Volume 1, Issue 1, Spring 2004 http://www.esecurity.ch/communications.html

Contents

1 Editorial

Welcome to the first issue of eSECURITY communications — the official newlsetter of eSECURITY Technologies Rolf Oppliger (`www.esecurity.ch`). As its name suggests, eSECURITY communications serves as a medium of eSECURITY Technologies Rolf Oppliger to talk to its clientele. If you are a customer or want to become one, then you may find it interesting to browse through eSECURITY communications and read some paragraphs.

eSECURITY communications is written in English and published twice a year (spring and fall issues). It is intended to follow a relatively constant structure and layout (and we use the first issues to actually find it).

eSECURITY communications is intended to be interactive. We hope that you are intellectually challenged, that you let us know your opinions and thoughts, and that we are able to publish your responses and counter-statements in future issues of eSECURITY communications accordingly.

In either case, we hope that you enjoy reading this first issue, and that you eventually become a regular reader of eSECURITY communications.

2 News

In October 2003, the eSECURITY logo (as used on the title page of eSECURITY communications) was officially registered as Trademark No. 514774 at the Registry of the Swiss Federal Institute of Intellectual Property.[1]

As its name suggests, we use this column to provide news in future issues of eSECURITY communications. Most of these news will be related to eSECURITY Technologies Rolf Oppliger in one way or another.

3 Publications

All publications of eSECURITY Technologies Rolf Oppliger are itemized on the company's Web site.[2] Some papers are electronically available at this site.

The next major publications will be two articles published in the *Communications of the ACM*. One article is about certified mail and the other article is about IT security professionals in general, and the role of security architects in particular. Furthermore, an introductory book about modern cryptography[3] is scheduled to be published in Artech House's computer security series in May 2005. If you are interested in reviewing and commenting on a preliminary version of the manuscript, then you may contact eSECURITY Technologies Rolf Oppliger in this matter.

In future issues of eSECURITY communications, we will us this column to announce and briefly summarize the new publications of eSECURITY Technologies Rolf Oppliger.

4 Security Analyses

eSECURITY Technologies Rolf Oppliger periodically analyzes the security of products and services and publishes some of the results. We use this column to briefly summarize them.

4.1 E-Voting

Two overview articles about e-voting and its security implications have been published in the *Neue Zürcher Zeitung* (Sonderbeilage Informatik, B3, February 4, 2003) and the *digma* magazine (Vol. 2, No. 4, December 2002, pp. 184–188). Furthermore, a technical paper (entitled "How to Address the Secure Platform Problem for Remote Internet Voting") that elaborates on the client-side security problems of remote Internet voting has been has been presented at the 5th Conference on "Sicherheit in Informationssystemen" (SIS 2002) in October 2002 in Vienna (Austria). The paper is electronically available at the company's Web site.

4.2 Microsoft Outlook Web Access

A security analysis of Microsoft Outlook Web Access is published in the *IEEE IT Professional* magazine (Vol. 5, No. 1, January/February 2003, pp. 27–31). In short, the article argues that Microsoft Outlook Web Access provides an interesting and important functionality (i.e., remote access to an Exchange server's user account), and discuss several possible configurations and its security implications.

4.3 Microsoft .NET Passport

A security analysis of Microsoft .NET Passport is published in the *IEEE Computer* magazine (Vol. 36, No. 7, July 2003, pp. 29–35). In short, the article overviews and discusses the working principles of Microsoft .NET

[1] `www.swissreg.ch/`

[2] `www.esecurity.ch/publications.html`

[3] `www.esecurity.ch/Books/cryptography`

Passport, and addresses some of its shortcomings and limitations from a security perspective.

4.4 Open Source Software

eSECURITY Technologies Rolf Oppliger has elaborated on the question whether open source software is inherently more secure than closed source software and published the corresponding results in a series of articles in the *Neue Zürcher Zeitung* (Sonderbeilage Orbit/Comdex, B15, September 23, 2003) and the *digma* magazine (Vol. 3, No. 3, October 2003, pp. 122–126). Most importantly, a technical report is electronically available[4] and published in the *Datenschutz und Datensicherheit (DuD)* magazine (Vol. 27, No. 11, November 2003, pp. 669–675). We invite you to comment on the theses presented in the report.

