Min Surp Rhee
Byoungcheon Lee (Eds.)

Information Security and Cryptology – ICISC 2006

LNCS 4296

9th International Conference
Busan, Korea, November/December 2006
Proceedings

Springer

Min Surp Rhee Byoungcheon Lee (Eds.)

Information Security and Cryptology – ICISC 2006

9th International Conference
Busan, Korea, November 30 - December 1, 2006
Proceedings

Springer

Volume Editors

Min Surp Rhee
Dankook University
San 29, Anseo-dong, Cheonan-shi
Chungnam, 330-714, Korea
E-mail: msrhee@dankook.ac.kr

Byoungcheon Lee
Joongbu University
101 Daehak-Ro, Chubu-Myeon, Guemsan-Gun
Chungnam, 312-702, Korea
E-mail: sultan@joongbu.ac.kr

Library of Congress Control Number: 2006936103

CR Subject Classification (1998): E.3, G.2.1, D.4.6, K.6.5, F.2.1, C.2, J.1

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-49112-0 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-49112-5 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11927587 06/3142 5 4 3 2 1 0

Lecture Notes in Computer Science 4296

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

Editorial Board

Preface

ICISC 2006, the Ninth International Conference on Information Security and Cryptology was held in Busan, Korea, during November 30 - December 1, 2006. It was organized by the Korea Institute of Information Security and Cryptology (KIISC) in cooperation with the Ministry of Information and Communication (MIC), Korea. The aim of this conference was to provide a forum for the presentation of new results in research, development, and application in information security and cryptology. It also intended to be a place where research information can be exchanged.

Started in 1998, ICISC has grown into an important international conference in the information security and cryptology area with an established reputation. Based on this maturity, we tried an important change in the publication policy this year. Until last year, pre-proceedings were distributed at the conference and proceedings in Springer's *Lecture Notes in Computer Science* (LNCS) were published after the conference. This year ICISC proceedings were published in LNCS before the conference and distributed to the participants at the conference. We appreciate Springer for their full support and help in making this possible.

The conference received 129 submissions from 17 countries, covering all areas of information security and cryptology. The review and selection processes were carried out in two stages by the Program Committee of 57 prominent researchers via online meetings through the iChair Web server. First, each paper was blind reviewed by at least three PC members, and papers co-authored by the PC members were reviewed by at least five PC members. Second, individual review reports were revealed to PC members, and detailed interactive discussion on each paper followed. Through this process the Program Committee finally selected 26 papers from 12 countries. The authors of selected papers had a few weeks to prepare final versions of their papers, aided by comments from the reviewers. The proceedings contain the revised versions of the accepted papers. However, most of these final revisions were not subject to any further editorial review.

The conference program included two invited talks from eminent researchers in information security and cryptology. Serge Vaudenay from EPFL gave an interesting talk on RFID privacy entitled "RFID Privacy Based on Public-Key Cryptography." Palash Sarkar from the Indian Statistical Institute talked on "Generic Attacks on Symmetric Ciphers," which showed various time-memory trade-off attacks on symmetric cipher algorithms.

We would like to thank everyone who contributed to the success of this conference. First, thanks to all the authors who submitted papers to this conference. Second, thanks to all 57 members of the Program Committee listed overleaf. It was a truly nice experience to work with such talented and hard-working researchers. Third, thanks to all the external reviewers for assisting the Program Committee in their particular areas of expertise. Fourth, we would like to thanks

all the participants of the event who made this event an intellectually stimulating one through their active contribution. We also would like to thank the iChair developers in EPFL for allowing us to use their software. Finally, we are delighted to acknowledge the partial financial support provided by Redgate, SECUi.COM, MarkAny, and EK Manpower.

