TABLE OF CONTENTS

VOLUME 1

Message from the Organizing Committee
ARES and Workshops Committees

SESSION 1: TRUST MODEL AND TRUST MANAGEMENT

Formalising Dynamic Trust Negotiations in Decentralised Collaborative e-Health Systems ................................................................. 1
  Oluwafemi Ajayi, Richard Sinnott, Anthony Stell

Why Trust is Not Proportional to Risk .......................................................... 9
  Bjørnar Solhaug, Dag Elgesem, Ketil Stølen

From Trust to Dependability through Risk Analysis .................................. 17
  Yudistira Asnar, Paolo Giorgini, Fabio Massacci, Nicola Zannone

Dynamic Trust Domains for Secure, Private, Technology-assisted Living .................. 25
  Jatinder Singh, Jean Bacon, Ken Moody

A Hybrid Trust Model for Enhancing Security in Distributed Systems ............ 33
  Ching Lin, Vijay Varadharajan

A Reliable Component-based Architecture for E-Mail Filtering ...................... 41
  Wilfried N. Gansterer, Andreas G.K. Janecek, Peter Lechner

SESSION 2: AVAILABILITY, FAULT- TOLERANT AND RECOVERY

Availability and Performance of the Adaptive Voting Replication Protocol ........ 49
  Johannes Osrael, Lorenz Froihofer, Norbert Chlaupek, Karl M. Goeschka

Distributed Stream Processing Analysis in High Availability Context .................. 57
  Marcin Gorawski, Pawel Marks

Implementing Network Partition-aware Fault-tolerant CORBA Systems ............ 65
  Stefan Beyer, Francesc D. Muñoz-Escoi, Pablo Galdámez

Failure Recovery in Cooperative Data Stream Analysis .................................. 73
  Bin Rong, Fred Douglis, Zhen Liu, Cathy H. Xia

A Recovery Protocol for Middleware Replicated Databases Providing GSI .......... 81
  J.E. Armendánz, F.D. Muñoz-Escoi, J.R. Juárez, J.R.G. de Mendivil, B. Kemme
Revisiting Hot Passive Replication
Rubén de Juan-Marín, Hendrik Decker, Francesc D. Muñoz-Escoi

SESSION 3: REPUTATION MANAGEMENT AND TRUST

Reputation Management Survey
Sini Ruohomaa, Lea Kutvonen, Eleni Koutrouli

Dirichlet Reputation Systems
Audun Jøsang, Jochen Haller

Compartmented Security for Browsers — Or How to Thwart a Phisher with Trusted Computing
Sebastian Gajek, Ahmad-Reza Sadeghi, Christian Stüble, Marcel Winandy

Secure Anonymous Union Computation among Malicious Partners
Stefan Böttcher, Sebastian Obermeier

SESSION 4: PRIVACY AND ACCESS CONTROL

A Privacy Enhancing Service Architecture for Ticket-based Mobile Applications
Oliver Jorns, Oliver Jung, Gerald Quirchmayr

Privacy in Pervasive Computing and Open Issues
Pankaj Bhaskar, Sheikh I. Ahamed

Context-dependent Access Control for Contextual Information
Christin Groba, Stephan Groß, Thomas Springer

Bytecode Verification for Enhanced JVM Access Control
Dongxi Liu

SESSION 5: FAILURE DETECTION AND ATTACK PREVENTION

Automatic Failure Detection with Separation of Concerns
P. Hazy, R.E. Seviora

A Failure Detection Service for Large-Scale Dependable Wireless Ad-Hoc and Sensor Networks
Mourad Elhadef, Azzedine Boukerche

Intrusion Detection System for Signal Based SIP Attacks through Timed HCPN
Yanlan Ding, Guiping Su

3G-WLAN Convergence: Vulnerability, Attacks Possibilities and Security Management Model
Muhammad Sher, Thomas Magedanz

Specification and Detection of TCP/IP Based Attacks Using the ADM-Logic
Meriam Ben Ghorbel, Mehdi Talbi, Mohamed Mejri

