2010 International Conference on Availability, Reliability, and Security

(ARES 2010)

Krakow, Poland
15-18 February 2010
ARES 2010 Full Papers

Network Security I

A Security Decision-Reaction Architecture for Heterogeneous Distributed Network .............................................................................................................................. 1

Christophe Feltus, Djamel Khadraoui, and Jocelyn Aubert

Dual-Level Attack Detection and Characterization for Networks under DDoS .............................................. 9

Anjali Sardana and Ramesh Chandra Joshi

Improving Effectiveness of Intrusion Detection by Correlation Feature Selection ............................................. 17

Hai Nguyen, Katrin Franke, and Slobodan Petrovic

Network Security II

Analytical Approach to Attack Graph Analysis for Network Security ......................................................... 25

Phongphun Kijsanayothin and Rattikorn Hewett

Affects of Queuing Mechanisms on RTP Traffic: Comparative Analysis of Jitter, End-to-End Delay and Packet Loss ........................................................................................................ 33

Gregory Epiphaniou, Carsten Maple, Paul Sant, and Matthew Reeve

A Computer Architecture with Hardware-based Malware Detection ........................................................... 41

Klaus Hildebrandt, Igor Podebrad, and Bernd Klauer

Identity Management, Authentication, and Authorization I

Solving the Transitive Access Problem for the Services Oriented Architecture ............................................. 46

Alistair H. Karp and Jun Li

Unified Public Key Infrastructure Supporting Both Certificate-Based and ID-Based Cryptography ......................................................................................................................... 54

Byoungcheon Lee

Secure Bindings of SAML Assertions to TLS Sessions .................................................................................. 62

Florian Kohlar, Jörg Schwenk, Metko Jensen, and Sebastian Gajek

Identity Management, Authentication, and Authorization II

From Contextual Permission to Dynamic Pre-obligation: An Integrated Approach ........................................ 70

Yehia Elrokayby, Frédéric Cuppens, and Nora Cuppens-Boulahia

2-clickAuth—Optical Challenge-Response Authentication ............................................................................. 79

Anna Vapen, David Byers, and Nahid Shahmehri

Architecture-Aware Adaptive Deployment of Contextual Security Policies ................................................... 87

Stere Preda, Nora Cuppens-Boulahia, Frédéric Cuppens, and Laurent Toutain
Availability and Reliability I

Using Smart Cards for Tamper-Proof Timestamps on Untrusted Clients ................................................................. 96
Guenther Stavnberger, Lorenz Froihofer, and Karl M. Goeschka

A Semi-Markov Survivability Evaluation Model for Intrusion Tolerant Database Systems .................................................. 104
Alex Hai Wang, Su Yan, and Peng Liu

Availability and Reliability II

FaT2D: Fault Tolerant Directed Diffusion for Wireless Sensor Networks ................................................................. 112
Fatima Zohra Benhamida and Yacine Challal

An Adaptive Redundancy Oriented Method to Tolerate Soft Errors in SRAM-Based FPGAs Using Unused Resources ................................................................. 119
Somayeh Bahranejad and Hamid Reza Zarandi

Analysis of Transient Faults on a MIPS-Based Dual-Core Processor ................................................................. 125
Iman Faraji, Moslem Didehban, and Hamid Reza Zarandi

Risk and Security Management I

Visualizing Past Personal Data Disclosures ................................................................. 131
Jan Kolter, Michael Netter, and Günther Pernul

Strategies for Reducing Risks of Inconsistencies in Access Control Policies ................................................................. 140
Bernard Stepien, Stan Matwin, and Amy Felty

Multi-dimensional Uncertainty Analysis in Secure and Dependable Domain ................................................................. 148
Yudistira Asnar and Paolo Giorgini

Risk and Security Management II

Information Flow in Disaster Management Systems ................................................................. 156
Achim D. Brucker and Dieter Hutter

Formal Specification and Analysis of an E-voting System ................................................................. 164
Komminist Weldemariam, Richard A. Kemmerer, and Adolfo Villafiorita

