Volume 19, 2022 http://www.esecurity.ch/communications.html

Contents

1 Editorial **2**

2 News **2**

3 Publications **2**

4 Information Security and Privacy Books **3**

5 Announcements **3**
5.1 University Lectures 3
5.2 Courses 3
5.3 Webinars 4
5.4 Invited Talks 4
5.5 Conferences and Workshops 4

1 Editorial

In the 2015 Editorial of eSECURITY communications, I wrote that I had been working on a method to engineer and plan cybersecurity measures in particularly large and heterogeneous organizations. In lack of a better name, I prematurely called the method OCEP, an acronym standing for "opportunistic cybersecurity engineering and planning." Due to other committments, I had to stop work on this topic in 2016. Meanwhile, I have been able to revisit the topic, and I think that I have finally found the right analogy to argue about cybersecurity in general, and cybersecurity management in particular. To the best of my knowledge, this analogy was first expressed and used by Ed Amoroso in an online lecture module entitled "Mapping Assets, Threats, Vulnerabilities, and Attacks" held at the New York University a few years ago.[1]

The analogy uses a doctor who manages the health risks of his or her patients. Instead of going through a list of possible diseases, the doctor measures some health parameters of his or her patients, and derives some medication from there. This approach is also applicable in cyberspace and cybersecurity management: Instead of doing a full-fledged threats and vulnerabilities analysis, the cybersecurity manager can measure some security parameters and make respective recommendations based on the respective results. There is no need to go through a threats and vulnerabilities analysis exercise—the results that can be gained from such an exercise are doomed to be illusive anyway. Based on the measurements of some well-selected security parameters, the cybersecurity manager has to team up with executive officers to select appropriate measures. These measure can either be technical, organizational, or legal. It goes without saying that anything that can be done technically should be done this way. But there are issues that cannot be addressed technically, and in these cases the use of organizational or legal measures may be appropriate to fill the gap.

The resulting approach is still risk-based in the sense that is considers risks, but it is somehow agnostic with regard to the causes of the risks. If, for example, the risk is data loss, then it does not really matter whether a hacker has deleted the data, some ransomware has irreversibly encrypted the data, some backup recovery method has not worked properly, or even a legitimate user has erroneously deleted the data. If the cause is irrelevant, then any probability measure is also irrelevant, and data loss must always be prevented in the first case. There are many possibilities to do so, but they all require backups to be made regularly and stored off-line. A similar line of argumentation applies to all relevant business risks. Instead of argueing about possible causes, it is more constructive and productive to discuss countermeasures. I think that this is more effective, but we will see. The ultimate benchmark is its usefulness in the field. I am open to challenge it in respective field trials.

[1] `https://www.coursera.org/lecture/intro-cyber-attacks/mapping-assets-threats-vulnerabilities-and-attacks-vwRNx`

2 News

During 2022, Rolf Oppliger has revised the book entitled *SSL and TLS: Theory and Practice*. The resulting third edition of the title is a major rewrite and is scheduled to appear in Q2 of 2023. Unfortunately, the cover has not been designed and cannot be shown here.

Also in 2022, Rolf Oppliger has done some consulting with regard to introducing digital signatures in business processes of a large company. In this context, he has been able to revisit the field in which he was working twenty years before (when the first digital signature law in Switzerland was enacted and put in place). On June 14, 2005, he had already given a talk entitled "Digital Signatures: From Theory to Practice" at the ZISC Information Security Colloquium of ETH Zurich, in which he promoted the idea of server-based signature services. This idea was quite ahead of its time, because the common widsdom at this time was still that it is absoltely necessary to hold the private signature key locally. But in the last decade, we have seen the proliferation of server-based architectures and cloud computing that have slowly paved the way for server-based signature services. Nowaydays, we have software as a service offerings from companies like Skribble[2] that make a living from providing such services to the public. This is exactly the type of service that was envisioned in the 2005 talk. This is a late confirmation of the talk's key message.

3 Publications

A short article (column) entitled "How To Manage Cyber Risks – Lessons Learnt from Medical Science" will appear in the January 2023 issue of the IEEE Computer magazine. The article is co-authored by Andreas Grünert (NCSC), and it continues some lines of thought that have their roots in a 2015 article in the IEEE

[2] `https://www.skribble.com`

Security & Privacy magazine (entitled "Quantitative Risk Analysis in Information Security Management: A Modern Fairy Tale") and a 2017 guest editor's introduction for an IEEE Computer magazine special issue on risk management (entitled "New Frontiers: Assessing and Managing Security Risks" and co-authored by Günther Pernul and Sokratis Katsikas). According to the ideas summarized in the Editorial, the article explains why cyber risk management based on a threats-and-vulnerabilities analysis doesn't work in the field, and how cyber risks can be managed instead. The suggested approach is conceptually related to medical science, and the way a doctor manages the health risks of his or her patients.

