ELSEVIER

Computer Networks 36 (2001) 377–379

COMPUTER NETWORKS

www.elsevier.com/locate/comnet

Editorial

Current directions in smart cards

Abstract

Smart cards are portable computing devices which are leaving their past role as mere key repositories to become full-fledged computers. This transition has been made possible by recent developments in smart card technology, regarding both hardware and software. This special issue covers some of these developments in depth. © 2001 Elsevier Science B.V. All rights reserved.

Keywords: Smart cards; Java Cards; Electronic cash; Standards; Cryptography; Authentication; Formal methods

1. Introduction

When the idea of using plastic cards to carry microelectronic chips was patented back in 1968 by Dethloff and Grötrupp, probably nobody (not even the inventors) believed that the resulting cards would become smart enough to accommodate real full-fledged computers. Well, this is exactly what is happening today.

This special issue of *Computer Networks* contains seven articles that survey key issues and solutions that support the development of smart card technology, systems and applications. Our intention was not to give comprehensive coverage of the field, but to gather articles that provide readers an in depth understanding of what the state of the art is, and how smart cards can impact their daily life.

Articles in this issue focus on the technology itself rather than on the applications. Indeed, important applications such as GSM (see for example [2]), pay-TV, software protection, etc., would fully justify another special issue and are not dealt with here.

2. Hardware

The first article "From smart cards to smart objects: the road to new smart technologies", by Praca and Barral, is an industry report that describes the current technological limits of smart cards from the hardware standpoint. Innovative solutions that are being developed by the industry to overcome those limits are then reviewed. The conclusion of this article is that hardware technology should not be regarded as a limitation to the expansion and growth of smart cards and their applications.

3. Software

While hardware poses no unsurmountable problems, software for smart cards remains a complicated issue; the latest advances in this field have been oriented to making application development easier, faster, more reliable and more Web-compatible. Java Card technology [1] has been a major step in this direction, allowing cards to be programmed in a subset of Java, known as the Java Card language. The second and third articles in this issue are related to Java Card technology.

"An integrated development environment for Java Card", by Attali et al., describes a Java Card programming environment which is largely generated from formal specifications of the Java Card language; the environment consists of a smart tool set, including a Java Card specific structure editor and a simulator that allows an application to be tested before downloading it to a card.

1389-1286/01/$ - see front matter © 2001 Elsevier Science B.V. All rights reserved.
PII: S1389-1286(01)00160-8

In “Formal specification of the Java Card API in JML: the APDU Class”, by Poll et al., formal specification and verification of Java Card source code are discussed; the specifications presented are suitable for automated software verification by smart tools such as those described in the previous article.

4. Security

The *raison d'être* of smart cards is security in its two flavors: privacy and authentication. In a killer application like GSM, the roles of the SIM are to manage the keys for user authentication and for encryption and decryption of the digitized voice.

The fourth article “Cryptography on smart cards”, by Borst et al., is an overview of the cryptographic primitives that are usually implemented on smart cards; the paper also discusses attacks that can be mounted on smart cards as well as possible countermeasures. Algorithms commonly implemented on cards include block ciphers, message authentication codes, hash functions and some form of asymmetric encryption, typically RSA or elliptic curves; special attention is devoted to the recently proposed Advanced Encryption Standard (AES), of which one of the co-authors is a co-designer. Attacks against smart cards do normally require specialized hardware and are not easy to implement by lay people; however, increasing awareness of their existence can help realizing to what extent can smart cards be considered secure devices.

Authentication in smart cards is of two kinds:

- *User authentication*. The card must recognize that a user is its legitimate owner. This kind of authentication is based on passwords (typically a four-digit Personal Identification Number or PIN) or on biometry, which requires measurement of some physical or behavioral characteristic of the would-be owner.
- *Computer authentication*. A verifying computer is to be convinced that a proving computer is authorized to perform a specific action, i.e., genuinely represents an authorized user. The smart card can play the role of either the verifying or the proving computer, the other computer being an external server or client. This type of authentication is based on cryptographic protocols.

User authentication based on passwords is quite straightforward. Physical and behavioral characteristics measured by biometrical authentication include recognition of iris, retina, vein pattern, face, hand and finger geometry, fingerprint, voice, keystrokes dynamics and handwritten signature dynamics. The goal is to achieve a tradeoff between cost (i.e., measure a characteristic for which sensors are cheap) and security (the chosen characteristic should be unforgeable). However, there is a feeling that biometrics is still an unstable field, where security is not yet well evaluated for all its characteristics; for example, very recently, the very popular and low-cost fingerprint recognition was shown to be easily forgeable [3]. Our choice was to leave biometrical authentication for future special issues and to concentrate on cryptographic computer authentication.

