Colin Boyd
Juan M. González Nieto (Eds.)

LNCS 3574

# Information Security and Privacy

## 10th Australasian Conference, ACISP 2005
## Brisbane, Australia, July 2005
## Proceedings

Springer

TP309-53
I43
2005

Colin Boyd Juan M. González Nieto (Eds.)

# Information Security and Privacy

10th Australasian Conference, ACISP 2005
Brisbane, Australia, July 4-6, 2005
Proceedings



Springer

Volume Editors

Colin Boyd
Juan M. González Nieto
Queensland University of Technology
Information Security Institute
GPO Box 2434, Brisbane 4000, Australia
E-mail: c.boyd@qut.edu.au, juanma@isrc.qut.edu.au

Library of Congress Control Number: 2005928379

CR Subject Classification (1998): E.3, K.6.5, D.4.6, C.2, E.4, F.2.1, K.4.1

ISSN 0302-9743
ISBN-10 3-540-26547-3 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-26547-4 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

springeronline.com

© Springer-Verlag Berlin Heidelberg 2005
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Boller Mediendesign
Printed on acid-free paper SPIN: 11506157 06/3142 5 4 3 2 1 0

Lecture Notes in Computer Science 3574

*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
*New York University, NY, 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. 1–3472

please contact your bookseller or Springer

Vol. 3574: C. Boyd, J.M. González Nieto (Eds.), Information Security and Privacy. XIII, 586 pages. 2005.

Vol. 3573: S. Etalle (Ed.), Logic Based Program Synthesis and Transformation. VIII, 279 pages. 2005.

Vol. 3572: C. De Felice, A. Restivo (Eds.), Developments in Language Theory. XI, 409 pages. 2005.

Vol. 3570: A. S. Patrick, M. Yung (Eds.), Financial Cryptography and Data Security. XII, 376 pages. 2005.

Vol. 3569: F. Bacchus, T. Walsh (Eds.), Theory and Applications of Satisfiability Testing. XII, 492 pages. 2005.

Vol. 3567: M. Jackson, D. Nelson, S. Stirk (Eds.), Database: Enterprise, Skills and Innovation. XII, 185 pages. 2005.

Vol. 3565: G.E. Christensen, M. Sonka (Eds.), Information Processing in Medical Imaging. XXI, 777 pages. 2005.

Vol. 3562: J. Mira, J.R. Álvarez (Eds.), Artificial Intelligence and Knowledge Engineering Applications: A Bioinspired Approach, Part II. XXIV, 636 pages. 2005.

Vol. 3561: J. Mira, J.R. Álvarez (Eds.), Mechanisms, Symbols, and Models Underlying Cognition, Part I. XXIV, 532 pages. 2005.

Vol. 3560: V.K. Prasanna, S. Iyengar, P.G. Spirakis, M. Welsh (Eds.), Distributed Computing in Sensor Systems. XV, 423 pages. 2005.

Vol. 3559: P. Auer, R. Meir (Eds.), Learning Theory. XI, 692 pages. 2005. (Subseries LNAI).

Vol. 3557: H. Gilbert, H. Handschuh (Eds.), Fast Software Encryption. XI, 443 pages. 2005.

Vol. 3556: H. Baumeister, M. Marchesi, M. Holcombe (Eds.), Extreme Programming and Agile Processes in Software Engineering. XIV, 332 pages. 2005.

Vol. 3555: T. Vardanega, A. Wellings (Eds.), Reliable Software Technology – Ada-Europe 2005. XV, 273 pages. 2005.

Vol. 3553: T.D. Hämäläinen, A.D. Pimentel, J. Takala, S. Vassiliadis (Eds.), Embedded Computer Systems: Architectures, Modeling, and Simulation. XV, 476 pages. 2005.

Vol. 3552: H. de Meer, N. Bhatti (Eds.), Quality of Service – IWQoS 2005. XV, 400 pages. 2005.