Near Optimal Protection Strategies against Targeted Attacks on the Core Node of a Network
Frank Yeong-Sung Lin, Po-Hao Tsang, Yi-Luen Lin
SESSION 6: AUTHENTICATION AND AUTHORISATION

Errors in Attacks on Authentication Protocols ................................................................. 209
Anders Moen Hagalisletto

Effects of Architectural Decisions in Authentication and Authorisation Infrastructures ......................................................................................................................... 216
Christian Schläger, Monika Ganslmayer

Vulnerability Analysis of EMAP — An Efficient RFID Mutual Authentication Protocol .......................................................................................................................... 224
Tieyan Li, Robert Deng

Authentication Mechanisms for Mobile Agents ............................................................... 232
Leila Ismail

Using SAML and XACML for Complex Authorisation Scenarios in Dynamic Resource Provisioning ................................................................................................................. 240
Yuri Demchenko, Leon Gommans, Cees de Laat

Implicit Authorization for Accessing Location Data in a Social Context .................... 249
Georg Treu, Florian Fuchs, Christiane Dargatz

SESSION 7: SECURITY ALGORITHM AND FRAMEWORK

Fingerprint Matching Algorithm Based on Tree Comparison Using Ratios of Relational Distances ............................................................................................................... 257
Abinandhan Chandrasekaran, Bhavani Thuraisingham

A Reconfigurable Implementation of the New Secure Hash Algorithm .......................... 265
M. Zeghida, B. Bouallegue, A. Baganne, M. Machhout, R. Tourki

Applications for Provably Secure Intent Protection with Bounded Input-Size Programs ......................................................................................................................... 270
J. Todd McDonald, Alec Yasinsac

A Framework for the Development of Secure Data Warehouse Based on MDA and QVT ....................................................................................................................... 278
Emilio Soler, Juan Trujillo, Eduardo Fernández-Medina, Mario Piattini

SESSION 8: SOFTWARE SECURITY

Design of a Process for Software Security ........................................................................ 283
David Byers, Nahid Shahmehri

STEF: A Secure Ticket-based En-Route Filtering Scheme for Wireless Sensor Networks ......................................................................................................................... 292
Christoph Krauß, Markus Schneider, Kpatcha Bayarou, Claudia Eckert

A Secure Architecture for the Pseudonymization of Medical Data ................................. 300
Bernhard Riedl, Thomas Neubauer, Gernot Goluch, Oswald Boehm, Gert Reinauer, Alexander Krumboeck

Collection of Quantitative Data on Security Incidents ...................................................... 307
Thomas Nowey, Hannes Federrath
### SESSION 9: SECURITY MODELS

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Vulnerabilities in DNS and DNSSEC</td>
<td>315</td>
</tr>
<tr>
<td>Suranjith Ariyapperuma, Chris J. Mitchell</td>
<td></td>
</tr>
<tr>
<td>Secure, Resilient Computing Clusters: Self-Cleansing Intrusion Tolerance with Hardware Enforced Security (SCIT/HES)</td>
<td>323</td>
</tr>
<tr>
<td>David Arsenault, Arun Sood, Yih Huang</td>
<td></td>
</tr>
<tr>
<td>Applying a Tradeoff Model (TOM) to TACT</td>
<td>331</td>
</tr>
<tr>
<td>Raihan Al-EKram, Ric Holt, Chris Hobbs</td>
<td></td>
</tr>
<tr>
<td>A Pattern System for Security Requirements Engineering</td>
<td>336</td>
</tr>
<tr>
<td>Denis Hatebur, Maritta Heisel, Holger Schmidt</td>
<td></td>
</tr>
<tr>
<td>Security Requirements for a Semantic Service-oriented Architecture</td>
<td>346</td>
</tr>
<tr>
<td>Stefan Dürbeck, Rolf Schillinger, Jan Kolter</td>
<td></td>
</tr>
<tr>
<td>Supporting Compliant and Secure User Handling — A Structured Approach for In-House Identity Management</td>
<td>354</td>
</tr>
<tr>
<td>Ludwig Fuchs, Günther Pernul</td>
<td></td>
</tr>
</tbody>
</table>

