eSECURITY®
communications

Volume 15, 2018 http://www.esecurity.ch/communications.html

Contents

1 Editorial

After the successful launch of the eSECURITY Education Center in 2017, we have reshaped the educational branch of eSECURITY Technologies Rolf Oppliger and relaunched it under the newly coined name eSECURITY Academy and the domain name `esecurity.academy` (that is redirected to a subdomain of `esecurity.ch`). We think that the `academy` top level domain (TLD) is more appropriate and better suits this type of offering than the `ch` TLD.

The aims and scope of the eSECURITY Academy remain the same, but the offerings are expanded in certain ways:

- First, the number of events is expanded to address more topics than just SSL/TLS, Bitcoin, and blockchain.
- Second, it is planned to offer events in English (in addition to German) and to organize them in Zürich (in addition to Bern). The events will certainly be aligned with the demand as far as possible.

The actual offerings are fleshed out and announced on the Web site of the eSECURITY Academy.[1] With this relaunch and expansion of offerings, I hope that the eSECURITY Academy better meets your needs, and that it can establish itself as a major source of knowledge for the cybersecurity professionals working in the field. Please, let me know if you have any additional ideas or wishes. I appreciate any feedback, and I am looking forward hearing from you in one way or another.

2 News

On July 23, 2018, Rolf Oppliger had the opportunity to visit the National Cryptologic Museum of the National Security Agency (NSA) located in Fort Meade, Maryland (USA).[2] The museum provides an interesting insight into the history of cryptology (both in terms of cryptography and cryptanalysis). Among many other things, the museum hosts a public library with all relevant books related to cryptography. This includes, among many other titles, the first edition of *Contemporary Cryptography* (ISBN 978-1-58053-642-4). During his visit, Rolf Oppliger was kindly asked to sign the copy of the book by the librarian in charge.

With the relaunch of the eSECURITY Academy (as mentioned above), a new logo (as displayed on the Web site of the eSECURITY Academy) and a new advertisement picture were created. This picture is used as often as possible to establish a recognition value. It looks as follows:

3 Publications

Rolf Oppliger is working up the working principles of the Signal protocol (also used in WhatsApp) and a few other messaging protocols and respective apps, such as OTR, iMessage, and Threema. On the one hand, the results of this work will be used for a course provided in the eSECURITY Academy. On the other hand, they will also be used for a new book. As of this writing, it is not clear yet whether the book will be a second edition of *Secure Messaging on the Internet* (ISBN 978-1-60807-717-5) or a new book with an entirely new title. In either case, the book will start from conventional approaches for secure e-mail on the Internet, such as PGP/OpenPGP and S/MIME, and then elaborate on the more modern approaches for secure messaging mentioned above. Most imporatntly, it will introduce, fully discuss, and put into perspective the Signal protocol

[1] `http://esecurity.academy`

[2] `https://www.nsa.gov/about/cryptologic_heritage/museum/`

that is omnipresent today. As there is no competing book so far, it may fill a market niche, and it may be useful for professionals working on secure and end-to-end encrypted (E2EE) messaging.

Rolf Oppliger is also rewriting major parts of *Contemporary Cryptography, Second Edition* (ISBN 978-1-60807-717-5) with regard to a 3rd edition. There are many changes and new developments that are now addressed in the manuscript, such as the cryptographic hash function Keccak/SHA-3, new modes of operation for block ciphers, such as CCM and GCM, authenticated encryption, new stream ciphers, such as Salsa20/ChaCha20, elliptic curve cryptography (ECC) and respective cryptosystems, as well as Carter-Wegman message authentication codes (MACs), such as UMAC and Poly1305. As mentioned below, the rewritten chapters 1 and 2 are also used as a text for self-study in the upcoming lecture of Rolf Oppliger. The publication date of the new book is still open and subject to negotiation. The year 2020 is a likely target for this endeavor.

4 Information Security and Privacy Books

In 2018, the following title was published in Artech House's book series on information security and privacy:

- Ari Takanen, Jared D. DeMott, Charlie Miller, and Atte Kettunen, *Fuzzing for Software Security Testing and Quality Assurance, Second Edition*, 978-1-60807-850-9, 2018, 330 pp.

This title is already the forty-sixth book published in the series. As such, the series is the most comprehensive one that addresses and is devoted to information security and privacy. We still intend to expand it in the future. So 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 the Acquisitions Editor in charge for North and South America, Australia and New Zealand (David Michelson). You may refer to the book series' homepage[3] for the respective coordinates.

