Volume 10, 2013 http://www.esecurity.ch/communications.html

Contents

1 Editorial

The Snowden or NSA affair has clearly dominated our field in 2013. From a bird's eye perspective, the affair has taught us two things:

- First, insider attacks are overwhelmingly powerful and difficult to protect against (this refers to the person of Eduard Snowden).
- Second, the threats model we usually have in mind when we discuss security is too conservative and optimistic (this refers to the NSA and similar agencies in other countries).

Security professionals have always been aware of the first point and the risks related to insiders. In fact, many security principles have their roots in trying to mitigate these risks. Exemplary principles include "separation of duties," "least privilege," and "four eyes." Applying these principles, one typically tries to control the (uncontrollable) insider, or at least make it more difficult for him or her to misbehave in a way that compromises the overall security of an organization. Eduard Snowden has clearly demonstrated that the power of a legitimate insider is huge, and that protecting against such an adversary is prohibitively expensive if not impossible (or at least next to impossible). Here the entire affair has accentuated something we already knew before.

The second point is more revolutionary, as it changes the way we have to think about the threats we are exposed to. Traditionally (an academic would say following the Dolev-Yao model), we have thought that the bad guys are sitting in the network, passively observing IP packets as they are sent back and forth. We have also been aware of the fact that the bad guys may compromise the security of the end systems, basically allowing them to mount active attacks (using, for example, various types of malware). But we have also thought that the standardization bodies and the hardware and software manufacturers are on our side, and that all of them have the common objective to provide as much security as possible for everybody. Here, the Snowden or NSA affair has taught us that we have been fundamentally wrong in this belief: Standardization bodies are undercut and the respective standards may not be free of trapdoors (the story that surrounds the Dual Elliptic Curve Deterministic Random Bit Generator standardized in NIST SP 800-90A clearly demonstrates this point). Similarly, the hardware and software manufacturers have some obscure (and mostly not revealed) "cooperation agreements" with the intelligence bodies and secret services in their home countries (most are located in the United States). In an environment in which the adversary is not only passively observing things but also actively manipulating standards and implementations, everything seems feasible. Discussing security in such a hostile environment is very involved (to say the least). In fact, it seems to be the case that the security discussions have to start from scratch. The bottom line is that the situation that we face is indeed worrisome and scary.

2 News

eSECURITY communications is no longer distributed by e-mail. Instead, it is stored at the homepage of eSECURITY Technologies Rolf Oppliger[1] and can downloaded from there at will.

In 2013, Rolf Oppliger has been busily preparing a new book entitled *Secure Messaging on the Internet*. The book is scheduled to be published and released in 2014. The book goes beyond what would be a second edition of *Secure Messaging with PGP and S/MIME* (a book that was published 12 years ago), mainly because it broadens the scope significantly, and now addresses additional topics, like Web-based messaging, gateway solutions, certified mail, delivery platforms, and instant messaging. The aim has been to draw a picture that is comprehensive and sufficiently complete when it comes to all aspects related to secure messaging on the Internet. Unfortunately, the book cover has not yet been designed or even drafted. This will be done early in 2014. The result will be included in the next issue of eSECURITY communications.

3 Publications

In 2013, Rolf Oppliger published an article entitled "Geld im digitalen Zeitalter — Eine Standortbestimmung" in a book jointly edited by Josette Baer and Wolfgang Rother (*Geld — Philosophische, literaturwissenschaftliche und ökonomische Perspektiven*, ISBN 978-3-7965-2913-9, Schwabe Verlag, Basel, 2013). The article appears on pages 187 to 207. It is based on an talk that Rolf Oppliger gave at the University of Zurich on October 17, 2012 (as part of a lecture series[2]). The article provides an overview about the history of money in the real and digital worlds.

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

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

An article entitled "Certification Authorities under Attack: A Plea for Certificate Legitimation" is still in the queue and waiting for publication in the *IEEE Internet Computing* magazine. If you are interested to get a preprint of the article, then plase feel free to contact eSECURITY Technologies Rolf Oppliger without any commitment. More recently, Google has come up with a technology called "certificate transparency" that is in line with the argumentation of the article. The basic idea is to replace the black-list approach of certificate revocation with a respective white list approach. This alterantive way of thinking does not solve all problems related to certificate revocation, but it does at least mitigate some of the relevant risks.

4 Information Security and Privacy Books

In 2013, Stefan Rass and Daniel Slamanig published a book entitled "Cryptography for Security and Privacy in Cloud Computing" in the book series (ISBN 978-1-60807-575-1). As its title suggests, the book introduces, discusses, and puts into perspective some security and privacy technologies that can be used and are particularly well suited for cloud computing. As such, the book targets an interesting and very timely market.