Vol. 3551: T. Härder, W. Lehner (Eds.), Data Management in a Connected World. XIX, 371 pages. 2005.

Vol. 3548: K. Julisch, C. Kruegel (Eds.), Intrusion and Malware Detection and Vulnerability Assessment. X, 241 pages. 2005.

Vol. 3547: F. Bomarius, S. Komi-Sirviö (Eds.), Product Focused Software Process Improvement. XIII, 588 pages. 2005.

Vol. 3543: L. Kutvonen, N. Alonistioti (Eds.), Distributed Applications and Interoperable Systems. XI, 235 pages. 2005.

Vol. 3541: N.C. Oza, R. Polikar, J. Kittler, F. Roli (Eds.), Multiple Classifier Systems. XII, 430 pages. 2005.

Vol. 3540: H. Kalviainen, J. Parkkinen, A. Kaarna (Eds.), Image Analysis. XXII, 1270 pages. 2005.

Vol. 3537: A. Apostolico, M. Crochemore, K. Park (Eds.), Combinatorial Pattern Matching. XI, 444 pages. 2005.

Vol. 3536: G. Ciardo, P. Darondeau (Eds.), Applications and Theory of Petri Nets 2005. XI, 470 pages. 2005.

Vol. 3535: M. Steffen, G. Zavattaro (Eds.), Formal Methods for Open Object-Based Distributed Systems. X, 323 pages. 2005.

Vol. 3533: M. Ali, F. Esposito (Eds.), Innovations in Applied Artificial Intelligence. XX, 858 pages. 2005. (Subseries LNAI).

Vol. 3532: A. Gómez-Pérez, J. Euzenat (Eds.), The Semantic Web: Research and Applications. XV, 728 pages. 2005.

Vol. 3531: J. Ioannidis, A. Keromytis, M. Yung (Eds.), Applied Cryptography and Network Security. XI, 530 pages. 2005.

Vol. 3530: A. Prinz, R. Reed, J. Reed (Eds.), SDL 2005: Model Driven. XI, 361 pages. 2005.

Vol. 3528: P.S. Szczepaniak, J. Kacprzyk, A. Niewiadomski (Eds.), Advances in Web Intelligence. XVII, 513 pages. 2005. (Subseries LNAI).

Vol. 3527: R. Morrison, F. Oquendo (Eds.), Software Architecture. XII, 263 pages. 2005.

Vol. 3526: S.B. Cooper, B. Löwe, L. Torenvliet (Eds.), New Computational Paradigms. XVII, 574 pages. 2005.

Vol. 3525: A.E. Abdallah, C.B. Jones, J.W. Sanders (Eds.), Communicating Sequential Processes. XIV, 321 pages. 2005.

Vol. 3524: R. Barták, M. Milano (Eds.), Integration of AI and OR Techniques in Constraint Programming for Combinatorial Optimization Problems. XI, 320 pages. 2005.

Vol. 3523: J.S. Marques, N. Pérez de la Blanca, P. Pina (Eds.), Pattern Recognition and Image Analysis, Part II. XXVI, 733 pages. 2005.

Vol. 3522: J.S. Marques, N. Pérez de la Blanca, P. Pina (Eds.), Pattern Recognition and Image Analysis, Part I. XXVI, 703 pages. 2005.

Vol. 3521: N. Megiddo, Y. Xu, B. Zhu (Eds.), Algorithmic Applications in Management. XIII, 484 pages. 2005.

Vol. 3520: O. Pastor, J. Falcão e Cunha (Eds.), Advanced Information Systems Engineering. XVI, 584 pages. 2005.

此为试读,需要完整PDF请访问: www.ertongbook.com

Vol. 3519: H. Li, P. J. Olver, G. Sommer (Eds.), Computer Algebra and Geometric Algebra with Applications. IX, 449 pages. 2005.

