Volume 12, 2015 http://www.esecurity.ch/communications.html

Contents

1 Editorial

There is a nice visualization of the world's biggest information security breaches available on the Internet.[1] According to this site, the year 2015 has been comparably calm. Many companies and organizations have been victimized, but the respective security breaches are neither critical nor devastating. It has, however, become evident that every company or organization may become a victim of a determined and sometimes quite sophisticated attack (such an attack is also known as "advanced persistent threat," or APT in short), and that information security (or cybersecurity) management is getting increasingly important these days.

As further addressed in Section 3, I have recently written an article that puts at stake the conventional wisdom regarding information security (or cybersecurity) management. In fact, most approaches in use today start with a quantitative risk analysis that is done first, before appropriate security controls and countermeasures are selected and implemented. In the article, I argue that and why these approaches are doomed to fail. The major argument is that quantitative risk analyses cannot be done in practice. This argument is not new, but it has persistently resisted its recognition among security professionals for quite a long time.

This is where we stand today: We—as a community of information security professionals—face an urgent need to manage information security, but we don't have the tools at hand to work in the field. We know that we must have something that does not require a quantitative risk analysis, but we currently don't know how this something may look like.

Against this background, I have recently started to develop a method to engineer and plan cybersecurity measures in particularly large and heterogeneous organizations. In lack of a better name, I have prematurely called the method OCEP, an acronym standing for "opportunistic cybersecurity engineering and planning." The characteristic feature of the method is its opportunistic flavor: Instead of starting with vulnerabilities, threats, and related risks, opportunistic cybersecurity engineering and planning primarily focuses on security measures. As of this writing, the OCEP method is neither available on paper nor is it supported by any tools that can be used (or tested) in the field. But if you are interested to get involved, then please feel free to contact me directly. I need case studies and real-world examples to further refine the method and to verify its applicability in the field. In either case, I will report on the progress in this area in future issues of eSECURITY communications. I firmly believe that information security (or cybersecurity) management and methods to handle it are key for the information age of today and the future.

[1] `http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/`

2 News

The second edition of the book entitled *SSL and TLS: Theory and Practice* has been finished, is currently in production, and will hit the shelves of the bookstores in the first quarter of 2016. Similar to the first edition that appeared in 2009, the book introduces, explains, and puts into perspective the SSL and TLS protocols that are in widespread use today. But in addition to this, the second edition also elaborates on the recent attacks against the SSL/TLS protocols that come along with funny names, such as BEAST, CRIME, TIME, BREACH, POODLE, FREAK, Logjam, and Lucky 13. These attacks are sophisticated and require a solid understanding of cryptography in general, and cryptographic pitfalls in particular. Furthermore, the book also addresses some topics related to SSL/TLS, such as datagram TLS (DTLS), firewall traversal, and public key infrastructures (PKIs). We think that the book is very comprehensive and that is provides everything that is needed to implement and make use of the SSL/TLS protocols in the field.

We are currently working on a complementary slide set that can be used to teach courses and lectures on the theory and practice of the SSL/TLS (and DTLS) protocols. If you are interested to get a preliminary draft of the slide set, then please feel to contact us directly. As soon as the slide set is finished, we will publish it on the book's homepage.[2] Feel free to use it at will.

3 Publications

Rolf Oppliger's article entitled "Quantitative Risk Analysis in Information Security Management: A Modern Fairy Tale" appeared in the November/December issue of *IEEE Security & Privacy*.[3] As already mentioned in the editorial, this article puts at stake the conventional wisdom regarding information security (or cybersecurity) management, namely the necessity to always start with a quantitative risk analysis. Instead,

[2] `http://books.esecurity.ch/ssltls2e.html`

[3] `http://dx.doi.org/10.1109/MSP.2015.118`

the article argues that any attempt to quantitatively analyze risks is doomed to fail or to provide results that are illusive and to some extent also meaningless. The article is controversial and controversially written on purpose. If you are interested to further discuss the topic, then please feel free to contact us directly. We are always looking forward to participate in controversial discussions about the state-of-the-art and the future of information security (or cybersecurity) management.

4 Information Security and Privacy Books

In 2015, Flavio Lombardi and Roberto Di Pietro finalized their book entitled *Security for Cloud Computing* (ISBN 978-1-60807-989-6) that is published in Artech House's information security and privacy series.

