Volume 2, Issue 1, Spring 2005 http://www.esecurity.ch/communications.html

Contents

1 Editorial

In 2004, we published the first volume and the first two issues of eSECURITY communications—the official newsletter of eSECURITY Technologies Rolf Oppliger. The feedback we have received so far is overwhelmingly positive and encouraging. Therefore, we continue our effort and publish two further issues in this year (spring and fall issues). Thanks for being with us! We hope that you enjoy reading eSECURITY communications, and we are looking forward hearing from you and receiving your feedback, comments, and criticism.

2 News

The new and upcoming book of Rolf Oppliger, entitled *Contemporary Cryptography* (ISBN 1-58053-348-5), will appear in April/May 2005 (see Secton 3.1).

eSECURITY Technologies Rolf Oppliger is about to launch the eSECURITY Technology Assessment program (see Section 4). The program takes off as soon as enough subscribers, supporters, and sponsors participate.

3 Publications

3.1 Books

As mentioned above, *Contemporary Cryptography* (Artech House Publishers, Norwood, MA, 2005, ISBN 1-58053-348-5), will appear in April/May 2005. It comprises 530 pages and is intended to provide an overview about contemporary cryptography. It targets computer scientists, electrical engineers, and mathematicians both in research and practice, as well as computer practitioners, consultants, and information officers who want to gain some insight into the fascinating and fastly evolving field.

Contemporary Cryptography starts with two chapters that introduce the topic and briefly overview the cryptographic systems (or cryptosystems) in use today. After a thorough introduction of the mathematical fundamentals and principles that are at the heart of contemporary cryptography (Part I), the cryptographic systems are addressed in detail and defined in a mathematically precise sense. The cryptographic systems are discussed in three separate parts, addressing unkeyed cryptosystems (Part II), secret key cryptosystems (Part III), and public key cryptosystems (Part IV). Part IV also includes cryptographic protocols that make use of public key cryptography. Finally, the book finishes with an epilogue (Part V) and two appendixes.

Gene Spafford from Purdue University (USA) was kind enough to provide the foreword for the book. He uses the following words to put the book into perspective:

> If you're a teacher, you now have a powerful textbook that can be used to prepare students for everything from basic comprehension of cryptographic concepts to reasonably advanced research in the field. As such, this is a much-needed instrument of pedagogy. This is the book colleagues and I wish we had over the last decade when teaching our graduate cryptography class; luckily, now we have it, and you do too.

You may refer to the book's home page[1] to get more information or to place an online order (with Amazon.com).

3.2 Refereed Articles

The following refereed articles have been published since the last issue of eSECURITY communications:

- An article (co-authored by Javier Lopez and Günter Pernul) entitled "Authentication and authorization infrastructures (AAIs): a comparative survey" appeared in *Computers & Security* (Vol. 23, No. 7, October 2004, pp. 578–590). The article overviews, discusses, and puts into perspective the different approaches that are available today to provide AAIs and corresponding services in heterogeneous environments.
- An article (co-authored by Ruedi Rytz) entitled "Does Trusted Computing Remedy Computer Security Problems?" appears in *IEEE Security & Privacy* (Vol. 3, No. 2, March/April 2005). In short, the article argues that trusted computing has some merits and that there are certainly some critical and highly dependable systems and applications that can make use of it, but that it does neither provide a complete remedy for the personal computer's security problems nor is it likely to prevail on the mass market for personal computers.
- An article entitled "Privacy-enhancing Technologies for the World Wide Web" will appears in *Computer Communications* (later this

[1] `www.esecurity.ch/Books/cryptography.html`

year). The article overviews, discusses, and puts into perspective some privacy-enhancing technologies (PETs) that can be used to provide anonymity services on the WWW. More specifically, it elaborates on PETs that can be used to browse anonymously through the Web and publish anonymously on the Web.

Another article entitled "IT Security: In Search of the Holy Grail" has been accepted for publication in the *Communications of the ACM* (date of publication is still unknown).