5 Announcements

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

5.1 University Lectures

In the spring semester of 2018, Rolf Oppliger held his regular lecture on "IT Security" at the University of Zurich. The lecture was popular and attended by more than 50 students. The slides that were used are electronically available at the lecture's Web site[4] (that is also accessible from outside the University of Zurich).

The lecture will be held again in the spring semester of 2019 (MINF4221, Course No. 2173). The respective slides are revised from scratch, and a preliminary version of them is available on this years lecture Web site.[5] Please, feel free to download the slides and provide some feedback. Instead of exercises, the lecture now requires a self-study of the cryptographic basics and fundamentals. As mentioned above, a respective extract from the updated version of *Contemporary Cryptography*, i.e., Chapters 1 and 2, is made available for this purpose.[6] Again, any feedback regarding the slide set and/or this extract is welcome and highly appreciated.

5.2 Courses

As mentioned in the Editorial, Rolf Oppliger continues his series on courses and bootcamps in the eSECURITY Academy. The tentative schedule for the year 2019 is as follows:

- *Bitcoin & Blockchain — Kryptografische Grundlagen und Funktionsweise* (German), March 7 - 8, 2018 (2 days), Bern
- *Bitcoin & Blockchain — Cryptographic Fundamentals and Working Principles* (English), March 14 - 15, 2018 (2 days), Zürich
- *SSL und TLS Sicherheit* (German), March 21 - 22, 2019 (2 days), Bern
- *TLS 1.3* (German), March 28, 2019 (1 day), Bern

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

[4] http://www.esecurity.ch/Teaching/uni-zh-2018.shtml

[5] http://www.esecurity.ch/Teaching/uni-zh-2019.shtml

[6] http://www.esecurity.ch/Books/Book3edChap1-2.pdf

- *Internet Messaging Sicherheit — Von PGP bis Signal und WhatsApp* (German), May 9, 2019 (1 day), Bern
- *Kryptografie — Entstehungsgeschichte und Funktionsweise der modernen Verschlüsselungstechnik* (German), May 23, 2019 (1 day), Bern
- *Crypto Bootcamp* (German), June 24 – 28, 2019 (5 days), Bern
- *Cybersecurity Bootcamp* (German), September 2 – 6, 2019 (5 days), Bern

There are several courses that are new and leading-edge. This includes, for example, the courses on TLS 1.3 (whose official specification has been available since Augst 2018) and the course on Internet messaging security (with the major focus on the Signal E2EE messaging protocol that is also used in WhatsApp). The second course itemized above is the one that is planned to be held in English and to take place in Zürich. The event location in Bern is probably Welle 7 nearby the main station,[7] whereas the event location in Zürich still needs to be determined. It is certainly going to be a location nearby the main station, too.

While courses refer to ex-cathedra teaching, bootcamps focus more on interaction and discussion (that's why they last longer). According to the current planning, there are two bootcamps scheduled for 2019: One on cryptography (June 24 – 28) and one on cybersecurity (September 2 – 6). Both events are customized to the security professional who wants to learn the state of the art and the open issues related to the respective topic (cryptography or cybersecurity). The exact modus operandi also depends on the participants and their personal preferences—we are open to any proposal here.

The courses and bootcamps that will eventually be carried out in the second halve of 2019 will be announced on the Web site of the eSECURITY Academy[8] at some later point in time. Again, if you have some topic preference, then please let us know. We are interested in offering events that actually serve your needs and interests.

If you want eSECURITY Academy to organize and put into effect a private event that meets your specific and unique requirements, then you may send us a request. It goes without saying that any such request is without any commitment or obligation.

5.3 Conferences and Workshops

In 2018, Rolf Oppliger served as a member of the programm committee for the following events (in chronological order):

- 15th International Conference on Security and Cryptography (SECRYPT 2018), Porto (Portugal), July 26 - 28, 2018
- 17th International Information Security South Africa Conference (ISSA 2018), Johannesburg (South Africa), August 15 - 16, 2018
- 23rd European Symposium on Research in Computer Security (ESORICS 2018), Barcelona (Spain), September 3 - 7, 2018
- 15th International Conference on Trust, Privacy & Security in Digital Business (TrustBus 2018), held in conjunction with the 29th International Conference on Database and Expert Systems Applications (DEXA 2018), Regensburg (Germany), September 5 - 6, 2018
- 6th International Symposium on Security in Computing and Communications (SSCC 2018), Bangalore (India), September 19 - 22, 2018
- 14th International Conference on Information Assurance and Security (IAS 2018), Porto (Portugal), December 13 - 15, 2018

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 2019. A respective overview is available on the Internet[9] and will be updated periodically.

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] `http://www.welle7.ch`

[8] `http://esecurity.academy`

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