
ISSE 2014 Securing Electronic Business Processes

Helmut Reimer • Norbert Pohlmann
Wolfgang Schneider (Eds.)

ISSE 2014 Securing Electronic Business Processes

Highlights of the Information Security
Solutions Europe 2014 Conference

Editors

Helmut Reimer
TeleTrusT – IT Security Association
Berlin, Germany

Wolfgang Schneider
Fraunhofer Institute SIT
Darmstadt, Germany

Norbert Pohlmann
Institute for Internet Security
Westfälische Hochschule
Gelsenkirchen, Germany

ISBN 978-3-658-06707-6
DOI 10.1007/978-3-658-06708-3

ISBN 978-3-658-06708-3 (eBook)

The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at <http://dnb.d-nb.de>.

Library of Congress Control Number: 2014952087

Springer Vieweg

© Springer Fachmedien Wiesbaden 2014

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Typesetting: Oliver Reimer, Großschwabhausen

Printed on acid-free paper

Springer Vieweg is a brand of Springer DE.
Springer DE is part of Springer Science+Business Media.
www.springer-vieweg.de

Contents

About this Book _____	xi
SAFECode Whitepaper: Fundamental Practices for Secure Software Development 2nd Edition _____	1
Editor: Stacy Simpson	
Security Management, CISO Inside _____	33
In-House Standardization of Security Measures: Necessity, Benefits and Real-world Obstructions _____	35
Eberhard von Faber	
An Effective Approach for Assessing the Risk of Acquired IT Products _____	49
Eric Baize · Steve Lipner	
IT-Security in Railway Signalling Systems _____	56
Christian Schlehuber · Erik Tews · Stefan Katzenbeisser	
13+ Real Ways to Destroy Business by Breaking Company's SAP Applications __	65
Alexander Polyakov	
Trust Services, eID and Cloud Security _____	79
Achieving the eIDAS Vision Through the Mobile, Social and Cloud Triad _____	81
Francisco Jordan · Helena Pujol · David Ruana	
Security Versus Usability – User-Friendly Qualified Signatures Based on German ID Cards _____	94
Gregor Bühler · Enrico Entschew · Marcel Selhorst	
Using the Semantic Web to Generate Trust Indicators _____	106
Marc Sel	

Cybersecurity, Cybercrime, Critical Infrastructures	121
Hidden and Uncontrolled – On the Emergence of Network Steganographic Threats	123
Steffen Wendzel · Wojciech Mazurczyk · Luca Caviglione · Michael Meier	
Restricting Excessive State-on-State Cyber Espionage under International Law: A Quest of Futility?	134
Murdoch Watney	
Securing Cloud: Elastic Key Management and Homomorphic Encryption	144
Alexander W. Koehler	
Secure Communication and Digital Sovereignty in Europe	155
Norbert Pohlmann · Michael Sparenberg · Illya Siromaschenko · Kilian Kilden	
The need of European White Knights for the TLS/SSL Certificate System	170
Arno Fiedler · Christoph Thiel	
BYOD and Mobile Security	175
Emerging Technologies, Disrupt or be Disrupted	177
Steven Ackx	
Hardware Intrinsic Security to Protect Value in the Mobile Market	188
Vincent van der Leest · Roel Maes · Geert-Jan Schrijen · Pim Tuyls	
On Cross-Border Mobile Government Systems	199
Milan Marković · Goran Đorđević	

Privacy, Data Protection, Human Factors	209
Privacy for Cloud Storage	211
Anders Andersen · Trygve Hardersen · Norbert Schirmer	
Enforcing Data Privacy in the Age of Google Glass	220
Christian Thiel · Christoph Thiel	
Internet of Trucks and Digital Tachograph – Security and Privacy Threats	230
Marc Sel · Dusko Karaklajic	
Regulation & Policies	239
Towards eIDAS as a Service	241
Detlef Hühnlein	
What now? Data Retention Scenarios After the ECJ Ruling	249
Alessandro Guarino	
From Research Results to Strategy: A Mapping Exercise.	256
Michele Bezzi · Frances Cleary · Luca Compagna	
Index	265

About this Book

The Information Security Solutions Europe Conference (ISSE) has been 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 range of topics has changed enormously since the founding of ISSE. In addition to our ongoing focus on securing IT applications and designing secure business processes, protecting against attacks on networks and their infrastructures is currently of vital importance. The ubiquity of social networks has also changed the role of users in a fundamental way: requiring increased awareness and competence to actively support systems security. ISSE offers a perfect platform 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 eleventh ISSE book – another mark of the event's success – and with 22 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:

