Norbert Pohlmann
Helmut Reimer
Wolfgang Schneider

ISSE/SECURE 2007
Securing Electronic Business Processes

Norbert Pohlmann
Helmut Reimer
Wolfgang Schneider

ISSE/SECURE 2007 Securing Electronic Business Processes

Highlights of the Information Security Solutions Europe/SECURE 2007 Conference

With 140 illustrations

vieweg

Bibliographic information published by Die Deutsche Nationalbibliothek
Die Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data is available in the Internet at <http://dnb.d-nb.de>.

Many of designations used by manufacturers and sellers to distinguish their products are claimed as trademarks.

1st edition 2007

Editorial office: Günter Schulz / Andrea Broßler

Vieweg is a company of Springer Science+Business Media.
www.vieweg.de

Cover design: Ulrike Weigel, www.CorporateDesignGroup.de
Typesetting: Oliver Reimer, Ilmenau
Printing and binding: MercedesDruck, Berlin
Printed on acid-free paper
Printed in Germany

ISBN 978-3-8348-0346-7

Contents

Preface ______ xi

About this Book ______ xiii

Welcome ______ xv

Microsoft: A Trustworthy Vision for Computing ______ xvii

Legal, Technical and Social Aspects of Security ______ 1

Regulating Information Security: A Matter of Principle? ______ 3
Andreas Mitrakas · Silvia Portesi

ISTPA Operational Analysis of International Privacy Requirements ______ 18
John T. Sabo

The Legal Conflict between Security and Privacy in Addressing Crime and Terrorism on the Internet ______ 26
Murdoch Watney

Data Encryption on File Servers ______ 38
Janusz Gebusia

Setting up an Effective Information Security Awareness Programme ______ 49
Dirk De Maeyer

Saferinternet.pl Project – Educational Activities for Internet Safety in Poland 59
Anna Rywczyńska · Agnieszka Wrzesień

Is Cyber Tribalism Winning Online Information Warfare? ______ 65
Godfried Williams · Johnnes Arreymbi

Phishing Across Interaction Channels: Methods, Experience and Best Practice ______ 73
Philip Hoyer

IT-Security Beyond Borders – an Assessment of Trust Levels Across Europe 82
Christian Wernberg-Tougaard

Analyzing and Improving the Security of Internet Elections ______ 93
Adam Wierzbicki · Krzystof Pietrzak

Remote Access Mechanics as a Source of Threats to Enterprise Network Infrastructure ______ 102
Paulina Januszkiewicz · Marek Pyka

“Private Investigation” in the Computer Environment: Legal Aspects ______110
Arkadiusz Lach

Identity, Information Security and Rights Management ____ 115

Design Rationale behind the Identity Metasystem Architecture______117
Kim Cameron · Michael B. Jones

Federated ID Management – Tackling Risk and Credentialing Users ______ 130
Marc Speltens · Patrick Patterson

Information Security Governance for Executive Management ______ 136
Yves Le Roux

Model Driven Security for Agile SOA-Style Environments ______ 147
Ulrich Lang · Rudolf Schreiner

The Business Perspective on Roles Including Root Causes of Implementation Problems ______ 157
Marc Sel

A Security Architecture for Enterprise Rights Management______ 166
Ammar Alkassar · Rani Husseiki · Christian Stüble · Michael Hartmann

Rights Management Technologies: A Good Choice for Securing Electronic Health Records? ____ 178
Milan Petković · Stefan Katzenbeisser · Klaus Kursawe

Case Studies from Fuzzing Bluetooth, WiFi and WiMAX ____ 188
Sami Petäjäsoja · Ari Takanen · Mikko Varpiola · Heikki Kortti

Evaluation of the Possible Utilization of anti-spam Mechanisms Against spit 196
Christian Dietrich · Malte Hesse

Modeling Trust Management and Security of Information ____ 207
Anna Felkner · Tomasz Jordan Kruk

Smart Tokens, eID Cards, Infrastructure Solutions and Interoperability ____ 217

Infrastructure for Trusted Environment: In Search of a Solution____ 219
Claire Vishik · Simon Johnson · David Hoffman

Integrity Check of Remote Computer SystemsTrusted Network Connect ___ 228
Marian Jungbauer · Norbert Pohlmann

Technical Guidelines for Implementation and Utilization of RFID-based Systems____ 238
Cord Bartels · Harald Kelter

