LNCS 4464

Ed Dawson
Duncan S. Wong (Eds.)

Information Security Practice and Experience

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

Springer

Ed Dawson Duncan S. Wong (Eds.)

Information Security Practice and Experience

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

Springer

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

Springer is a part of Springer Science+Business Media

springer.com

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

Lecture Notes in Computer Science 4464

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.

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 Baek	I2R, Singapore
Feng Bao	I2R, Singapore
Kefei Chen	SJTU, 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

Javier Herranz	CWI, The Netherlands
Lucas Hui	Hong Kong University, China
Min-Shiang Hwang	National Chung Hsing University, Taiwan
Tetsu Iwata	Nagoya University, Japan
Kazukuni Kobara	AIST, Japan
Kaoru Kurosawa	Ibaraki University, Japan
Kwangjo Kim	ICU, Korea
L. F. Kwok	City University of Hong Kong, China
Xuejia Lai	SJTU, China
Dong Hoon Lee	Korea University, Korea
Benoit Libert	UCL, Belgium
Joseph K. Liu	University of Bristol, UK
Javier Lopez	University of Malaga, Spain
Stefan Lucks	University of Mannheim, Germany
Richard Lui	City University of Hong Kong, China
Wenbo Mao	HP Lab, China
SangJae Moon	Kyungpook National University, Korea
Yi Mu	University of Wollongong, Australia
David Naccache	ENS and Paris II, France
Raphael C.-W. Phan	Swinburne University of Technology, Malaysia
Josef Pieprzyk	Macquarie University, Australia
Jean-Jacques Quisquater	UCL, Belgium
C. Pandu Rangan	Indian Institute of Technology, India
Reihaneh Safavi-Naini	University of Wollongong, Australia
Hovav Shacham	Weizmann Institute of Science, Israel
Ron Steinfeld	Macquarie University, Australia
Willy Susilo	University of Wollongong, Australia
Tsuyoshi Takagi	Future University - Hakodate, Japan
Xiaojian Tian	City University of Hong Kong, China
Guilin Wang	I2R, Singapore
Huaxiong Wang	Macquarie University, Australia
Stephen Wolthusen	University of London, UK
Duncan Wong	City University of Hong Kong, China (Co-chair)
Joe Yau	Hong Kong Baptist University, China
Sung-Ming Yen	National Central University, Taiwan
Yiqun Lisa Yin	Independent Consultant, USA
Siu-Ming Yiu	Hong Kong University, China
Fangguo Zhang	Sun Yat-sen University, China
Zhenfeng Zhang	Chinese Academy of Sciences, China
Yunlei Zhao	Fudan University, China
Yuliang Zheng	UNC Charlotte, USA
Jianying Zhou	I2R, Singapore
Huafei Zhu	I2R, Singapore