### SESSION 10: MISCELLANEOUS SECURITY TECHNIQUES

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A New Classification Scheme for Anonymization of Real Data Used in IDS Benchmarking</td>
<td>362</td>
</tr>
<tr>
<td>Vidar Evenrud Seeberg, Slobodan Petrovi?</td>
<td></td>
</tr>
<tr>
<td>Static Evaluation of Certificate Policies for GRID PKIs Interoperability</td>
<td>368</td>
</tr>
<tr>
<td>Valentina Casola, Nicola Mazzocca, Jesus Luna, Oscar Manso, Manel Medina, Massimiliano Rak</td>
<td></td>
</tr>
<tr>
<td>Towards an Ontology-based Risk Assessment in Collaborative Environments Using the SemanticLIFE</td>
<td>377</td>
</tr>
<tr>
<td>Mansoor Ahmed, Amin Anjomshoaa, Tho Manh Nguyen, A Min Tjoa</td>
<td></td>
</tr>
<tr>
<td>Universally Composable Three-party Key Distribution</td>
<td>385</td>
</tr>
<tr>
<td>TingMao Chang, YueFei Zhu, Jin Zhou, YaJuan Zhang</td>
<td></td>
</tr>
</tbody>
</table>

### SESSION 11: e-AUCTION AND e-VOTING PROTOCOL

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>An Efficient eAuction Protocol</td>
<td>392</td>
</tr>
<tr>
<td>Brian Curtis, Josef Pieprzyk, Jan Seruga</td>
<td></td>
</tr>
<tr>
<td>Enhancing the Security of Local Danger Warnings in VANETs — A Simulative Analysis of Voting Schemes</td>
<td>397</td>
</tr>
<tr>
<td>Benedikt Ostermaier, Florian Dötzer, Markus Strassberger</td>
<td></td>
</tr>
<tr>
<td>A Practical Verifiable e-Voting Protocol for Large Scale Elections over a Network</td>
<td>407</td>
</tr>
<tr>
<td>Orhan Cetinkaya, Ali Doganaksoy</td>
<td></td>
</tr>
</tbody>
</table>
SESSION 12: DEPENDABILITY IN DISTRIBUTED AND UBIQUITOUS COMPUTING

Decoupling Constraint Validation from Business Activities to Improve Dependability in Distributed Object Systems .................................................................................................................. 415
Lorenz Froihofer, Johannes Osrael, Karl M. Goeschka

Dependability Aspects of Ubiquitous Computing .......................................................................................................................... 423
Lu Yan, Kaisa Sere

Concurrency Control Using Subject- and Purpose-Oriented (SPO) Scheduler ........................................... 426
Tomoya Enokido, Makoto Takizawa

SESSION 13: ANOMALY AND INTRUSION DETECTION

Comparing Classifier Combining Techniques for Mobile-Masquerader Detection .......................... 434
Oleksiy Mazhelis, Seppo Puuronen

Process Profiling Using Frequencies of System Calls .................................................................................. 442
Surekha Mariam Varghese, K. Poulose Jacob

Terrorist Networks Analysis through Argument Driven Hypotheses Model ................................... 449
D.M. Akbar Hussain

INTERNATIONAL SYMPOSIUM ON FRONTIERS IN AVAILABILITY, RELIABILITY AND SECURITY (FARES)

SESSION 1: FAULT-TOLERANT AND AVAILABILITY

High Availability for Network Management Applications ................................................................. 457
Prabhu S., Venkat R.

