*e*SECURITY® communications

Volume 9, Issue 1, Spring 2012 http://www.esecurity.ch/communications.html

Contents

1 Editorial

In the hype that currently surrounds cloud computing, I recently made an instructive experience: A related girl had been a customer of a free e-mail service provided by a major cloud service provider and promoter for a couple of years. When she wanted to register for the social network service of the same provider, she was stopped and denied further access to her mailbox (and all previously received messages). The official answer for this lock out was the Children's Online Privacy Protection Act (COPPA[1]) and the fact that the girl was not yet 13 years old. But there is nothing new about these facts: The COPPA had been in place since 1998 and the girl had never lied about her true age. The point is that the provider had changed its interpretation and implementation of the COPPA, and the lock out occurred as a consequence of this change.

The story may not be very interesting, but the lessons learned are (I guess). The point is that such a change may always happen, i.e., the home country of the provider may enact a new law or the provider may change its interpretation and implementation of an existing law. In most cases, the consequences of such a change will be negligible, but in some cases, the customers may get into trouble. Imagine, for example, what happens if the customer is not a girl that has her mailbox stored in the cloud, but a company that has outsourced its entire data and is now locked out from access. There are many industries in which companies in this situation go out of business quite rapidly. For these companies, having permanent access to their data is critical and vitally important. This high dependency is often neglected and is certainly not in line with the claimed carelessness of cloud computing. One possibility to deal with this situation (or problem, respectively) is to make regular backups, but this contradicts the promises of cloud computing and is therefore not even recommended by the service providers.

Based on this disillusioning experience, I have written an article about security issues related to cloud computing (cf. Section 3). The article is inconsistent with the general claim that cloud computing poses no security risk. In fact, I think that cloud computing is just another form of outsourcing, and that this new form of outsourcing brings in new security problems and challenges that still need to be addressed and solved in one way or another. Some of the problems and challenges are interdisciplinary and must also be addressed legally, but this neither helps nor does it simplify the situation considerably. I am particularly curious about status reports of internationally operating companies that employ cloud computing, especially in the long term.

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

R. Oppliger

I am the author of this document
Qualified signed by Rolf Oppliger
Muri b. Bern, Switzerland, March 13, 2012

2 News

In December 2011, Rolf Oppliger was nominated and approved for the prestigious Distinguished Speakers Program (DSP) of the Association for Computing Machinery (ACM).[2] The speeches that are currently offered are as follows:

- SSL/TLS and Web Application (In-) Security
- Digital Signatures: Theory and Practice
- Contemporary Cryptography

The titles of the speeches speak for themselves. Also, the list is not exclusive, meaning that other speeches on security-related topics can be added at will. All speeches have a preferred length but are scalable in nature (this is particularly true for the speech on contemporary cryptography).

If any of these topics is of interest to you or your company, then you may establish contact with us—either directly or indirectly through the DSP.

3 Publications

In the last issue of eSECURITY communications, we mentioned that Bruno Wildhaber and Rolf Oppliger are collaborating in writing an essay about what they think are the most common misconceptions in computer and information security. A Kindle edition of the essay is available from Amazon,[3] and a shortened version will soon be published in the *IEEE Computer* magazine (the article is tentatively scheduled for the June 2012 issue of the magazine). In either case, we are keen on your

[1] http://www.coppa.org

[2] http://www.dsp.acm.org

[3] http://tinyurl.com/8679hun

feedback and remarks you may have to start a discussion. The topic is controversial, and we hope to have a respective controversy with interested people.

In this issue's Editorial, we have mentioned that Rolf Oppliger has written an article about some security issues related to cloud computing. The article is not a comprehensive treatment of cloud security, but it points to some questions that have not been seriously addressed and discussed so far. The article is written in German and will be published in the *digma* magazine. An electronic version of the article will be made available on Rolf Oppliger's homepage. Again, we are interested in receiving your feedback.

Last but not least, Rolf Oppliger has written a more technically-oriented paper about last year's attacks against Comodo and DigiNotar, and the implications thereof for the evolution of public key infrastructures (PKIs). The (working) title of the paper is "Certification Authorities under Attack: A Plea for Certificate Legitimation," and it has been submitted for publication (without decision so far). Using probability-theoretic arguments, the paper argues that such attacks will occur again and again, and that some of them are going to be successful. Hence, illegitimately issued certificates are going to exist, and respective countermeasures must be designed, implemented, and put in place. The paper addresses two problem areas in which countermeasures are needed: certificate revocation and certificate authorization. Both areas are related and can be subsumed under the term "certificate legitimation." The paper introduces the notion of certificate legitimation, discusses and puts into perspective some recent proposals, and outlines new areas of research and development. The paper is not intended to provide a complete solution, but it is intended to start a discussion that may lead to a solution one day. If you are interested in reading a draft version of the paper, you may drop us a note.

