Volume 16, 2019 http://www.esecurity.ch/communications.html

Contents

1 Editorial

In 2019, I have worked intensely on my new book entitled *End-to-End Encrypted (E2EE) Messaging* (ISBN 9781630817329) that is scheduled to be released next year. While the focus of my prior books on secure messaging was OpenPGP and S/MIME, the focus of this book now is the Signal protocol and its implementation in the Signal messenger, WhatsApp, Viber, Wire, and Riot, in comparison to some other E2EE messengers, such as iMessage, Wickr, Threema, and Telegram. OpenPGP and S/MIME are still addressed in the new book, but mainly for the sake of completeness. These standards are somehow out of date and hardly play a role in the secure and E2EE messaging arena today.

A recent story[1] in the New York Times has brought up an issue that is relevant but often forgotten when it comes to secure and E2EE messaging: A messaging app is usually configured to have full access to the smartphone on which it is installed. This, in turn, means that the provider of the app can access the contacts, location, and other personal information, and that this information can also be misused in many ways. This seems to have happened in the Emirates with the messaging app ToTok[2] that has been revealed (in the New York Times article) to be a spy tool. Any user who has installed ToTok on his or her smartphone must accept that the device may also be accessed by the provider or a third party acting on behalf of the provider, such as a government intelligence agency. There is no need to encrypt messages in transit, if they are decrypted and locally stored in unencrypted form and can be accessed there. Hence, the trustworthiness of the messaging app provider is key to its security. If this provider is not trustworthy, then there is no need to discuss the security of the app in the first place. One way to improve the trustworthiness of a messaging app is to reveal the protocol that is being used and to make the implementation open source. This is done, for example, in the case of the Signal messenger, and this is certainly one of the reasons why this messenger has such a good reputation in the community. Any messaging app that implements a proprietary protocol or is closed source must be considered skeptically. It may behave honestly, but it may also do the opposite and be a spy tool. As the case of ToTok has revealed, it is often difficult to distinguish the two cases, and any messaging app of dubious source must be considered with a grain of salt—the use of cryptography cannot change this.

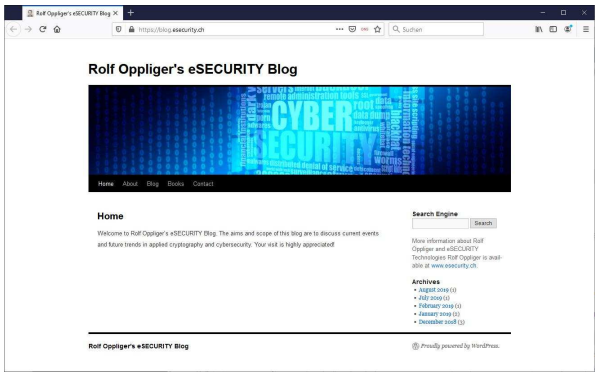
[1] https://www.nytimes.com/2019/12/22/us/politics/totok-app-uae.html

[2] https://totok.ai

2 News

Earlier this year, eSECURITY Technologies Rolf Oppliger has set up and is two blogs and a complementary Web site for the eSECURITY Academy. The administration software in use is WordPress.

Rolf Oppliger's eSECURITY Blog[3] is used to discuss current events and future trends in cybersecurity. The blog has started well and already comprises several posts. The front page looks as follows:

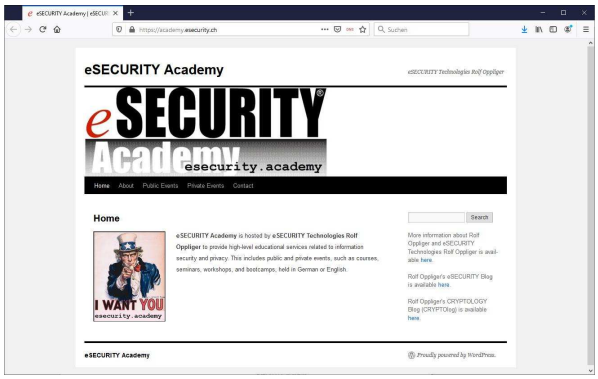


As its name suggests, **Rolf Oppliger's CRYPTOLOGY Blog (CRYPTOlog**[4]**)** is more focused on cryptology and applications thereof, and it provides respective questions and answers. Albert Einstein's quote is to emphasize the fact that good questions are generally more valuable than respective answers, and it should invite readers to ask good questions. The current posts address the Salsa20 and ChaCha20 stream ciphers, as well as the renegotiation and triple handshake attacks that affect the TLS protocol. The front page looks as follows:

[3] https://blog.esecurity.ch

[4] https://cryptolog.esecurity.ch

The complementary **eSECURITY Academy** Web site[5] is to publicly announce events, e.g., courses, seminars, and bootcamps, that are scheduled to take place in the next couple of months. The current schedule is outlined in Section 5.3. The front page looks as follows:



Please, feel free to visit any of these blogs or Web sites, and provide some feedback. As usual, this is welcome and highly appreciated.