November 2006

Min Surp Rhee
Byoungcheon Lee

Organization

General Chair

JooSeok Song	Yonsei University, Korea

Program Co-chairs

Min Surp Rhee	Dankook University, Korea
Byoungcheon Lee	Joongbu University, Korea

Program Committee

Giuseppe Ateniese	The Johns Hopkins University, USA
Joonsang Baek	Institute for Infocomm Research, Singapore
Alex Biryukov	University of Luxembourg, Luxembourg
John Black	University of Colorado, USA
Jean-Sebastien Coron	University of Luxembourg, Luxembourg
Jung Hee Cheon	Seoul National University, Korea
Kyo-il Chung	ETRI, Korea
Ed Dawson	Queensland University of Technology, Australia
Yevgeniy Dodis	New York University, USA
Serge Fehr	CWI Amsterdam, Netherlands
Pierre-Alain Fouque	Ecole Normale Superieure, France
Marc Girault	France Telecom, France
Philippe Golle	Palo Alto Research Center, USA
Dieter Gollmann	Hamburg University of Technology, Germany
Yongfei Han	ONETS, China
Goichiro Hanaoka	AIST, Japan
Marc Joye	Gemplus, France
Jonathan Katz	University of Maryland, USA
Hiroaki Kikuchi	Tokai University, Japan
Hwankoo Kim	Hoseo University, Korea
Kwangjo Kim	ICU, Korea
Kaoru Kurosawa	Ibaraki University, Japan
Taekyoung Kwon	Sejong University, Korea
Chi Sung Laih	Kun Shan University, Taiwan
Kwok-Yan Lam	Tsinghua University, China
Dong Hoon Lee	Korea University, Korea
Pil Joong Lee	POSTECH, Korea
Sang-Ho Lee	Ewha Womans University, Korea
Arjen Lenstra	EPFL, Switzerland
Yingjiu Li	Singapore Management University, Singapore

Helger Lipmaa	Cybernetica AS and University of Tartu, Estonia
Javier Lopez	University of Malaga, Spain
Masahiro Mambo	University of Tsukuba, Japan
Keith Martin	Royal Holloway, University of London, UK
Mitsuru Matsui	Mitsubishi Electric Corporation, Japan
Chris Mitchell	Royal Holloway, University of London, UK
Atsuko Miyaji	JAIST, Japan
SangJae Moon	Kyungpook National University, Korea
Yi Mu	University of Wollongong, Australia
Rei Safavi-Naini	Wollongong University, Australia
Jesper Buus Nielsen	Aarhus University, Denmark
DaeHun Nyang	Inha University, Korea
Rolf Oppliger	eSECURITY Technologies, Switzerland
Carles Padro	Technical University of Catalonia, Spain
Raphael Chung-Wei Phan	Swinburne University of Technology, Malaysia
Kouichi Sakurai	Kyushu University, Japan
Palash Sarkar	Indian Statistical Institute, India
Nigel Smart	University of Bristol, UK
Willy Susilo	University of Wollongong, Australia
Tsuyoshi Takagi	Future University - Hakodate, Japan
Serge Vaudenay	EPFL, Switzerland
Guilin Wang	Institute for Infocomm Research, Singapore
William Whyte	NTRU Cryptosystems, USA
Michael Wiener	Cryptographic Clarity, Canada
Dongho Won	Sungkyunkwan University, Korea
Sung-Ming Yen	National Central University, Taiwan
Yongjin Yeom	NSRI, Korea
Fangguo Zhang	Sun Yat-sen University, China
Alf Zugenmaier	DoCoMo Euro-Labs, Germany

Organizing Chair

Kyung-Hyune Rhee	Pukyong National University, Korea

Organizing Committee

Chang Kyu Kim	Dong-eui University, Korea
Heekuck Oh	Hanyang University, Korea
Im-Yeong Lee	Soonchunhyang University, Korea
Sang-Uk Shin	Pukyong National University, Korea
Weon Shin	Tongmyong University, Korea
HoonJae Lee	Dongseo University, Korea
Dong Kyue Kim	Hanyang University, Korea

