Ed Dawson Duncan S. Wong (Eds.)

# Information Security Practice and Experience

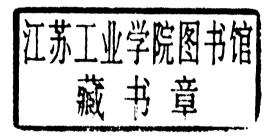
Third International Conference, ISPEC 2007 Hong Kong, China, May 2007 Proceedings



# Information Security Practice and Experience

Third International Conference, ISPEC 2007 Hong Kong, China, May 7-9, 2007

**Proceedings** 





### Volume Editors

Ed Dawson Queensland University of Technology Information Security Institute GPO Box 2434, Brisbane Qld 4001, Australia E-mail: e.dawson@qut.edu.au

Duncan S. Wong
City University of Hong Kong
Department of Computer Science
83 Tat Chee Ave, Hong Kong, China
E-mail: duncan@cityu.edu.hk

Library of Congress Control Number: 2007924822

CR Subject Classification (1998): E.3, C.2.0, D.4.6, H.2.0, K.4.4, K.6.5

LNCS Sublibrary: SL 4 - Security and Cryptology

ISSN 0302-9743

ISBN-10 3-540-72159-2 Springer Berlin Heidelberg New York ISBN-13 978-3-540-72159-8 Springer Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

Springer is a part of Springer Science+Business Media

springer.com

© Springer-Verlag Berlin Heidelberg 2007 Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India Printed on acid-free paper SPIN: 12055104 06/3180 5 4 3 2 1 0

### 4464

### Lecture Notes in Computer Science

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

### **Editorial Board**

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

University of Dortmund, Germany

Madhu Sudan

Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Moshe Y. Vardi

Rice University, Houston, TX, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

### Lecture Notes in Computer Science

For information about Vols. 1-4355

please contact your bookseller or Springer

- Vol. 4464: E. Dawson, D.S. Wong (Eds.), Information Security Practice and Experience. XIII, 361 pages. 2007.
- Vol. 4453: T. Speed, H. Huang (Eds.), Research in Computational Molecular Biology. XVI, 550 pages. 2007. (Sublibrary LNBI).
- Vol. 4450: T. Okamoto, X. Wang (Eds.), Public Key Cryptography – PKC 2007. XIII, 491 pages. 2007.
- Vol. 4448: M. Giacobini (Ed.), Applications of Evolutionary Computing. XXIII, 755 pages. 2007.
- Vol. 4447: E. Marchiori, J.H. Moore, J.C. Rajapakse (Eds.), Evolutionary Computation, Machine Learning and Data Mining in Bioinformatics. XI, 302 pages. 2007.
- Vol. 4446: C. Cotta, J. van Hemert (Eds.), Evolutionary Computation in Combinatorial Optimization. XII, 241 pages. 2007.
- Vol. 4445: M. Ebner, M. O'Neill, A. Ekárt, L. Vanneschi, A.I. Esparcia-Alcázar (Eds.), Genetic Programming. XI, 382 pages. 2007.
- Vol. 4444: T. Reps, M. Sagiv, J. Bauer (Eds.), Program Analysis and Compilation, Theory and Practice. X, 361 pages. 2007.
- Vol. 4443: R. Kotagiri, P.R. Krishna, M. Mohania, E. Nantajeewarawat (Eds.), Advances in Databases: Concepts, Systems and Applications. XXI, 1126 pages. 2007.
- Vol. 4440: B. Liblit, Cooperative Bug Isolation. XV, 101 pages. 2007.
- Vol. 4439: W. Abramowicz (Ed.), Business Information Systems. XV, 654 pages. 2007.
- Vol. 4438: L. Maicher, A. Sigel, L.M. Garshol (Eds.), Leveraging the Semantics of Topic Maps. X, 257 pages. 2007. (Sublibrary LNAI).
- Vol. 4433: E. Şahin, W.M. Spears, A.F.T. Winfield (Eds.), Swarm Robotics. XII, 221 pages. 2007.
- Vol. 4432: B. Beliczynski, A. Dzielinski, M. Iwanowski, B. Ribeiro (Eds.), Adaptive and Natural Computing Algorithms, Part II. XXVI, 761 pages. 2007.
- Vol. 4431: B. Beliczynski, A. Dzielinski, M. Iwanowski, B. Ribeiro (Eds.), Adaptive and Natural Computing Algorithms, Part I. XXV, 851 pages. 2007.
- Vol. 4430: C.C. Yang, D. Zeng, M. Chau, K. Chang, Q. Yang, X. Cheng, J. Wang, F.-Y. Wang, H. Chen (Eds.), Intelligence and Security Informatics. XII, 330 pages. 2007
- Vol. 4429: R. Lu, J.H. Siekmann, C. Ullrich (Eds.), Cognitive Systems. X, 161 pages. 2007. (Sublibrary LNAI).
- Vol. 4427: S. Uhlig, K. Papagiannaki, O. Bonaventure (Eds.), Passive and Active Network Measurement. XI, 274 pages. 2007.