3.3 Other Articles

In addition to these refereed articles, the following (German-speaking) articles have been published or are about to be published:

- An article entitled "Der Mann in der Mitte — Zur Sicherheit des Internet-Banking" appeared in the *Neue Zürcher Zeitung* (October 8, 2004, p. 65). It elaborates on the security of Internet banking solutions and puts phishing into perspective to other social engineering attacks.
- An article entitled "Hash auf Kollisionskurs — Hashfunktion SHA-1 möglicherweise geknackt" appeared in the *Neue Zürcher Zeitung* (February 25, 2005, p. 65). It assesses the recently published rumours regarding the successful collision attacks against the cryptographic hash function SHA-1.
- An article entitled "Sichere" Streichlisten" appears in *digma* (Vol. 5, No. 1, 2005). The article elaborates on a possibility to enhance the security of transaction authentication numbers (TANs). The idea is to physically protect a TAN list in a way that reading a TAN requires a physical act that can be detected easily at some later point in time. One possibility is to use a physical layer that hides the TANs, and that can easily be rasped away by the user (similar to lots in some lotteries). Furthermore, teh article proposes a simple extension to protect the user against some phishing attacks.
- An article preliminarily entitled "Informatiksicherheit und die Jagd nach dem heiligen Gral — Über den Sinn und Unsinn von 'ethischem' Hacken" appears in *digma* (Vol. 5, No. 2, 2005). The article elaborates on an analogy to explain and put into perspective the task(s) of an information security officer.

Please, feel free to request a paper copy of one (or all) of the articles if you don't have access to the proper source(s). We invite you to discuss the articles and their contents with us.

4 Security Analyses

There are many information security technologies and techniques available that are claimed to be new, pioneering, or ingenious, and it is getting more and more difficult to decide whether these claims are justified. Against this background, eSECURITY Technologies Rolf Oppliger is about to launch the eSECURITY Technology Assessment program. The aim of the program is to provide independent and vendor-neutral assessments of upcoming and leading-edge information security technologies and techniques. It is planned to issue four eSECURITY Technology Assessment reports per year. The reports are written in English and are professionally designed and printed. Each report focuses on a specific topic, and introduces, discusses, analyzes, and puts it into perspective all aspects that are relevant from a security viewpoint in a highly condensed form (20 pages at most). Also, the report explains what the topic is all about, overviews and discusses the research results that have been achieved in the past, and elaborates on future research challenges and business opportunities. Exemplary topics include (but are not limited to):

- Digital signatures and digital signature legislation
- Public key infrastructures
- Identity management
- E-voting
- Secure messaging
- Web services
- Trusted computing and digital rights management
- Pivacy-enhancing technologies
- Virtual private networking

The eSECURITY Technology Assessment program targets the chief information officer (CIO) and chief information security officer of large companies and organizations. More generally, all kinds of information security professionals may be interested in the program.

There are several possibilities to participate in the eSECURITY Technology Assessment program (as a

subscriber, supporter, or sponsor). All forms of participation are welcome and highly appreciated. The program takes off if enough subscribers, supporters, and sponsors participate. You may request further information about the eSECURITY Technology Assessment program.

5 Computer Security Series

Since the publication of the last issue of eSECURITY communications, the following three books have been published in the computer security book series of Artech House:[2]

- C. Warren Axelrod, *Outsourcing Information Security*, ISBN 1-58053-531-3, 2004, 266 pp.
- Michael A. Caloyannides, *Privacy Protection and Computer Forensics, Second Edition*, ISBN 1-58053-830-4, 2004, 364 pp.
- Alexander W. Dent and Chris J. Mitchell, *User's Guide to Cryptography and Standards*, ISBN 1-58053-530-5, 2005, 402 pp.

Furthermore, the following books are scheduled for 2005 and 2006:

- Rolf Oppliger, *Contemporary Cryptography*, ISBN 1-58053-642-5, scheduled for May 2005, approx. 530 pp.
- Thomas Hardjono and Lakshminath R. Dondeti, *Security in Wireless LANs und MANs*, ISBN 1-58053-755-3, scheduled for July 2005, approx. 306 pp.
- Panagiotis Papadimitratos, *Securing the Internet Infrastructure*, ISBN 1-58053-852-5, scheduled for February 2006, approx. 301 pp.
- John Velissarios, *Identity, Security and Anonymity on the Internet*, ISBN 1-58053-822-3, scheduled for April 2006, approx. 400 pp.
- Anthony M. Rutkowski, *Lawful Interception and Access*, ISBN 1-58053-880-0, scheduled for June 2006, approx. 354 pp.