High Density Smart Cards:New Security Challenges and Applications _____ 251
Helena Handschuh · Elena Trichina

ID Cards in Practice ____ 260
Detlef Houdeau

Large Scale Fingerprint Applications: Which Technology Should be Used? _ 266
Andreas M. Wolf

From the eCard-API-Framework Towards a Comprehensive eID-Framework for Europe ______ **276**
Detlef Hühnlein · Manuel Bach

Making Digital Signatures Work across National Borders ______ **287**
Jon Ølnes · Anette Andresen · Leif Buene · Olga Cerrato · Håvard Grindheim

Financial Fraud Information Sharing ______ **297**
Sharon Boeyen

Enterprise Key Management Infrastructure ______ **306**
Arshad Noor

Intrinsic Physical Unclonable Functions in Field Programmable Gate Arrays ______ **313**
Jorge Guajardo · Sandeep S. Kumar · Klaus Kursawe · Geert-Jan Schrijen · Pim Tuyls

Security Evaluation and Testing – Past, Present and Future ______ **322**
Peter Fischer

Economics of Security and PKI Applications ______ 329

Managing Information Security in Small and Medium Sized Enterprises: A Holistic Approach ______ **331**
Anas Tawileh · Jeremy Hilton · Stephen McIntosh

EKIAS – Success Criteria of PKI Implementations ______ **340**
Anja Beyer · Sophie Hellmann · Malte Hesse · Friedrich Holl · Peter Morcinek · Sachar Paulus · Helmut Reimer

Embedded PKI in Industrial Facilities ______ **347**
Marcus Hanke

SIM-enabled Open Mobile Payment System Based on Nation-wide PKI ______ **355**
Elena Trichina · Konstantin Hyppönen · Marko Hassinen

Evidence Record Syntax ______________________________________ **367**
Tobias Gondrom

PKI and Entitlement ____ **376**
Guido v. d. Heidt · Reinhard Schoepf

Future Diffusion of PKI-Technology – A German Delphi Study ___________ **386**
Michael Gaude

The Introduction of Health Telematics in Germany ____________________ **396**
Dirk Drees

The German Identity Card – Concepts and Applications ________________ **401**
Andreas Reisen

Infrastructures for Identification and Identity Documents _______________ **405**
Walter Landvogt

The Security Infrastructure of the German Core Application in Public Transportation____**411**
Joseph Lutgen

Applications of Citizen Portals __________________________________ **419**
Hannes Ziegler

Virtual Post Office in Practice __________________________________ **427**
Wilhelm Weisweber · Frank Planitzer

Index ____ **437**

Preface

ENISA is proud to be working with eema, TeleTrusT, NASK (the Polish research and development organization and leading Polish data networks operator) and the German Federal Ministry of the Interior as well as the German Federal Office for Information Security for this year's 9th annual Information Security Solutions Europe Conference.

The aim of the ISSE has always been to support the development of a European information security culture and especially a cross-border framework for trustworthy IT applications for citizens, industry and administration. ENISA is committed to these goals. In our work we assist and advise the European Commission, Member States as well as business community on network and information security as well as on legislative requirements, and we are delighted to support the ISSE again this year.

The security of communication networks and information systems is of increasing concern. In order to face today's complex information security challenges it is clear that working collaboratively with one another is the key to generating new strategies to address these problems. It has been an exciting opportunity to facilitate this collaboration at the ISSE 2007, pulling together the wealth of industry knowledge, information and research that we hold in Europe, as well as across the globe.

The success of this event in generating ideas and frank, lively debate around the complex topic of IT security is due also to the independent, varied nature of the programme, which was selected by worldwide specialists in the field.

Some of the key topics explored at this year's conference have been chosen as the basis for this book, which is an invaluable reference point for anyone involved in the IT security industry.

We hope that you will find it a thought-provoking and informative read.

Andrea Pirotti

Andrea Pirotti, Executive Director, ENISA

About this Book

The Information Security Solutions Europe Conference (ISSE) was started in 1999 by eema and TeleTrusT with the support of the European Commission and the German Federal Ministry of Technology and Economics. Today the annual conference is a fixed event in every IT security professional's calendar.

The integration of security in IT applications was initially driven only by the actual security issues considered important by experts in the field; currently, however, the economic aspects of the corresponding solutions are the most important factor in deciding their success. ISSE offers a suitable podium for the discussion of the relationship between these considerations and for the presentation of the practical implementation of concepts with their technical, organisational and economic parameters.