- Vol. 4426: Z.-H. Zhou, H. Li, Q. Yang (Eds.), Advances in Knowledge Discovery and Data Mining. XXV, 1161 pages. 2007. (Sublibrary LNAI).
- Vol. 4425: G. Amati, C. Carpineto, G. Romano (Eds.), Advances in Information Retrieval. XIX, 759 pages. 2007.
- Vol. 4424: O. Grumberg, M. Huth (Eds.), Tools and Algorithms for the Construction and Analysis of Systems. XX, 738 pages. 2007.
- Vol. 4423: H. Seidl (Ed.), Foundations of Software Science and Computational Structures. XVI, 379 pages. 2007.
- Vol. 4422: M.B. Dwyer, A. Lopes (Eds.), Fundamental Approaches to Software Engineering. XV, 440 pages. 2007.
- Vol. 4421: R. De Nicola (Ed.), Programming Languages and Systems. XVII, 538 pages. 2007.
- Vol. 4420: S. Krishnamurthi, M. Odersky (Eds.), Compiler Construction. XIV, 233 pages. 2007.
- Vol. 4419: P.C. Diniz, E. Marques, K. Bertels, M.M. Fernandes, J.M.P. Cardoso (Eds.), Reconfigurable Computing: Architectures, Tools and Applications. XIV, 391 pages. 2007.
- Vol. 4418: A. Gagalowicz, W. Philips (Eds.), Computer Vision/Computer Graphics Collaboration Techniques. XV, 620 pages. 2007.
- Vol. 4416: A. Bemporad, A. Bicchi, G. Buttazzo (Eds.), Hybrid Systems: Computation and Control. XVII, 797 pages. 2007.
- Vol. 4415: P. Lukowicz, L. Thiele, G. Tröster (Eds.), Architecture of Computing Systems ARCS 2007. X, 297 pages. 2007.
- Vol. 4414: S. Hochreiter, R. Wagner (Eds.), Bioinformatics Research and Development. XVI, 482 pages. 2007. (Sublibrary LNBI).
- Vol. 4412: F. Stajano, H.J. Kim, J.-S. Chae, S.-D. Kim (Eds.), Ubiquitous Convergence Technology. XI, 302 pages. 2007.
- Vol. 4411: R.H. Bordini, M. Dastani, J. Dix, A.E.F. Seghrouchni (Eds.), Programming Multi-Agent Systems. XIV, 249 pages. 2007. (Sublibrary LNAI).
- Vol. 4410: A. Branco (Ed.), Anaphora: Analysis, Algorithms and Applications. X, 191 pages. 2007. (Sublibrary LNAI).
- Vol. 4409: J.L. Fiadeiro, P.-Y. Schobbens (Eds.), Recent Trends in Algebraic Development Techniques. VII, 171 pages. 2007.
- Vol. 4407: G. Puebla (Ed.), Logic-Based Program Synthesis and Transformation. VIII, 237 pages. 2007.

