Available online at www.sciencedirect.com
ScienceDirect
Computer Networks 51 (2007) 2219–2222
Computer Networks
www.elsevier.com/locate/comnet

Advances in smart cards

Josep Domingo-Ferrer [a,*], Joachim Posegga [b], Francesc Sebé [a], Vicenç Torra [c]

[a] Rovira i Virgili University, Department of Computer Engineering and Mathematics, Av. Països Catalans 26, E-43007 Tarragona, Catalonia, Spain
[b] Universität Hamburg, Department of Informatics, Vogt-Kölln-Strasse 30, D-22527 Hamburg, Germany
[c] IIIA-CSIC, E-08193 Bellaterra, Catalonia, Spain

Available online 30 January 2007

Abstract

Since the turn of the century, smart card technology has pushed its borders both on the high end to integrate new functionalities (e.g., networking) and on the low end to adapt to new constrained environments (e.g., radio-frequency identification). This has required changes in the hardware, software and cryptography underpinning smart cards. This special issue covers some of these developments in depth.

Keywords: Smart cards; Smart devices; Network smart cards; Radio-frequency identification; Cryptographic primitives; Cryptographic protocols; Authentication

1. Introduction

Smart card technology has evolved a long way since the idea of using plastic cards to carry microelectronic chips was patented back in 1968 by Dethloff and Grötrupp. In July 2001, a special issue of *Computer Networks* was devoted to smart cards [1], with the purpose of surveying the key issues and solutions that had turned smart cards into full fledged computers (with or without a plastic card around the microchip). Since the turn of the century, another qualitative jump has occurred and smart cards have become *smart devices*, in the sense that they have conquered new application fields related to pervasive computing. On the high end, network smart cards have appeared which integrate networking capabilities; on the low end, smart cards have transformed into radio-frequency identification (RFID) tags.

This special issue of *Computer Networks* contains one invited article and seven contributed articles selected by anonymous review from the submissions received. Altogether, these papers cover key issues and research underpinning the aforementioned expansion of smart cards. The topics of the papers are cryptographic primitives, network smart cards, RFID protocols and other smart-card based protocols. Our intention as guest editors was not to give comprehensive coverage of the field, but to gather articles that provide readers with in-depth understanding of what the state of the art is, and what the future real-life impact of smart devices is likely to be.

* Corresponding author. Tel.: +34 977558270; fax: +34 977559710.
E-mail addresses: josep.domingo@urv.cat (J. Domingo-Ferrer), posegga@informatik.uni-hamburg.de (J. Posegga), francesc.sebe@urv.cat (F. Sebé), vtorra@iiia.csic.es (V. Torra).

1389-1286/$ - see front matter
doi:10.1016/j.comnet.2007.01.007

2. Cryptographic algorithms

The invited article "A survey of recent developments in cryptography for smart cards", by Preneel, presents an update on recent advances in cryptographic algorithms relevant for smart cards. In particular, it reviews hash functions, block ciphers, stream ciphers and authenticated encryption. Later in the paper, secure padding for the RSA algorithm is discussed in some detail. Finally, an update on Elliptic Curve Cryptography is given.

3. Network smart cards

The communications standards of current smart cards are inadequate to ensure their successful integration in the Internet world. Turning smart cards into network devices is therefore a challenge and a line of progress for high-end smart cards. This special issue features two papers on this subject.

The article "Network smart card review and analysis", by Lu, reviews the progress made by research on network smart cards. It then analyzes and compares various networking options for these devices. Furthermore, an outline is provided for the technical challenges that remain to be solved before smart cards can effectively couple with Internet computing.

In "Advances in network smart card authentication", by Torres et al., the authentication implications of using smart cards as network devices are examined. Traditionally, the role of smart cards in the authentication process has been one of simple hardware tokens connected to a larger, networked device (e.g., PC, teller machine, etc.). Directly plugging the smart card into the network changes the authentication scenario and results in new requirements and threats.

