Volume 13, 2016 http://www.esecurity.ch/communications.html

Contents

1 Editorial **2**

2 News **2**

3 Publications **3**

4 Information Security and Privacy Books **3**

5 Announcements **3**
5.1 University Lectures 3
5.2 Invited Talks 3
5.3 Courses 4
5.4 Conferences and Workshops 4

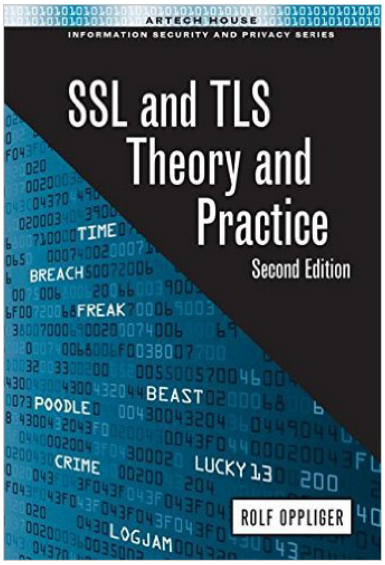
1 Editorial

In the Editorial of last year's issue of eSECURITY communications, I introduced the notion and the rationale behind a new method to engineer and plan cybersecurity measures in particularly large and heterogeneous organizations, and I therefore coined the term OCEP—an acronym standing for "opportunistic cybersecurity engineering and planning." To evaluate the current state-of-the-art in this research area, I have since then joined forces with two much valued colleagues — Prof. Dr. Günther Pernul from the University of Regensburg and Prof. Dr. Sokratis Katsikas from the Norwegian University of Science and Technology — to launch a special issue of the *Computer* magazine specifically dedicated to security risk assessment. The issue is scheduled for April 2017.

Unfortunately, the call for papers[1] for this special issue was not particularly well received in the community and almost went unnoticed. In the end, we had to personally invite some people to contribute articles. The lack of interest and respective contributions can also be seen as a confirmation of the thesis that currently available and promoted risk assessment methods are useless and not applicable in the field. This is why risk assessment is a topic that is mainly populated by consultants (rather than researchers). In fact, we have even found some recognized security professionals who argue that risk assessment is an approach that is so inherently flawed that it is not even worthwhile to scientifically argue about it. While I can understand this line of argumentation, I don't really agree with it. I think that if we recognized an approach to be wrong, then we should find some scientific arguments against it. Ignoring and not discussing the approach is not a valid option here.

Hence, I personally take the lack of interest and contributions for the special issue as a motivation to further delve into the topic, and to come up with a simplified approach that is useful and applicable in the field. This endeavor is scheduled for 2017. Also in 2017, I intend to expand the activities of the eSECURITY Education Center beyond cryptography and SSL/TLS, and to offer some additional courses or seminars on the blockchain technology in general, and Bitcoin in particular. The details have yet to be defined and will be announced at some later point in time. If you have a particular interest, then feel free to contact me in this matter. Any feedback is welcome and highly appreciated.

[1] `https://www.computer.org/web/computingnow/cocfp4`



2 News

The second edition of Rolf Oppliger's book entitled *SSL and TLS: Theory and Practice* (ISBN 978-1-60807-998-8) has finally reached the shelves of the bookstores. Its book cover looks is shown above.

The book provides a comprehensive overview and discussion of the SSL/TLS and DTLS protocols, and specifically addresses their security properties. This includes, among other things, the most recent attacks that have made press headlines, such as BEAST, CRIME, Lucky 13, POODLE, FREAK, Logjam, and many more (most of these acronyms can be found on the book cover). It also addresses related topics, like TLS extensions, firewall traversal, as well as public key certificates and Internet PKI. As such, the book is intended for anyone who has a basic understanding of cryptography and TCP/IP networking, and who wants to learn more about the SSL/TLS and DTLS protocols and their proper use. It speaks to both theorists and practitioners, and has been written to be used as complementary material for courses and seminars.

Since the official release of the book, a few new attacks against the SSL/TLS protocols have been published in the relevant literature, such as SLOTH, DROWN, HEIST, and Sweet32. The book's Web site[2] is used to compile some links that refer to these attacks.