4 Information Security and Privacy Books

In the last 12 years (in which Rolf Oppliger has served as the series editor), Artech House has published 36 titles in the information security and privacy book series. The number of books and diversity of the titles are remarkable and inimitable. In fact, to the best of our knowledge, Artech House's book series is the largest series entirely devoted to information security and privacy.

It is hoped that the series can be further expanded, and that new and seminal topics can be addressed in respective books. Against this background, the process of contracting new authors is going on. If you are working in the field and are interested to write and publish a book in the series, then you may contact either the Series Editor (Rolf Oppliger) or one of the Commissioning Editors (refer to the book series' home page[4] for the coordinates of the Commissioning Editors).

5 Announcements

There are a few announcements to make regarding university lectures, courses, invited talks, as well as involvement in international conferences and workshops.

5.1 University Lectures

In February 2012, Rolf Oppliger started this year's lecture on "Sicherheit in der Informationstechnik" at the University of Zurich, Switzerland. The lecture takes place annually and provides a thorough introduction to various topics related to information technology (IT) security. The lecture slides have entirely been redesigned to be compliant with the corporate identity of the University of Zurich. They are electronically available at the lecture's home page[5] (also accessible from outside the University of Zurich). The slides' content has only been moderately adapted since last year, but it is expected to pass a major revision in the next couple of months (to be ready next year). If you think that specific topics need to be addressed in the lecture, then you may drop us a note. Needless to say that we are very interested to learn about them.

5.2 Courses

The Swiss companies InfoGuard[6] and CRYPTO[7] 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. In 2012, the dates are tentatively scheduled as follows:

- April 30 - May 4
- September 17 - 21
- November 12 - 16

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

[5] `http://www.esecurity.ch/Teaching/uni-zh-2012.shtml`

[6] `http://www.infoguard.ch`

[7] `http://www.crypto.ch`

If you are interested in attending any of these seminars, then you may request a flyer from InfoGuard or eSECURITY Technologies Rolf Oppliger (the flyer is also electronically available on the Internet[8]). Either of these companies can take and 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 in your organization, then please feel free to contact eSECURITY Technologies Rolf Oppliger. We are looking forward discussing the respective possibilities with you. Needless to say that such a discussion is without any commitment for you.

5.3 Invited Talks

On October 17, 2012, Rolf Oppliger will give an invited talk at the University of Zurich. The title of the talk is "Geld im digitalen Zeitalter: Eine Standortbestimmung," and—as the title suggests—it is aimed at providing a general overview about the notion, role, and state-of-the-art of money in the digital age. Given the current diversity of Internet cash systems (including, for example, PayPal and Bitcoin), we think that it is time to sit back and deliberate a little bit on money in the digital age.

The talk will take place in the main building of the University of Zurich (Rämistrasse 71, room will be anouced later on) and will start at 18:15. It is scheduled for 45 minutes with additional 30 minutes for a subsequent discussion. Further information about the talk will be announced on the Web site of the organizing organisation.[9] You are cordially invited to attend the event (no registration is required) and to challenge Rolf Oppliger in the discussion (or even after the discussion).

5.4 Conferences and Workshops

In 2012, Rolf Oppliger serves as a member of the programm committee for the following international conferences and workshops (in chronological order):

- 9th Annual IEEE Consumer Communications & Networking Conference (CCNC 2012), Technical Track on Security and Content Protection, Las Vegas (USA), January 7 - 10, 2012
- International Summer FTRA Symposium on Advances in Cryptography, Security and Applications for Future Computing (FTRA ACSA 2012), Vancouver (Canada), June 26 - 28, 2012
- International Conference on Security and Cryptography (SECRYPT 2012), Rome (Italy), July 24 - 27, 2012
- 11th Annual Information Security South Africa Conference (ISSA 2012), Johannesburg (South Africa), August 15 - 17, 2012
- 13th International Workshop on Information Security Applications (WISA 2012), Jeju Island (Korea), August 16 - 18, 2012
- 7th International Conference on Availability, Reliability and Security (ARES 2012), Prague (Czech Republic), August 20 - 24, 2012
- 9th International Conference on Trust, Privacy and Security in Digital Business (TrustBus 2012) held in conjunction with the 23rd International Conference on Database and Expert Systems Applications (DEXA 2012), Vienna (Austria), September 3 - 7, 2012
- 8th European PKI Workshop: Research and Applications (EuroPKI 2012), held in conjunction with the 17th European Symposium on Research in Computer Security (ESORICS 2012), Pisa (Italy), September 13 - 14, 2012
- 7th International Conference on Systems and Networks Communications (ICSNC 2012), Lisbon (Portugal), November 18 - 23, 2012

In spite of the fact that Rolf Oppliger is not attending all of these conferences and workshops, they are still recommended events to attend and learn more about the current state-of-the-art in cryptography and IT security.

About the Company

eSECURITY Technologies Rolf Oppliger[10] 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 located in Muri b. Bern.

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

[9] http://www.pdverein.uzh.ch/aktuell/ringvorlesungen.html

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