3 Publications

Besides *End-to-End Encrypted (E2EE) Messaging*, Rolf Oppliger has not been able to publish anything else. This is not going to change in the foreseeable future, because the books on *Contemporary Cryptography* and *SSL and TLS: Theory and Practice* (both in their second edition) need to be updated and revised soon. The respective projects have already started and the publications are tentatively scheduled for 2021 and 2022.

4 Information Security and Privacy Books

In 2019, the following title was published in Artech House's book series on information security and privacy:

- Serge Borso, *The Penetration Tester's Guide to Web Applications*, 978-1-63081-622-3, 9781630816223 2019, 280 pp.

This title is the forty-seventh 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 (David Michelson). You may refer to the book series' homepage[6] for the respective coordinates.

5 Announcements

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

5.1 University Lectures

In the spring semester of 2019, Rolf Oppliger held his regular lecture on "IT Security" at the University of Zurich. It was attended by more than 50 graduate students.

The lecture will be held again in the spring semester of 2020 (MINF4221, Course No. 1573). A preliminary version of the lecture slides can be downloaded from the lecture Web site.[7] Please, feel free to download the slides and provide some feedback. Instead of exercises, the lecture requires a self-study of the cryptographic basics and fundamentals. A respective extract from the updated version of *Contemporary Cryptography*, i.e., Chapters 1 and 2, is made available for this purpose.[8] Again, any feedback regarding this extract is welcome and highly appreciated.

5.2 Invited Talks

On June 6, 2019, Rolf Oppliger gave a talk at the Conference on Applied Cryptography organized by the Cyber-Defence Campus in Thun, Switzerland.[9] In his talk, he gave an overview about secure and E2EE messaging, basically addressing the three solutions (1)

[5] `https://academy.esecurity.ch` or more directly `esecurity.academy`

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

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

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

[9] `https://eventmobi.com/conferenceonapplied-cryptography`

OpenPGP and S/MIME, (2) OTR, and (3) Signal. The slides used for the talk are publicly available and can be downloaded from the cloud.[10]

5.3 Courses

Rolf Oppliger continues his series on courses and bootcamps in the eSECURITY Academy. The event schedule for the first halve of 2020 is as follows:

- *Bitcoin & Blockchain — Kryptografische Grundlagen und Funktionsweise* (German), March 19 - 20, 2020 (2 days), Bern
- *SSL und TLS Sicherheit* (German), March 26 - 27, 2020 (2 days), Bern
- *TLS 1.3* (German), April 2, 2020 (1 day), Bern
- *Internet Messaging Sicherheit — Von PGP bis Signal und WhatsApp* (German), April 30, 2020 (1 day), Bern
- *Kryptografie — Entstehungsgeschichte und Funktionsweise der modernen Verschlüsselungstechnik* (German), May 7, 2020 (1 day), Bern
- *Crypto Bootcamp* (German), June 8 – 12, 2020 (5 days), Bern
- *Cybersecurity Bootcamp* (German), June 22 – 26, 2019 (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 2020 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 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.

5.4 Conferences and Workshops

In 2019, Rolf Oppliger has served as a member of the programm committee for the following events (in chronological order):

- 16th International Conference on Security and Cryptography (SECRYPT 2019), Prague (Czech Republic), July 26 - 28, 2019
- 18th International Information Security South Africa Conference (ISSA 2019), Johannesburg (South Africa), August 14 - 15, 2019
- 16th International Conference on Trust, Privacy and Security in Digital Business (TrustBus 2019), held in conjunction with the 30th International Conference on Database and Expert Systems Applications (DEXA 2019), Linz (Austria), August 26 - 29, 2019
- 24th European Symposium on Research in Computer Security (ESORICS 2019), Luxembourg, September 23 - 27, 2019
- 15th International Conference on Information Assurance and Security (IAS 2019), Bhopal (India), December 10 - 12, 2019
- 8th International Conference on e-Democracy (eDemocracy 2019), Athens (Greece), December 12 - 13, 2019
- 7th International Symposium on Security in Computing and Communications (SSCC 2019), Trivandrum (India), December 18 - 21, 2019

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 2020. A respective overview is available on the Internet[11] 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.

[10] `https://eventmobi-files.s3.amazonaws.com/events/35606/df24542d-0087-42cb-b1cd-cd1bf261a41e`

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