Vol. 3518: T.B. Ho, D. Cheung, H. Liu (Eds.), Advances in Knowledge Discovery and Data Mining. XXI, 864 pages. 2005. (Subseries LNAI).

Vol. 3517: H.S. Baird, D.P. Lopresti (Eds.), Human Interactive Proofs. IX, 143 pages. 2005.

Vol. 3516: V.S. Sunderam, G.D.v. Albada, P.M.A. Sloot, J.J. Dongarra (Eds.), Computational Science – ICCS 2005, Part III. LXIII, 1143 pages. 2005.

Vol. 3515: V.S. Sunderam, G.D.v. Albada, P.M.A. Sloot, J.J. Dongarra (Eds.), Computational Science – ICCS 2005, Part II. LXIII, 1101 pages. 2005.

Vol. 3514: V.S. Sunderam, G.D.v. Albada, P.M.A. Sloot, J.J. Dongarra (Eds.), Computational Science – ICCS 2005, Part I. LXIII, 1089 pages. 2005.

Vol. 3513: A. Montoyo, R. Muñoz, E. Métais (Eds.), Natural Language Processing and Information Systems. XII, 408 pages. 2005.

Vol. 3512: J. Cabestany, A. Prieto, F. Sandoval (Eds.), Computational Intelligence and Bioinspired Systems. XXV, 1260 pages. 2005.

Vol. 3510: T. Braun, G. Carle, Y. Koucheryavy, V. Tsaoussidis (Eds.), Wired/Wireless Internet Communications. XIV, 366 pages. 2005.

Vol. 3509: M. Jünger, V. Kaibel (Eds.), Integer Programming and Combinatorial Optimization. XI, 484 pages. 2005.

Vol. 3508: P. Bresciani, P. Giorgini, B. Henderson-Sellers, G. Low, M. Winikoff (Eds.), Agent-Oriented Information Systems II. X, 227 pages. 2005. (Subseries LNAI).

Vol. 3507: F. Crestani, I. Ruthven (Eds.), Information Context: Nature, Impact, and Role. XIII, 253 pages. 2005.

Vol. 3506: C. Park, S. Chee (Eds.), Information Security and Cryptology – ICISC 2004. XIV, 490 pages. 2005.

Vol. 3505: V. Gorodetsky, J. Liu, V. A. Skormin (Eds.), Autonomous Intelligent Systems: Agents and Data Mining. XIII, 303 pages. 2005. (Subseries LNAI).

Vol. 3504: A.F. Frangi, P.I. Radeva, A. Santos, M. Hernandez (Eds.), Functional Imaging and Modeling of the Heart. XV, 489 pages. 2005.

Vol. 3503: S.E. Nikoletseas (Ed.), Experimental and Efficient Algorithms. XV, 624 pages. 2005.

Vol. 3502: F. Khendek, R. Dssouli (Eds.), Testing of Communicating Systems. X, 381 pages. 2005.

Vol. 3501: B. Kégl, G. Lapalme (Eds.), Advances in Artificial Intelligence. XV, 458 pages. 2005. (Subseries LNAI).

Vol. 3500: S. Miyano, J. Mesirov, S. Kasif, S. Istrail, P. Pevzner, M. Waterman (Eds.), Research in Computational Molecular Biology. XVII, 632 pages. 2005. (Subseries LNBI).

Vol. 3499: A. Pelc, M. Raynal (Eds.), Structural Information and Communication Complexity. X, 323 pages. 2005.

Vol. 3498: J. Wang, X. Liao, Z. Yi (Eds.), Advances in Neural Networks – ISNN 2005, Part III. XLIX, 1077 pages. 2005.

Vol. 3497: J. Wang, X. Liao, Z. Yi (Eds.), Advances in Neural Networks – ISNN 2005, Part II. XLIX, 947 pages. 2005.

Vol. 3496: J. Wang, X. Liao, Z. Yi (Eds.), Advances in Neural Networks – ISNN 2005, Part II. L, 1055 pages. 2005.

