Volume 17, 2020 http://www.esecurity.ch/communications.html

Contents

1 Editorial

After a good start, 2020 has become the year of the COVID-19 pandemic and worldwide coronavirus crisis that has brought the global economy to their knees. Many countries, including Switzerland, have experienced a lockdown in spring, and are about to partly refresh this experience during the second wave.

The flip side of this situation is an incredible push towards digitization in many areas of our daily life, including education and work. We have all learned to use videoconferencing tools, like Microsoft Teams and Zoom, and we as security professionals have been asked numerous times whether the security features of these tools satisfy the requirements of today's business world. This particularly applies to the question whether the use of cryptography in these tools is appropriate and refers to the state of the art.

After having been asked this question over and over again, I decided to write a blog post[1] about the meaning of end-to-end encryption (E2EE) in the realm of voice and video conferencing. As is always the case in security, the answer depends—here, it mainly depends on the conference topic and the size of the group. The conference topic is a no-brainer. But the size of the group is also an issue, and the smaller the group size, the more meaningful E2EE tends to be. Beyond a certain group size, the meaning of E2EE is questionable and purely illusive. Remember Benjamin Franklin saying that "three may keep a secret if two of them are dead." This quote clearly makes the point that keeping a secret in a large group is next to impossible. Franklin is overly pessimistic with regard to the group size. But even if one is less pessimistic and allow groups of more than one person, it is still unrealistic that the group can prevent a secret from leaking.

To make the point without ambiguity: I am a strong proponent of E2EE messaging and conferencing, but I also think that groups need to be kept sufficiently small to allow E2EE to be effective. Making a group accessible to everybody and then using E2EE to keep it secure it not going to work. Security needs to be adjusted in many ways, and E2EE is only one mechanism that may work in some situations. It is not a silver bullet that works everywhere and under all circumstances. We have learned this lesson in many situations in the real world.

Against this background, I consider the research question addressed by the IETF Message Layer Security (MLS) working group to make E2EE messaging and the respective key management scalable to very large groups to be a very interesting and intellectually challenging, but I don't consider it to be highly relevant in practice. Beyond a certain group size, it is impossible to protect against information leakage, even if this information is end-to-end encrypted. Again, cryptography cannot achieve everything.

This viewpoint should not be taken as an argument not to follow the IETF MLS WG and the evolving MLS protocol. It is an important and intellectually stimulating topic, but it must be considered this way. It is about cleverly using cryptography and coming up with interesting results, but it is not primarily about security. If my most recent book *End-to-End Encrypted Messaging*[2] (ISBN 9781630817329) ever went into a second edition, then MLS would certainly be a major topic to be addressed in much more detail (simply because it is interesting and intellectually stimulating). I hope that the book sales are going to make this possible. In the meantime, it is mentioned for the sake of completeness, but it is not addressed in much detail.

2 News

One of the few positive side effects of the coronavirus crisis is that people have more time to work on topics that are important to them. This also applies to Rolf Oppliger who has been able to work extensively on the revision of his cryptography book. Due to the fact that the book has been revised fundamentally, it is going to be published as an entirely new book—instead of a third edition of *Contemporary Cryptography*. The new book is entitled *Contemporary 101: From Theory to Practice*, and it is scheduled to be publicly released in summer 2021.

The book will also be the basis for the Crypto Bootcamp that is scheduled to take place in June 2021 (cf. Section 5.2). Providing guidance in this increasingly important topic is important for anybody using cryptographic technologies and mechanisms to secure systems and applications. Such technologies and mechanisms should not be chosen at random, but should rather be selected with care and intuition. This is not simple (to say the least). The Crypto Bootcamp is to provide the basic knowledge that is necessary to make this selection. It would be nice, if there were sufficiently many attendees ($geq 4$) to make it happen this year.

[1] `https://blog.esecurity.ch/`p=534?

[2] `https://www.esecurity.ch/Books/e2ee.html`

3 Publications

Early in 2020, Rolf Oppliger's latest book entitled *End-to-End Encrypted Messaging* was published. The book cover looks as follows:

While the primary focus of his prior books on secure messaging was on PGP, OpenPGP, and S/MIME, the focus of this book is the Signal protocol and its implementation in the Signal messenger, WhatsApp, Viber, Wire, and Riot, also in comparison to some other E2EE messengers, such as iMessage, Threema, Wickr, and Telegram. The Signal protocol clearly marks the state of the art when it comes to end-to-end encrypted (E2EE) messaging on the Internet. It is being adapted by most messaging and conferencing apps, most recently even by Google in its Messages app (that is otherwise an RCS client, where the acronym RCS stands for "Rich Communication Services" that is supposedly the successor service of SMS and MMS).