- Vol. 4406: W. De Meuter (Ed.), Advances in Smalltalk. VII, 157 pages. 2007.
- Vol. 4405: L. Padgham, F. Zambonelli (Eds.), Agent-Oriented Software Engineering VII. XII, 225 pages. 2007.
- Vol. 4403: S. Obayashi, K. Deb, C. Poloni, T. Hiroyasu, T. Murata (Eds.), Evolutionary Multi-Criterion Optimization. XIX, 954 pages. 2007.
- Vol. 4401: N. Guelfi, D. Buchs (Eds.), Rapid Integration of Software Engineering Techniques. IX, 177 pages. 2007.
- Vol. 4400: J.F. Peters, A. Skowron, V.W. Marek, E. Orłowska, R. Słowiński, W. Ziarko (Eds.), Transactions on Rough Sets VII, Part II. X, 381 pages. 2007.
- Vol. 4399: T. Kovacs, X. Llorà, K. Takadama, P.L. Lanzi, W. Stolzmann, S.W. Wilson (Eds.), Learning Classifier Systems. XII, 345 pages. 2007. (Sublibrary LNAI).
- Vol. 4398: S. Marchand-Maillet, E. Bruno, A. Nürnberger, M. Detyniecki (Eds.), Adaptive Multimedia Retrieval: User, Context, and Feedback. XI, 269 pages. 2007.
- Vol. 4397: C. Stephanidis, M. Pieper (Eds.), Universal Access in Ambient Intelligence Environments. XV, 467 pages. 2007.
- Vol. 4396: J. García-Vidal, L. Cerdà-Alabern (Eds.), Wireless Systems and Mobility in Next Generation Internet. IX, 271 pages. 2007.
- Vol. 4395: M. Daydé, J.M.L.M. Palma, Á.L.G.A. Coutinho, E. Pacitti, J.C. Lopes (Eds.), High Performance Computing for Computational Science VEC-PAR 2006. XXIV, 721 pages. 2007.
- Vol. 4394: A. Gelbukh (Ed.), Computational Linguistics and Intelligent Text Processing. XVI, 648 pages. 2007.
- Vol. 4393: W. Thomas, P. Weil (Eds.), STACS 2007. XVIII, 708 pages. 2007.
- Vol. 4392: S.P. Vadhan (Ed.), Theory of Cryptography. XI, 595 pages. 2007.
- Vol. 4391: Y. Stylianou, M. Faundez-Zanuy, A. Esposito (Eds.), Progress in Nonlinear Speech Processing. XII, 269 pages. 2007.
- Vol. 4390: S.O. Kuznetsov, S. Schmidt (Eds.), Formal Concept Analysis. X, 329 pages. 2007. (Sublibrary LNAI).
- Vol. 4389: D. Weyns, H.V.D. Parunak, F. Michel (Eds.), Environments for Multi-Agent Systems III. X, 273 pages. 2007. (Sublibrary LNAI).
- Vol. 4385: K. Coninx, K. Luyten, K.A. Schneider (Eds.), Task Models and Diagrams for Users Interface Design. XI, 355 pages. 2007.
- Vol. 4384: T. Washio, K. Satoh, H. Takeda, A. Inokuchi (Eds.), New Frontiers in Artificial Intelligence. IX, 401 pages. 2007. (Sublibrary LNAI).
- Vol. 4383: E. Bin, A. Ziv, S. Ur (Eds.), Hardware and Software, Verification and Testing. XII, 235 pages. 2007.
- Vol. 4381: J. Akiyama, W.Y.C. Chen, M. Kano, X. Li, Q. Yu (Eds.), Discrete Geometry, Combinatorics and Graph Theory. XI, 289 pages. 2007.