RWAR: A Resilient Window-consistent Asynchronous Replication Protocol .................................. 463
Yanlong Wang, Zhanhuai Li, Wei Lin

Fault-Tolerant Semi-Passive Coordination Protocol for a Multi-Actuator/Multi-Sensor Model ........................................................................................................................... 470
Keiji Ozaki, Naohiro Hayashibara, Tomoya Enokido, Makoto Takizawa

SESSION 2: ACCESS CONTROL

Realizing Fine-Granular Read and Write Rights on Tree Structured Documents ......................... 478
Franz Kollmann

Access Control Model for Web Services with Attribute Disclosure Restriction ............................. 485
Vipin Singh Mewar, Subhendu Aich, Shamik Sural

Aggregating and Deploying Network Access Control Policies ......................................................... 493
Joaquín G. Alfaro, Frédéric Cuppens, Nora Cuppens-Boulahia
SESSION 3: AUTHENTICATION

Secure Spatial Authentication Using Cell Phones ................................................................. 501
   Arjan Durresi, Vamsi Paruchuri, Mimoza Durresi, Leonard Barolli

Broadcast Authentication Protocol with Time Synchronization and Quadratic Residues Chain ................................................................. 508
   Bogdan Groza

A Secure Key Exchange and Mutual Authentication Protocol for Wireless Mobile Communications ................................................................. 516
   Yijun He, Nan Xu, Jie Li

Improved Client-to-Client Password-Authenticated Key Exchange Protocol ................................................................. 522
   Gang Yao, Dengguo Feng, Xiaoxi Han

SESSION 4: REAL-TIME SYSTEM AND SENSOR NETWORK

Adaptation Mechanisms for Survivable Sensor Networks against Denial of Service Attacks ................................................................. 530
   Dong Seong Kim, Chung Su Yang, Jong Sou Park

   Christian Buckl, Matthias Regensburger, Alois Knoll, Gerhard Schrott

A Near-Real-Time Behaviour Control Framework ................................................................. 543
   Bastian Preindl, Alexander Schatten

SESSION 5: RFID TECHNIQUES AND APPLICATIONS

RFID Security Issues in Military Supply Chains ................................................................. 551
   Qinghan Xiao, Cam Boulet, Thomas Gibbons

The Cost of Preserving Privacy: Performance Measurements of RFID Pseudonym Protocols ................................................................. 558
   Jens Mache, Chris Allick

Mobile Phone Based RFID Architecture for Secure Electronic Payments Using RFID Credit Cards ................................................................. 562
   Geethapriya Venkataramani, Srividya Gopalan

SESSION 6: SECURE SOLUTION AND APPLICATIONS

A Modular Architecture for Secure and Reliable Distributed Communication ................................................................. 570
   C.M. Jayalath, R.U. Fernando

Security Oriented e-Infrastructures Supporting Neurological Research and Clinical Trials ................................................................. 578
   Anthony Stell, Richard Sinnott, Oluwafemi Ajayi, Jipu Jiang

VOLUME 2

Securing Medical Sensor Environments: The CodeBlue Framework Case ................................................................. 586
   Georgios Kambourakis, Eleni Klaoudatou, Stefanos Gritzalis
A Set of QVT Relations to Transform PIM to PSM in the Design of Secure Data Warehouses
Emilio Soler, Juan Trujillo, Eduardo Fernández-Medina, Mario Piattini

SESSION 7: SECURITY ISSUE IN BUSINESS MANAGEMENT

Agent Alliances: A Means for Practical Threshold Signature
Regine Endsuleit, Christoph Amma

Protecting Online Transactions with Unique Embedded Key Generators
Martin Boesgaard, Erik Zenner

A Research Agenda for Autonomous Business Process Management
Thomas Neubauer, Gernot Goluch, Bernhard Riedl

SESSION 8: WEB, XML, CONTENT MANAGEMENT

Secure Web Application Development and Global Regulation
William Bradley Glisson, L. Milton Glisson, Ray Welland

Query Assurance Verification for Dynamic Outsourced XML Databases
Viet Hung Nguyen, Tran Khanh Dang, Nguyen Thanh Son, Josef Küng

