Lecture Notes in Computer Science 1854

Springer
Berlin
Heidelberg
New York
Barcelona
Hong Kong
London
Milan
Paris
Singapore
Tokyo

Gérard Lacoste Birgit Pfitzmann
Michael Steiner Michael Waidner (Eds.)

SEMPER - Secure Electronic Marketplace for Europe

Springer

Volume Editors

Gérard Lacoste
Compagnie IBM France, Centre d'Etudes et Recherches
Le Plan du Bois, 06610 La Gaude, France
E-mail: lacoste@fr.ibm.com

Birgit Pfitzmann
Universität des Saarlandes, Fachbereich Informatik
Im Stadtwald, 66123 Saarbrücken, Germany
E-mail: pfitzmann@cs.uni-sb.de

Michael Steiner
Michael Waidner
IBM Zurich Research Laboratory
Säumerstrasse 4, 8803 Rüschlikon, Switzerland
E-mail: steiner@acm.org, wmi@zurich.ibm.com

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

SEMPER - secure electronic marketplace for Europe / Gérard Lacoste ...
(ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ;
London ; Milan ; Paris ; Singapore ; Tokyo : Springer, 2000
(Lecture notes in computer science ; Vol. 1854)
ISBN 3-540-67825-5
CR Subject Classification (1998): E.3, C.2, D.4.6, K.4.4, K.6.5, J.1

ISSN 0302-9743
ISBN 3-540-67825-5 Springer-Verlag Berlin Heidelberg New York

SEMPER is part of the European Commission's ACTS Programme (Advanced Communications Technologies and Services). Funding is provided by the partner organisations, the European Union, and the Swiss Federal Department for Education and Science.

Springer-Verlag is a company in the BertelsmannSpringer publishing group.

Printed in Germany

Disclaimer: Some of the systems mentioned in this book may be protected by trademarks, copyrights, or patents. They are the property of their owners.

Typesetting: Camera-ready by author
Printed on acid-free paper SPIN: 10722159 06/3142 5 4 3 2 1 0

Foreword

Some years ago, businesses could choose whether to migrate to electronic commerce, however, today it seems they have no choice. Predictions indicate that companies that do not make the necessary changes will be overrun by competition and ultimately fail. Therefore, we see more and more companies undergoing tremendous transformation in order to adapt to the new business paradigm. At the same time new companies are being established. One thing these companies have in common is the increased dependency on security technology. The invention of electronic commerce has changed the role of security technologies from being merely a protector to being also an enabler of electronic commerce, and it is clear that the development of security technology is a key enabler in the growth and deployment of electronic commerce. This has been recognised at European level (European Union 1997e).

The launch of a comprehensive EU policy in the area of security in open networks is fairly recent with the adoption of a Communication on cryptography in October 1997 (European Union 1997c). A very important complement and support to the European policy is the European Commission's contribution to overcome technological barriers by giving special importance to R&D (Research and Development) activities.

The *SEMPER* project was launched in September 1995 and was funded partly by the European Community within the *Advanced Communication Technologies and Services* (ACTS) specific research programme part of the Fourth Framework Program (1994-1998). In this book the *SEMPER* project team presents in a coherent, integrated, and readable form the issues addressed, the motivation for the work carried out, and the key results obtained.

SEMPER is an innovative project in several aspects. What really makes it innovative and impressive is the integration of the following components into an overall security framework for electronic commerce:

- *SEMPER* is the first project aiming at securing electronic commerce as a whole by developing a technical security framework realised as a middleware. This brings forward two advantages. First, such a technical security framework supports multiple business scenarios by providing powerful security services to applications implementing the business processes. A novelty compared to other security middleware is the provision of security mechanisms through a more commerce-oriented application programming

interface. Second, the development environment shields application designers from the security implementation details and their evolution over time.
- *SEMPER* provides an open security platform which can be configured with relevant modules in order to cope with national regulations.
- A trustworthy user interface, TINGUIN, which ensures that users can securely manage information. TINGUIN provides a single point of interaction between users and their secure platform. Such a single interface is essential to ensure users' consistent perception of their security.
- *SEMPER* has proposed a legal framework for establishing legal predictability of electronic commerce. An interesting result is the adaptation of the technical and legal frameworks to each other by enabling the user's tools to visualize important legal aspects and to manage legal parameters.