- Vol. 4380: S. Spaccapietra, P. Atzeni, F. Fages, M.-S. Hacid, M. Kifer, J. Mylopoulos, B. Pernici, P. Shvaiko, J. Trujillo, I. Zaihrayeu (Eds.), Journal on Data Semantics VIII. XV, 219 pages. 2007.
- Vol. 4379: M. Südholt, C. Consel (Eds.), Object-Oriented Technology. VIII, 157 pages. 2007.
- Vol. 4378: I. Virbitskaite, A. Voronkov (Eds.), Perspectives of Systems Informatics. XIV, 496 pages. 2007.
- Vol. 4377: M. Abe (Ed.), Topics in Cryptology CT-RSA 2007. XI, 403 pages. 2006.
- Vol. 4376: E. Frachtenberg, U. Schwiegelshohn (Eds.), Job Scheduling Strategies for Parallel Processing. VII, 257 pages. 2007.
- Vol. 4374: J.F. Peters, A. Skowron, I. Düntsch, J. Grzymała-Busse, E. Orłowska, L. Polkowski (Eds.), Transactions on Rough Sets VI, Part I. XII, 499 pages. 2007.
- Vol. 4373: K. Langendoen, T. Voigt (Eds.), Wireless Sensor Networks. XIII, 358 pages. 2007.
- Vol. 4372: M. Kaufmann, D. Wagner (Eds.), Graph Drawing. XIV, 454 pages. 2007.
- Vol. 4371: K. Inoue, K. Satoh, F. Toni (Eds.), Computational Logic in Multi-Agent Systems. X, 315 pages. 2007. (Sublibrary LNAI).
- Vol. 4370: P.P Lévy, B. Le Grand, F. Poulet, M. Soto, L. Darago, L. Toubiana, J.-F. Vibert (Eds.), Pixelization Paradigm. XV, 279 pages. 2007.
- Vol. 4369: M. Umeda, A. Wolf, O. Bartenstein, U. Geske, D. Seipel, O. Takata (Eds.), Declarative Programming for Knowledge Management. X, 229 pages. 2006. (Sublibrary LNAI).
- Vol. 4368: T. Erlebach, C. Kaklamanis (Eds.), Approximation and Online Algorithms. X, 345 pages. 2007.
- Vol. 4367: K. De Bosschere, D. Kaeli, P. Stenström, D. Whalley, T. Ungerer (Eds.), High Performance Embedded Architectures and Compilers. XI, 307 pages. 2007.
- Vol. 4366: K. Tuyls, R. Westra, Y. Saeys, A. Nowé (Eds.), Knowledge Discovery and Emergent Complexity in Bioinformatics. IX, 183 pages. 2007. (Sublibrary LNBI).
- Vol. 4364: T. Kühne (Ed.), Models in Software Engineering. XI, 332 pages. 2007.
- Vol. 4362: J. van Leeuwen, G.F. Italiano, W. van der Hoek, C. Meinel, H. Sack, F. Plášil (Eds.), SOFSEM 2007: Theory and Practice of Computer Science. XXI, 937 pages. 2007.
- Vol. 4361: H.J. Hoogeboom, G. Păun, G. Rozenberg, A. Salomaa (Eds.), Membrane Computing. IX, 555 pages. 2006.
- Vol. 4360: W. Dubitzky, A. Schuster, P.M.A. Sloot, M. Schroeder, M. Romberg (Eds.), Distributed, High-Performance and Grid Computing in Computational Biology. X, 192 pages. 2007. (Sublibrary LNBI).
- Vol. 4358: R. Vidal, A. Heyden, Y. Ma (Eds.), Dynamical Vision. IX, 329 pages. 2007.
- Vol. 4357: L. Buttyán, V. Gligor, D. Westhoff (Eds.), Security and Privacy in Ad-Hoc and Sensor Networks. X, 193 pages. 2006.

### Preface

The third international conference on Information Security Practice and Experience (ISPEC 2007) was held in Hong Kong, China, May 7 – 9, 2007. The conference was organized and sponsored by City University of Hong Kong.

As applications of information security technologies become pervasive, issues pertaining to their deployment and operation are becoming increasingly important. ISPEC is an annual conference that brings together researchers and practitioners to provide a confluence of new information security technologies, their applications and their integration with IT systems in various vertical sectors. In 2005 and 2006, the first and second conferences were held successfully in Singapore and Hangzhou, China, respectively. The conference proceedings were published by Springer in the *Lecture Notes in Computer Science* series.

The Program Committee received 135 submissions, and accepted 24 papers for presentation. The final versions of the accepted papers, which the authors finalized on the basis of comments from the reviewers, are included in the proceedings. The entire reviewing process took nine weeks, each paper was carefully evaluated by at least three members from the Program Committee. The individual reviewing phase was followed by a Web-based discussion. Papers over which the reviewers significantly disagreed were further reviewed by external experts. Based on the comments and scores given by reviewers, the final decisions on acceptance were made. We appreciate the hard work of the members of the Program Committee and external referees, who gave many hours of their valuable time.