The fifth paper “Cryptographic authentication protocols for smart cards”, by Guillou et al., describes cryptographic protocols for computer authentication. First, symmetrical authentication protocols are considered, i.e., protocols where the verifier knows the secret of the prover or at least an image of it. Then, asymmetrical authentication is dealt with, in which the verifier knows a public key corresponding to a private key (the prover’s secret).

5. E-commerce

One of the basic applications of smart cards is electronic commerce. In this field, smart cards are used as electronic payment instruments and also as enabling devices for wireless communication; both roles are addressed in the sixth article of this issue “E-commerce applications of smart cards”, by M’Raïhi and Yung, E-payments are almost a meta-application, because they underlie other (more visible) applications such as Internet e-commerce or pay-TV. While e-commerce transactions of regular value can be performed using magnetic stripe cards instead of smart cards, low-value transactions are only feasible through smart card-based micropayments. Use of smart cards for wireless communications is another meta-application, which opens the way to m-commerce (mobile e-commerce).

6. Standards

Last but not least, standards are dealt with in the article ‘‘Standards in the smart card world’’, by Husemann. Even if smart cards are no longer a young technology (in fact smart cards are about thirty years old), they are currently a hot topic and this has resulted in a plethora of standards, which may be confusing without the guidance provided in Husemann’s paper. Starting with the ISO 7816 standard, the paper continues with standards for smart card operating systems and then with middleware standards. For operating systems, Java Card, Multos, Windows for smart cards and BasicCard are compared. For middleware, OCF, PC/SC and the hybrid MUSCLE are described.

7. Final remarks

The aim of this issue is to provide a structured insight into the building blocks of smart card technology, rather than focusing on the star applications of it. We hope that readers will get enough knowledge so as to be able to assess the current status and the potential of smart cards. If so, all what is left is to open one’s imagination to new applications that will further boost the technology. For further details on current research we recommend the proceedings of the CARDIS conference series. The most recent edition of the series is mentioned in the references.

Acknowledgements

We thank the authors for their work and Peter Honeyman who was very helpful in assisting in the reviewing task.

References

[1] Z. Chen, Java Card Technology for Smart Cards: Architecture and Programmer’s Guide, Addison-Wesley, Reading, MA, 2000.

[2] S. Guthery, R. Kehr, J. Posegga, How to turn a GSM SIM into a Web Server, in: J. Domingo-Ferrer, D. Chan, A. Watson (Eds.), Smart Card Research and Advanced Applications – Proceedings of IFIP CARDIS’2000, Kluwer Academic Publishers, Dordrecht, 2000, pp. 209–222.

[3] T. van der Putte, J. Keuning, Biometrical fingerprint recognition: don’t get your fingers burned, in: J. Domingo-Ferrer, D. Chan, A. Watson (Eds.), Smart Card Research and Advanced Applications – Proceedings of IFIP CARDIS’2000, Kluwer Academic Publishers, Dordrecht, 2000, pp. 289–303.

Josep Domingo-Ferrer
Department of Computer Engineering and Mathematics, Universitat Rovira i Virgili, Autovia de Salou s/n, E-43006 Tarragona Catalonia, Spain

Pieter Hartel
Department of Computer Science, University of Twente, P.O. Box 217, 7500 AE Enschede, Netherlands
E-mail address: pieter@cs.utwente.nl

Josep Domingo-Ferrer received with honors the M.Sc. and Ph.D. degrees in Computer Science from the Universitat Autònoma de Barcelona, in 1988 and 1991, respectively. He also holds an M.Sc. in Mathematics. Dr. Domingo-Ferrer is currently an Associate Professor at the Universitat Rovira i Virgili, Tarragona, Catalonia. His fields of expertise are data security, cryptography and statistical confidentiality. In these fields, he has authored one patent and over 60 publications, and has won US Government and European Commission research contracts. He has chaired the program committees of *Statistical Data Protection’98* (sponsored by Eurostat) and *IFIP CARDIS’2000* and has served in a number of program committees of IT security conferences. He currently serves as Chairman of the IEEE Information Theory Society Spanish Chapter.

Pieter Hartel received a Doctorate in Computer Science from the University of Amsterdam in 1989. He has worked at CERN in Geneva and the Universities of Nijmegen and Amsterdam (Netherlands), and the University of Southampton (UK). He is currently a full professor at the University of Twente. Dr Hartel consults for IT companies in the USA and in Europe. He has written over 80 publications in the areas of computer architecture, programming language design, formal methods, and security. He is chair and founding member of the IFIP Working Group 8.8 on smart cards.