Vol. 3495: P. Kantor, G. Muresan, F. Roberts, D.D. Zeng, F.-Y. Wang, H. Chen, R.C. Merkle (Eds.), Intelligence and Security Informatics. XVIII, 674 pages. 2005.

Vol. 3494: R. Cramer (Ed.), Advances in Cryptology – EUROCRYPT 2005. XIV, 576 pages. 2005.

Vol. 3493: N. Fuhr, M. Lalmas, S. Malik, Z. Szlávik (Eds.), Advances in XML Information Retrieval. XI, 438 pages. 2005.

Vol. 3492: P. Blache, E. Stabler, J. Busquets, R. Moot (Eds.), Logical Aspects of Computational Linguistics. X, 363 pages. 2005. (Subseries LNAI).

Vol. 3489: G.T. Heineman, I. Crnkovic, H.W. Schmidt, J.A. Stafford, C. Szyperski, K. Wallnau (Eds.), Component-Based Software Engineering. XI, 358 pages. 2005.

Vol. 3488: M.-S. Hacid, N.V. Murray, Z.W. Raś, S. Tsumoto (Eds.), Foundations of Intelligent Systems. XIII, 700 pages. 2005. (Subseries LNAI).

Vol. 3486: T. Helleseth, D. Sarwate, H.-Y. Song, K. Yang (Eds.), Sequences and Their Applications - SETA 2004. XII, 451 pages. 2005.

Vol. 3483: O. Gervasi, M.L. Gavrilova, V. Kumar, A. Laganà, H.P. Lee, Y. Mun, D. Taniar, C.J.K. Tan (Eds.), Computational Science and Its Applications – ICCSA 2005, Part IV. LXV, 1362 pages. 2005.

Vol. 3482: O. Gervasi, M.L. Gavrilova, V. Kumar, A. Laganà, H.P. Lee, Y. Mun, D. Taniar, C.J.K. Tan (Eds.), Computational Science and Its Applications – ICCSA 2005, Part III. LXV, 1340 pages. 2005.

Vol. 3481: O. Gervasi, M.L. Gavrilova, V. Kumar, A. Laganà, H.P. Lee, Y. Mun, D. Taniar, C.J.K. Tan (Eds.), Computational Science and Its Applications – ICCSA 2005, Part II. LXV, 1316 pages. 2005.

Vol. 3480: O. Gervasi, M.L. Gavrilova, V. Kumar, A. Laganà, H.P. Lee, Y. Mun, D. Taniar, C.J.K. Tan (Eds.), Computational Science and Its Applications – ICCSA 2005, Part I. LXV, 1234 pages. 2005.

Vol. 3479: T. Strang, C. Linnhoff-Popien (Eds.), Location- and Context-Awareness. XII, 378 pages. 2005.

Vol. 3478: C. Jermann, A. Neumaier, D. Sam (Eds.), Global Optimization and Constraint Satisfaction. XIII, 193 pages. 2005.

Vol. 3477: P. Herrmann, V. Issarny, S. Shiu (Eds.), Trust Management. XII, 426 pages. 2005.

Vol. 3476: J. Leite, A. Omicini, P. Torroni, P. Yolum (Eds.), Declarative Agent Languages and Technologies II. XII, 289 pages. 2005. (Subseries LNAI).

Vol. 3475: N. Guelfi (Ed.), Rapid Integration of Software Engineering Techniques. X, 145 pages. 2005.

Vol. 3474: C. Grelck, F. Huch, G.J. Michaelson, P. Trinder (Eds.), Implementation and Application of Functional Languages. X, 227 pages. 2005.

¥641.92元

# Preface

The 2005 Australasian Conference on Information Security and Privacy was the tenth in the annual series that started in 1996. Over the years ACISP has grown from a relatively small conference with a large proportion of papers coming from Australia into a truly international conference with an established reputation. ACISP 2005 was held at Queensland University of Technology in Brisbane, during July 4–6, 2005.