External Reviewers

Manfred Aigner
Man Ho Au
Philippe Bulens
Xuefei Cao
Julien Cathalo
Zhenchuan Chai
Chris Charnes
Chien-Ning Chen
Haibo Chen
Jing Chen
Lily Chen
Xiaofeng Chen
Yongxi Cheng
Benoit Chevallier-Mames
Yvonne Cliff
Scott Contini
Kim-Kwang Raymond Choo
Andrew Clark
Hanane Fathi
Benoit Feix
Evan Fleischmann
David Galindo
Zheng Gong
Qianhong Huang
Qiong Huang
Dennis Hofheinz
Xuan Hong
Jeffrey Horton
Chao-Chih Hsu
Zoe Jiang
Haimin Jin
Marc Joye
Tanmoy Kanti Das
Stefan Katzenbeisser
Eike Kiltz
Jongsung Kim
Hirotsugu Kinoshita
Divyan M. Konidala
Ulrich Kühn
Byoungcheon Lee
HoonJae Lee
Sang Gon Lee
Lan Li
Vo Duc Liem
Hsi-Chung Lin
Jenny Liu
Yu Long
Miao Ma
Adrian McCullagh
Pablo Najera
Dang Ngyuen Duc
Lan Nguyen
Juan Gonzalez Nieto
Peng Ning
Miyako Ohkubo
Yasuhiro Ohtaki
Pascal Paillier
Kun Peng
Ying Qiu
Rodrigo Roman
Chun Ruan
Eun-Kyung Ryu
Hendra Saptura
Werner Schindler
Francesc Sebé
Weijun Shen
Nicholas Sheppard
Mi Na Shim
SeongHan Shin
Masaaki Shirase
Nigel Smart
Dirk Stegemann
Purui Su
Willy Susilo
Tsuyoshi Takagi
Keisuke Tanaka
Hitoshi Tanuma
Emin Islam Tatli
Feng Tu
Jheng-Hong Tu
Damien Vergnaud
Lionel Victor
Jose L. Vivas
Eric Wang
Shuhong Wang
Zhenghong Wang
Brent Waters
Baodian Wei
Mi Wen
Jian Weng
Chi-Dian Wu
Qianhong Wu
Guomin Yang
Kee-Young Yoo
Jin Yuan
Erik Zenner
Rui Zhang
Chang'an Zhao

Sponsoring Institutions

City University of Hong Kong, China

Table of Contents

Invited Talks

Cryptanalysis

Signatures

Network Security and Security Management

Privacy and Applications

Cryptographic Algorithms and Implementations

Authentication and Key Management

Cryptosystems

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 sub-systems, 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.

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.

Table 1. OECD Parameters

Parameter	OECD-Category of Security Control
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

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 electrical 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.

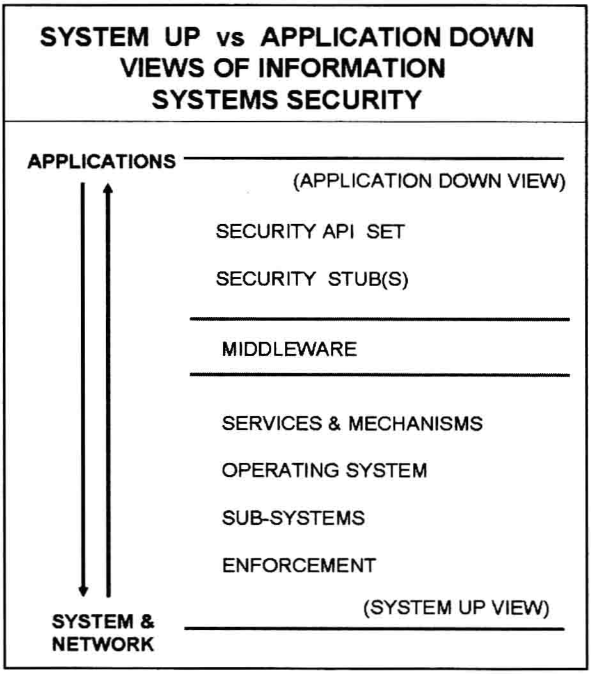

Fig. 1. Differing Views

The system up paradigm assumes that security 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 and management 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, government 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.

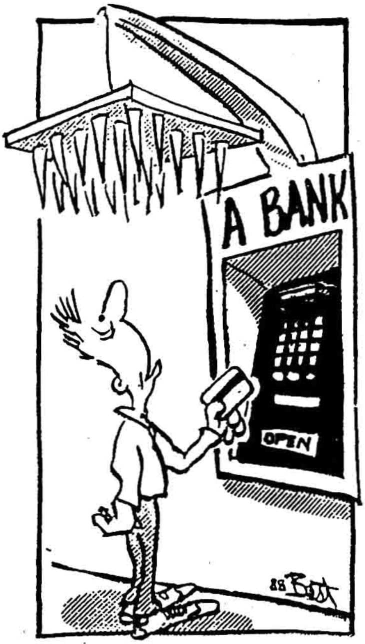

Fig. 2. ATM Security - 1983

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,