

The Second International Conference on Availability, Reliability and Security



ARES 2007

DEXA

10 - 13 April 2007

Vienna, Austria

In Cooperation with



TECHNISCHE
UNIVERSITÄT
WIEN
VIENNA
UNIVERSITY OF
TECHNOLOGY

[SECURE]
Business Austria
Kompetenz für Wissenschaft und Industrie.



OESTERREICHISCHE
COMPUTER GESELLSCHAFT
AUSTRIAN
COMPUTER SOCIETY



Los Alamitos, California

Washington • Tokyo



Second International Conference on Availability,
Reliability and Security

(ARES 2007)

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
<i>Oluwafemi Ajayi, Richard Sinnott, Anthony Stell</i>	
Why Trust is Not Proportional to Risk	9
<i>Bjørnar Solhaug, Dag Elgesem, Ketil Stølen</i>	
From Trust to Dependability through Risk Analysis	17
<i>Yudistira Asnar, Paolo Giorgini, Fabio Massacci, Nicola Zannone</i>	
Dynamic Trust Domains for Secure, Private, Technology-assisted Living	25
<i>Jatinder Singh, Jean Bacon, Ken Moody</i>	
A Hybrid Trust Model for Enhancing Security in Distributed Systems	33
<i>Ching Lin, Vijay Varadharajan</i>	
A Reliable Component-based Architecture for E-Mail Filtering	41
<i>Wilfried N. Gansterer, Andreas G.K. Janecek, Peter Lechner</i>	

SESSION 2: AVAILABILITY, FAULT- TOLERANT AND RECOVERY

Availability and Performance of the Adaptive Voting Replication Protocol	49
<i>Johannes Osrael, Lorenz Frohofer, Norbert Chlaupke, Karl M. Goeschka</i>	
Distributed Stream Processing Analysis in High Availability Context	57
<i>Marcin Gorawski, Pawel Marks</i>	
Implementing Network Partition-aware Fault-tolerant CORBA Systems	65
<i>Stefan Beyer, Francesc D. Muñoz-Escóí, Pablo Galdámez</i>	
Failure Recovery in Cooperative Data Stream Analysis	73
<i>Bin Rong, Fred Douglass, Zhen Liu, Cathy H. Xia</i>	
A Recovery Protocol for Middleware Replicated Databases Providing GSI	81
<i>J.E. Armendáriz, F.D. Muñoz-Escóí, J.R. Juárez, J.R.G. de Mendivil, B. Kemme</i>	

Revisiting Hot Passive Replication	89
<i>Rubén de Juan-Marín, Hendrik Decker, Francesc D. Muñoz-Escóí</i>	

SESSION 3: REPUTATION MANAGEMENT AND TRUST

Reputation Management Survey	97
<i>Sini Ruohomaa, Lea Kutvonen, Eleni Koutrouli</i>	
Dirichlet Reputation Systems	106
<i>Audun Jøsang, Jochen Haller</i>	
Compartmented Security for Browsers — Or How to Thwart a Phisher with Trusted Computing	114
<i>Sebastian Gajek, Ahmad-Reza Sadeghi, Christian Stübke, Marcel Winandy</i>	
Secure Anonymous Union Computation among Malicious Partners.....	122
<i>Stefan Böttcher, Sebastian Obermeier</i>	

SESSION 4: PRIVACY AND ACCESS CONTROL

A Privacy Enhancing Service Architecture for Ticket-based Mobile Applications	130
<i>Oliver Jorns, Oliver Jung, Gerald Quirchmayr</i>	
Privacy in Pervasive Computing and Open Issues	138
<i>Pankaj Bhaskar, Sheikh I. Ahamed</i>	
Context-dependent Access Control for Contextual Information	146
<i>Christin Groba, Stephan Groß, Thomas Springer</i>	
Bytecode Verification for Enhanced JVM Access Control	153
<i>Dongxi Liu</i>	

