the Same Origin Policy 133
Masaru Takesue

Email Worm Mitigation by Controlling the Name Server Response Rate 139
Nikolaos Chatzis and Enric Pujol
Anti-counterfeiting with a Random Pattern 146
Cheun Ngen Chong, Dan Jiang, Jiagang Zhang, and Long Guo
Efficient Anomaly Detection System for Mobile Handsets 154
Yuka Ikebe, Takehiro Nakayama, Masaji Katagiri, Satoshi Kawasaki, Hirotake Abe, Takahiro Shinagawa, and Kazuhiko Kato

SECURWARE 6: Ecosystem Security and Trust

Providing Secure Access to Unsecure Web Services 161
V. F. Pais and V. Stancalie
Towards Decentralised Security Policies for e-Health Collaborations 165
Oluwafemi Ajayi, Richard Sinnott, and Anthony Stell
Rating Agencies Interoperation for Peer-to-Peer Online Transactions 173
Mihaela Ion, Hristo Koshutanski, Volker Hoyer, and Luigi Telesca
Optimal Trust Network Analysis with Subjective Logic 179
Audun Josang and Touhid Bhuiyan
From Monitoring Templates to Security Monitoring and Threat Detection 185
Nuno Amálio and George Spanoudakis

SECURWARE 7: Cryptography

A Body-Centered Cubic Method for Key Agreement in Dynamic Mobile Ad Hoc Networks 193
Ioannis G. Askoxylakis, Damien Sauveron, Konstantinos Markantonakis, Theodore Tryfonas, and Apostolos Traganitis
Family of Parameterized Hash Algorithms 203
P. Rodwald and J. Stokłosa
Public Key Cryptography: A Dynamical Systems Perspective 209
Roland Schmitz
A Related-Key Attack on TREYFER 213
Aleksandar Kircanski and Amr M. Youssef

SECURWARE 8: Information Security I

Security and Adoption of Internet Payment 218
Jean-Michel Sahut
Appraisal of the Effectiveness and Efficiency of an Information Security Management System Based on ISO 27001 224
Wolfgang Boehmer
Generic and Complete Three-Level Identity Management Model 232
M. Dąbrowski and P. Pacyna
A Novel Approach against DoS Attacks in WiMAX Authentication Using Visual Cryptography 238
Ayesha Altaf, Rabia Sirhindi, and Attiq Ahmed

A New Anti-phishing Method in OpenID 243
HwanJin Lee, InKyung Jeun, Kilsoo Chun, and Junghwan Song

SECURWARE 9: Information Security II

Toward the Engineering of Security of Information Systems (ESIS): UML and the IS Confidentiality 248
Wilson Goudalo and Dominique Seret
Designing an Undergraduate Software Security Course 257
Cynthia Y. Lester and Frank Jamerson
High-Speed Private Information Retrieval Computation on GPU 263
Carlos Aguilar Melchor, Benoit Crespin, Philippe Gaborit, Vincent Jolivet, and Pierre Rousseau
Vulnerability Dependencies in Antivirus Software 273
Kreetta Askola, Rauli Puuperä, Pekka Pietikäinen, Juhani Eronen, Marko Laakso, Kimmo Halunen, and Juha Röning

SECURWARE 10: Information Security III

Security Governance for Enterprise VoIP Communication 279
Rainer Falk and Steffen Fries
ToLeRating UR-STD 287
Jan Feyereisl and Uwe Aickelin
Collaborative Approach to Automatic Classification of Heterogeneous Information Security 294
Fatiha Benali, Stéphane Ubéda, and Véronique Legrand
Infusing Information Assurance into an Undergraduate CS Curriculum 300
Cynthia Y. Lester, Hira Narang, and Chung-Han Chen

SECURWARE 11: Profiling Data Mining

On the Portability of Trained Machine Learning Classifiers for Early Application Identification 306
Giacomo Verticale
Activity- and Inactivity-Based Approaches to Analyze an Assisted Living Environment 311
Martin Floeck and Lothar Litz
Analysis of Computer Infection Risk Factors Based on Customer Network Usage 317
Yannick Carlinet, Ludovic Mé, Hervé Debar, and Yvon Gourhant

DEPEND I

Design-Time Learning for Operational Planning Improvement 326
Daniel J. Martinez, Juan M. Marin, Jorge Bernal, Manuel Gil, and Antonio F. Gomez-Skarmeta
Molecular Approach Paves the Way towards High Resilience for Large Mission-Critical Information Systems 332
André Cotton, Maurice Israël, and Julien Borgel
Heuristics to Perform Molecular Decomposition of Large Mission-Critical Information Systems 338
Maurice Israel, Julien Borgel, and Andre Cotton
Generation of Diagnostic Plans for Large ICT Systems 344
Marco D. Aime and Andrea Atzeni

DEPEND II

Dependability Analysis of Information Systems with Hierarchical Reconfiguration of Services 350
Dariusz Caban and Wojciech Zamojski
Hierarchical Approach to Dependability Analysis of Information Systems by Modeling and Simulation 356
Katarzyna Michalska and Tomasz Walkowiak
Towards the Definition of a Web Service Based Management Framework 362
Juan Manuel Marín Pérez, Jorge Bernal Bernabé, Daniel J. Martínez Manzano, Gregorio Martínez Pérez, and Antonio F. Gómez Skarmeta
Dependability and Security Metrics in Controlling Infrastructure 368
Imre Kocsis, György Csertán, Péter László Pásztor, and András Pataricza

DEPEND III

Advanced Rule-Based Techniques in Mission Critical Systems 375
Maite Avelino and Francisco de la Torre
Fast Algorithms for Local Inconsistency Detection in Firewall ACL Updates 381
S. Pozo, R. Ceballos, R. M. Gasca, and A. J. Varela-Vaca
Event-Driven Architecture for Intrusion Detection Systems Based on Patterns 391
Jesús J. Martínez Molina, Miguel A. Hernández Ruíz, Manuel Gil Pérez, Gregorio Martínez Pérez, and Antonio F. Gómez Skarmeta
Agent Based Approach to Events Monitoring in Complex Information Systems 397
Marek Woda and Tomasz Walkowiak

DEPEND IV

A Synchronization Attack and Defense in Energy-Efficient Listen-Sleep Slotted MAC Protocols 403
Xiaoming Lu, Matt Spear, Karl Levitt, Norman S. Matloff, and S. Felix Wu
On System Security Metrics and the Definition Approaches 412
Artur Hecker
Policy-Driven System Configuration for Dependability 420
Marco D. Aime, Paolo C. Pomi, and Marco Vallini
A Dependability Case Approach to the Assessment of IP Networks 426
Ilkka Norros, Pirkko Kuusela, and Pekka Savola

Author Index