External Reviewers

Imad Aad
Imad Abbadi
Michelle Abdalla
Toru Akishita
Patrick Amon
Thomas Baigneres
Simon Blackburn
Marina Blanton
Brian Carrier
Michael Cheng
Sangrae Cho
Seokhyang Cho
Yong-Je Choi
Sherman Chow
Andrew Clark
Yang Cui
John Daugman
Alain Durand
Andrzej Drygajlo
Dang Nguyen Duc
Gerardo Fernandez
Matthieu Finiasz
Aline Gouget
Matthew Green
JaeCheol Ha
Genebeck Hahn
Javier Herranz
Susan Hohenberger
Jungdae Hong
Yoshiaki Hori
Jeffrey Horton
Xinyi Huang
John Ioannidis
Toshiyuki Isshiki
Tetsuya Izu
Jingak Jang
Ik rae Jeong
Seny Kamara
Jeonil Kang
Eike Kiltz
Hyung Chan Kim
Jonghyun Kim
Tae Hyun Kim
Youngsoo Kim
Shinsaku Kiyomoto
Tetsutaro Kobayashi
Divyan M. Konidala
Noboru Kunihiro
Nam-Suk Kwarc
Sven Lachmund
Julien Laganier
Vinh The Lam
HoonJae Lee
Jin Li
Wanqing Li
Hsi-Chung Lin
JongHyup Lee
MunKyu Lee
Soo-hyung Lee
Yunho Lee
Jiqiang Lu
Liang Lu
Tal Malkin
Kanta Matsuura
Breno de Medeiros
Kunihiko Miyazaki
George Mohay
Jean Monnerat
Dae Sung Moon
Kazuto Ogawa
Takeshi Okamoto
Dan Page
Jung Hyung Park
Sangjoon Park
Tae Jun Park
Sylvain Pasini
Geong Sen Poh
Rodrigo Roman
Louis Salvail
Farzad Salim
Christian Schaefer
Jae Woo Seo
Nicholas Sheppard
Jong Hoon Shin
SeongHan Shin
Douglas Sicker
Hongwei Sun
Clark Thomborson
Dongvu Tonien
Eran Tromer
Yoshifumi Ueshige
Masashi Une
Frederik Vercauteren
Duc Liem Vo
Martin Vuagnoux
Camille Vuillaume
Thomas Walter
Baodian Wei
Chung-Huang Yang
Yeon Hyeong Yang
Eunsun Yoo
Sung-Soo Yoon
Dae Hyun Yum
Rui Zhang
Chang'an Zhao
Sebastien Zimmer

Sponsoring Institutions

Redgate, Korea	http://www.redgate.co.kr/
SECUi.COM, Korea	http://www.secui.com/
MarkAny, Korea	http://www.markany.com/
EK Manpower, Korea	http://www.ekmanpower.co.kr/

Lecture Notes in Computer Science

For information about Vols. 1–4212

please contact your bookseller or Springer

Vol. 4313: T. Margaria, B. Steffen (Eds.), Leveraging Applications of Formal Methods. IX, 197 pages. 2006.

Vol. 4312: S. Sugimoto, J. Hunter, A. Rauber, A. Morishima (Eds.), Digital Libraries: Achievements, Challenges and Opportunities. XVIII, 571 pages. 2006.

Vol. 4311: K. Cho, P. Jacquet (Eds.), Technologies for Advanced Heterogeneous Networks II. XI, 253 pages. 2006.

Vol. 4302: J. Domingo-Ferrer, L. Franconi (Eds.), Privacy in Statistical Databases. XI, 383 pages. 2006.

Vol. 4300: Y.Q. Shi (Ed.), Transactions on Data Hiding and Multimedia Security I. IX, 139 pages. 2006.

Vol. 4296: M.S. Rhee, B. Lee (Eds.), Information Security and Cryptology – ICISC 2006. XIII, 358 pages. 2006.

Vol. 4293: A. Gelbukh, C.A. Reyes-Garcia (Eds.), MICAI 2006: Advances in Artificial Intelligence. XXVIII, 1232 pages. 2006. (Sublibrary LNAI).

Vol. 4292: G. Bebis, R. Boyle, B. Parvin, D. Koracin, P. Remagnino, A. Nefian, G. Meenakshisundaram, V. Pascucci, J. Zara, J. Molineros, H. Theisel, T. Malzbender (Eds.), Advances in Visual Computing, Part II. XXXII, 906 pages. 2006.