In addition to the contributed papers, there were four invited talks: Bill Caelli spoke on "Application Security—Myth or Reality?", Robert H. Deng on "Towards Efficient and Novel Security Solutions—A Marriage of Crypto and Trusted Computing Platform," Lucas Hui on "Computer Forensics Tools and Technology: Research and Development in Hong Kong" and Victor K. Wei on "E-voting by Zero-Knowledge."

We would like to thank all the people involved in organizing this conference. In particular, we would like to thank colleagues from the Department of Computer Science, City University of Hong Kong, for their time and efforts, as well as Dennis Liu, Chung Ki Li and Qiong Huang for their excellent work on maintaining the submission/reviewing software and taking care of all the technical aspects of the review process. Finally, we would like to thank all the authors who submitted papers to the conference.

May 2007

Ed Dawson Duncan Wong

### Organization

ISPEC 2007 was organized by the Department of Computer Science, City University of Hong Kong, China.

### General Chair

Xiaotie Deng City University of Hong Kong, China C. H. Lee City University of Hong Kong, China

### **Program Committee Co-chairs**

Ed Dawson QUT, Australia

Duncan Wong City University of Hong Kong, China

### Steering Committee

Feng Bao I2R, Singapore

Robert H. Deng Singapore Management U, Singapore

### **Organizing Committee**

Xiaotie Deng City University of Hong Kong, China L. F. Kwok City University of Hong Kong, China C. H. Lee City University of Hong Kong, China Duncan Wong City University of Hong Kong, China

Giovanna Yau

### **Program Committee**

Joonsang BaekI2R, SingaporeFeng BaoI2R, SingaporeKefei ChenSJTU, China

Liqun Chen HP Bristol Labs, UK Mathieu Ciet Gemplus, France

Ed Dawson QUT, Australia (Co-chair)

Cunsheng Ding HKUST, China

Dengguo Feng Chinese Academy of Sciences, China

Dieter Gollmann TU Hamburg, Germany

### VIII Organization

Javier Herranz Lucas Hui

Min-Shiang Hwang

Tetsu Iwata

Kazukuni Kobara Kaoru Kurosawa Kwangjo Kim L. F. Kwok Xuejia Lai

Dong Hoon Lee Benoit Libert Joseph K. Liu

Stefan Lucks Richard Lui Wenbo Mao SangJae Moon

Javier Lopez

Yi Mu

David Naccache Raphael C.-W. Phan

Josef Pieprzyk

Jean-Jacques Quisquater

C. Pandu Rangan Reihaneh Safavi-Naini

Hovav Shacham Ron Steinfeld Willy Susilo Tsuyoshi Takagi Xiaojian Tian Guilin Wang Huaxiong Wang Stephen Wolthusen

Duncan Wong

Joe Yau
Sung-Ming Yen
Yiqun Lisa Yin
Siu-Ming Yiu
Fangguo Zhang
Zhenfeng Zhang
Yunlei Zhao
Yuliang Zheng
Jianying Zhou
Huafei Zhu

CWI, The Netherlands

Hong Kong University, China

National Chung Hsing University, Taiwan

Nagoya University, Japan

AIST, Japan

Ibaraki University, Japan

ICU, Korea

City University of Hong Kong, China

SJTU, China

Korea University, Korea

UCL, Belgium

University of Bristol, UK University of Malaga, Spain

University of Mannheim, Germany City University of Hong Kong, China

HP Lab, China

Kyungpook National University, Korea University of Wollongong, Australia

ENS and Paris II, France

Swinburne University of Technology,

Malaysia

Macquarie University, Australia

UCL, Belgium

Indian Institute of Technology, India University of Wollongong, Australia Weizmann Institute of Science, Israel Macquarie University, Australia University of Wollongong, Australia Future University - Hakodate, Japan City University of Hong Kong, China

I2R, Singapore

Macquarie University, Australia

University of London, UK

City University of Hong Kong, China

(Co-chair)

Hong Kong Baptist University, China National Central University, Taiwan Independent Consultant, USA Hong Kong University, China