A Reflection-based Framework for Content Validation
Lars-Helge Netland, Yngve Espelid, Khalid A. Mughal

SESSION 9: SECURITY POLICIES AND TECHNIQUES

Web Engineering Security: Essential Elements
William Glisson, Ray Welland

Designing a Security Policy According to BS 7799 Using the OCTAVE Methodology
Paulina Januszkiewicz, Marek Pyka

CSP-based Firewall Rule Set Diagnosis Using Security Policies
S. Pozo, R. Ceballos, R.M. Gasca

CASSIS — Computer-based Academy for Security and Safety in Information Systems
Gernot Goluch, Andreas Ekelhart, Stefan Fenz, Stefan Jakoubi, Bernhard Riedl, Simon Tjoa

SESSION 10: TRUST MANAGEMENT AND TRUST MODEL

Trust in Global Computing Systems as a Limit Property Emerging from Short Range Random Interactions
V. Liagkou, E. Makri, P. Spirakis, Y.C. Stamatiou

A Trust Overlay Architecture and Protocol for Enhanced Protection against Spam
Jimmy McGibney, Dmitri Botvich

HICI: An Approach for Identifying Trust Elements — The Case of Technological Trust Perspective in VBEs
Simon Samwel Msanjila, Hamideh Afsaranesh
A Semantic and Time Related Recommendation-Feedback Trust Model........................................ 704
Lin Zhang, Feng Xu, Yuan Wang, Jian Lv

SESSION 11: MISCELLANEOUS APPLICATIONS

AsmLSec: An Extension of Abstract State Machine Language for Attack Scenario Specification ................................................................. 711
Mohammad Raihan, Mohammad Zulkernine

Error Modeling in RF-based Location Detection (EMLD) for Pervasive Computing Environments ................................................................................. 719
Niraj Swami, Sheikh I. Ahamed

A Performance Model to Cooperative Itinerant Agents (CIA): A Security Scheme to IDS ............................................................... 727
Rafael Páez, Cristina Satizábal, Jordi Forné

On the Assessment of the Interaction Quality of Users with Cerebral Palsy .......................................................... 735
C. Mauria, T. Granollers, A. Solanas

Research and Design of Mobile Impeachment System with Semi-cryptonym ........................................................................... 742
Chaobo Yang, Ming Qi

Efficient Malicious Agreement in a Virtual Subnet Network ........................................................................ 748
Shu-Ching Wang, Shyi-Ching Liang, Kuo-Qin Yan, Guang-Yan Zheng

Extended RBAC–Based Design and Implementation for a Secure Data Warehouse ........................................ 755
Bhavani Thuraisingham, Srinivasan Iyer

Application of QVT for the Development of Secure Data Warehouses: A Case Study ................................................................................. 763
Emilio Soler, Juan Trujillo, Eduardo Fernández-Medina, Mario Piattini

Protecting Private Information by Data Separation in Distributed Spatial Data Warehouse ........................................................................ 771
Marcin Gorawski, Jakub Bularz

Applying a Flexible Mining Architecture to Intrusion Detection .................................................................................. 779
Marcello Castellano, Giuliano Bellone de Grecis, Giuseppe Mastronardi, Angela Aprile, Flaviano Fiorino

An Application of Learning Problem in Anomaly-based Intrusion Detection Systems ........................................................................ 787
Veselina G. Jecheva, Evgeniya P. Nikolova

Detecting Critical Regions in Covert Networks: A Case Study of 9/11 Terrorists Network .................................................... 795
Nasrullah Memon, Kim C. Kristoffersen, David L. Hicks, Henrik Legind Larsen

Access Control and Integration of Health Care Systems: An Experience Report and Future Challenges ........................................................................... 805
Lillian Røstad, Øystein Nytra, Inger Anne Tøndel, Per Håkon Meland

A Collaborative Inter Data Grids Strong Semantic Model with Hybrid Namespace ........................................... 812
Dalia El-Mansy, Ahmed Sameh