3.1. RFID protocols

Low-end smart cards have a brilliant future as RFID tags. The main challenge here is to offer reasonable security and privacy with lightweight protocols which can be cost-effectively implemented in tags and readers. There are two papers in the issue dealing with RFID protocols.

"HB-MP: A further step in the HB-family of lightweight authentication protocols", by Munilla and Peinado, presents a new authentication protocol called HB-MP which is intended to repair the HB and HB^{+} protocols earlier broken by cryptanalysts. Protocols in the HB-family are especially suitable for RFID systems in which every tag has to be authenticated by the reader.

In addition to authentication of tags by readers, tag privacy is a desirable property of RFID systems if these must be accepted by the citizenship. "A distributed architecture for scalable private RFID tag identification", by Solanas et al., presents a cell-based architecture and a communication protocol whereby readers co-operate to conduct tag identification in a private and scalable way. In this way, a large population of operating tags does not result in unacceptable computing time for private identification of a particular tag by a particular reader.

4. Other smart-card based protocols

The remaining three papers in this special issue describe cryptographic protocols for applications that exploit the tamper-resistance of smart cards.

"Security enhancement of an IC-card-based remote login mechanism", by Cheng et al., describes a repaired version of an earlier remote password authentication scheme using smart cards. The new protocol withstands forgery attacks and provides mutual authentication between a remote server and login users. A time-stamping mechanism is used to prevent replay attacks in which an intruder tries to gain access to a remote server by using a previously intercepted login request.

"Smart card-based agents for fair non-repudiation", by Marín et al., presents a new fair non-repudiation protocol. This kind of protocol is of paramount importance for electronic transactions. A good non-repudiation protocol should work even if the computational power of the parties is substantially different and the communication channel is unreliable. Additionally, it should minimize the involvement of trusted third parties (TTPs). In the new protocol proposed in this paper, the TTP role is played by notary agents executing inside a smart card. Furthermore, the protocol can run on unreliable channels, disconnected from the certification authority, which makes it very attractive for ad hoc networks.

The last paper in this issue, "Secure many-to-one symbol transmission for implementation on smart cards", by Sebé et al., exploits the tamper-resistance of smart cards to provide secure many-to-one transmission from a set of emitting leaves to a receiving root node, where security means confidentiality and authenticity in the leaf-to-root traffic. The method described offers secure and scalable many-to-one communication in a computationally simpler, more

general and more bandwidth-efficient way than previous proposals in the literature. In particular, computation at the leaves is simple enough to be encap- sulated in a smart card, which guarantees suitable protection for the key material held by the leaves.

5. Final remarks

The aim of this issue is to provide insight into the expanding directions of smart card technology. Although most of these new directions are application-driven, the focus is on the technology. We hope the readership will get a view of the current trends and appreciate the potential of smart cards and smart devices in different fields. For further details on current research we recommend the proceedings of the CARDIS conference series; a reference [2] to the proceedings of the most recent edition of the series is given below.

Acknowledgments

We thank the authors for their work and the following people for helping us in reviewing anonymized versions of the submissions received: Asad Ali, Paolo D'Arco, Gildas Avoine, Jordi Castellà, Vanesa Daza, Josep Lluís Ferrer, Christian Floerkemeier, Eiji Okamoto, Heinrich Poehls and François-Xavier Standaert.

References

[1] J. Domingo-Ferrer, P.H. Hartel (Eds.), Current directions in smart cards, Computer Networks, Special issue on smart cards, 36 (4) (2001) 377–379.

[2] J. Domingo-Ferrer, J. Posegga, D. Schreckling (Eds.), Smart Card Research and Advanced Applications-7th IFIP WG 8.8/11.2 International Conference CARDIS'2006, Lecture Notes in Computer Science, vol. 3928, Springer, Berlin, 2006.

