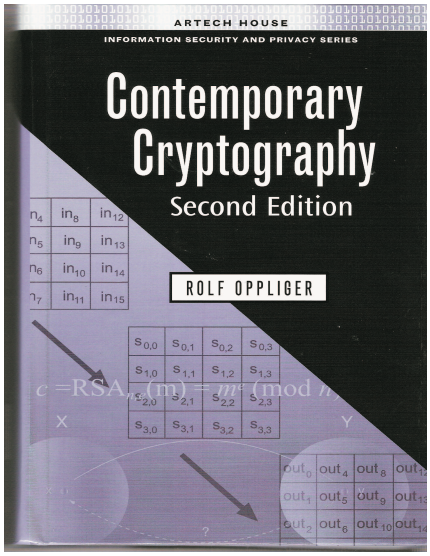
Volume 8, Issue 2, Fall 2011 http://www.esecurity.ch/communications.html

Contents

1 Editorial

The year 2011 has come off badly for the PKI industry. In March, it became public that a Comodo reseller in Italy called GlobalTrust had been compromised and a few SSL/TLS server certificates had been fraudulently issued in the aftermath. Some of these certificates were so important that revoking them (using certificate revocation lists or OCSP responses) seemed to be insufficient, and the browser vendors therefore decided to patch their software on the fly. The event was unfortunate and casted a damning light on Comodo and the PKI industry as a whole. To make things worse, a few months later (in late August), it became obvious that DigiNotar (a Vasco company) had also been compromised, resulting in several hundred fraudulently issued SSL/TLS server certificates (including many wildcard certificates for very prominent sites). This set the seal on the end of DigiNotar, also acting as a trusted certification authority (CA) for the Dutch government (the respective governmental CA is known as PKIoverheid). It also revealed the fact that CAs and PKIs better work in theory than in practice. In fact, the high level of security that is claimed to be achievable with public key certificates has turned out to be illusive. A CA or PKI that operates in the real world is a social-technical system, and as such it has social and technical shortcomings and vulnerabilities. Some of these shortcomings and vulnerabilities can be eliminated using appropriate security mechanisms (be they technical, organizational, or legal), but some of them cannot be eliminated. For example, the operators of the respective systems are always going to have special privileges and can misbehave accordingly. Even if the four-eye-principle is put in place and enforced, the adversary can blackmail or bribe two persons (instead of one). This makes an attack more expensive, but it does not entirely eliminate the possibility. As long as human beings are involved, it seems that there are always possibilities to attack a CA or PKI. This is disillusioning but real; i.e., the discussions that surround public key certificates, CAs, and PKIs have finally arrived in reality and are subject to real-world security reasoning.

I hope that you enjoy reading this issue of e-SECURITY communications, and I am looking forward hearing from you and receiving your feedback, comments, or criticism in one way or another.



2 News

Rolf Oppliger's new book entitled *Contemporary Cryptography, Second Edition* (ISBN 978-1-60807-145-6) is now available in Artech House's information security and privacy series.[1] It can be purchased from Artech House, Amazon, or any local bookstore. Feel free to review it and post some comments on any forums of your choice. I sincerely appreciate any criticism, be it positive or negative.

3 Publications

In his role as an editorial board member of the *IEEE Computer* magazine, Rolf Oppliger has served as the guest editor for the September 2011 special issue on "Security and Privacy in an Online World." The rationale behind this special issue was that "it is increasingly difficult if not impossible to define the perimeter that separates the trusted inside from the untrusted outside," and that "many security and privacy mechanisms no longer work in an online world." Many companies and organizations are struggling with these issues, and hence new buzzwords like "perimeterization" and acronyms like BYOD (standing for "bring your own device") have appeared in public discussions. It seems that nobody has appropriate answers to the (security)

[1] `http://www.esecurity.ch/serieseditor.html`

challenges of the online world. This disillusioning fact was also reflected by the manuscripts that had been submitted during summertime. While most of them are interesting to read and address some important issues, none of them really addresses the core of the problem, namely how to properly manage IT security in an online world. Against this background, Rolf Oppliger has written and published an appetizer and introduction for the special issue that is available online.[2] All articles finally published in the special issue are recommended reading and provide answers to relevant problems.