- **Ammar Alkassar** (TeleTrusT/Sirrix AG)
- **John Colley** ((ISC)²)
- **Marijke De Soete** (Security4Biz)
- **Jos Dumortier** (KU Leuven)
- **Walter Fumy** (Bundesdruckerei)
- **David Goodman** (EEMA)
- **Michael Hartmann** (SAP)
- **Marc Kleff** (Unify)
- **Jaap Kuipers** (Id Network)
- **Patrick Michaelis** (AC – The Auditing Company)
- **Lennart Oly** (ENX)

- **Norbert Pohlmann** (TeleTrusT/Institute for Internet Security – if(is))
- **Bart Preneel** (KU Leuven)
- **Helmut Reimer** (TeleTrusT)
- **Wolfgang Schneider** (Fraunhofer Institute SIT)
- **Marc Sel** (PwC)
- **Jon Shamah** (EEMA/EJ Consultants)
- **Franky Thrasher** (Electrabel)
- **Erik R. van Zuuren** (Deloitte)
- **Claire Vishik** (Intel)

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. With this book TeleTrusT aims to continue documenting the many valuable contributions to ISSE.

Norbert Pohlmann

Helmut Reimer

Wolfgang Schneider

TeleTrusT – IT Security Association Germany

TeleTrusT – IT Security Association Germany TeleTrusT is a widespread competence network for IT security comprising members from industry, administration, research as well as national and international partner organizations with similar objectives. With a broad range of members and partner organizations TeleTrusT embodies the largest competence network for IT security in Germany and Europe. TeleTrusT provides interdisciplinary fora for IT security experts and facilitates information exchange between vendors, users and authorities. TeleTrusT comments on technical, political and legal issues related to IT security and is organizer of events and conferences. TeleTrusT is a non-profit association, whose objective is to promote information security professionalism, raising awareness and best practices in all domains of information security. TeleTrusT is carrier of the “European Bridge CA” (EBCA; PKI network of trust), the quality seal “IT Security made in Germany” and runs the IT expert certification programs “TeleTrusT Information Security Professional” (T.I.S.P.) and “TeleTrusT Engineer for System Security” (T.E.S.S.). TeleTrusT is a member of the European Telecommunications Standards Institute (ETSI). The association is headquartered in Berlin, Germany.

Keeping in mind the raising importance of the European security market, TeleTrusT seeks co-operation with European and international organisations and authorities with similar objectives. Thus, this year’s European Security Conference ISSE is again being organized in collaboration with TeleTrusT’s partner organisation eema and supported by the European Commission.

Contact:

TeleTrusT – IT Security Association Germany
Dr. Holger Muehlbauer
Managing Director
Chausseestrasse 17, 10115 Berlin, GERMANY
Tel.: +49 30 4005 4306, Fax: +49 30 4005 4311
<http://www.teletrust.de>

EEMA

EEMA is a non-profit membership association registered in Brussels. For over 25 years, from the dawn of the digital age, EEMA has helped European companies gain a competitive advantage and make informed technology choices and business decisions. Today it is the place where professionals gather to meet, network and define best practice in the areas of identity management and cybersecurity. EEMA's member representatives are drawn from leading corporate and multi-national end-user organisations, service providers, consultancies, academia, as well as local, national and European governmental agencies

In addition to a regular online newsletter and other information dissemination activities, EEMA benefits its members through conferences, thought leadership seminars and workshops, often in collaboration with partners such as ENISA, OECD, BCS, TDL, LSEC, TeleTrusT, ECP, Chamber of Commerce, CEN/ETSI, Digital Policy, ITU, Alliance, e-Forum, FAIB, FEDICT, IDESG, ISC2, United Nations, Oasis, SANS, SECEUR, GSMA, OIX and the Kantara Initiative. Recent EEMA events include 'Digital Enterprise Europe – Managing Identity for the Future' in London, 'Trust in the Digital World' in Vienna (in partnership with Trust in Digital Life) as well as special interest group meetings on 'Evolution & Future of eSignature & eSeal' and 'Cybersecurity – State of Play' in Brussels.

With its European partners, EEMA also participates in several high profile EU-sponsored projects including STORK 2.0 (Large scale pilot for e-ID interoperability between governments), SSEDIC (Scoping the single European digital identity community), Cloud for Europe (Public sector pre-commercial procurement in the Cloud) and FutureID (Shaping the future of electronic identity).

Visit www.eema.org or contact EEMA directly on +44 1386 793028 or info@eema.org