Sun Yat-sen University, China Chinese Academy of Sciences, China

Fudan University, China UNC Charlotte, USA

I2R, Singapore

I2R, Singapore

### External Reviewers

Manfred Aigner Tanmov Kanti Das Weijun Shen Stefan Katzenbeisser Nicholas Sheppard Man Ho Au Eike Kiltz Mi Na Shim Philippe Bulens Xuefei Cao Jongsung Kim SeongHan Shin Julien Cathalo Hirotsugu Kinoshita Divyan M. Konidala Zhenchuan Chai Nigel Smart Chris Charnes Ulrich Kühn Purui Su Chien-Ning Chen Byoungcheon Lee Haibo Chen HoonJae Lee Willy Susilo Sang Gon Lee Jing Chen Lily Chen Lan Li Vo Duc Liem Xiaofeng Chen Yongxi Cheng Hsi-Chung Lin Benoit Chevallier-Mames Jenny Liu Feng Tu Yvonne Cliff Yu Long Jheng-Hong Tu Scott Contini Miao Ma Adrian McCullagh Lionel Victor Kim-Kwang Raymond Pablo Najera Jose L. Vivas Choo Andrew Clark Dang Ngyuen Duc Eric Wang Hanane Fathi Lan Nguven Shuhong Wang Benoit Feix Juan Gonzalez Nieto Evan Fleischmann Brent Waters Peng Ning David Galindo Miyako Ohkubo Baodian Wei Zheng Gong

Qiong Huang Dennis Hofheinz Xuan Hong Jeffrey Horton Chao-Chih Hsu Zoe Jiang Haimin Jin Marc Joye

Qianhong Huang

Yasuhiro Ohtaki Pascal Paillier Kun Peng Chi-Dian Wu Ying Qiu Qianhong Wu Rodrigo Roman Guomin Yang Chun Ruan Kee-Young Yoo Eun-Kyung Ryu Jin Yuan Hendra Saptura Erik Zenner Werner Schindler Rui Zhang Francesc Sebé Chang'an Zhao

Masaaki Shirase Dirk Stegemann Tsuyoshi Takagi Keisuke Tanaka Hitoshi Tanuma Emin Islam Tatli Damien Vergnaud Zhenghong Wang Mi Wen Jian Weng

### Sponsoring Institutions

City University of Hong Kong, China

### **Table of Contents**

Invited Talks

IIIVIOCA TAIMS	
Application Security – Myth Or Reality?	1
Tools and Technology for Computer Forensics: Research and Development in Hong Kong	11
Cryptanalysis	
A Linear Analysis of Blowfish and Khufu	20
Related-Key Rectangle Attack on 43-Round SHACAL-2	33
On the Ability of AES S-Boxes to Secure Against Correlation Power Analysis	43
Signatures	
A Sanitizable Signature Scheme with Aggregation	51
A Novel Verifiably Encrypted Signature Scheme Without Random Oracle	65
Certificate Based (Linkable) Ring Signature	79
An Efficient ID-Based Verifiably Encrypted Signature Scheme Based on Hess's Scheme	93
On the Sequentiality of Three Optimal Structured Multisignature Schemes	105

### **Network Security and Security Management** 116 Di Ma An Economical Model for the Risk Evaluation of DoS Vulnerabilities in Cryptography Protocols ..... 129 Zhen Cao, Zhi Guan, Zhong Chen, Jianbin Hu, and Liyong Tang Practical Uses of Virtual Machines for Protection of Sensitive User 145 Peter C.S. Kwan and Glenn Durfee Formalization of RBAC Policy with Object Class Hierarchy ..... 162 Jung Hwa Chae and Nematollaah Shiri Privacy and Applications Privacy-Preserving Credentials Upon Trusted Computing Augmented 177 Yanjiang Yang, Robert H. Deng, and Feng Bao Two-Party Privacy-Preserving Agglomerative Document Clustering . . . . 193 Chunhua Su, Jianying Zhou, Feng Bao, Tsuyoshi Takaqi, and Kouichi Sakurai Efficient Bid Validity Check in ElGamal-Based Sealed-Bid E-Auction . . . 209 Kun Peng and Ed Dawson Cryptographic Algorithms and Implementations How to Prevent DPA and Fault Attack in a Unified Way for ECC 225 Yoo-Jin Baek and Ihor Vasyltsov Secure Signed Radix-r Recoding Methods for Constrained-Embedded 238 Dong-Guk Han, Sung-Kyoung Kim, Ho Won Kim, Kyo IL Chung, and Jongin Lim Some Efficient Algorithms for the Final Exponentiation of $\eta_T$ Pairing... 254 Masaaki Shirase, Tsuyoshi Takaqi, and Eiji Okamoto Towards Minimizing Memory Requirement for Implementation of Hyperelliptic Curve Cryptosystems ..... 269 Pradeep Kumar Mishra, Pinakpani Pal, and Palash Sarkar