Together with Bruno Wildhaber, Rolf Oppliger is also writing an article about the 10 most commonly found misconceptions in computer and information security. The misconceptions that are discussed in the article are as follows:

1. People care about computer and information security
2. Computer and information security is a technical field of study
3. The data flow can be controlled and the "need to know" principle works
4. The CIO controls the information infrastructure
5. Computer and information security must start with a formal risk analysis
6. The return on security investment (ROSI) yields a decision parameter
7. Isolated audit and penetration tests reveal the current state of security
8. Computer and information security measures must be preventive
9. Certificates help
10. Computer and information security is continuous

The rationale behind the article is to reveal and unmask arguments and lines of argumentation that are inherently flawed. If you are interested in the topic, then feel free to contact any of the two authors, request a copy of the draft article, and eventually join the discussion. It goes without saying that the topic (and some misconceptions it suggests) is not without controversy.

[2] `http://www.esecurity.ch/Flyers/IEEE-Computer-SI-Intro.pdf`

4 Information Security and Privacy Books

Later this year, a new book entitled *Biometrics in Identity Management: Concepts to Applications* (ISBN 978-1-60807-017-6) will be published in Artech House's information security and privacy series. It is going to be the 36^{th} title published in the series. The book is authored by Shimon K. Modi from Purdue University. It provides a comprehensive coverage of commercially available biometric technologies, their underlying principles, operational challenges and benefits, and deployment considerations. As such, it is recommended reading for anybody working the field.

The process of contracting new authors is going on. If you are interested in writing and publishing a book in the series, then you may contact either the Series Editor (Rolf Oppliger) or a Commissioning Editor. In the second case, you may want to refer to the book series' home page[3] for the coordinates of the respective editors.

5 Announcements

There are some announcements to make regarding university lectures, courses, as well as conferences and workshops.

5.1 University Lectures

In 2012, Rolf Oppliger will lecture again at the University of Zürich on "Sicherheit in der Informationstechnik." The lecture dates are tentatively scheduled as follows:

- February 20, 2012
- March 5, 2012
- March 19, 2012
- April 2, 2012
- April 23, 2012
- May 7, 2012
- Mai 21, 2012

The lecture provides a thorough introduction into all questions and aspects related to IT security. As such, it is also open for new topics and respective proposals and suggestions.

Later this year, the lecture slides will be revisited and made available online.

[3] `http://www.esecurity.ch/serieseditor.html`

5.2 Courses

InfoGuard AG[4] and CRYPTO AG[5] regularly host a seminar on contemporary cryptography, in which four out of five days are taught by Rolf Oppliger. The seminars are held in English and take place in the Zug area (Switzerland). The next course will possibly take place on November 14–18, 2011. For next year, the three seminars are tentatively scheduled as follows:

- May 14–18, 2012
- September 17–21, 2012
- November 12–16, 2012

If you are interested to attend any of these seminars, then you may request a flyer from InfoGuard AG or eSECURITY Technologies Rolf Oppliger. The flyer is also electronically available on the Internet.[6] Either company is to answer questions related to the seminar.

If you are interested to host a course on contemporary cryptography or any other topic related to IT security, then please feel free to contact eSECURITY Technologies Rolf Oppliger. We are looking forward discussing the respective possibilities with you without any commitment.

5.3 Conferences and Workshops

In addition to the conferences and workshops announced in previous issues of eSECURITY communications, Rolf Oppliger has served or is about to serve as a member of the programm committee of the following conferences and workshops (in chronological order):

- 5th International Conference on Information Security and Assurance (ISA 2011), Brno University, Czech Republic, August 15 - 17, 2011
- 12th International Workshop on Information Security Applications (WISA 2011), Jeju Island (Korea), August 22 - 24, 2011
- 8th European Workshop on Public Key Infrastructures, Services, and Applications (EuroPKI 2011), Leuven (Belgium), September 15 - 16, 2011
- 14th International Conference on Information Security and Cryptology (ICISC 2011), Seoul (Korea), November 30 - December 2, 2011
- International Conference on Security Technology (SecTech 2011), Jeju Island (Korea), December 8 - 10, 2011
- 9th Annual IEEE Consumer Communications & Networking Conference (CCNC 2012), Technical Track on Security and Content Protection, Las Vegas (USA), January 7 - 10, 2012

More programm committee memberships will be announced in future issues of eSECURITY communications. It goes without saying that all conferences and workshops are recommended events to attend and learn more about the current state-of-the-art in cryptography and IT security. Rolf Oppliger is not personally attending all conferences and workshops itemized above, but he's still vouching for their quality.

About the Company

eSECURITY Technologies Rolf Oppliger[7] 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 Muri b. Bern (Switzerland).

[4] http://www.infoguard.ch

[5] http://www.crypto.ch

[6] http://www.esecurity.ch/Flyers/CCC_brochure.pdf

[7] http://www.esecurity.ch