From the beginning ISSE has been carefully prepared. The organisers succeeded in giving the conference a profile that combines a scientifically sophisticated and interdisciplinary discussion of IT security solutions while presenting pragmatic approaches for overcoming current IT security problems.

An enduring documentation of the presentations given at the conference which is available to every interested person thus became important. This year sees the publication of the fifth ISSE book – another mark of the event's success – and with about 50 carefully edited papers it bears witness to the quality of the conference.

An international programme committee is responsible for the selection of the conference contributions and the composition of the programme:

- **Ronny Bjones,** Microsoft (Belgium)
- **Gunter Bitz,** SAP (Germany)
- **Lucas Cardholm,** Ernst&Young (Sweden)
- **Roger Dean,** eema (UK)
- **Ronald De Bruin,** ENISA
- **Jan De Clercq,** HP (Belgium)
- **Marijke De Soete,** NXP Semiconductors (Belgium)
- **Jos Dumortier,** KU Leuven (Belgium)
- **Walter Fumy,** Siemens (Germany)
- **Michael Hange,** BSI (Germany)
- **John Hermans,** KPMG (The Netherlands)
- **Jeremy Hilton,** Cardiff University (United Kingdom)
- **Frank Jorissen,** SafeBoot (Belgium)
- **Matt Landrock,** Cryptomathic (Denmark)

- **Mirosław Maj,** CERT Polska (Poland)
- **Tim Mertens,** ENISA
- **Attila Péterfalvi,** Parliamentary Commissioner for Data Protection and Freedom of Information (Hungary)
- **Norbert Pohlmann,** University of Applied Sciences Gelsenkirchen, Chairman of the Programme Committee (Germany)
- **Bart Preneel,** KU Leuven (Belgium)
- **Helmut Reimer,** TeleTrusT (Germany)
- **Joachim Rieß,** Daimler Chrysler (Germany)
- **Paolo Rossini,** TELSY, Telecom Italia Group (Italy)
- **Wolfgang Schneider,** Fraunhofer Institute SIT (Germany)
- **Jon Shamah,** CoreStreet (UK)
- **Krzysztof Silicki,** NASK (Poland)
- **Robert Temple,** BT (United Kingdom)

The editors have endeavoured to allocate the contributions in these proceedings – which differ from the structure of the conference programme – to topic areas which cover the interests of the readers.

Norbert Pohlmann *Helmut Reimer* *Wolfgang Schneider*

eema (www.eema.org):

Established in 1987, eema is an independent association of IT professionals, businesses and governments providing business and technical networking opportunities at both local and regional levels in the broad areas associated with e-Identity and its related applications, such as security. Our mission is to stimulate the growth and effectiveness of our members' business in these areas through increased market awareness, cooperation and opportunity creation.

We aim to bring our 1,500 member representatives together in a neutral environment for education and networking purposes. We enable members to share experiences and best practice by holding meetings and conferences, by facilitating working groups who produce reports on topical subjects, and by helping members to connect with the right person to help them solve business issues or develop beneficial business relationships. All work produced by members is available free to other members, and previous papers include: Towards Understanding Identity, Role Based Access Control – a Users Guide, Secure e-mail within a Corporate Environment and Secure e-mail between Organisations.

Contact: Roger Dean
Executive Director of eema
roger.dean@eema.org

TeleTrusT Deutschland e.V. (www.teletrust.de)

TeleTrusT Deutschland e.V. was founded in 1989 as a non profit association promoting the trustworthiness of information and communication technology in open system environments. Today, TeleTrusT counts more than 80 institutional members. Within the last 17 years TeleTrusT evolved into a well known and highly regarded competence network for applied cryptography and biometrics.

In the various working groups of TeleTrusT ICT-security experts, users and interested parties meet frequently at workshops, round-tables and expert talks. The activities focus on reliable and trustworthy solutions complying with international standards, laws and statutory requirements. TeleTrusT is keen to promote the acceptance of solutions supporting identification, authentification and signature (IAS) schemes in electronic business.

TeleTrusT facilitates the information and knowledge exchange between vendors, users and authorities., This helps innovative ICT-security solutions to enter the market more quickly and effectively. TeleTrusT aims to create standard compliant solutions in interoperable schemes.