5 Computer Security Series

Since 1999, Rolf Oppliger has been the series editor for Artech House's computer security book series.[5] The available and scheduled book titles are enumerated below. You are invited to browse through the list and order the titles that are relevant for you (or your work, respectively). The books are available and can be ordered, for example, through the eSECURITY BOOKSTORE[6] that is operated in association with Amazon.

In future issues of eSECURITY communications, we will use this column to announce and briefly summarize new books that are published in the series.

5.1 Available Books

1. R. Oppliger, *Security Technologies for the World Wide Web*, ISBN 1-58053-045-1, 2000, 444 pp.
2. S. Katzenbeisser and F. Petitcolas (Eds.), *Information Hiding Techniques for Steganography and Digital Watermarking*, ISBN 1-58053-035-4, 2000, 240 pp.
3. V. Hassler, *Security Fundamentals for E-Commerce*, ISBN 1-58053-108-3, 2001, 416 pp.
4. R. Oppliger, *Secure Messaging with PGP and S/MIME*, ISBN 1-58053-161-X, 2001, 332 pp.
5. S. Frankel, *Demystifying the IPsec Puzzle*, ISBN 1-58053-079-6, 2001, 296 pp.
6. D. O'Mahony, M. Peirce and H. Tewari, *Electronic Payment Systems for E-Commerce, Second Edition*, ISBN 1-58053-268-3, 2001, 368 pp.
7. J. Zhou, *Non-repudiation in Electronic Commerce*, ISBN 1-58053-247-0, 2001, 216 pp.
8. M. Caloyannides, *Computer Forensics and Privacy*, ISBN 1-58053-283-7, 2001, 394 pp.
9. V. Hassler, et al., *Java Card for E-Payment Applications*, ISBN 1-58053-291-8, 2002, 382 pp.
10. R. Oppliger, *Internet and Intranet Security, Second Edition*, ISBN 1-58053-166-0, 2002, 430 pp.
11. T.D. Tarman and E.L. Witzke, *Implementing Security for ATM Networks*, ISBN 1-58053-293-4, 2002, 318 pp.
12. U. Lang and R. Schreiner, *Developing Secure Distributed Systems with CORBA*, ISBN 1-58053-295-0, 2002, 332 pp.
13. C. Radu, *Implementing Electronic Card Payment Systems*, ISBN 1-58053-305-1, 2003, 464 pp.
14. R. Oppliger, *Security Technologies for the World Wide Web, Second Edition*, ISBN 1-58053-348-5, 2003, 444 pp.
15. G. Mohay, et al., *Computer and Intrusion Forensics*, ISBN 1-58053-369-8, 2003, 420 pp.
16. D.F. Ferraiolo, D.R. Kuhn, and R. Chandramouli, *Role-based Access Controls*, ISBN 1-58053-370-1, 2003, 338 pp.
17. T. Hardjono and L.R. Dondeti, *Multicast and Group Security*, ISBN 1-58053-342-6, 2003, 334 pp.
18. M. Arnold, M. Schmucker and S.D. Wolthusen, *Digital Watermarking and Content Protection: Techniques and Applications*, ISBN 1-58053-111-3, 2003, 296 pp.
19. J. Nazario, *Defense and Detection Strategies Against Internet Worms*, ISBN 1-58053-537-2, 2003, 318 pp.

5.2 Scheduled Books

1. C. Gehrmann and J. Persson, *Bluetooth Security*, 1-58053-504-6, scheduled for May 2004, approx. 266 pp.
2. C.W. Axelrod, *Outsourcing Information Security*, ISBN 1-58053-531-3, scheduled for September 2004, approx. 272 pp.

