Volume 20, 2023 http://www.esecurity.ch/communications.html

Contents

1 Editorial

In today's increasingly complex and dynamic world, it has become important not only to have expert knowledge in a particular field of study, but also to fully understand it and be able to properly apply it in the field. Textbooks are commonly used to provide this level of knowledge and in-depth understanding, and I have been active as a book author and series editor on information security and privacy for the past 30 years.[1]

Unfortunately, technical reference books are somehow out of fashion today, and people are looking for alternative and/or complementary ways and formats of knowledge transfer that are more timely and correlated with their personal requirements and needs. They make heavy use of Youtube videos, podcasts, blog posts, and so on and so forth, and the common denominators of all of these formats are that they are everywhere and at any time available, fast, direct, personal and interactive, as well as multimedia.

Some of these requirements (in particular, the interactivity requirement) can be met with lectures, courses, and seminars that may take place physically or virtually. During the Corona pandemic we have learned to utilize to the full all kinds of online lectures and courses, as well as webinars (be they massive open or not). Again, I have been active in this area, as I have been teaching for both the University of Zurich and the eSECURITY Academy[2] (among others). The requirement that a format of knowledge transfer must be everywhere and at any time available can be met by recording the event and making the respective recordings publicly available on the Internet.

Having all of these possibilities in front of us, the question that pops up immediately is what format(s) serve(s) best the purpose of knowledge transfer. Luckily, the formats are not mutually exclusive, meaning that they can be combined in unique ways. I think that textbooks are still valuable and even required in all fields of study that are non-trivial, including, of course, cybersecurity. But I also think that they are best complemented with specifically crafted educational videos that are multimedia in nature. The core of knowledge and understanding is best transferred with slides and oral explanations (that complement the textbooks). But because humanity is a special kind of storyteller, the explanations should be as personal as possible given the subject matter. This also asks for a video feed that shows the knowledge broker be integrated into the videos.

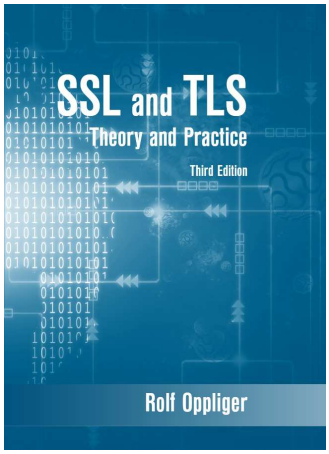
Against this background, I firmly believe that the future of knowledge transfer is a mixture of high quality textbooks that are complemented with educational videos to provide background information and additional stories in a more recreational and anecdotal way (than textbooks do). I am currently aligning and reshaping the eSECURITY Academy towards this vision, and I also intend to create respective videos for my own books. The overall goal is to launch teachware that serves the needs of practitioners working in the field.

[1] Refer to `https://blog.esecurity.ch/?p=599` to learn more about the importance of technical reference books (or textbooks, respectively).

[2] `https://esecurity.academy`

2 News

In summer 2023, Rolf Oppliger's new book entitled *SSL and TLS: Theory and Practice, Third Edition* (ISBN 978-1-68569-015-1) was released and is now available in the shelves of the bookstores. The book cover looks as follows (in case you are looking for it):



Kenny Paterson from ETH Zurich has been kind enough to provide the foreword. More information is available on the book's web site. This also includes a slide deck for each chapter of the book (just in case you want to use the book to teach classes or give courses about the SSL and TLS protocols).

3 Publications

A short article (and Cybertrust column) entitled "How To Manage Cyber Risks – Lessons Learnt from Medical Science" appeared 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 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). 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.

Work on this topic has continued meanwhile, and in February 2024, a follow-up article entitled "How To Measure Cybersecurity and Why Heuristics Matter," will appear—again as a Cybertrust column—in the IEEE Computer magazine. This time, the article argues that heuristics are required in cyberspace to complement or even replace the threats-and-vulnerabilities analyses that have been tried out in the past without success. We know that the article is contraversial, and we would like to start a respective discussion in the community. Also, we plan to continue this line of research in the future.

4 Information Security and Privacy Books

As mentioned above, the third edition of *SSL and TLS: Theory and Practice* (ISBN 978-1-68569-015-1) was published in Artech House's book series on information security and privacy in 2023.

