Peng Ning
Sihan Qing
Ninghui Li (Eds.)

LNCS 4307

Information and Communications Security

8th International Conference, ICICS 2006
Raleigh, NC, USA, December 2006
Proceedings

Springer

Peng Ning Sihan Qing Ninghui Li (Eds.)

Information and Communications Security

8th International Conference, ICICS 2006
Raleigh, NC, USA, December 4-7, 2006
Proceedings

Springer

Volume Editors

Peng Ning
North Carolina State University
Raleigh, NC 27695-8206, USA
E-mail: pning@ncsu.edu

Sihan Qing
Chinese Academy of Sciences
Beijing 100080, P.R. China
E-mail: qsihan@ercist.iscas.ac.cn

Ninghui Li
Purdue University
West Lafayette, Indiana 47907-2066, USA
E-mail: ninghui@cs.purdue.edu

Library of Congress Control Number: 2006936899

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 3-540-49496-0 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-49496-6 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: 11935308 06/3142 5 4 3 2 1 0

Lecture Notes in Computer Science 4307

Preface

It is our great pleasure to welcome you to the Eighth International Conference on Information and Communications Security (ICICS 2006), held in Raleigh, North Carolina, USA, December 4–7, 2006. The ICICS conference series is an established forum that brings together researchers and scholars involved in multiple disciplines of Information and Communications Security in order to foster exchange of ideas. The past seven ICICS conferences were held in Beijing, China (ICICS 1997); Sydney, Australia (ICICS 1999); Xi'an China (ICICS 2001); Singapore (ICICS 2002); Hohhot City, China (ICICS 2003); Malaga, Spain (ICICS 2004); and Beijing, China (ICICS 2005). The conference proceedings of the past seven events have been published by Springer in the *Lecture Notes in Computer Science series*, in LNCS 1334, LNCS 1726, LNCS 2229, LNCS 2513, LNCS 2836, LNCS 3269, and LNCS 3783, respectively.

This year we received a total of 119 submissions on various aspects of ad-hoc and sensor network security. The Program Committee selected 22 regular papers and 17 short papers that cover a variety of topics, including security protocols, applied cryptography and cryptanalysis, access control in distributed systems, privacy, malicious code, network and systems security, and security implementations.

Putting together ICICS 2006 was a team effort. First of all, we would like to thank the authors of every paper, whether accepted or not, for submitting their papers to ICICS 2006. We would like to express our gratitude to the Program Committee members and the external reviewers, who worked very hard in reviewing the papers and providing suggestions for their improvements. We would also like to thank the Organizing Committee members, who did a wonderful job in organizing the conference. We would like to thank our sponsor, North Carolina State University (NCSU)/Duke University Center for Advanced Computing and Communications (CACC), for supporting the conference. Finally, we would like to express our gratitude to the US Army Research Office and the US National Science Foundation for the generous financial support of this conference. Their grants provided travel supports for graduate students to attend the conference.

We hope that you will find these proceedings interesting and thought-provoking.

September 2006

Peng Ning and Sihan Qing
Program Chairs, ICICS 2006

Organization

ICICS 2006 was organized by the North Carolina State University (NCSU)/Duke University Center for Advanced Computing and Communication (CACC), with support from the US Army Research Office (ARO) and the US National Science Foundation (NSF).

Organizing Committee

General Chair
Douglas S. Reeves — North Carolina State University, USA

Program Chairs
Peng Ning — North Carolina State University, USA
Sihan Qing — Chinese Academy of Sciences, China