Reliability Markov Chains for Security Data Transmitter Analysis ........................................................................ 820
Calin Ciufudean, Bianca Satco, Constantin Filote

Requirements and Evaluation Procedures for eVoting ........................................................................................................ 827
Melanie Volkamer, Margaret McGaley
Towards Secure E-Elections in Turkey: Requirements and Principles ........................................ 835
Orhan Cetinkaya, Deniz Cetinkaya

On Coercion-Resistant Electronic Elections with Linear Work ............................................ 840
Stefan G. Weber, Roberto Araújo, Johannes Buchmann

Maria Grazia Fugini

eTVRA, a Threat, Vulnerability and Risk Assessment Method and Tool for eEurope .................... 857
Judith E.Y. Rossebø, Scott Cadzow, Paul Sijben

Framework for Information Sharing Across Multiple Government Agencies under Dynamic Access Policies ............................................................................................................. 866
K. Bhoopalam, K. Maly, R. Mukkamala, M. Zubair

Secure Distributed Dossier Management in the Legal Domain ............................................... 873
Martijn Warnier, Frances Brazier, Martin Apistola, Anja Oskamp

Building a Dependable Messaging Infrastructure for Electronic Government ....................... 880
Elsa Estevez, Tomasz Janowski

WORKSHOP ON FOUNDATIONS OF FAULT-TOLERANT DISTRIBUTED COMPUTING (FOFDC 2007)

A Universal Construction for Concurrent Objects .................................................................... 888
Rachid Guerraoui, Michel Raynal

FCPre: Extending the Arora-Kulkarni Method of Automatic Addition of Fault-Tolerance ................................................................................................................................. 896
Bastian Braun

On the Implementation of the Omega Failure Detector in the Crash-Recovery Failure Model .......................................................... 904
Cristian Martin, Mikel Larrea, Ernesto Jiménez

Self-Diagnosing Wireless Mesh and Ad-Hoc Networks Using an Adaptable Comparison-Based Approach .................................................................................................................. 912
Mourad Elhadef, Azzedine Boukerche, Hisham Elkadiki

Self-Stabilization as a Foundation for Autonomic Computing .................................................. 920
Olga Brukman, Shlomi Dolev, Yinnon Haviv, Reuven Yagel

On Programming Models for Service-Level High Availability ............................................. 928
C. Engelmann, S.L. Scott, C. Leangsuksun, X. He

FIRST INTERNATIONAL WORKSHOP ON SECURE SOFTWARE ENGINEERING (SECSE 2007)

Using Privacy Process Patterns for Incorporating Privacy Requirements into the System Design Process .......................................................................................................................... 936
Christos Kalloniatis, Evangelia Kavaki, Stefanos Gritzalis

How Can the Developer Benefit from Security Modeling? ....................................................... 944
Shanai Ardi, David Byers, Per Håkon Meland, Inger Anne Tøndel, Nahid Shahmehri

AProSec: An Aspect for Programming Secure Web Applications ......................................... 953
Gabriel Hermosillo, Roberto Gomez, Lionel Seinturier, Laurence Duchien
Empirical and Statistical Analysis of Risk Analysis-Driven Techniques for Threat Management ................................................................. 961
  Koen Buyens, Bart De Win, Wouter Joosen

Secure Software Development through Coding Conventions and Frameworks ................................................................. 969
  Takao Okubo, Hidehiko Tanaka

Pastures: Towards Usable Security Policy Engineering ................................................................. 979
  Sergey Bratus, Alex Ferguson, Doug McIlroy, Sean Smith

Security Objectives within a Security Testing Case Study ................................................................. 987
  Kaarina Karppinen, Reijo Savola, Mikko Rapeli, Esa Tikkala

CppTest: A Prototype Tool for Testing C/C++ Programs ................................................................. 993
  Chengying Mao, Yansheng Lu

A Novel Approach to Building Secure Systems ........................................................................ 1001
  Dragan Vidakovic, Dejan Simic