4 Information Security and Privacy Books

In 2022 (or early in 2023), the following book is published as the 52^{nd} title in Artech House's book series on information security and privacy:

- Michael Roytman, and Ed Bellis, *Cybersecurity, Risk-based Vulnerability Management*, ISBN 978-1-63081-938-5, 2022, 265 pp.

As mentioned above, the third edition of *SSL and TLS: Theory and Practice* will also be published in 2023.

Last but not least, the process of contracting new authors is going on. If you are working in the field and you 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 them).

5 Announcements

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

5.1 University Lectures

In the spring semester of 2022, Rolf Oppliger held his annual lecture on "IT Security" at the University of Zurich.[4] After two years of pandemic, the entire lecture and even the final exam took place onsite (and Microsoft Teams was only used as a complementary tool).

The lecture will be held again in the spring semester of 2023. As of this writing, the lecture is scheduled to take place onsite. A preliminary version of the lecture slides can be downloaded from the lecture Web site.[5] Please, feel free to download the slides and provide feedback.

5.2 Courses

On May 19, 2022, Rolf Oppliger gave a public one-day course entitled "Bitcoin & Blockchain — Kryptografische Grundlagen und Funktionsweise" for the eSECURITY Academy[6]. The course was well received and met the expectations of the attendees.

The following courses and bootcamps are scheduled for 2023:

- Kryptografie — Entstehungsgeschichte und Funktionsweise der modernen Verschlüsselungstechnik, March 16, 2023 (1 day)
- Signal-Protokoll — Moderne End-zu-End- Nachrichtenverschlüsselung für Messaging-Dienste wie WhatsApp, March 23, 2023 (1 day)
- SSL und TLS Sicherheit, March 30 – 31, 2023 (2 days)
- Bitcoin & Blockchain — Kryptografische Grundlagen und Funktionsweise, April 6, 2023 (1 day)
- Crypto Bootcamp, June 5 – 9, 2023 (5 days)
- Cybersecurity Bootcamp, June 19 – 23, 2022 (5 days)

All courses are German-speaking and will take place in Bern. You may find descriptions of the public courses and download respective flyers from the eSECURITY Academy's Web site (referenced in the footnotes). Also, if you want eSECURITY Academy to organize and put into effect a private event that meets your specific needs and requirements, then you may contact us. A private event can be held onsite or online, e.g., using Microsoft Teams. It can also be customized in terms of scope and content.

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

[4] `http://www.esecurity.ch/Teaching/uni-zh-2022.shtml`

[5] `http://www.esecurity.ch/Teaching/uni-zh-2023.shtml`

[6] `esecurity.academy`

5.3 Webinars

On February 17, 2022, Rolf Oppliger gave a 2.5-hours Webinar entitled "Authentication: From Passwords to FIDO2 and Zero-Knowledge" for the members of the Information Security Society Switzerland (ISSS[7]). The slides are available for download.[8] One of the key takeaways from the Webinar is that FIDO2 provides a good solution and is likely to take off. We see this today with the proliferation and success of passkeys (that are to replace passwords in many applications and respective use cases).

5.4 Invited Talks

During 2022, Rolf Oppliger repeated his introductory talk at the monthly held SBB security champions onboarding events. The talk is generally well received and feeds a lot of questions and points to discuss. The event series is to continue in 2023.

On May 11, 2023, Rolf Oppliger will give a computer science insights talk entitled "Evolution of E2EE Messaging on the Internet — From PGP to WhatsApp and Beyond" at the University of St. Gallen (HSG). The entire evolution (and hence the core content of the talk) is summarized in a slide that is available online.[9] The talk will mostly be centered around this slide, with a deep dive into the Signal protocol. If you want to attend the talk (without being a HSG student or faculty memebre), then please contact Rolf Oppliger before the event.

5.5 Conferences and Workshops

In 2022, Rolf Oppliger has served as a member of the program committee for the following events (in chronological order):

- 17th ACM ASIA Conference on Computer and Communications Security (ACM ASIACCS 2022), Nagasaki (Japan), May 30 – June 3, 2022
- 19th International Conference on Security and Cryptography (SECRYPT 2022), Lisbon (Portugal), July 11 – 13, 2022
- 19th International Conference on Trust, Privacy and Security in Digital Business (TrustBus 2022), held in conjunction with the 33rd International Conference on Database and Expert Systems Applications (DEXA 2022), Vienna (Austria), August 22 – 24, 2022
- 24th International Conference on Information and Communications Security (ICICS 2022), Kent (UK), September 5 – 8, 2022

Rolf Oppliger has already agreed to serve as a member of the program committee for several international conferences and workshops that will take place in 2023. A respective overview is available online.[10]

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 security. The company is registered in the commercial register of Bern-Mittelland (CH-035.1.023.622-7) and located in Muri b. Bern.

[7] https://isss.ch

[8] https://www.esecurity.ch/ISSSWebinar17.2.2022.pdf

[9] https://www.esecurity.ch/Academy/E2EEMessagingFlyer.jpg

[10] https://rolf.esecurity.ch/?page_id=16