Publication Chair
Ninghui Li — Purdue University, USA

Panel and Keynote Chair
David Evans — University of Virginia, USA

Publicity Chair
Haining Wang — College of William and Mary, USA

Local Arrangement Chair
Errin Fulp — Wake Forrest University, USA

Posters and Demos Chair
Yong Guan — Iowa State University, USA

Financial Chair
Donggang Liu — University of Texas at Arlington, USA

Program Committee

Mikhail Atallah — Purdue University, USA
Vijay Atluri — Rutgers University, USA

Tuomas Aura	Microsoft Research, USA
Michael Backes	Saarland University, Germany
Elisa Bertino	Purdue University, USA
Sabrina De Capitani di Vimercati	Università degli Studi di Milano, Italy
Srdjan Capkun	ETH Zurich, Switzerland
Hao Chen	University of California at Davis, USA
Scott Contini	Macquarie University, Australia
Yvo Desmedt	University College London, UK
Wenliang (Kevin) Du	Syracuse University, USA
David Evans	University of Virginia, USA
Yong Guan	Iowa State University, USA
Sushil Jajodia	George Mason University, USA
Angelos Keromytis	Columbia University, USA
Paris Kitsos	Helen Open University, Greece
Christopher Kruegel	Technical University Vienna, Austria
Yingjiu Li	Singapore Management University, Singapore
Donggang Liu	University of Texas at Arlington, USA
Peng Liu	Penn State University, USA
Javier Lopez	University of Malaga, Spain
Radha Poovendran	University of Washington, USA
Phil Porras	SRI International, USA
Indrajit Ray	Colorado State University, USA
Rei Safavi-Naini	University of Wollongong, Australia
Pierangela Samarati	Università degli Studi di Milano, Italy
Kent Seamons	Brigham Young University, USA
R. Sekar	Stony Brook University, USA
Sean Smith	Dartmouth College, USA
Tim Strayer	BBN, USA
Wade Trappe	Rutgers University, USA
Haining Wang	College of William and Mary, USA
Xiaofeng Wang	Indiana University, USA
Andreas Wespi	IBM Zurich, Switzerland
S. Felix Wu	University of California at Davis, USA
Jun Xu	Google, USA
Alec Yasinsac	Florida State University, USA
Ting Yu	North Carolina State University, USA
Diego Zamboni	IBM Zurich, Switzerland
Yongguang Zhang	Microsoft Research Asia, China
Yuliang Zheng	University of North Carolina at Charlotte, USA
Jianying Zhou	Institute for Infocomm Research, Singapore
Sencun Zhu	Penn State University, USA

External Reviewers

Abdulhran Alarifi
Abdulraham Alarifi
Elli Androulaki
Joonsang Baek
Kun Bai
Abhilasha Bhargav-Spantzel
Marina Blanton
Mike Burmester
Matt Burnside
Su Chang
Shu Chen
Shuo Chen
Jong Youl Choi
Gabriela Cretu
Deepak Kumar Dalai
Kanti Das
Christophe Doche
Markus Duermuth
Yann Duponchel
Sarah Edwards
Min Feng
Keith Frikken
Tim van der Horst
Jeff Horton
Jeffrey Horton
Hungyuan Hsu
Zhengli Huang
Sotiris Ioannidis
Pandurang Kamat
Kameswari Kotapati
Fengjun Li
Lunquan Li
Zhuowei Li
Anyi Liu
Michael Locasto
Liang Lu
Andreas Moser
Karsten Nohl
Joseph Pamula
Chi-Chun Pan
Nathanael Paul
James Riordan
Sankardas Roy
Farzad Salim
Emre Sezer
Siamak Fayyaz Shahandashti
Nicholas Sheppard
Stelios Sidiroglou
Hui Song
Alok Tongaonkar
Mercan Topkara
Umut Topkara
Dominique Unruh
Hai Wang
Haodong Wang
Huaxiong Wang
Pan Wang
Ronghua Wang
Shuhong Wang
Xinran Wang
Yawen Wei
Liang Xie
Mengjun Xie
Ping Xie
Yongqiang Xiong
Wenyuan Xu
Yi Yang
Chao Yao
Zhen Yu
Chuan Yue
Linfeng Zhang
Qinghua Zhang
Yukai Zou

Lecture Notes in Computer Science

For information about Vols. 1–4226

please contact your bookseller or Springer

Vol. 4329: R. Barua, T. Lange (Eds.), Progress in Cryptology - INDOCRYPT 2006. XXXXX, 454000 pages. 2006.

Vol. 4318: H. Lipmaa, M. Yung, D. Lin (Eds.), Information Security and Cryptology. XI, 305 pages. 2006.

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. 4307: P. Ning, S. Qing, N. Li (Eds.), Information and Communications Security. XIV, 558 pages. 2006.

Vol. 4306: Y. Avrithis, Y. Kompatsiaris, S. Staab, N.E. O'Connor (Eds.), Semantic Multimedia. XII, 241 pages. 2006.

Vol. 4304: A. Sattar, B.-H. Kang (Eds.), AI 2006: Advances in Artificial Intelligence. XXVII, 1303 pages. 2006. (Sublibrary LNAI).

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. XIII, 358 pages. 2006.