This year there were 185 paper submissions and from these 45 papers were accepted. Accepted papers came from 13 countries, with the largest proportions coming from Australia (12), China (8) and Japan (6). India and Korea both contributed 2 papers and one came from Singapore. There were also 11 papers from European countries and 3 from North America. We would like to extend our sincere thanks to all authors who submitted papers to ACISP 2005.

The contributed papers were supplemented by four invited talks from eminent researchers in information security. The father-and-son team of Prof. and Dr. Bob Blakley (Texas A&M University and IBM) gave a talk entitled "All Sail, No Anchor III," following up on a theme started at their ACISP 2000 invited talk. Adrian McCullagh (Phillips Fox Lawyers and QUT) talked on the benefit and perils of Internet banking. Ted Dunstone (Biometix) enlightened us on multimodal biometric systems. Yvo Desmedt (University College London) elucidated the growing gap between theory and practice in information security.

We were fortunate to have an energetic team of experts who formed the Program Committee. Their names may be found overleaf, and we thank them warmly for their considerable efforts. This team was helped by an even larger number of individuals who reviewed papers in their particular areas of expertise. A list of these names is also provided; we hope it is complete.

We are delighted to acknowledge the generous financial sponsorship of ACISP 2005 by Eracom Technologies and RNSA (a research network funded by the Australian Research Council). The conference was hosted by the Information Security Institute at Queensland University of Technology who provided first-class facilities and material support. The excellent Local Organizing Committee was led by the ACISP 2005 General Chair, Ed Dawson, and included Lauren May, Elizabeth Hansford and Christine Orme. We made use of electronic submission and reviewing software expertly written and supported by Andrew Clark from the Information Security Institute at QUT; this software was invaluable in easing our administrative tasks.

July 2005

Colin Boyd
Juan M. González Nieto

# ACISP 2005
# 10th Australasian Conference on Information Security and Privacy

*Sponsored by*
Information Security Institute, Queensland University of Technology
ARC Research Network for a Secure Australia (RNSA)
Eracom Technologies Pty. Ltd.

## General Chair

| | |
|---|---|
| Ed Dawson | *Queensland University of Technology, Australia* |

## Program Chairs

| | |
|---|---|
| Colin Boyd | *Queensland University of Technology, Australia* |
| Juan M. González Nieto | *Queensland University of Technology, Australia* |

## Program Committee

| | |
|---|---|
| Paul Ashley | *IBM, Australia* |
| Tuomas Aura | *Microsoft Research, UK* |
| Feng Bao | *Institute for Infocomm Research, Singapore* |
| Lynn Batten | *Deakin University, Australia* |
| Matt Bishop | *University of California at Davis, USA* |
| Bob Blakley | *Texas A&M University, USA* |
| Mike Burmester | *Florida State University, USA* |
| Marc Dacier | *Eurecom, France* |
| Yvo Desmedt | *University College London, UK* |
| Josep Domingo | *Universitat Rovira i Virgili, Spain* |
| Jordi Forné | *Universitat Politècnica de Catalunya, Spain* |
| Virgil Gligor | *University of Maryland, USA* |
| Dieter Gollmann | *TU Hamburg-Harburg, Germany* |
| Peter Gutmann | *University of Auckland, New Zealand* |
| Bill Hutchinson | *Edith Cowan University, Australia* |
| Audun Josang | *DSTC, Australia* |
| Marc Joye | *CIM-PACA, France* |
| Svein Knapskog | *Norwegian University of Science and Technology, Norway* |