The results in this book constitute a major contribution to the development of secure electronic commerce and the work presented has set the scene for future directions in secure electronic commerce. The last chapter of the book highlights some open problems related to the work done by the project. However, many more exist and there is still a lot to be done before the goal of secure electronic commerce will be reached. This has been recognised at European level, and the security-related R&D activities will be intensified under the new 5th Framework Program (1998–2002). Within the 5th Framework Program, the Information Society Technology (IST) Programme addresses the technologies of the online world.

Everyone interested in investigating the state of the art and future directions for secure electronic commerce should find this book extremely valuable and it is without any reservation that I strongly recommend it.

May 2000

Spyros Konidaris
European Commission
Director a.i. – DG XIII-F

Preface

Since the invention of the World-Wide Web (WWW) in 1991, Internet-based electronic commerce has been transformed from a mere idea into reality. Customers browse through catalogues, search for best offers, order goods, and pay for them electronically. Information services can be subscribed online, and many newspapers and scientific journals are readable via the Internet. Most financial institutions have some sort of online presence, allowing their customers to access and manage their accounts, make financial transactions, trade stocks, and so on. Some countries already support filing tax declarations electronically. Electronic mails are exchanged within and between enterprises and often already replace fax copies. Soon there will be no enterprise left without some Internet presence, if only for advertisement reasons. In early 1998 more than 2 million web servers were connected to the Internet, and more than 30 million host computers (Zakon 1998). Internet business is estimated to have reached \$50 to \$100 billion in 1998, mostly in business-to-business trade, and continues to increase at a high rate of growth (Henry, Cooke, Buckley, Dumagan, Gill, Pastore, and LaPorte 1999).

Thus, doing some electronic business on the Internet is already an easy task. As is cheating and snooping. Several reasons contribute to this insecurity. The Internet does not offer much security per se. Eavesdropping and acting under false identity is simple. Stealing data is undetectable in most cases. Popular PC operating systems offer little or no security against viruses and other malicious software, which means that users cannot even trust the information displayed on their own screens. At the same time, user awareness of security risks is threateningly low.

The only well-accepted security tool for the World-Wide Web is the Secure Sockets Layer protocol (SSL), which provides a secure pipe between web client and web server (Freier, Karlton, and Kocher 1996). It cannot generate signed messages or signed receipts, which naturally makes it unsuitable to tasks like electronic online payments and contract signing. And even for SSL, the problem of *visualizing* security to the user is unsolved: most WWW browsers only distinguish between “secure” and “insecure” connections, but do not tell the users in a simple way with *whom* exactly they are communicating over an established “secure” channel.

Such user interface problems are amplified by the fact that today's electronic-commerce systems offer little support in maintaining consistency in data and security among the different parts of a business process. As in the paper world, users have to fill in the same data again and again, copy data on several forms, accumulate data from different transactions by hand, and so on. More problems are revealed if one looks at the legal aspects: often it is not clear—or not even decided—who bears liability and which country's law is applicable in a specific situation.

In 1994 we, the *SEMPER* consortium, came up with the idea that all these security problems could best be solved by grouping all necessary security technologies under a coherent and open software framework, and a single, consistent user interface. Such a framework should allow automatic linking of parts of a business process. Necessarily, it should support not only secure communication and payments, but also the negotiation of business and security parameters, fair exchange of documents (as in contract signing and certified mail), handling of disputes among the parties, etc. Besides keeping data confidential, it should also grant its users some degree of anonymity and unobservability—like users on physical marketplaces can act anonymously. All this should be based on requirements from the market, and should be consistent with the legal systems.

The idea was turned into a proposal to the European Commission, with the result that we started work on implementing this idea in September 1995. We concluded the project early 1999. Some partners are currently exploiting parts of *SEMPER*, but we also aim at more complete use of the framework in successor projects and products. This book summarizes our main results.

