eSECURITY® communications

Volume 14, 2017 http://www.esecurity.ch/communications.html

Contents

1 Editorial

In the Editorial of last year's issue of eSECURITY communications, I announced that I was going to expand the activities of the eSECURITY Education Center in the subsequent year. This expansion has actually taken place. On November 30 and December 1, 2017, I carried out a 2-day seminar on SSL and TLS security, and on December 7, 2017, I carried out a 1-day seminar on the cryptographic fundamentals and working principles of Bitcoin and blockchain. The venue for both seminars was the Welle7[1] at the railway station Bern PostParc. Each seminar was attended by 10 people, and—according to the feedback forms—was well received by the audience.

Due to the successful launch, I am going to continue the seminar series in 2018. In addition to the seminars on SSL and TLS as well as Bitcoin and blockchain (that is going to be extended from 1 to 2 days), I am also going to carry out a 5-day seminar on cryptography in theory and practice. This seminar is aimed at providing the cryptographic fundamentals the are necessary to understand cryptographic applications and protocols currently used in the field. Depending on the success of these seminars, I will then decide in which direction the series is going to be expanded in the future. I still think that there is a lack of opportunities for high-quality educational services that address security professionals in Switzerland. The aim of the eSECURITY Education Center is to fill this gap in the long term. If you have an opinion or suggestion in what direction the eSECURITY Education Center should evolve, then please let me know. I want to provide courses, seminars, and workshops on topics that are actually interesting for the community.

2 News

As mentioned above, the major news are (i) the successful launch of the eSECURITY Education Center in December 2017 and (ii) the continuation of the respective seminar series in the future. The education program for the first halve of 2018 is ready and available from the eSECURITY Education Center's Web site.[2] More courses, seminars, and workshops will be announced soon.

[1] http://www.welle7.ch

[2] https://education.esecurity.ch

3 Publications

Early in 2017, I coedited a special issue of the IEEE Computer magazine (Vol. 50, No. 4, April 2017, pp. 48–51) with Prof. Dr. Günter Pernul from the University of Regensburg and Prof. Dr. Sokratis Katsikas from the Norwegian University of Science and Technology (NTNU). The special issue was about the assessment and management of risks related to cybersecurity. Unfortunately, the call for papers was not well received and did not attract many authors. In the end, we had difficulties in finding a sufficiently large number of valuable contributions. Nevertheless, the special issue was still released in April 2017, and we wrote an editorial entitled "New Frontiers: Assessing and Managing Security Risks" for the issue.[3] The abstract is as follows: "Like the Wild West, cyberspace respects few laws and resists order. As essential, life-sustaining systems increasingly connect in this space, how will we go about identifying, assessing, anticipating, and managing risk?" If you are interested in reading the full article, then please let us know.

Later in 2017, I also contributed an article entitled "Disillusioning Alice and Bob" to the IEEE Security & Privacy magazine (Vol. 15, No. 5, September/October 2017, pp. 82–84).[4] The article starts from the observation that the use of "Alice," "Bob," and the rest of the gang in the description of cryptographic protocols largely oversimplifies the setting and is therefore not appropriate. Based on this observation, the article then argues against their further use and claims to use symbols like A, B, and C instead. This is less fun, but more appropriate. If you have a strong opinion about this topic, then I am more than happy to discuss it with you — it refers to an utmost concern of mine.

4 Information Security and Privacy Books

In 2017, the following title was published in Artech House's book series on information security and privacy (that I have been editing since 1999):

- Vincent C. Hu, David F. Ferraiolo, Ramaswamy Chandramouli, and D. Richard Kuhn, *Attribute-Based Access Control*, 978-1-63081-134-1, 2017, 280 pp.

[3] http://ieeexplore.ieee.org/document/7912165/

[4] http://ieeexplore.ieee.org/document/8055680/

This title is already the forty-fifth book published in the series. As such, the series is the most comprehensive one that addresses 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 one of the Commissioning Editors (refer to the book series' homepage[5] for the coordinates of them).

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 2017, Rolf Oppliger gave a lecture on "IT Security" at the University of Zurich. The slides are electronically available at the lecture's Web site[6] (that is also accessible from outside the University of Zurich). Please, feel free to download the slides and provide feedback.