For 2014, the following two book titles are scheduled and currently in production:

- Amir Herzberg and Haya Shulman, *DNS Poisoning: Attacks and Defenses*
- Rolf Oppliger, *Secure Messaging on the Internet*

Also, the process of contracting new authors is steadily 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' homepage[3] 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.

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

5.1 University Lectures

In the spring semester of 2013, Rolf Oppliger gave a German lecture on "Sicherheit in der Informationstechnik" at the University of Zurich. The lecture basically provided an introduction to the broad field of IT security. The slides are electronically available at the lecture's homepage[4] (also accessible from outside the University of Zurich). Feel free to download the slides, have a look at them, and hopefully provide some feedback (it goes without saying that any feedback is weleome and highly appreciated).

In the upcoming spring semester of 2014, Rolf Oppliger will give the same lecture in English (the lecture is now entitled "IT Security"). Again, the slides will be made electronically available at the lecture's homepage[5] as soon as they are finished (hopefully early in 2014).

5.2 Courses

The Swiss company CRYPTO AG[6] regularly hosts 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 Steinhausen (near Zug). In 2013, a respective seminar took place in September. For 2014, the following seminars are tentatively scheduled:

- May 19 - 23, 2014
- October 13 - 17, 2014

Feel free to register for and attend one of these seminars. The seminars take place if and only if a sufficiently large number of attendees actually registers. So the decision whether a particular seminar takes place can usually be made a few weeks ahead of the planned starting date.

If you are interested to host a course on contemporary cryptography or any other topic related to lT 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 again without any commitment for you.

[4] `http://www.esecurity.ch/Teaching/uni-zh-2013.shtml`

[5] `http://www.esecurity.ch/Teaching/uni-zh-2014.shtml`

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

5.3 Invited Talks

On April 10, 2013, Rolf Oppliger gave an invited talk at the Technical University of Lisbon in Portugal. The title of the talk was "SSL/TLS Session-Aware User Authentication Against Man-In-The-Middle (MITM) Attacks," and its aim was to introduce, discuss, and put into perspective a technology that can be used to protect SSL/TLS-based Web applications against MITM attacks. The idea is to bind the user authentication information to a particular SSL/TLS session, so that the information is invalid if submitted on another SSL/TLS session than the one the user originally employed when he or she sent out the information (note that in an MITM setting, there are two different SSL/TLS sessions in place—one between the user and the MITM and another one between the MITM and the target server, and that this difference is exploited by the technology). The technology is fully described in many scientific papers and articles mentioned in previous issues of eSECURITY communications (most of these publications are coauthored by Ralf Hauser and David Basin).

5.4 Conferences and Workshops

In 2013, Rolf Oppliger served as a member of the programm committee for the following events (in reverse chronological order):

- 9th International Conference on Information Assurance and Security (lAS 2013), Tunis (Tunisia), December 4 - 6, 2013
- 5th IEEE International Conference on Cloud Computing and Science (IEEE CloudCom 2013), Security and Privacy Track, Bristol (UK), December 2 - 5, 2013
- 16th International Conference on Information Security and Cryptology (ICISC 2013), Seoul (South Korea), November 27 - 29, 2013
- 10th Buropean Workshop on Public Key Infrastructures, Services and Applications (EuroPKI 2013), held in conjunction with the 18th European Symposium on Research in Computer Security (ESORICS 2013), London (UK), September 12 - 13, 2013
- 8th International Conference on Availability, Reliability and Security (ARES 2013), Regensburg (Germany), September 2 - 6, 2013
- 10th International Conference on Trust, Privacy and Security in Digital Business (TrustBus 2013), held in conjunction with the 24rd International Conference on Database and Expert Systems Applications (DEXA 2013), Prague (Czech Republic), August 26 - 30, 2013
- 12th Annual Information Security South Africa Conference (ISSA 2013), Johannesburg (South Africa), August 14 - 16, 2013
- 10th International Conference on Security and Cryptography (SECRYPT 2013), Reykjavik (Iceland), July 29 - 31 2013
- 7th International Conference on Information Security and Assurance (ISA 2013), Cebu (Philippines), April 26 - 28, 2013

In the past, there has been a misunderstanding regarding the fact that being a member of a program committee does not necessarily mean that one has to attend the conference or workshop. This is unfortunate but represents reality. In fact, Rolf Oppliger has not attended any of the events mentioned above (this is unfortunate, because some events have actually taken place at some nice locations).

About the Company

eSECURITY Technologies Rolf Oppliger 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.