| | |
|---|---|
| Byoungcheon Lee | *Joongbu University, Korea* |
| Javier López | *University of Málaga, Spain* |
| Wenbo Mao | *HP Laboratories, UK* |
| Chris Mitchell | *Royal Holloway, UK* |
| George Mohay | *QUT, Australia* |
| Paul Montague | *Motorola, Australia* |
| SangJae Moon | *Kyungpook National University, Korea* |
| Winfried Mueller | *University of Klagenfurt, Austria* |
| Eiji Okamoto | *University of Tsukuba, Japan* |
| Susan Pancho-Festin | *University of the Philippines, Philippines* |
| Radia Perlman | *Sun Microsystems, USA* |
| Josef Pieprzyk | *Macquarie University, Australia* |
| Bart Preneel | *Katholieke Universiteit Leuven, Belgium* |
| Pandu Rangan | *Indian Institute of Technology, India* |
| Anthony Rhodes | *Zayed University, UAE* |
| Carsten Rudolph | *Fraunhofer SIT, Germany* |
| Rei Safavi-Naini | *University of Wollongong, Australia* |
| Pierangela Samarati | *University of Milan, Italy* |
| Akashi Satoh | *IBM Research, Japan* |
| Jennifer Seberry | *University of Wollongong, Australia* |
| Miquel Soriano | *Universitat Politècnica de Catalunya, Spain* |
| Sridha Sridharan | *QUT, Australia* |
| Vijay Varadharajan | *Macquarie University, Australia* |
| Kapali Viswanathan | *SETS, India* |
| Huaxiong Wang | *Macquarie University, Australia* |
| Matt Warren | *Deakin University, Australia* |
| Chuan-Kun Wu | *Australian National University, Australia* |
| Yuliang Zheng | *University of North Carolina, Charlotte, USA* |

## External Reviewers

Riza Aditya
Isaac Agudo
Toru Akishita
Stig Andersson
André Årnes
Joonsang Baek
Mark Branagan
Gareth Brisbane
Jordi Castellà-Roca
Vinod Chandran
Liqun Chen
Joe Cho
Mathieu Ciet
Andrew Clark
Scott Contini
Nora Dabbous
Breno de Medeiros
Christophe De Cannière
Alex Dent
Jintai Ding
Hans Dobbertin
Christophe Doche
Jiang Du
Oscar Esparza
Serge Fehr
Clinton Fookes
Steven Galbraith
Praveen Gauravaram
Pierre Girard
Goichiro Hanaoka
Keith Harrison
Yvonne Hitchcock
Michael Hitchens
Zhenjie Huang
Sarath Indrakanti
Kouichi Itoh
Udaya Kiran Tupakula
Lars Knudsen
Joe Lano
HoonJae Lee
Ching Lin
Ling Liu
Subhamoy Maitra
Antoni Martínez-Ballesté
Michael Mason
Anish Mathuria
Bill Millan
Jose A. Montenegro
Sumio Morioka
Yi Mu
Jose Luis Muoz
Gregory Neven
Lan Nguyen
Katsuyuki Okeya
Jose A. Onieva
Kenny Paterson
Josep Pegueroles
Kun Peng
Angela Piper
Fabien Pouget
Geraint Price
Michaël Quisquater
Jason Reid
Christian Ritz
Bruno Robisson
Rodrigo Roman
Chun Ruan
Francesc Sebé
Bouchra Senadji
Leonie Simpson
Nigel Smart
Agusti Solanas
Martijn Stam
Ron Steinfeld
Chris Steketee
Hung-Min Sun
Willy Susilo
Gelareh Taban
Dong To
Guillaume Urvoy-Keller
Tri Van Le
N. Vijayarangan
R. Vijayasarathy
Guilin Wang
Yongge Wang
Duncan S. Wong
Yongdong Wu
Alec Yasinsac
Fangguo Zhang
Janson Zhang
Weiliang Zhao
Yunlei Zhao
Huafei Zhu
Jacob Zimmermann