The lecture will be held again in the spring semester of 2018 (MINF4221).[7] The respective slides are currently being revised from scratch, and a preliminary version is available on the lecture's Web site. The slides will be further refined during the semester. Also, the exercises of which 3 out of 6 are mandatory are currently being revised.

5.2 Invited Talks

On June 9, 2017, Rolf Oppliger gave a talk entitled "SSL/TLS Angriffe und Gegenmassnahmen" at the Bern University of Applied Sciences in Biel (Switzerland). The talk was hosted by the research group of Prof. Gerhard Hassenstein[8] and was attended by a few dozens of students. It was well received and initiated a lively debate about the pros and cons as well as the future of the SSL and TLS protocols. More recently, it has become clear that the migration to TLS 1.3 is going to take more time than originally anticipated. This was not envisaged when the talk took place.

5.3 Courses

As mentioned in the Editorial, Rolf Oppliger carried out two seminars in the eSECURITY EDUCATION CENTER in 2017. The seminars will be repeated in 2018, but the seminar on Bitcoin and blockchain will be extended from 1 to 2 days. Also, the seminar offerings will be complemented by a 5-day seminar about the theory and practice of modern cryptography. All three seminars will take place in Bern (probably again in the Welle7) and will be held in German.

For the first halve of 2018, the eSECURITY EDUCATION CENTER schedule looks as follows:

- *Kryptografie — Theorie und Praxis* (German), March 12 - 16, 2018 (5 days)
- *Bitcoin & Blockchain — Kryptografische Grundlagen und Funktionsweise* (German), March 22 - 23, 2018 (2 days)
- *SSL und TLS Sicherheit* (German), May 3 - 4, 2018 (2 days)

The seminars that will be carried out in the second halve of 2018 will be announced on the Web site for the eSECURITY EDUCATION CENTER[9] at some later point in time. Again, if you have some topic preferences, then please let us know. We are interested in offering courses, seminars, and workshops that serve your needs and interests.

Unfortunately, the seminars on Contemporary Cryptography that Rolf Oppliger usually carries out for CRYPTO AG[10] did not take place in 2017. In 2018, the following two seminars are scheduled to take place in Steinhausen (near Zug):

- April 23 – 27, 2018
- September 17 – 21, 2018

Please, feel free to attend any of these seminars. Also, if you are interested to host an internal course on any other topic related to information security (or cybersecurity) in your organization, then please feel free to contact us. We are looking forward discussing the respective possibilities with you. Needless to say that such a discussion is alays without any commitment for you.

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

[6] http://www.esecurity.ch/Teaching/uni-zh-2017.shtml

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

[8] https://web.ti.bfh.ch/∼hegl/

[9] https://education.esecurity.ch

[10] http://www.crypto.ch

5.4 Conferences and Workshops

In 2017, Rolf Oppliger served as a member of the programm committee for the following events (again, in chronological order):

- 4th Workshop on Security in Highly Connected IT Systems (SHCIS 2017), held in conjunction with the 12th International Federated Conference on Distributed Computing Techniques (DisCoTec 2017), Neuchâtel (Switzerland), June 22, 2017
- 14th International Conference on Security and Cryptography (SECRYPT 2017), Madrid (Spain), July 24 - 26, 2017
- 16th International Information Security South Africa Conference (ISSA 2017), Johannesburg (South Africa), August 16 - 17, 2017
- 14th International Conference on Trust, Privacy & Security in Digital Business (TrustBus 2017), held in conjunction with the 28th International Conference on Database and Expert Systems Applications (DEXA 2017), Lyon (France), August 28 - 31, 2017
- 1st ESORICS Doctoral Consortium — COINS Nordic PhD Workshop, held in conjunction with ESORICS 2017, Oslo (Norway), September 14 - 15, 2017
- 22nd European Symposium on Research in Computer Security (ESORICS 2017), Oslo (Norway), September 11 - 15, 2017
- 7th International Conference on e-Democracy, Athens (Greece), December 14 - 15, 2017

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 2018. A respective overview is available on the Internet[11] and will be kept up-to-date.

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.

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