Towards a Privacy-Enhanced Social Networking Site ................................................................. 172
Esma Aïmeur, Sébastien Gambs, and Ai Ho

Risk and Security Management III

A Formal Approach Towards Risk-Aware Service Level Analysis and Planning ................................................................. 180
Stefan Jakoubi, Simon Tjoa, Sigrun Goluch, and Gerhard Kitzler

Threat- and Risk-Analysis During Early Security Requirements Engineering ................................................................. 188
Holger Schmidt

An Analysis of Information Security Awareness within Home and Work Environments ................................................................. 196
Shuhaili Talib, Nathan L. Clarke, and Steven M. Furnell
ARES 2010 Short Papers

Security and Privacy

Trust Based Multi Path DSR Protocol .................................................................204
  Poonam Gera, Kumkum Garg, and Manoj Misra
Enhanced Chaotic Stream Cipher for WSNs ......................................................210
  Rui Miguel Soares Silva, Rui Gustavo Nunes Pereira Crespo,  
  and Mário Serafim dos Santos Nunes
Zone Based Systems Design Framework for the Realisation of Efficient Block  
  Cipher Based Message Authentication Code Algorithms ....................................216
  A.A. Adekunle and S.R. Woodhead

Identity Management, Authentication, and Authorization

A Semantic Security Architecture for Web Services—The Access-eGov  
  Solution .............................................................................................................222
  Stefan Dürbeck, Christoph Fritsch, Günther Pernul, and Rolf Schillinger
FedWare: Middleware Services to Cope with Information Consistency  
  in Federated Identity Management .....................................................................228
  Thorsten Hoellrigl, Jochen Dinger, and Hannes Hartenstein
Owner-Based Role-Based Access Control OB-RBAC ..........................................236
  Mohsen Saffarian and Babak Sadighi

Cryptography and Secure Protocols

Program Obfuscation by Strong Cryptography ....................................................242
  Željko Vrba, Pål Halvorsen, and Carsten Griwodz
Pitfalls in Formal Reasoning about Security Protocols .......................................248
  Nina Moebius, Kurt Stenzel, and Wolfgang Reif
Secure Group Communication Using Fractional Public Keys ..............................254
  Sigurd Eskeland and Vladimir Oleshchuk

Risk and Security Management

Extending the Gordon and Loeb Model for Information Security Investment ..........258
  Jan Willemsen
Risk-Based Methodology for Real-Time Security Monitoring  
  of Interdependent Services in Critical Infrastructures .....................................262
  Jocelyn Aubert, Thomas Schaberreiter, Christophe Incoul, Djamel Khadraoui,  
  and Benjamin Gâteau
Planning Dynamic Activity and Resource Allocations Using a Risk-Aware  
  Business Process Management Approach .......................................................268
  Simon Tjoa, Stefan Jakoubi, Sigrun Goluch, and Gerhard Kitzler
Miscellaneous

Security and Usability: Analysis and Evaluation .................................................................275
Ronald Kainda, Ivan Fléchais, and A.W. Roscoe

Recovery of Skype Application Activity Data from Physical Memory .............................283
Matthew Simon and Jill Slay

Rejuvenating High Available Virtualized Systems ............................................................289
Arash Rezaei and Mohsen Sharifi

Fifth International Workshop on Frontiers in Availability, Reliability, and Security
(FARES 2010)

Fraud and Misuse Detection

Detection of Spyware by Mining Executable Files ..............................................................295
Raja Khurram Shahzad, Syed Imran Haider, and Niklas Lavesson

A Probabilistic Approach for On-Line Sum-Auditing .........................................................303
Gerardo Canfora and Bice Cavallo

Towards an Ontology-Based Solution for Managing License Agreement Using
Semantic Desktop ..................................................................................................................309
Mansoor Ahmed, Amin Anjomshoaa, Muhammad Asfandeyar, A. Min Tjoa, and Abid Khan

Intrusion Detection

Optimising IDS Sensor Placement .......................................................................................315
Hao Chen, John A. Clark, Siraj A. Shaikh, Howard Chivers, and Philip Nobles