SESSION 5: FAILURE DETECTION AND ATTACK PREVENTION

Automatic Failure Detection with Separation of Concerns	161
<i>P. Hazy, R.E. Seviora</i>	
A Failure Detection Service for Large-Scale Dependable Wireless Ad-Hoc and Sensor Networks.....	170
<i>Mourad Elhadef, Azzedine Boukerche</i>	
Intrusion Detection System for Signal Based SIP Attacks through Timed HCPN	178
<i>Yanlan Ding, Guiping Su</i>	
3G-WLAN Convergence: Vulnerability, Attacks Possibilities and Security Management Model.....	186
<i>Muhammad Sher, Thomas Magedanz</i>	
Specification and Detection of TCP/IP Based Attacks Using the ADM-Logic	194
<i>Meriam Ben Ghorbel, Mehdi Talbi, Mohamed Mejri</i>	
Near Optimal Protection Strategies against Targeted Attacks on the Core Node of a Network	201
<i>Frank Yeong-Sung Lin, Po-Hao Tsang, Yi-Luen Lin</i>	

SESSION 6: AUTHENTICATION AND AUTHORISATION

Errors in Attacks on Authentication Protocols	209
<i>Anders Moen Hagalisletto</i>	
Effects of Architectural Decisions in Authentication and Authorisation Infrastructures	216
<i>Christian Schläger, Monika Ganslmayer</i>	
Vulnerability Analysis of EMAP — An Efficient RFID Mutual Authentication Protocol	224
<i>Tieyan Li, Robert Deng</i>	
Authentication Mechanisms for Mobile Agents	232
<i>Leila Ismail</i>	
Using SAML and XACML for Complex Authorisation Scenarios in Dynamic Resource Provisioning	240
<i>Yuri Demchenko, Leon Gommans, Cees de Laat</i>	
Implicit Authorization for Accessing Location Data in a Social Context	249
<i>Georg Treu, Florian Fuchs, Christiane Dargatz</i>	

SESSION 7: SECURITY ALGORITHM AND FRAMEWORK

Fingerprint Matching Algorithm Based on Tree Comparison Using Ratios of Relational Distances	257
<i>Abinandhan Chandrasekaran, Bhavani Thuraisingham</i>	
A Reconfigurable Implementation of the New Secure Hash Algorithm	265
<i>M. Zeghida, B. Bouallegue, A. Baganne, M. Machhout, R. Tourki</i>	
Applications for Provably Secure Intent Protection with Bounded Input-Size Programs	270
<i>J. Todd McDonald, Alec Yasinsac</i>	
A Framework for the Development of Secure Data Warehouse Based on MDA and QVT	278
<i>Emilio Soler, Juan Trujillo, Eduardo Fernández-Medina, Mario Piattini</i>	

SESSION 8: SOFTWARE SECURITY

Design of a Process for Software Security	283
<i>David Byers, Nahid Shahmehri</i>	
STEF: A Secure Ticket-based En-Route Filtering Scheme for Wireless Sensor Networks	292
<i>Christoph Krauß, Markus Schneider, Kpatcha Bayarou, Claudia Eckert</i>	
A Secure Architecture for the Pseudonymization of Medical Data	300
<i>Bernhard Riedl, Thomas Neubauer, Gernot Goluch, Oswald Boehm, Gert Reinauer, Alexander Krumboeck</i>	
Collection of Quantitative Data on Security Incidents	307
<i>Thomas Nowey, Hannes Federrath</i>	

SESSION 9: SECURITY MODELS

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

SESSION 10: MISCELLANEOUS SECURITY TECHNIQUES

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

SESSION 11: e-AUCTION AND e-VOTING PROTOCOL

An Efficient eAuction Protocol	392
<i>Brian Curtis, Josef Pieprzyk, Jan Seruga</i>	
Enhancing the Security of Local Danger Warnings in VANETs — A Simulative Analysis of Voting Schemes	397
<i>Benedikt Ostermaier, Florian Dötzer, Markus Strassberger</i>	
A Practical Verifiable e-Voting Protocol for Large Scale Elections over a Network.....	407
<i>Orhan Cetinkaya, Ali Doganaksoy</i>	

SESSION 12: DEPENDABILITY IN DISTRIBUTED AND UBIQUITOUS COMPUTING

Decoupling Constraint Validation from Business Activities to Improve Dependability in Distributed Object Systems	415
<i>Lorenz Frohofer, Johannes Osrael, Karl M. Goeschka</i>	
Dependability Aspects of Ubiquitous Computing	423
<i>Lu Yan, Kaisa Sere</i>	
Concurrency Control Using Subject- and Purpose-Oriented (SPO) Scheduler	426
<i>Tomoya Enokido, Makoto Takizawa</i>	