Authentication and Key Management	
Achieving End-to-End Authentication in Intermediary-Enabled Multimedia Delivery Systems	284
Scalable Group Key Management Protocol Based on Key Material Transmitting Tree	301
A Time-Based Key Management Protocol for Wireless Sensor  Networks	314
Cryptosystems	
Identity-Based Threshold Decryption Revisited	329
Visual Cryptography Schemes with Dihedral Group Access Structure for Many Images	344
Author Index	361

Table of Contents

XIII

### **Application Security – Myth Or Reality?**

### William J. Caelli

Information Security Institute
Queensland University of Technology,
GPO Box 2434, Brisbane. Qld. 4001. Australia
w.caelli@qut.edu.au
Senior Consultant-Information Assurance and Director
International Information Security Consultants (IISEC) Pty Ltd
21 Castle Hill Drive South, Gaven. Qld. 4211. Australia
w.caelli@iisec.com.au

Abstract. The Security services within applications have received recent attention. It has been suggested that this may be the only way to increase overall information system assurance in an era where ICT governance and compliance have taken on new force and the use of commodity level ICT products for critical information systems continues. While it has been argued that an application can be no more secure than its underlying computer subsystems, security at the application layer was always envisaged as playing a major role, e.g. in the "Open Systems Interconnection (OSI)" security model. At a time when "end-user" programming is being advocated, the needs and parameters of security education and training are rapidly changing, and increased threats from global Internet connection are rapidly rising, there is a need to reconsider security schemes at the application level. This paper examines current trends in application design, development, deployment and management and evaluates these against known system vulnerabilities and threats.

**Keywords:** OSI security, access control, mandatory access control, security education, operating system security, application security, web services security.

# 1 Introduction – Security "Ignorant" Versus Security "Aware" Applications

Even by 1992 the Organisation for Economic Cooperation and Development (OECD) had set up a set of recommendations that set out guidelines for the security of information systems [1]. These guidelines were accompanied by a call for their implementation in the following statement:

".... Governments are urged to establish legal, administrative and other measures, practices and institutions for the security of information systems."

E. Dawson and D.S. Wong (Eds.): ISPEC 2007, LNCS 4464, pp. 1–10, 2007. © Springer-Verlag Berlin Heidelberg 2007

This theme was taken up in 1995 by the then Australian Governor-General who set the scene for information security and its future in the following statement reported by "The Australian" newspaper [2]:

"... Hayden also said it was 'incumbent on us as individual Australians' to seriously consider issues such as privacy, information security and copyright, equity and access and not just leave such concerns up to governments."

By this time the British Standards Association had published its BS7799 standard, labelled as a "Code of Practice for Information Security Management" which was heralded as a document to "provide a common basis for companies to develop, implement and measure effective security management practice" and to "provide confidence in intercompany trading". Its origin had been with the United Kingdom's Department of Trade and Industry (DTI) and a group of companies and other organisations. It set out ten categories of security controls, all of which are vital in the consideration of computer application security. These categories were, and still are, based upon the parameters shown in Table 1.

Parameter	<b>OECD-Category of Security Control</b>
1	Security Policy
2	Security Organisation
3	Assets Classification and Control
4	Personnel Security
5	Physical and Environmental Security
6	Computer and Network Management
7	Systems Access Control
8	System Development and Maintenance
9	Business Contingency Planning
10	Compliance

Table 1. OECD Parameters

Considering these admonitions in the light of global information networking it is vital to assess the simple fact that users "see" applications and seldom any underlying computer or data network structure. These can be quite specific, e.g. an inventory control package for an elect-

rical products distributor, or generic by nature, e.g. web browser, office productivity suite, etc.