Vol. 4295: J.D. Carswell, T. Tezuka (Eds.), Web and Wireless Geographical Information Systems. XI, 269 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. 4288: T. Asano (Ed.), Algorithms and Computation. XXXX, 753333 pages. 2006.

Vol. 4285: Y. Matsumoto, R. Sproat, K.-F. Wong, M. Zhang (Eds.), Computer Processing of Oriental Languages. XXXX, 55000 pages. 2006. (Sublibrary LNAI).

Vol. 4284: X. Lai, K. Chen (Eds.), Advances in Cryptology – ASIACRYPT 2006. XIV, 468 pages. 2006.

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

Vol. 4282: Z. Pan, A. Cheok, M. Haller, R.W.H. Lau, H. Saito, R. Liang (Eds.), Advances in Artificial Reality and Tele-existence. XXIII, 1347 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. 4274: Q. Huo, B. Ma, E.-S. Chng, H. Li (Eds.), Chinese Spoken Language Processing. XXXX, 8000 pages. 2006. (Sublibrary LNAI).

Vol. 4273: I. 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. 4262: K. Havelund, M. N\'u\~nez, G. Ro\csu, B. Wolff (Eds.), Formal Approaches to Software Testing and Runtime Verification. XXXXXX, 24555555 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, J. Wijsen (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.D. 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.

Table of Contents

Security Protocols

Applied Crytography

Access Control and Systems Security

Privacy and Malicious Code

Network Security

Systems Security

Cryptanalysis

Applied Cryptography and Network Security

Security Implementations

Strong and Robust RFID Authentication Enabling Perfect Ownership Transfer

Chae Hoon Lim and Taekyoung Kwon*

Dept. of Computer Engineering, Sejong University, Seoul 143-747, Korea
{tkwon, chlim}@sejong.ac.kr

Abstract. RFID technology arouses great interests from both its advocates and opponents because of the promising but privacy-threatening nature of low-cost RFID tags. A main privacy concern in RFID systems results from clandestine scanning through which an adversary could conduct silent tracking and inventorying of persons carrying tagged objects. Thus, the most important security requirement in designing RFID protocols is to ensure untraceability of RFID tags by unauthorized parties (even with knowledge of a tag secret due to no physical security of low-cost RFID tags). Previous work in this direction mainly focuses on backward untraceability, requiring that compromise of a tag secret should not help identify the tag from past communication transcripts. However, in this paper, we argue that forward untraceability, i.e., untraceability of future events even with knowledge of a current tag secret, should be considered as an equally or even more important security property in RFID protocol designs. Furthermore, RFID tags may often change hands during their lifetime and thus the problem of tag ownership transfer should be dealt with as another key issue in RFID privacy problems; once ownership of a tag is transferred to another party, the old owner should not be able to read the tag any more. It is rather obvious that complete transfer of tag ownership is possible only if some degree of forward untraceability is provided. We propose a strong and robust RFID authentication protocol satisfying both forward and backward untraceability and enabling complete transfer of tag ownership.

1 Introduction

Radio Frequency Identification (RFID) is an automated identification technology in which a small transponder, attached to a real world object, receives and responds to radio-frequency queries from a transceiver. The transponder is usually called an RFID *tag* while the transceiver is an RFID *reader*. The RFID tag incorporates silicon chips with radio antennas for electronic operations and wireless data transmissions. It tends to have extremely limited capabilities in every aspect of computation, communication, and storage for economic viability. Passive tags are not equipped with an internal power source, contrary to

* Research by the 2nd author was supported by grant No. R01-2005-000-11261-0 from Korea Science and Engineering Foundation in Ministry of Science & Technology.

P. Ning, S. Qing, and N. Li (Eds.): ICICS 2006, LNCS 4307, pp. 1–20, 2006.

semi-passive or active tags with built-in batteries. They store authentic data and respond for identification and authentication, with neither physical nor visual contact. The RFID reader communicates with tags and cooperates with a backend database which contains information on the tagged objects.

In fact, this technology is not fundamentally new; rather it has been around since the late 1960s and is being used in the public domain [11]. Recently, RFID has aroused a great interest from various communities due to the promising nature of small low-cost RFID tags in future smart applications. Rapid RFID progress has already been made in retail sectors, such as Wal-Mart and Procter & Gamble, as well as in government sectors, such as U.S. DoD and Postal Service [14]. The U.S. government also has mandated adoption by Oct 26, 2006 of *e-passports* (biometrically-enabled RFID tags) by the 27 countries in the Visa-Waiver Program [16]. It is widely believed that RFID tags will more rapidly spread over and its cost will go down fast in the near future.