SESSION 13: ANOMALY AND INTRUSION DETECTION

Comparing Classifier Combining Techniques for Mobile-Masquerader Detection	434
<i>Oleksiy Mazhelis, Seppo Puuronen</i>	
Process Profiling Using Frequencies of System Calls	442
<i>Surekha Mariam Varghese, K. Poullose Jacob</i>	
Terrorist Networks Analysis through Argument Driven Hypotheses Model	449
<i>D.M. Akbar Hussain</i>	

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

SESSION 1: FAULT-TOLERANT AND AVAILABILITY

High Availability for Network Management Applications	457
<i>Prabhu S., Venkat R.</i>	
RWAR: A Resilient Window-consistent Asynchronous Replication Protocol	463
<i>Yanlong Wang, Zhanhuai Li, Wei Lin</i>	
Fault-Tolerant Semi-Passive Coordination Protocol for a Multi-Actuator/Multi-Sensor Model	470
<i>Keiji Ozaki, Naohiro Hayashibara, Tomoya Enokido, Makoto Takizawa</i>	

SESSION 2: ACCESS CONTROL

Realizing Fine-Granular Read and Write Rights on Tree Structured Documents	478
<i>Franz Kollmann</i>	
Access Control Model for Web Services with Attribute Disclosure Restriction	485
<i>Vipin Singh Mewar, Subhendu Aich, Shamik Sural</i>	
Aggregating and Deploying Network Access Control Policies	493
<i>Joaquín G. Alfaro, Frédéric Cuppens, Nora Cuppens-Boulahia</i>	

SESSION 3: AUTHENTICATION

Secure Spatial Authentication Using Cell Phones	501
<i>Arjan Durresi, Vamsi Paruchuri, Mimoza Durresi, Leonard Barolli</i>	
Broadcast Authentication Protocol with Time Synchronization and Quadratic Residues Chain	508
<i>Bogdan Groza</i>	
A Secure Key Exchange and Mutual Authentication Protocol for Wireless Mobile Communications	516
<i>Yijun He, Nan Xu, Jie Li</i>	
Improved Client-to-Client Password-Authenticated Key Exchange Protocol	522
<i>Gang Yao, Dengguo Feng, Xiaoxi Han</i>	

SESSION 4: REAL-TIME SYSTEM AND SENSOR NETWORK

Adaptation Mechanisms for Survivable Sensor Networks against Denial of Service Attacks	530
<i>Dong Seong Kim, Chung Su Yang, Jong Sou Park</i>	
Models for Automatic Generation of Safety-Critical Real-Time Systems	535
<i>Christian Buckl, Matthias Regensburger, Alois Knoll, Gerhard Schrott</i>	
A Near-Real-Time Behaviour Control Framework	543
<i>Bastian Preindl, Alexander Schatten</i>	

SESSION 5: RFID TECHNIQUES AND APPLICATIONS

RFID Security Issues in Military Supply Chains	551
<i>Qinghan Xiao, Cam Boulet, Thomas Gibbons</i>	
The Cost of Preserving Privacy: Performance Measurements of RFID Pseudonym Protocols	558
<i>Jens Mache, Chris Allick</i>	
Mobile Phone Based RFID Architecture for Secure Electronic Payments Using RFID Credit Cards	562
<i>Geethapriya Venkataramani, Srividya Gopalan</i>	

SESSION 6: SECURE SOLUTION AND APPLICATIONS

A Modular Architecture for Secure and Reliable Distributed Communication	570
<i>C.M. Jayalath, R.U. Fernando</i>	
Security Oriented e-Infrastructures Supporting Neurological Research and Clinical Trials	578
<i>Anthony Stell, Richard Sinnott, Oluwafemi Ajayi, Jipu Jiang</i>	

VOLUME 2

Securing Medical Sensor Environments: The CodeBlue Framework Case	586
<i>Georgios Kambourakis, Eleni Kladoudatou, Stefanos Gritzalis</i>	

A Set of QVT Relations to Transform PIM to PSM in the Design of Secure Data Warehouses	593
<i>Emilio Soler, Juan Trujillo, Eduardo Fernández-Medina, Mario Piattini</i>	