Vol. 4291: G. Bebis, R. Boyle, B. Parvin, D. Koracin, P. Remagnino, A. Nefian, G. Meenakshisundaram, V. Pascucci, J. Zara, J. Molineros, H. Theisel, T. Malzbender (Eds.), Advances in Visual Computing, Part I. XXXI, 916 pages. 2006.

Vol. 4290: M. van Steen, M. Henning (Eds.), Middleware 2006. XIII, 425 pages. 2006.

Vol. 4283: Y.Q. Shi, B. Jeon (Eds.), Digital Watermarking. XII, 474 pages. 2006.

Vol. 4281: K. Barkaoui, A. Cavalcanti, A. Cerone (Eds.), Theoretical Aspects of Computing - ICTAC 2006. XV, 371 pages. 2006.

Vol. 4280: A.K. Datta, M. Gradinariu (Eds.), Stabilization, Safety, and Security of Distributed Systems. XVII, 590 pages. 2006.

Vol. 4279: N. Kobayashi (Ed.), Programming Languages and Systems. XI, 423 pages. 2006.

Vol. 4278: R. Meersman, Z. Tari, P. Herrero (Eds.), On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops, Part II. XLV, 1004 pages. 2006.

Vol. 4277: R. Meersman, Z. Tari, P. Herrero (Eds.), On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops, Part I. XLV, 1009 pages. 2006.

Vol. 4276: R. Meersman, Z. Tari (Eds.), On the Move to Meaningful Internet Systems 2006: CoopIS, DOA, GADA, and ODBASE, Part II. XXXII, 752 pages. 2006.

Vol. 4275: R. Meersman, Z. Tari (Eds.), On the Move to Meaningful Internet Systems 2006: CoopIS, DOA, GADA, and ODBASE, Part I. XXXI, 1115 pages. 2006.

Vol. 4273: I.F. Cruz, S. Decker, D. Allemang, C. Preist, D. Schwabe, P. Mika, M. Uschold, L. Aroyo (Eds.), The Semantic Web - ISWC 2006. XXIV, 1001 pages. 2006.

Vol. 4272: P. Havinga, M. Lijding, N. Meratnia, M. Wegdam (Eds.), Smart Sensing and Context. XI, 267 pages. 2006.

Vol. 4271: F.V. Fomin (Ed.), Graph-Theoretic Concepts in Computer Science. XIII, 358 pages. 2006.

Vol. 4270: H. Zha, Z. Pan, H. Thwaites, A.C. Addison, M. Forte (Eds.), Interactive Technologies and Sociotechnical Systems. XVI, 547 pages. 2006.

Vol. 4269: R. State, S. van der Meer, D. O'Sullivan, T. Pfeifer (Eds.), Large Scale Management of Distributed Systems. XIII, 282 pages. 2006.

Vol. 4268: G. Parr, D. Malone, M. Ó Foghlú (Eds.), Autonomic Principles of IP Operations and Management. XIII, 237 pages. 2006.

Vol. 4267: A. Helmy, B. Jennings, L. Murphy, T. Pfeifer (Eds.), Autonomic Management of Mobile Multimedia Services. XIII, 257 pages. 2006.

Vol. 4266: H. Yoshiura, K. Sakurai, K. Rannenberg, Y. Murayama, S. Kawamura (Eds.), Advances in Information and Computer Security. XIII, 438 pages. 2006.

Vol. 4265: L. Todorovski, N. Lavrač, K.P. Jantke (Eds.), Discovery Science. XIV, 384 pages. 2006. (Sublibrary LNAI).

Vol. 4264: J.L. Balcázar, P.M. Long, F. Stephan (Eds.), Algorithmic Learning Theory. XIII, 393 pages. 2006. (Sublibrary LNAI).

Vol. 4263: A. Levi, E. Savas, H. Yenigün, S. Balcisoy, Y. Saygin (Eds.), Computer and Information Sciences – ISCIS 2006. XXIII, 1084 pages. 2006.