Including these titles, the computer security book series will comprise 28 titles. As such, it is the largest book series devoted to computer security only.[3]

The process of contracting new and promising authors is ongoing. If you interested in writing and publishing a book in the series you may contact either the Series Editor (Rolf Oppliger) or any of the Commissioning Editors (Julie Lancashire or Wayne Yuhasz). The coordinates of these persons can be found on the series' home page.

6 Outlook

6.1 University Lecture

In summer 2005, Rolf Oppliger will lecture on "Sicherheit in der Informationstechnik" at the University of Zürich. The lecture will give an introduction into cryptography, computer security, and communication and network security. It will also elaborate on specific topics, such as digital signatures and digital signature legislation, electronic voting, and trusted computing. The slides for the lecture are electronically available at the lecture's home page.[4]

6.2 Courses

We are still in the process of planning the previously announced introductory courses on IT security and cryptography. If you are interested to attend, then we invite you to contact us and get involved into the planning process.

6.3 Invited Talk

On June 14, 2005, Rolf Oppliger will give a talk entitled "Digital Signatures: From Theory to Practice" at the ZISC Information Security Colloquium (ETH Zürich). The abstract of the talk is as follows:

> Digital signatures are the security mechanisms of choice to provide non-repudiation services for electronic commerce. From a theoretical point of view, digital signatures and corresponding systems are well understood and we have systems that are (provably) secure against existential forgery, even if one assumes an adversay who is powerful enough to mount an adaptive chosen message attack. From a practical point of view, however, things are more involved.

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

[3] The competing book series are itemized at `www.esecurity.ch/links.html#bookseries`.

[4] `http://www.ifi.unizh.ch/~oppliger/Teaching/uni-zh-ifi-ss05.html`

> There are shortcomings and limitations of (even theoretically secure) digital signature systems when implemented and deployed in the real world. In this talk, we overview and discuss some of these shortcomings and limitations, and we elaborate on possibilities to address them. We argue that digital signature legislation is more involved than originally anticipated, that it must go beyond the regulation of public key infrastructures (PKIs) and certification service providers (CSPs), and that the requirement for non-repudiation is somehow contraversial (at least from the user's viewpoint). We conclude with the prediction that digital signature laws will continue to have a negligible impact on the large-scale deployment and acceptance of digital signatures and corresponding systems, and that these systems will rather prevail in a subliminal way. Last but not least, we argue that there is room for trusted services related to digital signatures, and we propose an architecture for a server-based signature system that can be used to provide such services on the Internet.

The talk will be made available on the seminar Web site.[5] In the meantime, you may contact eSECURITY Technologies Rolf Oppliger for a preliminary version of the slides.

6.4 Conferences and Workshops

In 2005, Rolf Oppliger serves as a member of the programm committee for the following international conferences and workshops:

- 2nd European PKI Workshop on Research and Applications, Kent (UK), June 30-July 1, 2005
- 6th International Conference on Electronic Commerce and Web Technologies (EC-Web '05) held in conjunction with the 16th International Conference on Database and Expert Systems Applications (DEXA 2005), Copenhagen (Denmark), August 22-26, 2005
- 2nd International Conference on Trust, Privacy, and Security in Digital Business (TrustBus '05) held in conjunction with the 16th International Conference on Database and Expert Systems Applications (DEXA 2005), Copenhagen (Denmark), August 22-26, 2005
- 8th Information Security Conference (ISC '05), Singapore, September 20-23, 2005
- 4th International Workshop for Applied PKI (IWAP 05), Singapore, September 21-23, 2005
- International Association of Science and Technology for Development (IASTED) International Conference on Communications and Computer Networks (CCN 2005), Marina Del Rey, CA (USA), October 24-26, 2005
- International Association of Science and Technology for Development (IASTED) International Conference on Communication, Network, and Information Security (CNIS 2005), Phoenix, AZ (USA), November 14-16, 2005

Feel free to register and attend any of these events. The papers we have reviewed so far look promising.

About the Company

eSECURITY Technologies Rolf Oppliger[6] is an independent and privately owned company founded in October 1999 to provide scientific and state-of-the-art consulting, education, and engineering services related to information technology (IT) security. The company is registered in the commercial register of Bern-Mittelland (CH-035.1.023.622-7) and is located in Gümligen near Berne (Switzerland).

[5] www.zisc.ethz.ch/events/infseccolloquium2005

[6] www.esecurity.ch