Part I gives an overview of our solutions, i.e., the technical framework and a proposal how to tackle the open legal questions. This part is intended to be readable by everyone, i.e., it does not presuppose a specific technical background except some basic familiarity with the Internet.

Part II covers topics for which fundamentally new scientific or engineering results were obtained, and looking at them in detail would be beneficial to everybody working in the field. See the introduction of Part II for more details.

The results of *SEMPER*, including the full architecture, prototype description, and results from expert surveys and trial evaluations, are documented in a number of public, formal deliverables. These are available online from `http://www.semper.org`, or by writing to: IBM Zurich Research Laboratory, Computer Science Department/Project *SEMPER*, Säumerstrasse 4, CH-8803 Rüschlikon, Switzerland.

May 2000

Gérard Lacoste
Birgit Pfitzmann
Michael Steiner
Michael Waidner

Authors of this report: Part I was written, based on the results of the entire project, by *Birgit Baum-Waidner, Gérard Lacoste, Birgit Pfitzmann, Michael Steiner, Michael Waidner,* and *Arnd Weber*. Chapter 5 was written by *Michael Waidner*. Chapter 6 was written by *N. Asokan, Birgit Baum-Waidner, Torben P. Pedersen, Birgit Pfitzmann, Matthias Schunter, Michael Steiner,* and *Michael Waidner*. Chapter 7 was written by *Dale Whinnett* and *Reinder Wolthuis*. Chapter 8 was written by *Akis Hamamtzoglou, Thomas Hecht, Giannis Papadopoulos,* and *Arnd Weber*. Chapter 9 was written by *Rolf Michelsen, Stig Mjølsnes, Petros Pantis,* and *Kostas Tzelepis*. Chapter 10 was written by *Matthias Schunter*. Chapter 11 was written by *N. Asokan* and *Michael Steiner* and is based on (Abad-Peiro, Asokan, Steiner, and Waidner 1998; Asokan 1998; Asokan, Herreweghen, and Steiner 1998). Chapter 12 was written by *Maria Gatziani, Torben P. Pedersen,* and *Kambiz Zangeneh*. Chapter 13 was written by *Birgit Baum-Waidner*. Chapter 14 was written by *Birgit Baum-Waidner* and *Rita Zihlmann*. Chapter 15 was written by *Michael Waidner*.

People and organizations who contributed to *SEMPER*: *Fabrice Clerc, Philippe Magliulo, Marc Mazoué,* and *Marie-Jo Revillet* from CNET - France Télécom. *Holger Erichsen* and *Bernd Horsch* from the Commerzbank. *Bjarke Dahl Ebert, Maria Gatziani, Peter Landrock, Kim Lueders-Jensen, Timmy G. Madsen, Jesper Drud Nielsen, Thomas Sepstrup Nielsen,* and *Torben P. Pedersen* from Cryptomathic. *Paul Dinnissen, Berry Schoenmakers,* and *Bryce Wilcox* from Digicash. *Akis Hamamtzoglou, John Katakis, Sophia Koutsoukou, Dimitrios Livas,* and *Giannis Papadopoulos* from EUROCOM EXPERTISE. *Christoph Baert, John Schey,* and *John West* from Europay International. *Michael Ehrl, Thomas Hecht,* and *Ralf Kuron* from FOGRA Forschungsgesellschaft Druck e.V.. *Horst Ehmke, Matthias Enzmann, Rüdiger Grimm, Tobias Himstedt, Basawarai Patil, Wolfgang Putz,* and *Kambiz Zangeneh* from the Forschungszentrum Informationstechnik mbH (GMD). *Jean-Marie Blanchère, Sylvain Cornillon, Gerard Lacoste, Philippe Leblanc, Jean-Pierre Le Heiget,* and *Christian Navarro* from IBM France, Centre d'Études et Recherches; *Ulrich Einig, Karsten Riede,* and *Christian Thiel* from IBM Heidelberg; *Jose L. Abad-Peiro, N. Asokan, Andreas Fleuti, Ceki Gülcü, Günter Karjoth, Ferdinando Loiacono, Mehdi Nassehi, Thomas Schweinberger, Michael Steiner, Els van Herreweghen,* and *Michael Waidner* from IBM Research, Zürich. *Petros Pantis, Maria Tsakali,* and *Kostas Tzelepis* from INTRACOM. *Sylvain Cornillon, Sharon Prins, Jako Swanenburg, Matthijs de Vries,* and *Reinder Wolthuis* from KPN Research Netherlands. *D.M.A. Schaap* from MARIS. *Mathias Flenker, Stefan Liesem, Christian Petersen,* and *Ingo Saleck* from Otto Versand. *Mogens Rom Anderson, Birgit Baum-Waidner, Klaus Becker, Felix Jaggi, Thomas Mittelholzer, Armin Müller, Claus Rasmussen, Rainer Rueppel, Bruno Wildhaber,* and