# Table of Contents



此为试读,需要完整PDF请访问: www.ertongbook.com

## Elliptic Curve Cryptography



## Mobile Security



## Side Channel Attacks



## Evaluation and Biometrics



## Public Key Cryptosystems

## Access Control I



## Signatures I



## Invited Talk



## Access Control II



## Threshold Cryptography

## Protocols I



## Group Signatures



## Protocols II



## Signatures II



## Invited Talk



## Credentials

## Symmetric Cryptography

# All Sail, No Anchor III: Risk Aggregation and Time's Arrow

Bob Blakley[1] and G.R. Blakley[2]

[1] IBM,
Austin, TX 78758, USA
blakley@us.ibm.com
[2] Texas A&M University
College Station, TX 77843-3368, USA
blakley@math.tamu.edu

**Abstract.** This paper explains why protection mechanisms which distribute even the protected forms of information assets lead to increased risks. It describes a mechanism (called a "lethal secret sharing system") which enables the imposition of "forgetfulness" by an asset owner on the receiver of a protected asset. This forgetfulness, or "lethe", is enforced by allowing the asset owner to give information about a piece of knowledge to the asset receiver in such a way that the receiver can be prevented at a future time from using the knowledge to recover the information.

## 1 Introduction

*All Sail, No Anchor I: Cryptography, Risk, and e-Commerce* [1] examined how the passage of time creates risk in electronic information systems.

This paper will extend the discussion to consider how re-use of cryptographic and other information protection artifacts aggregates risks and thereby makes electronic information systems more dangerous as time passes.

When a system is designed so that a cascade of failures, or a single failure with multiple adverse results can lead to large losses, that system is said to aggregate risks. Many critical systems are designed to avoid risk aggregation problems by eliminating "single points of failure".

Risk aggregation is often thought of in spatial terms (routing hydraulics through a single point in airliners; siting multiple telecommunications hostels in the basement of a single building, etc...) But it can also be thought of in temporal terms - adding more risk to a single artifact or system over time.

Information security systems often aggregate risks in poorly-understood ways, by re-using protection mechanisms which are assumed to be very strong but whose strength is in fact poorly understood.

C. Boyd and J.M. González Nieto (Eds.): ACISP 2005, LNCS 3574, pp. 1-16, 2005.
© Springer-Verlag Berlin Heidelberg 2005

## 2 Instantaneous Protection Decay

We consider two information protection scenarios which are common in today's information systems, and discuss how each of these scenarios leads to aggregation of risk.

### Encrypted Storage

Information systems often protect sensitive data against disclosure by encrypting the data when it is stored on media.
In this scenario:

- The asset (for example, a file or database) is protected for a long time.
- The protected form of the asset is in the possession of its owner.
- Compromise of one asset does not (necessarily) diminish the protection of other assets.
- Compromise of a single cryptographic key can devalue multiple assets – but smart key management can help with this by ensuring that a unique key is used for each asset, as can smart management of physical media and access thereto.
- Compromise of a mechanism (e.g. cryptosystem or block cipher mode of operation) can devalue multiple assets, but smart management of physical media and accesss thereto can help with this by allowing the owner to fall back to simple physical access protections when he learns that the mechanism has been broken.

### Digital Rights Management

Media distribution systems often protect valuable content against unlicensed use by encrypting the data before it is distributed, and relying upon specialized media players to prevent copying or other misuse of the content in violation of license terms.

In this scenario:

- The asset is protected for a long time.
- The asset (at least in its protected form) is in the possession of the enemy.
- Compromise of one asset does devalue other instances of the same asset, but does not necessarily weaken the protection of instances of different assets.
- Compromise of a single key may devalue multiple assets, but smart key management may be able to help with this, by ensuring that a unique key is used to protect each asset.
- Compromise of a mechanism can devalue all assets.

## 3 Risk Aggregation

[1] introduced a taxonomy of asset types to facilitate discussions of the evolution of risk over time. That paper went on to discuss risk associated with "Alice-type"

此为试读,需要完整PDF请访问: www.ertongbook.com