As already mentioned in the News section, Rolf Oppliger is also finishing up his new book on cryptography, entitled *Contemporary 101: From Theory to Practice*. It is scheduled to be released in 2021. If you want to proofread parts of it, then you can still volunteer (and contact Rolf Oppliger with e-mail or phone).

4 Information Security and Privacy Books

In addition to *End-to-End Encrypted Messaging*, the following title was published in Artech House's book series on information security and privacy in 2020:

- Axel Wirth, Christopher Gates, and Jason Smith, *Medical Device Cybersecurity for Engineers and Manufacturers*, 978-1-63081-815-9, 2020, 260 pp.

This title is the forty-ninth book published in the series. As such, the series is the most comprehensive one that addresses and is devoted to information security and privacy. It is still intend to expand it in the future, and hence 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, then you may contact either the Acquisitions Editor for North and South America, Australia and New Zealand (David Michelson), the Senior Commissioning Editor for Europe, Middle East, Africa and Asia (Merlin Fox), or the Series Editor (Rolf Oppliger). 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 2020, Rolf Oppliger held his annual lecture on "IT Security" at the University of Zurich.[4] While the beginning of the lecture took place in front-of-class teaching mode, the second half was held virtually (using Microsoft Teams). Even the final exam took place this way, and it posed a tremendous challenge to all participants (and, of course, the lecturer).

The lecture will be held again virtually in the spring semester of 2021. 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 some feedback. Instead of exercises, the lecture again requires a self-study of the cryptographic basics and fundamentals. A respective extract from the book *Contemporary 101: From Theory to Practice* (mentioned above), i.e., Chapters 1 and 2, is made available for this purpose.[6] It may be interested reading, even for people not attending the lecture in the first place.

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

[4] `http://www.esecurity.ch/Teaching/uni-zh-2020.shtml`

[5] `http://www.esecurity.ch/Teaching/uni-zh-2021.shtml`

[6] `http://www.esecurity.ch/Books/BookChap1-2.pdf`

5.2 Courses

On November 5, 2020, Rolf Oppliger held a course on Internet messaging security in a newly established business center called zentroom[7] in the main station of Bern. The course was well received and stimulated a lot of interesting discussions.

Rolf Oppliger continues his series on courses and bootcamps in the eSECURITY Academy.[8] The events schedule for the first halve of 2021 are as follows:

- *Bitcoin & Blockchain — Kryptografische Grundlagen und Funktionsweise* (German), April 1, 2021 (1 day), Bern
- *SSL und TLS Sicherheit* (German), April 8 - 9, 2021 (2 days), Bern
- *Internet Messaging Sicherheit — Von PGP bis Signal und WhatsApp* (German), April 29, 2021 (1 day), Bern
- *Kryptografie — Entstehungsgeschichte und Funktionsweise der modernen Verschlüsselungstechnik* (German), May 6, 2021 (1 day), Bern
- *Crypto Bootcamp* (German), June 14 – 18, 2021 (5 days), Bern
- *Cybersecurity Bootcamp* (German), June 28 – July 2, 2021 (5 days), Bern

While courses refer to ex-cathedra teaching, bootcamps focus more on interaction and discussion (that's why they last longer).

The courses and bootcamps that will eventually be carried out in the second halve of 2021 will be announced on the Web site of the eSECURITY Academy at some later point in time. If you have some topic preference, then please let us know. We are interested in offering events that serve your needs meet your interests.

If you want the 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 (also indicating the topic of your choice). It goes without saying that any such request is without any commitment or obligation.

5.3 Conferences and Workshops

In 2020, Rolf Oppliger has served as a member of the programm committee for the following events (in chronological order):

- 17th International Conference on Security and Cryptography (SECRYPT 2020), Paris (France), July 8 - 10, 2020
- 22th International Conference on Information and Communications Security (ICICS 2020), Copenhagen (Denmark), August 24 - 27, 2020
- 19th International Information Security South Africa Conference (ISSA 2020), Pretoria (South Africa), August 25 26, 2020
- 17th International Conference on Trust, Privacy and Security in Digital Business (TrustBus 2020), held in conjunction with the 31st International Conference on Database and Expert Systems Applications (DEXA 2020), Bratislava (Slovakia), September 14 17, 2020
- 25th European Symposium on Research in Computer Security (ESORICS 2020), Guildford (UK), September 14 - 18, 2020
- 8th International Symposium on Security in Computing and Communications (SSCC 2020), Chennai (India), December 14 17, 2020
- 16th International Conference on Information Assurance and Security (IAS 2020), takes place virtually, December 15 - 18, 2020

Rolf Oppliger has already agreed to serve as a member of the programm committee for some international conferences and workshops that will take place in 2021. A respective overview is available online.[9]

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.

© 2020 eSECURITY Technologies Rolf Oppliger

[7] `https://zentroom.ch`

[8] `esecurity.academy`

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