[4] `www.esecurity.ch/OpenSourceSecurity.pdf`
[5] `www.esecurity.ch/serieseditor.html`
[6] `www.esecurity.ch/bookstore.html`

3. C. Mitchell, *A User's Guide to Cryptography and Standards*, ISBN 1-58053-530-5, scheduled for October 2004, approx. 404 pp.
4. M. Caloyannides, *Computer Forensics and Privacy, Second Edition*, ISBN 1-58053-830-4, scheduled for October 2004, approx. 296 pp.
5. R. Oppliger, *Introduction to Modern Cryptography*, ISBN 1-58053-642-5, scheduled for May 2005, approx. 500 pp.
6. T. Hardjono and L.R. Dondeti, *Security in Wireless LANs und MANs*, ISBN 1-58053-755-3, scheduled for June 2005, approx. 306 pp.

5.3 Call for Authors

If you are working in a field related to computer security, then you may also be interested in writing and publishing a book in the series. In this case, we invite you to contact either the series editor or the commissioning editor. The coordinates of both editors are available on the series' Web site.[7]

6 Recommended Reading

Security is a hot topic today. Consequently, there are many periodicals and books that are written and published about security-related topics. For example, Artech House's computer security series (see Section 5) comprises such books. Similar series are itemized on the Web.[8]

In future issues of eSECURITY communications, we will use this column to briefly introduce recommended reading that is published outside Artech House's computer security series.

7 Outlook

In this column, we announce lectures, courses, invited talks, and conferences in which eSECURITY Technologies Rolf Oppliger is involved in one way or another.

7.1 University Lectures

In spring and summer 2004, Rolf Oppliger lectures at the University of Zürich on "Sicherheit in der Informationstechnik." The slides are electronically available on the lecture's Web site.[9]

7.2 Courses

A German course (preliminarily entitled "Informatiksicherheit: Grundlagen und Umsetzung in der Praxis") will be organized by the eSECURITY EDUCATION CENTER[10] later this year. The course will last 3 days and take place in Zürich. Please, send an e-mail message at `education@esecurity.ch` if you are interested in participating or getting more information (as soon as it becomes available).

In 2005, the eSECURITY EDUCATION CENTER will organize an introductory course about modern cryptography. If you want to learn more about the current state-of-the-art in cryptography, then this course may provide an interesting source of information for you.

7.3 Invited Talks

On October 26, 2004, Rolf Oppliger will give a talk entitled "Digitale Dokumente: Alte und neue Herausforderungen sowie Lösungsansätze." The talk and a brief summary will be made available on the conference Web site.[11]

7.4 Conferences

In 2004, Rolf Oppliger serves as a member of the programm committee for the following conferences, workshops, and symposia:

- 1st European PKI Workshop on Research and Applications, Samos Island (Greece), June 25 - 26, 2004
- International Association for Development of the Information Society (IADIS) e-Society Conference, Spain, July 16 - 19, 2004
- 5th International Conference on Electronic Commerce and Web Technologies (EC-Web 2004) held in conjunction with the 15th International Conference on Database and Expert Systems Applications (DEXA 2004), Zaragoza (Spain), August 30 - September 3, 2004

[7] `www.esecurity.ch/serieseditor.html`
[8] `www.esecurity.ch/links.html#bookseries`
[9] `www.ifi.unizh.ch/~oppliger/Teaching/uni-zh-ifi-ss04.html`
[10] `www.esecurity.ch/education.html`
[11] `www.rechtsinformatik.ch/`

- 1st International Conference on Trust and Privacy in Digital Business (TrustBus '04) held in conjunction with the 15th International Conference on Database and Expert Systems Applications (DEXA 2004), Zaragoza (Spain), August 30 - September 3, 2004
- IEEE GLOBECOM 2004 Symposium on Security and Network Management, Dallas, TX (USA), November 29 - December 3, 2004

Please, feel free to register and attend any of these events. The papers that have been reviewed so far look promising.

About the Company

eSECURITY Technologies Rolf Oppliger was founded in October 1999. It is an independent and privately owned company located in Gümligen near Berne (Switzerland). The company provides scientific and state-of-the-art consulting, education, and engineering services related to information and information technology (IT) security. The core competence is the design, customization, and implementation of appropriate IT security processes and corresponding security architectures. Furthermore, the company is able to provide scientific investigations, analyses, and expert opinions related to all areas of IT security.