Keeping in mind the growing importance of the European security market, TeleTrusT seeks the co-operation with European organisations and authorities with similar objectives. Thus, the European Security Conference ISSE is organised in collaboration with eema, ENISA and NASK this year.

Contact: Dr. Günther Welsch
Managing Director of TeleTrusT Deutschland e.V.
guenther.welsch@teletrust.de

Welcome

We are honoured to be hosting and co-organising this year`s ISSE/SECURE 2007 Conference in Warsaw.

As Minister of Interior and Administration, I am responsible for the development and diffusion of Information Technology in Poland, especially for implementing e-Administration and for the development of the Information Society.

Aware of the increasing concern for ICT in all the fields of economic and social activity, the Ministry of Interior and Administration plays a highly active role in legislation, strategy development as well as projects implementation.

A high priority has been given to projects aimed at higher personal data protection and secure electronic systems in public administration. As an example, the Electronic Platform of Public Administration Services project provides for a single platform with e-services of public administration for citizens and businesses. One of its tasks will be to provide public administration with common tools for user's authorization and certification.

The Ministry also took over the competences concerning digital signature implementation in reason of activities strongly related to its policy lines concerning implementation of eID and registers security for the forthcoming public e-services.

The Ministry of Interior and Administration's concern for ISSE/SECURE 2007 conference is an excellent prove of its deep interest for issues concerning the European information security challenges.

We look forward to create a good field for effective transfer of ideas, knowledge and best practices among policy makers, experts in ICT security and industrials.

Władysław Stasiak
Minister of Interior and Administration

Microsoft: A Trustworthy Vision for Computing

The continually evolving computing landscape of today has two primary macro-level developments: more people and businesses rely on computing every day, and the threats that can undermine trust in computing are increasingly sophisticated and malicious.

From the customer's perspective, it is increasingly important that sensitive data are protected, that software businesses adhere to business practices that promote trust with users, and that the technology industry renews its focus on solid engineering and best practices to ensure the delivered product or service is more reliable and secure.

Microsoft's approach to this environment is Trustworthy Computing (TwC), a long-term, collaborative effort to create and deliver secure, private, and reliable computing experiences for everyone. Microsoft formed TwC in January 2002, when Bill Gates committed the company to fundamentally changing its mission and strategy in the key areas of Security, Privacy, Reliability, and Business Practices.

TwC's five-year milestone seems an appropriate time to examine our efforts to date and to affirm the promise of TwC. What follows is an update on some of the things we're doing to ensure that customers can count on every one of our new and exciting innovations.

Pricacy

Microsoft is working with policymakers and industry leaders in the United States to encourage federal laws that establish baseline privacy protections for consumers while still allowing commerce to flourish. And, since privacy threats know no borders, we're also working with governments around the world to make privacy laws as consistent as possible.

Security

Microsoft works closely with other software vendors, the research community and security companies to find better ways to build more secure software, locate vulnerabilities, collaboratively address issues as they arise, and establish best practices across the industry. We partner with law enforcement worldwide to help find and catch individuals who write and distribute malicious software. And, when a new issue threatens customers, our Security Response Center mobilizes teams to investigate, fix and learn from security vulnerabilities. We continue to release security updates on a regular schedule.

Reliability

Over the past few years, we‘ve made great progress in improving the reliability of our products, as well as other software built on our platform, through continuous improvement technologies – software that can diagnose, report, and fix problems as they arise. For example, the error-reporting features in Microsoft Office 2007 perform thorough diagnostics when applications hang or crash, including checking the computer‘s hard disk and memory and verifying that the customer‘s software is up-to-date and uncorrupted. It can dynamically keep track of system resources, and help avoid performance and reliability issues when running a large number of applications.

Looking Ahead

Microsoft has spent the past five years working to transform the company around TwC, and it has improved by an order of magnitude in each of the areas noted above. But, there‘s still plenty of work to do. We‘ve only tapped a fraction of computing‘s vast potential, and the coming years will continue to bring new innovations that transform how we live and work.

The world of PCs and servers is evolving into a rich web of connected devices and services and computing has become enmeshed into the fabric of our lives. This is why TwC has to do more than address today‘s challenges – it must ensure that the innovations people will rely on tomorrow are designed from the outset to be reliable and secure, respectful of their privacy, and supported by trustworthy and responsive companies.