Vol. 4261: Y. Zhuang, S. Yang, Y. Rui, Q. He (Eds.), Advances in Multimedia Information Processing - PCM 2006. XXII, 1040 pages. 2006.

Vol. 4260: Z. Liu, J. He (Eds.), Formal Methods and Software Engineering. XII, 778 pages. 2006.

Vol. 4259: S. Greco, Y. Hata, S. Hirano, M. Inuiguchi, S. Miyamoto, H.S. Nguyen, R. Słowiński (Eds.), Rough Sets and Current Trends in Computing. XXII, 951 pages. 2006. (Sublibrary LNAI).

Vol. 4257: I. Richardson, P. Runeson, R. Messnarz (Eds.), Software Process Improvement. XI, 219 pages. 2006.

Vol. 4256: L. Feng, G. Wang, C. Zeng, R. Huang (Eds.), Web Information Systems – WISE 2006 Workshops. XIV, 320 pages. 2006.

Vol. 4255: K. Aberer, Z. Peng, E.A. Rundensteiner, Y. Zhang, X. Li (Eds.), Web Information Systems – WISE 2006. XIV, 563 pages. 2006.

Vol. 4254: T. Grust, H. Höpfner, A. Illarramendi, S. Jablonski, M. Mesiti, S. Müller, P.-L. Patranjan, K.-U. Sattler, M. Spiliopoulou (Eds.), Current Trends in Database Technology – EDBT 2006. XXXI, 932 pages. 2006.

Vol. 4253: B. Gabrys, R.J. Howlett, L.C. Jain (Eds.), Knowledge-Based Intelligent Information and Engineering Systems, Part III. XXXII, 1301 pages. 2006. (Sublibrary LNAI).

Vol. 4252: B. Gabrys, R.J. Howlett, L.C. Jain (Eds.), Knowledge-Based Intelligent Information and Engineering Systems, Part II. XXXIII, 1335 pages. 2006. (Sublibrary LNAI).

Vol. 4251: B. Gabrys, R.J. Howlett, L.C. Jain (Eds.), Knowledge-Based Intelligent Information and Engineering Systems, Part I. LXVI, 1297 pages. 2006. (Sublibrary LNAI).

Vol. 4249: L. Goubin, M. Matsui (Eds.), Cryptographic Hardware and Embedded Systems - CHES 2006. XII, 462 pages. 2006.

Vol. 4248: S. Staab, V. Svátek (Eds.), Managing Knowledge in a World of Networks. XIV, 400 pages. 2006. (Sublibrary LNAI).

Vol. 4247: T.-D. Wang, X. Li, S.-H. Chen, X. Wang, H. Abbass, H. Iba, G. Chen, X. Yao (Eds.), Simulated Evolution and Learning. XXI, 940 pages. 2006.

Vol. 4246: M. Hermann, A. Voronkov (Eds.), Logic for Programming, Artificial Intelligence, and Reasoning. XIII, 588 pages. 2006. (Sublibrary LNAI).

Vol. 4245: A. Kuba, L.G. Nyúl, K. Palágyi (Eds.), Discrete Geometry for Computer Imagery. XIII, 688 pages. 2006.

Vol. 4244: S. Spaccapietra (Ed.), Journal on Data Semantics VII. XI, 267 pages. 2006.

Vol. 4243: T. Yakhno, E.J. Neuhold (Eds.), Advances in Information Systems. XIII, 420 pages. 2006.

Vol. 4242: A. Rashid, M. Aksit (Eds.), Transactions on Aspect-Oriented Software Development II. IX, 289 pages. 2006.

Vol. 4241: R.R. Beichel, M. Sonka (Eds.), Computer Vision Approaches to Medical Image Analysis. XI, 262 pages. 2006.

Vol. 4239: H.Y. Youn, M. Kim, H. Morikawa (Eds.), Ubiquitous Computing Systems. XVI, 548 pages. 2006.

Vol. 4238: Y.-T. Kim, M. Takano (Eds.), Management of Convergence Networks and Services. XVIII, 605 pages. 2006.

Vol. 4237: H. Leitold, E. Markatos (Eds.), Communications and Multimedia Security. XII, 253 pages. 2006.