It is an accepted principle of computer science and engineering that a computer application can be **no more** secure than the libraries and middleware it incorporates that can themselves be **no more** secure than the operating system and sub-systems that support them which in turn can be **no more** secure than the underlying hardware and firmware of the computer or network system. While this is an obvious truth, applications themselves can be further subdivided into two broad classes, i.e. security "aware" versus security "ignorant" applications. In simple terms, a security "aware" program incorporates appropriate security mechanisms and services relative to the needs of the application and appropriate to the security environment of the information system in which it operates. By contrast, a security "ignorant" application simply depends upon other system wide security services and mechanisms to provide

necessary protection, e.g. operating system relevant access control parameters, network boundary/perimeter controls, and the like.

This broad dichotomy then further leads to a set of two differing "views" of such applications and their operation in any information system. These can be broadly categorised, as per Figure 1, as being the;

- a. "system-up" view, versus the
- b. "application down" view.

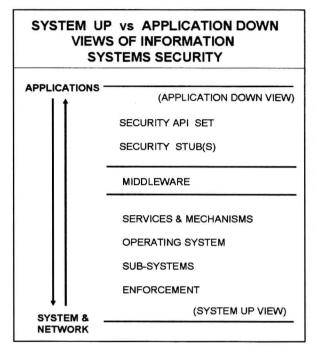


Fig. 1. Differing Views

The system up paradigm that security assumes responsibility for an information system, in general, lies outside the scope of the applications developer and belongs to the overall information system manager who controls those applica-tions according to a documented enterprise risk assessment management and policy. Indeed, it can be argued that this view if the one prevalent in such ICT processes as "business process management (BPM)" and allied schemes used for the creation of any overall information system. The alternative, but often co-existent, scheme of "application down" views of security can be clearly identified in particular application sectors, e.g. the banking and finance, healthcare, govern-

ment services and allied areas. The main question for the ICT professional is one of how to balance these differing views and to determine just "where they meet".

For example, national and international standards exist for application security parameters in the banking/finance and healthcare sectors and these vary markedly in the degree of detail involved. From definition of actual security processes to data formats and storage parameters these specific requirements must form part of any enterprise analysis activity undertaken and must be an integral part of an overall application system. These security parameters, being application specific, have the property that they do not readily lend themselves to incorporation into "lower level" services in a system, e.g. access control schemes provided by an operating system. For the immediate future, application security specifics seem likely to remain for certain industry sectors. However, there is growing interest in the concept of a "regulatory layer", similar to the Open Systems Interconnection's (OSI) "presentation

layer" (Layer 6 of the OSI model) as shown in Table 2 at the end of this paper. In this model, security enforcing aspects of an application, particularly where security requirements are defined by legal and/or regulatory bodies, are isolated from the main application "logic" and placed in this "regulatory layer". Essentially what is demanded is reliable enforcement of international, national, state/province, local and enterprise security laws, regulations, guidelines and policies. Indeed, information security or information "assurance" is now an integral part of any enterprise information systems model in the public or private sectors alike. The important point is one of matching user expectations for simplified and understood access with these security/assurance parameters at the application level as illustrated in a newspaper cartoon from the early 1980s [3], given in Figure 2.



Fig. 2. ATM Security - 1983

## 2 The Open Systems Interconnection (OSI) Model as a Framework

The OSI model, with its 7-layer structure, also defined an architecture for the protection of interconnected systems; in principle, those applications and related systems that needed to communicate. At the management level, the "OSI Management" architecture, clearly identified five major sets of principles that governed:

- naming and configuration,
- · security,
- error and fault handling,
- · performance, and
- accounting.

OSI then clearly stated its security philosophy as follows:

"At various times, security controls must be established in order to protect information exchanged between application processes. Such controls should make the cost of obtaining or modifying data greater than the potential value of so doing, or make the time required to obtain the data so great that the value of the data is lost." This led to the definition of three security management relevant parameters as follows:

 Mandatory security policies imposed by owners and administrators of communicating entities,