SESSION 7: SECURITY ISSUE IN BUSINESS MANAGEMENT

Agent Alliances: A Means for Practical Threshold Signature	601
<i>Regine Endsuleit, Christoph Amma</i>	
Protecting Online Transactions with Unique Embedded Key Generators.....	609
<i>Martin Boesgaard, Erik Zenner</i>	
A Research Agenda for Autonomous Business Process Management.....	616
<i>Thomas Neubauer, Gernot Goluch, Bernhard Riedl</i>	

SESSION 8: WEB, XML, CONTENT MANAGEMENT

Secure Web Application Development and Global Regulation.....	624
<i>William Bradley Glisson, L. Milton Glisson, Ray Welland</i>	
Query Assurance Verification for Dynamic Outsourced XML Databases.....	632
<i>Viet Hung Nguyen, Tran Khanh Dang, Nguyen Thanh Son, Josef Küng</i>	
A Reflection-based Framework for Content Validation	640
<i>Lars-Helge Netland, Yngve Espelid, Khalid A. Mughal</i>	

SESSION 9: SECURITY POLICIES AND TECHNIQUES

Web Engineering Security: Essential Elements	648
<i>William Glisson, Ray Welland</i>	
Designing a Security Policy According to BS 7799 Using the OCTAVE Methodology	656
<i>Paulina Januszkiewicz, Marek Pyka</i>	
CSP-based Firewall Rule Set Diagnosis Using Security Policies	664
<i>S. Pozo, R. Ceballos, R.M. Gasca</i>	
CASSIS — Computer-based Academy for Security and Safety in Information Systems	671
<i>Gernot Goluch, Andreas Ekelhart, Stefan Fenz, Stefan Jakoubi, Bernhard Riedl, Simon Tjoa</i>	

SESSION 10: TRUST MANAGEMENT AND TRUST MODEL

Trust in Global Computing Systems as a Limit Property Emerging from Short Range Random Interactions	680
<i>V. Liagkou, E. Makri, P. Spirakis, Y.C. Stamatiou</i>	
A Trust Overlay Architecture and Protocol for Enhanced Protection against Spam	688
<i>Jimmy McGibney, Dmitri Botvich</i>	
HICI: An Approach for Identifying Trust Elements — The Case of Technological Trust Perspective in VBEs	696
<i>Simon Samwel Msanjila, Hamideh Afsarmanesh</i>	

A Semantic and Time Related Recommendation-Feedback Trust Model	704
<i>Lin Zhang, Feng Xu, Yuan Wang, Jian Lv</i>	

SESSION 11: MISCELLANEOUS APPLICATIONS

AsmLSec: An Extension of Abstract State Machine Language for Attack Scenario Specification	711
<i>Mohammad Raihan, Mohammad Zulkernine</i>	
Error Modeling in RF-based Location Detection (EMLD) for Pervasive Computing Environments	719
<i>Niraj Swami, Sheikh I. Ahamed</i>	
A Performance Model to Cooperative Itinerant Agents (CIA): A Security Scheme to IDS	727
<i>Rafael Pérez, Cristina Satizábal, Jordi Forné</i>	
On the Assessment of the Interaction Quality of Users with Cerebral Palsy	735
<i>C. Mauria, T. Granollers, A. Solanas</i>	
Research and Design of Mobile Impeachment System with Semi-cryptonym	742
<i>Chaobo Yang, Ming Qi</i>	
Efficient Malicious Agreement in a Virtual Subnet Network	748
<i>Shu-Ching Wang, Shyi-Ching Liang, Kuo-Qin Yan, Guang-Yan Zheng</i>	
Extended RBAC-Based Design and Implementation for a Secure Data Warehouse	755
<i>Bhavani Thuraisingham, Srinivasan Iyer</i>	
Application of QVT for the Development of Secure Data Warehouses: A Case Study	763
<i>Emilio Soler, Juan Trujillo, Eduardo Fernández-Medina, Mario Piattini</i>	
Protecting Private Information by Data Separation in Distributed Spatial Data Warehouse	771
<i>Marcin Gorawski, Jakub Bularz</i>	
Applying a Flexible Mining Architecture to Intrusion Detection	779
<i>Marcello Castellano, Giuliano Bellone de Grecis, Giuseppe Mastronardi, Angela Aprile, Flaviano Fiorino</i>	
An Application of Learning Problem in Anomaly-based Intrusion Detection Systems	787
<i>Veselina G. Jecheva, Evgeniya P. Nikolova</i>	
Detecting Critical Regions in Covert Networks: A Case Study of 9/11 Terrorists Network	795
<i>Nasrullah Memon, Kim C. Kristoffersen, David L. Hicks, Henrik Legind Larsen</i>	
Access Control and Integration of Health Care Systems: An Experience Report and Future Challenges	805
<i>Lillian Røstad, Øystein Nytrø, Inger Anne Tøndel, Per Håkon Meland</i>	
A Collaborative Inter Data Grids Strong Semantic Model with Hybrid Namespace	812
<i>Dalia El-Mansy, Ahmed Sameh</i>	
Reliability Markov Chains for Security Data Transmitter Analysis	820
<i>Calin Ciufudean, Bianca Satco, Constantin Filote</i>	
Requirements and Evaluation Procedures for eVoting	827
<i>Melanie Volkamer, Margaret McGaley</i>	