Rita Zihlmann from Entrust/r3 security engineering ag. *Rolf Michelsen* and *Stig Frode Mjølsnes* from SINTEF Telecom and Informatics. *Peter Bosch, Dick Bulterman, Ray Hirschfeld, Jaap Henk Hoepman, Sjoerd Mullender,* and *Louis Salvail* from the Stichting Mathematisch Centrum (CWI). *Matthias Schunter* from the Universität Dortmund. *Ingo Pippow, Jan Reichert, Arnd Weber,* and *Dale Whinnett* from the Universität Freiburg, Institut für Informatik und Gesellschaft. *Birgit Pfitzmann* and *Matthias Schunter* from the Universität Hildesheim, Institut für Informatik. *Tom Beiler, Jürgen Brauckmann, Lothar Fritsch, Birgit Pfitzmann,* and *Matthias Schunter* from the Universität des Saarlandes, Saarbrücken, Fachbereich Informatik. Sponsoring partners of *SEMPER* were Banksys (Belgium), Banque Générale du Luxembourg (Luxembourg), Enyca (Spain), and Telekurs/Payserv (Switzerland). The project was led by IBM.

The following organisations provided the infrastructure for the *SEMPER* trials: in France: ACRI, Actimedia, Centre d'Études et Recherches IBM France, Centre International de Communications Avancées, France-Télécom, and IDATE; in Germany: Commerzbank, FOGRA Forschungsgesellschaft Druck e.V., Forschungszentrum Informationstechnik mbH (GMD), Gesellschaft für Zahlungssysteme (GZS), Otto Versand, Universität Freiburg, Institut für Informatik und Gesellschaft, and Universität des Saarlandes, Saarbrücken, Fachbereich Informatik; in Greece: EUROCOM EXPERTISE; in The Netherlands: KPN Research, MARIS, and Stichting Mathematisch Centrum (CWI); in Switzerland: IBM Research, Zürich; in the UK: Oil and Gas Product Library Ltd. (OPL); in the USA: GTE; and the members of the MOMENTS consortium.

SEMPER was part of the Advanced Communication Technologies and Services (ACTS) research program established by the European Commission for 1994-1998, and received funding under contract *AC026* from the European Commission DGXIII and the Swiss Bundesamt für Bildung und Wissenschaft.

Acknowledgments: Interesting discussions with several people outside the consortium helped us to develop and to refine the ideas presented in this book. In particular, we would like to thank *Alain André, Patrick Aubry, Ali Bahreman, Philippe Bardet, Annarosa Baum, Joachim Biskup, Jay Black, Michel Bosco, Peter Büttner, Mario Campolargo, David Chaum, Anne Clarke, Marc Dacier, Michel Dauphin, Michel Fossaert, Renaud di Francesco, Michel Frenkiel, Philippe Garnesson, Mark Greene, Phil Janson, Spiros Konidaris, Jens Kristensen, Philippe Lefevbre, Karine Lieres, Mark Linehan, Jean-Pierre Meyer, Refik Molva, François Montagner, Kostas Papanikolaou, Peter de Rooij, Paul Rottier, Jukka Salo, Boris Saulnier, Tom Scanlan, Julia Sime, Hansrudolf Thomann, Paul Timmers, Gene Tsudik, Joep Van de Veer, Pierre Vannel, Hans-Dieter Zimmermann, and Rosalie Zobel.*

Table of Contents

Part I. The Vision of *SEMPER*

Part II. Project Achievements