Josep Domingo-Ferrer is a Full Professor of Computer Science at Rovira i Virgili University of Tarragona, Catalonia. He received with honors his M.Sc. and Ph.D. degrees in Computer Science from the Autonomous University of Barcelona in 1988 and 1991 (Outstanding Graduation Award). He also holds a M.Sc. in Mathematics. His fields of activity are data privacy, data security and cryptographic protocols. In 2003, he was a co-recipient of a research prize from the Association of Telecom Engineers of Catalonia. In 2004, he got the TOYPS'2004 Award from the Junior Chambers of Catalonia. He has authored three patents and over 170 publications, one of which became an ISI highly cited paper in early 2005. He was the co-ordinator of EU FP5 project CO-ORTHOGONAL and of several Spanish funded and US funded research projects. He has chaired or co-chaired eight international conferences (including two CARDIS conferences) and has served in the program committee of over 42 conferences on privacy and security. He is an Associate Editor of three international journals and has been a Guest Editor of *Computer Networks*, *IJUFKS* and *Data Mining and Knowledge Discovery*. In 2004, he was a Visiting Fellow at Princeton University. He is the Secretary of IFIP WG 8.8 on Smart Cards and he is the founder and chairholder of the forthcoming UNESCO Chair in Data Privacy.

Joachim Posegga received his diploma in Computer Science in 1987 from the University of Kaiserslautern. He then worked for the R&D Division of AEG Informationstechnik and in 1998 he went back to academia (Universities of Edinburgh and Karlsruhe). He earned a Ph.D. from Karlsruhe University in 1993. In 1995 he became a project manager at Deutsche Telekom's Research Organization (FTZ-FI); he was in charge of security projects for mobile networks and in particular working on smartcard technologies like JavaCard. In 2000, he joined SAP Corporate Research and founded their security research program, intitially consisting of a group in Karlsruhe that expanded to SAP Labs France in Sophia Antipolis. The focus of research was security technologies for future e-business systems, in particular for mobile and pervasive applications and for collaborative scenarios. In 2004 he moved to the Department of Computer Science at the University of Hamburg, and became a full professor for Security in Distributed Systems. He is the author of four books in the area of computer science, and numerous scientific papers in journals and conference proceedings; he regularly lectured on security at the universities of Darmstadt, Frankfurt, and Karlsruhe during his career in industry.

Francesc Sebé is a tenure-track Assistant Professor in Telematics Engineering at Rovira i Virgili University of Tarragona. He got his M.Sc. in Computer Engineering from Rovira i Virgili University in 2001 and his Ph.D. in Telematics Engineering from the Polytecnical University of Catalonia, Barcelona, in 2003. He has participated in several European and Spanish funded research projects. He has authored over 40 international publications. His fields of interest are cryptography and information privacy. In 2003, he was a co-recipient of a research prize from the Association of Telecom Engineers of Catalonia. In 2004, he was a visiting researcher at LAAS-CNRS, Toulouse, France.

Vicenç Torra (Barcelona, Catalonia, 1968; B.Sc. 1991, M.Sc. 1992, Ph.D. 1994, all in Computer Science) is an Associate Research Professor at the Artificial Intelligence Research Institute (IIIA-CSIC) near Barcelona, Catalonia. His fields of interest are information fusion tools, in a broad sense, and their application to privacy issues. He has led several research projects funded by Catalan, Spanish, European and U.S. sources. His research has been published in refereed journals (more than 50 articles in ISI JCR journals and LNCS) and major conferences. He has written a book on Artificial Intelligence (in Catalan) and another entitled "Information Fusion and Aggregation Operators" (Springer). He is a member of the editorial board of the Journal of Privacy Technology, Fuzzy Sets and Systems, and Mathware and Soft Computing. In 2004, he was co-founder with Y. Narukawa of the conference series Modeling Decisions for Artificial Intelligence (MDAI), whose successive editions he has co-chaired ever since. He was also a Co-chairman of the Privacy in Statistical Databases conference (PSD 2004).