eSECURITY®
communications

Volume 18, 2021 http://www.esecurity.ch/communications.html

Contents

1 Editorial

2021 has been the second year of the COVID-19 pandemic. This is unfortunate and there is currently no end in sight. Many people are therefore working from home and the notion of strong user authentication has become an issue. Some people are still using passwords, sometimes augmented and improved by 2-factor-authentication (2FA) technologies, such as SecurID, OATH-HOTP according to RFC 4226, or OATH-TOTP according to RFC 6238. OATH-TOTP is, for example, implemented in the Google and Microsoft Authenticators and has become a leading industry standard when it comes to 2FA.

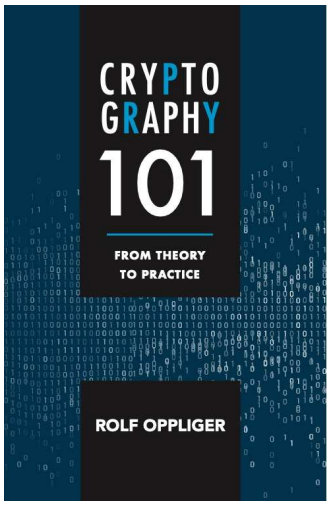
A few years ago, the Fast IDentity Online (FIDO) alliance[1] came up with a FIDO2 standard to unify the formerly used Universal Authentication Framework (UAF) and the Universal 2nd Factor (U2F) standards for biometrics and 2FA. FIDO2 consists of two protocols: WebAuthn[2] that is used between the browser (i.e., the client) and the relying party (i.e., the server), and the Client-To-Authenticator Protocol 2 (CTAP2) that is used between the browser and the authenticator that can be built-in the client platform (platform authenticator) or be an external token connected to the client (roaming authenticator) through Universal Serial Bus (USB), Bluetooth Low Energy (BLE), or Near Field Communication (NFC).

FIDO2 is the technology of choice to mitigate all attacks that have bothered password users in the past, such as social engineering (phishing in particular), password guessing, sniffing, and replay attacks. If used with token binding, FIDO2 is even able to mitigate some man-in-the-middle (MITM) attacks that operate at the transport layer (even if TLS is put in place). Technically speaking, token binding refers to a TLS extenstion, i.e., `token_binding`, that can be negotiated between the client and the server. If mutually supported, the client generates a public key pair and transmits the public key to the server (referenced with a Token Binding ID). When the client later generates its response to the relying party's challenge, it includes the Token Binding ID in the signature. This ensures that the challenge-response mechanism is bound to the proper TLS entities, and this, in turn, mitigates respective MITM attacks. FIDO2 with token binding clearly marks the state of the art when it comes to strong user authentication. From a security perspective, it is conceptually similar to mutually authenticated TLS connections, for example, using client-side smartcards.

Most vendors support FIDO2 in one way or another. This evn includes Apple nowadays. The bottom line is that FIDO2 has the potential to really bring the password (as an authentication technology) to the end of its life cycle. From a security and usability perspective, this would be greatly appreciated, and hence we hope that the ride is going to be successful as soon as possible. We are all keen on getting rid of our passwords — the sooner the better.

2 News

Earlier this year, Rolf Oppliger's new book *Contemporary 101: From Theory to Practice* (ISBN 978-1-63081-846-3) was published in Artech House's book series on information security and privacy. The book cover looks as follows:



The book is tutorial in nature and addresses all topics that are related to cryptography as used in the field. It can be used to teach courses and classes on cryptography, but it can also be used for self-study. Once again, Gene Spafford has been kind enough to provide a foreword.

More information about the book is available on its Web site.[3] This includes some 25% discount flyers for the US or UK offices of Artech House, as well as a comprehensive errata list (you may even contribute to this list by finding some additional errors).

[1] `https://fidoalliance.org`

[2] `https://www.w3.org/TR/webauthn-2/`

[3] `https://books.esecurity.ch/crypto101.html`

3 Publications

During the second half of 2021, Rolf Oppliger has spent a considerable amount of time creating slide decks for all 18 chapters of *Contemporary 101: From Theory to Practice*. The slides are published with a Creative Commons Attribution No Derivatives (CC BY-ND) 4.0 license, meaning that they can be freely downloaded (from the book's Web site mentioned above) and used at will. The slides are going to be used in the Crypto Bootcamp of the eSECURITY Academy (Section 5.2), as well as an advanced 5-day course on cryptography that will take place in the Swiss Federal Administration in 2022 (probably online).

4 Information Security and Privacy Books

In addition to *Contemporary 101: From Theory to Practice*, the following book was published as the 51^{th} title in Artech House's book series on information security and privacy in 2021:

- Kaustubh Dhondge, *Lifecycle IoT Security for Engineers*, ISBN 978-1-63081-803-6, 2021, 230 pp.

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[4] for the coordinates of them).