Towards Secure E-Elections in Turkey: Requirements and Principles	835
<i>Orhan Cetinkaya, Deniz Cetinkaya</i>	
On Coercion-Resistant Electronic Elections with Linear Work	840
<i>Stefan G. Weber, Roberto Araújo, Johannes Buchmann</i>	
A Security Model and Architecture for Multichannel E-Government Systems	849
<i>MariaGrazia Fugini</i>	
eTVRA, a Threat, Vulnerability and Risk Assessment Method and Tool for eEurope.....	857
<i>Judith E.Y. Rossebø, Scott Cadzow, Paul Sijben</i>	
Framework for Information Sharing Across Multiple Government Agencies under Dynamic Access Policies	866
<i>K. Bhoopalam, K. Maly, R. Mukkamala, M. Zubair</i>	
Secure Distributed Dossier Management in the Legal Domain	873
<i>Martijn Warnier, Frances Brazier, Martin Apistola, Anja Oskamp</i>	
Building a Dependable Messaging Infrastructure for Electronic Government	880
<i>Elsa Estevez, Tomasz Janowski</i>	

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

A Universal Construction for Concurrent Objects	888
<i>Rachid Guerraoui, Michel Raynal</i>	
FCPre: Extending the Arora-Kulkarni Method of Automatic Addition of Fault-Tolerance	896
<i>Bastian Braun</i>	
On the Implementation of the Omega Failure Detector in the Crash-Recovery Failure Model	904
<i>Cristian Martín, Mikel Larrea, Ernesto Jiménez</i>	
Self-Diagnosing Wireless Mesh and Ad-Hoc Networks Using an Adaptable Comparison-Based Approach	912
<i>Mourad Elhadef, Azzedine Boukerche, Hisham Elkadiki</i>	
Self-Stabilization as a Foundation for Autonomic Computing.....	920
<i>Olga Brukman, Shlomi Dolev, Yinnon Haviv, Reuven Yagel</i>	
On Programming Models for Service-Level High Availability	928
<i>C. Engelmann, S.L. Scott, C. Leangsuksun, X. He</i>	

FIRST INTERNATIONAL WORKSHOP ON SECURE SOFTWARE ENGINEERING (SECSE 2007)

Using Privacy Process Patterns for Incorporating Privacy Requirements into the System Design Process	936
<i>Christos Kalloniatis, Evangelia Kavakli, Stefanos Gritzalis</i>	
How Can the Developer Benefit from Security Modeling?	944
<i>Shanai Ardi, David Byers, Per Håkon Meland, Inger Anne Tøndel, Nahid Shahmehri</i>	
AProSec: An Aspect for Programming Secure Web Applications	953
<i>Gabriel Hermosillo, Roberto Gomez, Lionel Seinturier, Laurence Duchien</i>	

Empirical and Statistical Analysis of Risk Analysis-Driven Techniques for Threat Management	961
<i>Koen Buyens, Bart De Win, Wouter Joosen</i>	
Secure Software Development through Coding Conventions and Frameworks	969
<i>Takao Okubo, Hidehiko Tanaka</i>	
Pastures: Towards Usable Security Policy Engineering	979
<i>Sergey Bratus, Alex Ferguson, Doug McIlroy, Sean Smith</i>	
Security Objectives within a Security Testing Case Study	987
<i>Kaarina Karppinen, Reijo Savola, Mikko Rapeli, Esa Tikkala</i>	
CppTest: A Prototype Tool for Testing C/C++ Programs	993
<i>Chengying Mao, Yansheng Lu</i>	
A Novel Approach to Building Secure Systems	1001
<i>Dragan Vidakovic, Dejan Simic</i>	