Vol. 4236: L. Breveglieri, I. Koren, D. Naccache, J.-P. Seifert (Eds.), Fault Diagnosis and Tolerance in Cryptography. XIII, 253 pages. 2006.

Vol. 4234: I. King, J. Wang, L. Chan, D. Wang (Eds.), Neural Information Processing, Part III. XXII, 1227 pages. 2006.

Vol. 4233: I. King, J. Wang, L. Chan, D. Wang (Eds.), Neural Information Processing, Part II. XXII, 1203 pages. 2006.

Vol. 4232: I. King, J. Wang, L. Chan, D. Wang (Eds.), Neural Information Processing, Part I. XLVI, 1153 pages. 2006.

Vol. 4231: J. F. Roddick, R. Benjamins, S. Si-Saïd Cherfi, R. Chiang, C. Claramunt, R. Elmasri, F. Grandi, H. Han, M. Hepp, M. Hepp, M. Lytras, V.B. Mišić, G. Poels, I.-Y. Song, J. Trujillo, C. Vangenot (Eds.), Advances in Conceptual Modeling - Theory and Practice. XXII, 456 pages. 2006.

Vol. 4230: C. Priami, A. Ingólfsdóttir, B. Mishra, H.R. Nielson (Eds.), Transactions on Computational Systems Biology VII. VII, 185 pages. 2006. (Sublibrary LNBI).

Vol. 4229: E. Najm, J.F. Pradat-Peyre, V.V. Donzeau-Gouge (Eds.), Formal Techniques for Networked and Distributed Systems - FORTE 2006. X, 486 pages. 2006.

Vol. 4228: D.E. Lightfoot, C.A. Szyperski (Eds.), Modular Programming Languages. X, 415 pages. 2006.

Vol. 4227: W. Nejdl, K. Tochtermann (Eds.), Innovative Approaches for Learning and Knowledge Sharing. XVII, 721 pages. 2006.

Vol. 4226: R.T. Mittermeir (Ed.), Informatics Education – The Bridge between Using and Understanding Computers. XVII, 319 pages. 2006.

Vol. 4225: J.F. Martínez-Trinidad, J.A. Carrasco Ochoa, J. Kittler (Eds.), Progress in Pattern Recognition, Image Analysis and Applications. XIX, 995 pages. 2006.

Vol. 4224: E. Corchado, H. Yin, V. Botti, C. Fyfe (Eds.), Intelligent Data Engineering and Automated Learning – IDEAL 2006. XXVII, 1447 pages. 2006.

Vol. 4223: L. Wang, L. Jiao, G. Shi, X. Li, J. Liu (Eds.), Fuzzy Systems and Knowledge Discovery. XXVIII, 1335 pages. 2006. (Sublibrary LNAI).

Vol. 4222: L. Jiao, L. Wang, X. Gao, J. Liu, F. Wu (Eds.), Advances in Natural Computation, Part II. XLII, 998 pages. 2006.

Vol. 4221: L. Jiao, L. Wang, X. Gao, J. Liu, F. Wu (Eds.), Advances in Natural Computation, Part I. XLI, 992 pages. 2006.

Vol. 4220: C. Priami, G. Plotkin (Eds.), Transactions on Computational Systems Biology VI. VII, 247 pages. 2006. (Sublibrary LNBI).

Vol. 4219: D. Zamboni, C. Kruegel (Eds.), Recent Advances in Intrusion Detection. XII, 331 pages. 2006.

Vol. 4218: S. Graf, W. Zhang (Eds.), Automated Technology for Verification and Analysis. XIV, 540 pages. 2006.

Vol. 4217: P. Cuenca, L. Orozco-Barbosa (Eds.), Personal Wireless Communications. XV, 532 pages. 2006.

Vol. 4216: M.R. Berthold, R. Glen, I. Fischer (Eds.), Computational Life Sciences II. XIII, 269 pages. 2006. (Sublibrary LNBI).

Vol. 4215: D.W. Embley, A. Olivé, S. Ram (Eds.), Conceptual Modeling - ER 2006. XVI, 590 pages. 2006.