Layered Higher Order N-grams for Hardening Payload Based Anomaly
Intrusion Detection ..................................................................................................................321
Neminath Hubballi, Santosh Biswas, and Sukumar Nandi

Improving Network Intrusion Detection by Means of Domain-Aware Genetic
Programming .......................................................................................................................327
Jorge Blasco, Agustín Orfila, and Arturo Ribagorda

Privacy and Trust

On the Simulation of a Software Reputation System .........................................................333
Martin Boldt, Anton Borg, and Bengt Carlsson

Model-Driven Application-Level Encryption for the Privacy of E-health Data .................341
Yun Ding and Karsten Klein

Communal Reputation and Individual Trust (CRIT) in Wireless Sensor
Networks ...............................................................................................................................347
Tanveer A Zia and Md Zahidul Islam
Global Information Security
A Multi-stage Methodology for Ensuring Appropriate Security Culture and Governance ................................................................. 353
   Solange Ghernouti-Hélie, Igli Tashi, and David Simms
Development of ICT Infrastructure for Local Socio-Economic System in Japan—Another Approach Toward Cybersecurity in the Non-urban Area ................................................................. 361
   Hiroshi Nagano
A National Strategy for an Effective Cybersecurity Approach and Culture ................................................................. 370
   Solange Ghernouti-Hélie

Software Security and Authentication
Choosing Authentication Techniques in E-procurement System in Serbia ................................................................. 374
   Miloš Milovanović, Marija Bogićević, Miroslav Lazović, Dejan Simić, and Dušan Starčević
A Continuous Authentication System Based on User Behavior Analysis ................................................................. 380
   Ines Brosso, Alessandro La Neve, Graça Bressan, and Wilson Vicente Ruggiero
Identifying Security Relevant Warnings from Static Code Analysis Tools through Code Tainting ................................................................. 386
   Dejan Baca

Digital Content Security
Reselling Digital Content ........................................................................................................................................ 391
   Laila El Aimani and Yona Raekow
A New DRM Architecture with Strong Enforcement ................................................................................................. 397
   Sascha Müller and Stefan Katzenbeisser
A Secure and Scalable Grid-Based Content Management System ......................................................................................... 404
   Benjamin Aziz, Alvaro Arenas, Giovanni Cortese, Bruno Crispo, and Silvio Cauzetti
A Design Pattern for Event-Based Processing of Security-Enriched SOAP Messages ................................................................................................. 410
   Nils Gruschka, Meiko Jensen, and Luigi Lo Iacono

The Second International Workshop on Organizational Security Aspects (OSA 2010)

Organizational Aspects of Security: Session 1
Challenging IS and ISM Standardization for Business Benefits ......................................................................................... 416
   Juhani Anttila and Jorma Kajava
Managing the Asset Risk of SMEs ........................................................................................................................................ 422
   Luis Enrique Sánchez, Carlos Ruiz, Eduardo Fernández-Medina, and Mario Piattini
Organizational Aspects of Security: Session 2

A Generic Metamodel for IT Security—Attack Modeling for Distributed Systems ........................................................................................................................................430

André Miede, Nedislav Nedyalkov, Christian Gottron, André König, Nicolas Repp, and Ralf Steinmetz

Combining Misuse Cases with Attack Trees and Security Activity Models ........................................................................................................................................438

Inger Anne Tondel, Jostein Jensen, and Lillian Rostad

External Insider Threat: A Real Security Challenge in Enterprise Value Webs .........................................................................................................................................446

Virginia N.L. Franqueira, André van Cleeff, Pascal van Eck, and Roel Wieringa

Organizational Aspects of Security: Session 3

Secure Monitoring of Service Level Agreements ..........................................................................................................................................................454

K.P. Clark, M.E. Warmer, F.M.T. Brazier, and T.B. Quillinan

Fighting Phishing with Trusted Email ........................................................................................................................................................................462