The next title to be published (probably in 2024) is entitled *Learning and Experiencing Cryptography with CrypTool and SageMath* (ISBN 978-1-68569-017-5). The book was written by Bernhard Esslinger and his colleagues, and—as its title suggests—it addresses CrypTool,[3] i.e., a suite of free e-learning programs in the area of cryptography and cryptanalysis, and SageMath,[4] i.e., a free open-source mathematics software system. As such, the book mainly targets practitioners working on applied cryptography.

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[5] for the coordinates of them).

[3] `https://www.cryptool.org`

[4] `https://www.sagemath.org`

5 Announcements

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

5.1 University Lectures

In the spring semester of 2023, Rolf Oppliger held his annual lecture on "IT Security" at the University of Zurich.[6] Again, the lecture (including the final exam) took place onsite and was recorded with Zoom.

The lecture will take place again in the spring semester of 2024 (onsite). A preliminary version of the completely revised lecture slides can be downloaded from the lecture web site.[7] Please, feel free to download the slides and provide feedback.

5.2 Courses

In 2023, no eSECURITY Academy course took place. But for the year 2024, the following courses and bootcamps are currently scheduled:

- SSL und TLS Sicherheit, April 4 – 5, 2024 (2 days)
- Tor & Darkweb, April 23, 2024 (1 day)
- Bitcoin & Blockchain — Kryptografische Grundlagen und Funktionsweise, April 25, 2024 (1 day)
- Kryptografie — Entstehungsgeschichte und Funktionsweise der modernen Verschlüsselungstechnik, April 30, 2024 (1 day)
- Signal-Protokoll — Moderne End-zu-End- Nachrichtenverschlüsselung für Messaging-Dienste wie WhatsApp, May 2, 2024 (1 day)
- Crypto Bootcamp, October 14 – 18, 2024 (5 days)
- Cybersecurity Bootcamp, October 21 – 25, 2024 (5 days)

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

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

[7] `http://www.esecurity.ch/Teaching/uni-zh-2024.shtml`

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 a footnote above). 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. We are open in most regards.

5.3 Invited Talks

During 2023, Rolf Oppliger repeated his introductory talk at the monthly held SBB security champions onboarding events. The event series is scheduled to be continued in 2024.

In addition to these talks, Rolf Oppliger also gave the following three invited talks in 2023:

- On May 11, 2023, he gave 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.[8]
- On August 28, 2023, he gave a related talk entitled "End-to-End Encrypted (E2EE) Messaging with Forward Secrecy and Post-Compromise Security" at the Singapore Management University (SMU). This talk particularly addresses the security features of E2EE messaging.
- On September 14, 2023, he participated in the 2nd Zürcher Datenschutztagung (in German) and gave a talk about the current state of the art in encryption (entitled "Verschlüsselung: Tour d'Horizon").

In 2024, an invited talk is scheduled to take place on July 2 as part of the ISSS Zürcher Tagung on risk management.[9] The title of the German-speaking talk will be "Riskomanagement in der Informatiksicherheit: Was wir von der Medizin lernen können." It would be nice if you were able to participate in this event.

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

[9] `https://isss.ch/veranstaltungeb-kurse/isss-zuercher-tagung-risk-management/`

5.4 Conferences and Workshops

In 2023, Rolf Oppliger has served as a member of the program committee for the following events (in chronological order):

- 4th Silicon Valley Cybersecurity Conference (SVCC 2023), San Jose (USA), May 17 – 19, 2023
- 18th ACM ASIA Conference on Computer and Communications Security (ACM ASIACCS 2023), Melbourne (Australia), June 5 – 9, 2023
- IEEE International Conference on Metaverse Computing, Networking and Applications (ACM MetaCom 2023), Track 5: Security, Privacy and Trust, Kyoto (Japan), June 26 – 28, 2023
- 20th International Conference on Security and Cryptography (SECRYPT 2023), Rome (Italy), July 10 – 12, 2023
- 17th International Conference on Network and System Security (NSS 2023), Kent (UK), August 14 - 16, 2023
- 25th International Conference on Information and Communications Security (ICICS 2023), Tianjin (China), November 18 – 20, 2023
- 9th International Symposium on Security in Computing and Communications (SSCC 2023), Bangalore (India), December 18 - 20, 2023

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 2024.[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.

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