Vol. 4213: J. Fürnkranz, T. Scheffer, M. Spiliopoulou (Eds.), Knowledge Discovery in Databases: PKDD 2006. XXII, 660 pages. 2006. (Sublibrary LNAI).

Table of Contents

Invited Talks

Hash Functions – I

Block and Stream Ciphers

Efficient Implementation and Hardware

Network Security and Access Control

Mobile Communications Security

Forensics

Copyright Protection

Biometrics

Hash Functions – II

Public Key Cryptosystems

Digital Signatures

RFID Privacy Based on Public-Key Cryptography (Abstract)

Serge Vaudenay

EPFL
CH-1015 Lausanne, Switzerland
http://lasecwww.epfl.ch

Abstract. RFID systems makes it possible for a server to identify known tags in wireless settings. As they become more and more pervasive, people privacy is more and more threatened. In this talk, we list a few models for privacy in RFID and compare them. We review a few protocols. We further show that strong privacy mandates the use of public-key cryptography. Finally, we present a new cryptosystem which is dedicated to tiny hardware and which can be used to design secure RFID systems achieving strong privacy.

Note: this paper contains new definitions and results that are announced in this talk. Details and proofs will appear in future papers.

Credits: the work on RFID was done together with Salvatore Bocchetti as a part of his Master Thesis [3]. We received many suggestions from Gildas Avoine. The work on the new cryptosystem was done together with Matthieu Finiasz [4] and was extended together with Jean-Philippe Aumasson, and Willi Meier. Part of it was done in the Master Thesis of Jean-Philippe Aumasson [2].

1 RFID Schemes

We consider an environment with several participants. Some are called *systems*, others are called *tags*. Every tag is associated to a system. We say that the tag *belongs* to the system. Every tag is given an identification string ID. The purpose of RFID protocols is to design a communication protocol between a system and a tag so that the system knows whether or not the tag belongs to the system and learns the tag identification string ID when the tag belongs to the system.

Tags have memory which contains a *state*. Systems have a database which contains pairs of data associated to the tags that they own. This pair consists of the ID and a key. Systems may also have cryptographic key materials.

An RFID scheme is defined by the following processes.

- An initialization algorithm for the system. This produces cryptographic key materials (if any).
- An algorithm to set up a tag. This algorithm takes an ID as input and produces a tag key K and an initial state. The latter is the initial state of the tag. The former is inserted together with ID in the database of the system that owns the tag. Note that

M.S. Rhee and B. Lee (Eds.): ICISC 2006, LNCS 4296, pp. 1–6, 2006.

from this definition tags do not necessarily know their own ID and key. This may (or not) be part of the initial state though.
- A 2-party communication protocol between a system and a tag. Protocols are usually initiated by the system and produce two types of outputs on the reader side: a public output and a private output. We distinguish two types of protocol: identification protocols and authentication protocols. As for public outputs, the two kinds of protocols do the same. The private output of an identification protocol should be the tag ID if it belongs to the system or $\perp$ if it does not. Both outputs of an authentication protocol should be the tag 1 if it belongs to the system or 0 if it does not.

A protocol is *complete* if the output of the protocol is correct with high probability. Depending on the application, we may want to have a stronger security notion, namely *soundness*, which says whether an adversary can make the protocol output some wrong information. A critical issue is *privacy*, which means that protocols do not leak any information which may be used by adversaries to trace tags.

2 Adversaries

In an *attack*, one system is first initialize and an adversary can play with it. In addition to this, he can create tags with chosen *ID* which belong to the system or not. That is, the tag initialization algorithm is run, the tag with specified initial state is created, and the database of the system is updated in the case where the tag belongs to the system. Here the adversary does not see the tag key or initial state. In addition to creating new tags, the adversary can play with the system and the tags. We distinguish two kinds of tags: tags that are *free* from tags that are *drawn*. Tags can move from a free status to a drawn one and vice versa. A drawn tag is a tag which is close to the adversary so that the adversary can trace it during the entire time it is a drawn tag. For this, drawn tags are identified by a temporary identity that we call a *virtual tag*.