Jordan Crain, Lukasz Opprchal, and Atul Prakash

Application and Economic Implications of an Automated Requirement-Oriented and Standard-Based Compliance Monitoring and Reporting Prototype ..................................................................................................................468

Matthias Kehlenbeck, Thorben Sandner, and Michael H. Breitner

Organizational Aspects of Security: Session 4

A Taxonomy Refining the Security Requirements for Electronic Voting: Analyzing Helios as a Proof of Concept ........................................................................................................................................475

Lucie Longer, Axel Schmidt, Johannes Buchmann, and Melanie Volkamer

Secured Key Distribution Scheme for Cryptographic Key Management System ........................................................................................................481

Kyawt Kyawt Khain and Khin Mi Mi Aung

One Size Fits None: The Importance of Detector Parameterization ......................................................................................................................487

Natasha Bodorik and A. Nur Zincir-Heywood

Fourth International Workshop on Secure Software Engineering (SecSE 2010)

Agile Development and Hot Patching

Supporting Authorization Policy Modification in Agile Development of Web Applications ........................................................................................................495

Steffen Bartsch

The Road to Hell is Paved with Good Intentions: A Story of (In)secure Software Development ..................................................................................................................501

Richard Sasson, Martin Gilje Jaatun, and Jostein Jensen

Katana: A Hot Patching Framework for ELF Executables .................................................................................................................................507

Ashwin Ramaswamy, Sergey Bratus, Sean W. Smith, and Michael E. Locasto
Testing, Monitoring, and Validation

Investigating the Limitations of Java Annotations for Input Validation .............................................513
Federico Mancini, Dag Hovland, and Khalid A. Mughal

Classification of Buffer Overflow Vulnerability Monitors .................................................................519
Hossain Shahriar and Mohammad Zulkernine

Configuration Fuzzing for Software Vulnerability Detection ..........................................................525
Huning Dai, Christian Murphy, and Gail Kaiser

Security Modeling and Vulnerabilities

Practical Experience Gained from Modeling Security Goals: Using SGITs in an Industrial Project ..........531
Christian Jung, Frank Elberzhager, Alessandra Bagnato, and Fabio Raiteri

Security Modeling and Tool Support Advantages .............................................................................537
Egil Trygve Baadshaug, Gencer Erdogan, and Per Håkon Meland

Analysing and Visualising Security and Usability in IRIS ................................................................543
Shamal Faily and Ivan Fléchaïs

Security and Performance Aspects of an Agent-Based Link-Layer Vulnerability Discovery Mechanism ..........549
Ziyad S. Al-Salloum and Stephen D. Wolthusen

Fourth International Workshop on Secure Systems Methodologies Using Patterns (SPattern 2010)

SPattern Application

Model-Driven Security Patterns Application Based on Dependences among Patterns ................................555
Yuki Shiroma, Hironori Washizaki, Yoshiaki Fukazawa, Atsuto Kubo, and Nobukazu Yoshioka

Refining the Pattern-Based Reference Model for Electronic Invoices by Incorporating Threats ..............560
Michael Netter, Eduardo B. Fernandez, and Günther Pernul

Measuring the Level of Security Introduced by Security Patterns ......................................................565
Eduardo B. Fernandez, Nobukazu Yoshioka, Hironori Washizaki, and Michael VanHilst

SPattern Development

Patterns for Secure Boot and Secure Storage in Computer Systems ......................................................569
Hans Löhr, Ahmad-Reza Sadeghi, and Marcel Winandy
Fourth International Workshop on Advances in Information Security (WAIS 2010)

Identity and Privacy

A Consideration of the Reliability of Registration and Attribute Exchange ..............................................574
Yoshio Kakizaki and Keiichi Iwamura

Binomial-Mix-Based Location Anonymizer System with Global Dummy
Generation to Preserve User Location Privacy in Location-Based Services ..................................................580
Minh-Triet Tran, Isao Echizen, and Anh-Duc Duong

Multiple Designated Verifiers Signatures Reconsidered ............................................................................586
Mebae Ushida, Tetsuya Izu, Masahiko Takenaka, and Kazuo Ohta