RFID systems however raise a lot of privacy concerns, mainly due to the possibility of clandestine tracking and inventorying of tags [27,30,24,5,15,16,14]. For example, adversarial parties equipped with commodity RFID readers may trace a person carrying a tagged item by recognizing the same tag in different places at different times. This traceability problem is considered as the biggest security challenge to general acceptability and wide-scale deployment of RFID technology. Actually the boycott movement from those fearing privacy infringement made companies like Benetton and Gillette drop or reconsider their RFID-tagging plans [7,29]. Fortunately, a number of studies have also been done for handling such security and privacy issues in RFID systems [17,24,10,13,19,4,8,23]. The approaches taken in these studies vary, from schemes based on weak but realistic models to strong cryptographic techniques, and each approach may have its own merit and demerit.

In this paper, we are more interested in a stronger security model, assuming that tag secrets may be read by an adversary, since most low-cost RFID tags have no protection capability of the tag memory. Since reading the tag memory content endows the adversary with full capability of the tag from the moment, it is very important to see how the past and the future transactions of the tag are related with the current internal state of the tag at the time of memory break-in. This observation brings us the security notions of backward (resp. forward) untraceability, meaning that knowledge of a tag's current internal state must not help identify the tag's past (resp. future) interactions.[1] Most previous studies focus on backward untraceability and, as far as we know, no attention has been paid explicitly to forward untraceability yet. In this paper, we would like to call our attention to the importance of forward untraceability and related issues.

We argue that *forward untraceability* is even more important than backward untraceability in RFID systems. Suppose that compromise of tag secrets results in complete loss of control over the tags. Then, it may be catastrophic if tag secrets are compromised in some point of tag deployment or during their cir-

[1] Note that we used the terms 'forward' and 'backward' opposite to usual definitions. See Section 2 for our justification.

culation within supply chains; then it would be much easier to trace the tags and reproduce cloned tags. Another important related issue is the problem of *ownership transfer*. Since tags may change hands frequently during their lifetime, it is certainly necessary to provide some means of ownership transfer of a tag from one party to another. Ownership of a tag means the ability to read the tag and thus ownership transfer should guarantee that once ownership of a tag is transferred, the tag should be able to be read only by the new owner but never by the old owner. Such a complete transfer of tag ownership would be impossible unless some degree of forward untraceability is provided, since the old owner would have already owned all the information necessary to control the tag. Note that we are talking about perfect ownership transfer between users, contrary to Molnar et al.'s temporary ownership transfer or time-limited access delegation [23] (See Section 4 for more details).

Our Contribution. As discussed above, there is of no doubt on the importance of forward untraceability, in addition to traditional backward untraceability, in designing RFID authentication protocols. Backward untraceability is easy to achieve by updating tag secrets based on a one-way key chain and has been widely studied in the literature. However, it is never easy to achieve forward untraceability using cryptographic techniques in low-cost RFID tags, due to the very limited resources available in such tags. The mobility of tagged items is our primary finding as a means of achieving forward untraceability with little increase of complexity. That is, even if an adversary learns the tag secret of a particular person's belonging, he will not be able to physically track the target item all the way from the moment of tag break-in. Thus, assuming that it is not possible for the adversary to eavesdrop all the interactions of the target tag afterwards, we will be able to completely refresh the tag secret in synchronization with the backend database by injecting into the tag secret the shared randomness involved in every successful authentication. In this paper, we first bring the notion of forward untraceability explicitly and rigorously in the design of RFID authentication protocols and propose such a protocol achieving both requirements of forward and backward untraceability. Furthermore, we show that our protocol enables perfect transfer of tag ownership between users. This feature will be essential in trading tagged objects in the real world. We also show that this feature can be used to delegate access to tags to potentially untrustworthy readers for distributed processing of a central database and may help thwart tag cloning by refreshing the tag secret whenever necessary.

2 RFID Systems and Security

2.1 The Communication Model

An RFID system consists of three main entities such as RFID tags, RFID readers, and a backend database server, along with communication channels between them. Figure 1 depicts the high-level view of the communication and security model for conducting RFID authentication in general. The channels between the