More concretely, we assume that the adversary has access to the following oracles.

- $\mathsf{Init}(\mathsf{ID}, b)$ initializes new (free) tags of specified ID which belongs to System or not depending on bit b.
- $\mathsf{GetTag}(\mathsf{distribution}) \to (\mathsf{vtag}_1, b_1, \ldots, \mathsf{vtag}_n, b_n)$ draws one or several free tags at random with chosen probability distribution. This oracle returns "virtual tags" names and bits telling whether they belong to the system or not.
- $\mathsf{Free}(\mathsf{vtag})$ frees a drawn tag.
- $\mathsf{Launch} \to \pi$ launches a new protocol instance with reader.
- $\mathsf{SendReader}(m, \pi) \to m'$ resp. $\mathsf{SendTag}(m, \mathsf{vtag}) \to m'$ sends protocol message m to reader resp. a drawn tag and returns the answer m' (if any). By convention, we write $\mathsf{Execute}(\mathsf{vtag}) \to (\pi, \mathsf{transcript})$ as a macro oracle call instead of one $\mathsf{Launch} \to \pi$ followed by a succession of $\mathsf{SendReader}(m_i, \pi) \to m_{i+1}$ and $\mathsf{SendTag}(m_{i+1}, \mathsf{vtag}) \to m_{i+2}$ calls. The protocol transcript is the concatenation of all messages m_i.
- $\mathsf{Result}(\pi) \to x$ tells 1 if the output of the protocol instance π is a tag ID or 0 if the output is $\perp$.
- $\mathsf{Corrupt}(\mathsf{vtag}) \to S$ corrupts a drawn tag and gets its internal state S.

We define several classes of adversaries.

- *Strong* adversaries can use the oracles as they want.
- *Forward* adversaries can only use Corrupt queries at the end of the attack. That is, a Corrupt query can only be followed by other Corrupt queries.
- *Weak* adversaries are not allowed to make Corrupt queries.
- *Narrow-strong* (resp. narrow-forward, narrow-weak) adversaries are strong (resp. forward, weak) adversaries who are not allowed to make Result queries.

3 Security of RFID Schemes

Let us consider an arbitrary adversary which can be written as follows.

1: $\mathsf{Init}(1,b_1)$, ..., $\mathsf{Init}(n,b_n)$
2: pick $i \in \{1,\ldots,n\}$ at random
3: $(\mathsf{vtag},b) \leftarrow \mathsf{GetTag}(i)$
4: $\pi \leftarrow \mathsf{Execute}(\mathsf{vtag})$

The adversary creates n tags which belong or not to the system. Then, it draws one tag and runs a protocol. We say that this adversary fails iff the output of the protocol is what it is meant to be, namely i when $b_i = 1$ and $\perp$ otherwise. We say that the protocol is *complete* iff the probability of success of any of these adversaries is negligible.

Let us consider an arbitrary adversary which can be written as follows.

1: **for** $i = 1$ to n **do**
2: $\quad \mathsf{Init}(i,1)$
3: $\quad \mathsf{vtag}_i \leftarrow \mathsf{GetTag}(i)$
4: **end for**
5: (training phase) do any oracle call except Init, GetTag, Free
6: $\pi \leftarrow$ Launch
7: (attack phase) do any oracle call except Init, GetTag, Free

We say that the adversary succeeds iff

- instance π is complete at the end of the attack phase,
- the output of π is $\mathsf{ID} \neq \perp$ (i.e. π identified a legitimate tag ID),
- tag ID did not complete a protocol run during the attack phase,
- tag ID was not corrupted.

We say that the protocol is *sound* iff the probability of success of any of these adversaries is negligible.

4 Privacy

To define privacy, we consider adversaries who output a list of virtual tags and a relation between their ID strings. The adversary wins if the ID strings of these tags satisfy the relation. Since some adversaries may win by giving trivial relations, we define the significance of an adversary by his ability to distinguish from a simulated run. More concretely, a *blinder* is an interface between the adversary and the oracles which let all