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

Exception Handling in an Event-Driven System	1009
<i>Jan Ploski, Wilhelm Hasselbring</i>	
Issues in Testing Dependable Event-based Systems at a Systems Integration Company	1017
<i>Armin Beer, Matthias Heindl</i>	
Optimizing Events Traffic in Event-based Systems by Means of Evolutionary Algorithms	1025
<i>Jiri Kubalik, Richard Mordinyi</i>	
Event-based Monitoring of Open Source Software Projects.....	1032
<i>Dindin Wahyudin, A. Min Tjoa</i>	
Using Space-based Computing for More Efficient Group Coordination and Monitoring in an Event-based Work Management System.....	1040
<i>Marcus Mor, Richard Mordinyi, Johannes Riemer</i>	
Indexing and Search of Correlated Business Events	1048
<i>Roland Vecera, Szabolcs Rozsnyai, Heinz Roth</i>	

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

An Approach for Adaptive Intrusion Prevention Based on The Danger Theory	1056
<i>Alexander Krizhanovsky, Alexander Marasanov</i>	
A Human-Verifiable Authentication Protocol Using Visible Laser Light.....	1064
<i>Rene Mayrhofer, Martyn Welch</i>	
Insider-secure Hybrid Signcryption Scheme without Random Oracles	1069
<i>Chik How Tan</i>	
ZeroBio — Evaluation and Development of Asymmetric Fingerprint Authentication System Using Oblivious Neural Network Evaluation Protocol	1076
<i>Kei Nagai, Hiroaki Kikuchi, Wakaha Ogata, Masakatsu Nishigaki</i>	

A Policy Language for the Extended Reference Monitor in Trusted Operating Systems	1081
<i>Hyung Chan Kim, R.S. Ramakrishna, Wook Shin, Koiuchi Sakurai</i>	
Analysis on Bleichenbacher's Forgery Attack	1088
<i>Tetsuya Izu, Masahiko Takenaka, Takeshi Shimoyama</i>	
A New Method for Reducing the Revocation Delay in the Attribute Authentication	1096
<i>Yoshio Kakizaki, Hidekazu Tsuji</i>	
Efficient Multiparty Computation for Comparator Networks	1104
<i>Koji Chida, Hiroaki Kikuchi, Gembu Morohashi, Keiichi Hirota</i>	
Pseudo-Voter Identity (PVID) Scheme for e-Voting Protocols	1111
<i>Orhan Cetinkaya, Ali Doganaksoy</i>	
Attacks are Protocols Too	1118
<i>Anders Moen Hagalisletto</i>	
Evaluation Function for Synthesizing Security Protocols by Means of Genetic Algorithms	1128
<i>Luis Zarza, Josep Peguerols, Miguel Soriano</i>	
On the Use of One-Way Chain Based Authentication Protocols in Secure Control Systems	1135
<i>Bogdan Groza, Toma-Leonida Dragomir</i>	
Bypassing Data Execution Prevention on Microsoft Windows XP SP2	1143
<i>Nenad Stojanovski, Marjan Gušev, Danilo Gligoroski, Svein J. Knapskog</i>	
A Security Framework for RFID Multi-Domain System	1148
<i>Dong Seong Kim, Taek-Hyun Shin, Jong Sou Park</i>	

WORKSHOP ON "SECURITY IN E-LEARNING" (SEL)

E-Learning 2.0 = e-Learning 1.0 + Web 2.0?	1154
<i>Martin Ebner</i>	
Blended Learning Technology in Information Security Management Courses	1159
<i>Gerald Quirchmayr</i>	
Defining a Trusted Service-oriented Network Environment	1164
<i>Emmanuel A. Adigun, J.H.P. Eloff</i>	
Designing a Cryptographic Scheme for e-Surveys in Higher-Education Institutions	1170
<i>Alan Ward, Jordi Castellà-Roca, Aleix Dorca Josa</i>	

Author Index