In addition, the following book titles have been written and are scheduled to appear early in 2016:

- Stefan Katzenbeisser and Fabien Petitcolas' update of their 2000-title *Information Hiding Techniques for Steganography and Digital Watermarking*, now entitled *Information Hiding* (ISBN 978-1-60807-928-5).
- Edward Humphreys' update of his 2007-title *Implementing the ISO/IEC 27000 Information Security Management System Standard*, now entitled *Implementing the ISO/IEC 27001:2013 ISMS Standard* (ISBN 978-1-60807-930-8).
- Rolf Oppliger's update and second edition of his 2009-title *SSL and TLS: Theory and Practice*.

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[4] for the coordinates of them).

5 Announcements

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

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

5.1 University Lectures

In the spring semester of 2015, Rolf Oppliger gave a lecture on "IT Security" at the University of Zurich. The slides are electronically available at the lecture's homepage[5] (they are also accessible from outside the University of Zurich). Please, feel free to download the slides and provide feedback at will.

The lecture will be held again in the spring semester of 2016.[6] The respective slide set is currently being revised. A preliminary version is already available, but it will still be modified until the lecture officially starts on February 22, 2016.

5.2 Courses

The Swiss company CRYPTO AG[7] 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 2015, a seminar took place in October.

In 2016, the following seminars are tentatively scheduled:

- April 25 - 29, 2016
- October 17 - 21, 2016

Feel free to register for and attend any of these seminars.

We are currently considering the possibility to organize a one or two-day course on the theory and practice of the SSL/TLS protocols to be held in the second half of 2016. If you are interested to participate in such a course and have some preferences about its length, date, and location, then please let us know. We try to customize the course as much as possible to meet the requirements of our customers.

Furthermore, if you are interested to host an internal course on any other topic related to information security (or cybersecurity) in your organization, then please feel free to contact us, too. We are looking forward discussing the respective possibilities with you. Needless to say that such a discussion is alays without any commitment for you.

[5] `http://www.esecurity.ch/Teaching/uni-zh-2015.shtml`

[6] `http://www.esecurity.ch/Teaching/uni-zh-2016.shtml`

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

5.3 Conferences and Workshops

In 2015, Rolf Oppliger served as a member of the programm committee for the following events (in chronological order):

- 12th Annual IEEE Consumer Communications & Networking Conference (CCNC 2015), Las Vegas (USA), January 9 - 12, 2015
- 12th International Conference on Wirtschaftsinformatik (WI 2015), Track 8: Data Privacy and Security, Osnabrück (Germany), March 4 - 6, 2015
- 12th International Conference on Security and Cryptography (SECRYPT 2015), Colmar (France), July 20 - 22, 2015
- 14th Annual Information Security South Africa Conference (ISSA 2015), Johannesburg (South Africa), August 12 - 14, 2015
- 10th International Conference on Availability, Reliability and Security (ARES 2015), Toulouse (France), August 24 - 28, 2015
- 12th International Conference on Trust, Privacy & Security in Digital Business (TrustBus 2015), held in conjunction with the 26th International Conference on Database and Expert Systems Applications (DEXA 2015), Valencia (Spain), September 1 - 4, 2015
- 2nd Workshop on Security in Highly Connected IT Systems (SHCIS 2015), held in conjunction with the 20th European Symposium on Research in Computer Security (ESORICS 2015), Vienna (Austria), September 21 - 25, 2015
- 20th European Symposium on Research in Computer Security (ESORICS 2015), Vienna (Austria), September 21 - 25, 2015
- 18th International Conference on Information Security and Cryptology (ICISC 2015), Seoul (South Korea), November 25 - 27, 2015
- 8th International Conference on Security Technology (SecTech 2015), Jeju Island (Korea), November 25 - 28, 2015
- 11th International Conference on Information Assurance and Security (IAS 2015), Bhubaneswar (India), December 5 - 6, 2015
- 6th International Conference on e-Democracy (eDemocracy 2015), Athens (Greece), December 10 - 11, 2015

Rolf Oppliger has already agreed to serve as a member of the programm committee for a few international conferences and workshops that will take place in 2016. A respective overview is available on the Internet[8] and will be kept up-to-date.

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.

[8] `http://www.esecurity.ch/pc.html`