5 Announcements

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

5.1 University Lectures

In the spring semester of 2021, Rolf Oppliger held his annual lecture on "IT Security" at the University of Zurich.[5] The entire lecture and even the final exam took place online (again using Microsoft Teams).

The lecture will be held again in the spring semester of 2022. As of this writing, the lecture is still scheduled to take place onsite. This decision, however, may be subject to change, and it is currently unclear whether the plan will match reality. Anyway, a preliminary version of the lecture slides can be downloaded from the lecture Web site.[6] Please, feel free to download the slides and provide some feedback.

5.2 Courses and Webinars

All public courses provided by the eSECURITY Academy[7] had to be postponed to 2022 (also due to the pandemic). Consequently, the course program for 2022 looks as follows:

- Internet Messaging Sicherheit – Von PGP bis Signal und WhatsApp, April 6, 2022 (1 day)
- Kryptografie – Entstehungsgeschichte und Funktionsweise der modernen Verschlüsselungstechnik, April 8, 2022 (1 day)
- SSL und TLS Sicherheit, May 5 6, 2022 (2 days)
- Bitcoin & Blockchain – Kryptografische Grundlagen und Funktionsweise, May 19, 2022 (1 day)
- Crypto Bootcamp, June 27 July 1, 2022 (5 days)
- Cybersecurity Bootcamp, July 4 8, 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.

In 2021, Rolf Oppliger gave two 2.5-hours Webinars for the members of the Information Security Society Switzerland (ISSS[8]):

- On March 3, 2021, he gave a Webinar on "End-to-End Encrypted (E2EE) Messaging," basically addressing all technologies that can be used to provide E2EE messaging services on the Internet. The culminating point of the Webinar was the Signal protocol that is used in most E2EE

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

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

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

[7] `esecurity.academy`

[8] `https://isss.ch`

messengers, including WhatsApp. This protocol is involved and requires a thorough introduction and explanation. The Webinar did not address E2EE conferencing, such as currently implemented by Zoom or Microsoft Teams.

- On June 24, 2021, he gave another Webinar on "TLS 1.3: Evolutionary History and Innovations." As the title suggests, the Webinar outlined the evolutionary history of TLS 1.3 and explained the rationale behind all innovations and changes from previous versions of the SSL/TLS protocols (including all attacks that have been mounted and have made several press headlines in the recent past). This is a very timely topic, because most companies have deprecated SSL 3.0, TLS 1.0, and TLS 1.1, and only support TLS 1.2 (with a restricted set of cipher suites) and TLS 1.3.

According to the feedback, both Webinars were well received by the attendees. As such, the series will continue and a new Webinar entitled "Authentication: From Passwords to FIDO2 and Zero-Knowledge" is scheduled to take place on February 17, 2022. Again, ISSS members can freely register[9] and attend the Webinar. It would be great to meet you there and have an online discussion about the topic.

5.3 Invited Talks

In the second half of 2021, Rolf Oppliger was invited by the SBB Company[10] to give an introductory talk at each of the monthly held onboarding event for their newly assigned security champions. So far, the talk has been given 5 times, and it will supposedly held another 5 times in the first half of 2022. The talk introduces and briefly outlines the cybersecurity field from both a historical and personal perspective. It also addresses the major challenges for the future, such as increasing virtualization in cyberspace, cloud computing, and autonomous cyber-physical systems. Most importantly, the talk concludes with a quote from Charles Darwin who basically said that "it is not the strongest or most intelligent of the species that survives, but the one that is most adaptable to change." This rquote also applies to cybersecurity, and it means that cybersecurity professionals must fully understand their job and tool case, and that they must be as adaptive as possible. It also means that they must evolve from a naysayer to a yeasayer (or enabler). This will change the job of a security professional quite fundamentally, and it will also make it even more different from the job of a compliant officer or auditor. Cybersecurity is more involved than simply crossing the bullets in a checklist.

5.4 Conferences and Workshops

In 2021, Rolf Oppliger has served as a member of the program committee for the following events (in chronological order):

- 18th International Conference on Security and Cryptography (SECRYPT 2021), online-only event, July 6 8, 2021
- 23th International Conference on Information and Communications Security (ICICS 2021), Chongqing (China), September 17 - 19, 2021
- 18th International Conference on Trust, Privacy and Security in Digital Business (TrustBus 2021), held in conjunction with the 32nd International Conference on Database and Expert Systems Applications (DEXA 2021), Linz (Austria), September 27 30, 2021
- 26th European Symposium on Research in Computer Security (ESORICS 2021), Darmstadt (Germany), October 4 8, 2021

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 2022. A respective overview is available online.[11]

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.

[9] https://isss.ch/veranstaltungeb-kurse/isss-webinar-authentifikation-vom-passwort-zu-fido2-und-zero-knowledge/

[10] https://www.sbb.ch

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