System Security

LSM-Based Secure System Monitoring Using Kernel Protection Schemes ....................................................591
Takamasa Isohara, Keisuke Takemori, Yutaka Miyake, Ning Qu, and Adrian Perrig

Formalization of Viruses and Malware Through Process Algebras ...............................................................597
Grégoire Jacob, Eric Filiol, and Hervé Debar

Heuristics for Detecting Botnet Coordinated Attacks .................................................................................603
Kazuya Kuwabara, Hiroaki Kikuchi, Masato Terada, and Masashi Fujiwara

Experimental and Physical Security

An Improvement of Robustness Against Physical Attacks and Equipment
Independence in Information Hiding Based on the Artificial Fiber Pattern ...................................................608
Kitahiro Kaneda, Yuki Fujii, Keiichi Iwamura, and Seiichiro Hangai

Large Scale Demonstration Experiments Towards Achieving Practical
Traceback on the Internet .................................................................................................................................613
Ken Wakasa, Hiroaki Hazeyama, Toshifumi Kai, Akira Hashiguchi, Masaya Yamagata,
Masahiko Fujinaga, Ryunosuke Ohshima, and Takashi Shintani

Quantum Detection of Wavelength Division Multiplexing Optical Coherent
Signals in Lossy Channels ...............................................................................................................................619
Atsushi Waseda, Masahide Sasaki, Masahiro Takeoka, Mikio Fujiwara,
Morio Toyoshima, and Hidema Tanaka

Experimental Results on Cheon’s Algorithm .................................................................................................625
Tetsuya Izu, Masahiko Takenaka, and Masaya Yasuda

Third International Workshop on Digital Forensics (WSDF 2010)

Digital Forensic Workshop: Session 1

The ‘Explore, Investigate and Correlate’ (EIC) Conceptual Framework
for Digital Forensics Information Visualisation ..............................................................................................629
Grant Osborne, Benjamin Turnbull, and Jill Slay

A Model for Computer Profiling .....................................................................................................................635
Andrew Marrington, George Mohay, Hasmukh Morarji, and Andrew Clark
Using Normalized Compression Distance for Classifying File Fragments .................................................. 641
   Stefan Axelsson

**Digital Forensic Workshop: Session 2**

A Multi-component View of Digital Forensics ................................................................. 647
   C.P. Grobler, C.P. Louwrens, and S.H. von Solms

Blind Steganalysis: A Countermeasure for Binary Image Steganography .............................................. 653
   Kang Leng Chiew and Josef Pieprzyk

Log Analysis Towards an Automated Forensic Diagnosis System ....................................................... 659
   Jorge Herreras and Roberto Gómez

**Digital Forensic Workshop: Session 3**

A Function Oriented Methodology to Validate and Verify Forensic Copy Function of Digital Forensic Tools ................................................................. 665
   Yinghua Guo and Jill Slay

A Complexity Based Model for Quantifying Forensic Evidential Probabilities ...................................... 671
   Richard E. Overill, Jantje A.M. Silomon, and Kam-Pui Chow

A Framework to Guide the Implementation of Proactive Digital Forensics in Organisations ................. 677
   C.P. Grobler, C.P. Louwrens, and S.H. von Solms

Estimating Hidden Message Length in Binary Image Embedded by Using Boundary Pixels Steganography ....................................................... 683
   Kang Leng Chiew and Josef Pieprzyk

**Digital Forensic Workshop Session 4**

Information Flow Control Using the Java Virtual Machine Tool Interface (JVMTI) ........................................ 689
   Jason Howarth, Irfan Altas, and Barney Dalgarno

A Prototype for Support of Computer Forensic Analysis Combined with the Expected Knowledge Level of an Attacker to More Efficiently Achieve Investigation Results ....................................................... 696
   Maximilian Bielecki and Gerald Quirchmayr

A Novel Image Hiding Scheme Using Content Aware Seam Carving Method ....................................... 702
   Zahra Toony and Mansour Jamzad

**Author Index**