WORKSHOP ON “MODELING, DESIGNING, AND TESTING CORRECT, SECURE, AND DEPENDABLE EVENT-BASED SYSTEM” (EBITS2007)

Exception Handling in an Event-Driven System ................................................................. 1009
  Jan Ploski, Wilhelm Hasselbring

Issues in Testing Dependable Event-based Systems at a Systems Integration Company ................................................................. 1017
  Armin Beer, Matthias Heindl

Optimizing Events Traffic in Event-based Systems by Means of Evolutionary Algorithms ................................................................. 1025
  Jiri Kubalik, Richard Mordinyi

Event-based Monitoring of Open Source Software Projects ................................................................. 1032
  Dindin Wahyudin, A. Min Tjoa

Using Space-based Computing for More Efficient Group Coordination and Monitoring in an Event-based Work Management System ................................................................. 1040
  Marcus Mor, Richard Mordinyi, Johannes Riemer

Indexing and Search of Correlated Business Events ........................................................................ 1048
  Roland Vecera, Szabolcs Rozsnyai, Heinz Roth

FIRST INTERNATIONAL WORKSHOP ON ADVANCES IN INFORMATION SECURITY (WAIS 2007)

An Approach for Adaptive Intrusion Prevention Based on The Danger Theory ................................................................. 1056
  Alexander Krizhanovsky, Alexander Marasanov

A Human-Verifiable Authentication Protocol Using Visible Laser Light ................................................................. 1064
  Rene Mayrhofer, Martyn Welch

Insider-secure Hybrid Signcryption Scheme without Random Oracles ................................................................. 1069
  Chik How Tan

  Kei Nagai, Hiroaki Kikuchi, Wakaha Ogata, Masakatsu Nishigaki
A Policy Language for the Extended Reference Monitor in Trusted Operating Systems
Hyung Chan Kim, R.S. Ramakrishna, Wook Shin, Koiuchi Sakurai .......................................................... 1081

Analysis on Bleichenbacher’s Forgery Attack
Tetsuya Izu, Masahiko Takenaka, Takeshi Shimoyama .......................................................... 1088

A New Method for Reducing the Revocation Delay in the Attribute Authentication
Yoshio Kakizaki, Hidekazu Tsuji ........................................................................................................ 1096

Efficient Multiparty Computation for Comparator Networks
Koji Chida, Hiroaki Kikuchi, Gembu Morohashi, Keiichi Hirota .......................................................... 1104

Pseudo-Voter Identity (PVID) Scheme for e-Voting Protocols
Orhan Cetinkaya, Ali Doganaksoy ........................................................................................................ 1111

Attacks are Protocols Too
Anders Moen Hagalisletto ........................................................................................................ 1118

Luis Zarza, Josep Pegueroles, Miguel Soriano .................................................................................. 1128

On the Use of One-Way Chain Based Authentication Protocols in Secure Control Systems
Bogdan Groza, Toma-Leonida Dragomir .......................................................................................... 1135

Bypassing Data Execution Prevention on Microsoft Windows XP SP2
Nenad Stojanovski, Marjan Gušev, Danilo Gligoroski, Svein J. Knapskog ............................................. 1143

A Security Framework for RFID Multi-Domain System
Dong Seong Kim, Taek-Hyun Shin, Jong Sou Park .............................................................................. 1148

WORKSHOP ON “SECURITY IN E-LEARNING” (SEL)

E-Learning 2.0 = e-Learning 1.0 + Web 2.0?
Martin Ebner ........................................................................................................................................ 1154

Blended Learning Technology in Information Security Management Courses
Gerald Quirchmayr .......................................................................................................................... 1159

Defining a Trusted Service-oriented Network Environment
Emmanuel A. Adigun, J.H.P. Eloff ..................................................................................................... 1164

Designing a Cryptographic Scheme for e-Surveys in Higher-Education Institutions
Alan Ward, Jordi Castellà-Roca, Aleix Dorca Josa ............................................................................. 1170

Author Index