[2] `http://books.esecurity.ch/ssltls2e.html`

They will be addressed in the third edition of the book that will hopefully appear in a couple of years.

3 Publications

As mentioned in the preface, a special issue of the *Computer* magazine dedicated to security risk assessment will be published in April 2017. Together with Proff. Günther Pernul and Sokratis Katsikas, Rolf Oppliger serves as guest editor for this issue, and together they will author a respective lead article. The article is to introduce the topic and to put the published articles into perspective. The bottom line is that there are still many research opportunities when it comes to security risk assessment and management used in the field.

4 Information Security and Privacy Books

In addition to Rolf Oppliger's Second Edition of *SSL and TLS: Theory and Practice*, the following two book titles have been published in 2016:

- Edward Humphreys, *Implementing the ISO/IEC 27001:2013 ISMS Standard*, 978-1-60807-930-8, 2016, 224 pp.
- Ghassan O. Karame, and Elli Androulaki, *Bitcoin and Blockchain Security*, 978-1-63081-013-9, 2016, 240 pp.

Both titles have been received well by the audience of the series.

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[3] 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.

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

5.1 University Lectures

In the spring semester of 2016, Rolf Oppliger gave a lecture on "IT Security" at the University of Zurich. The slides are electronically available at the lecture's Web site[4] (that is also accessible from outside the University of Zurich). Please, feel free to download the slides and provide some feedback.

The lecture will be held again in the spring semester of 2017.[5] The respective slides are currently being revised from scratch. A preliminary version is already available, but it will still be modified until the lecture officially starts on February 20, 2017. The slides comprise three plug-in modules on the evolution of symmetric encryption (including, for example, some historical notes on the Enigma machine), the SSL/TLS protocols, and the Kerberos authentication and key distribution system.

5.2 Invited Talks

In 2016, Rolf Oppliger gave the following invited talks in Switzerland and the United States (in chronological order):

- On April 18, he gave a talk on "Certification Authorities Under Attack: A Plea for Certificate Legitimation" at the University of Lausanne (Switzerland).
- On May 26, he gave a beer talk on "SSL/TLS: Angriffe und Gegenmassnahmen" in Berne (Switzerland). The talk was repeated on June 9 in Jona (Switzerland).
- On July 20, he gave an introductory talk on the "State-of-the-Art in Information Security" at the University of Houston in Houston (Texas).
- On July 25, he gave an advanced talk on "SSL/TLS: Playing 'Cops and Robbers' on the Internet" at the University of Florida in Gainesville (Florida).

Overall, the talks were well received and can be repeated at will. If you host an event on one of these topics, then I may be interested to give a respective talk.

[4] `http://www.esecurity.ch/Teaching/uni-zh-2016.shtml`

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

5.3 Courses

The Swiss company CRYPTO AG[6] regularly hosts a seminar on contemporary cryptography, in which four out of five days are taught by Rolf Oppliger. The seminars are held in English and take place in Steinhausen (near Zug). In 2016, the two seminars that were scheduled took place. In 2017, the following two seminars are scheduled:

- March 27 – 31, 2017
- October 16 – 20, 2017

Please, feel free to register for and attend any of these seminars.

In cooperation with Compass Security Schweiz AG,[7] Rolf Oppliger has launched a 2-day seminar on the theory and practice of the SSL/TLS protocols—called SSL/TLS Security Lab.[8] The theoretical parts of the seminar follow the new book of Rolf Oppliger, whereas the practical parts are based on Compass' Hacking Lab.[9] The seminar took place for the first time on November 15 – 16, 2016, in Berne. It is planned to repeat the seminar on August 31 – September 1, 2017, in Zurich. You may contact either Compass Security Schweiz AG or eSECURITY Technologies Rolf Oppliger to get more information about it.

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, too. We are looking forward discussing the respective possibilities with you. Needless to say that such a discussion is alays without any commitment for you.

5.4 Conferences and Workshops

In 2016, Rolf Oppliger served as a member of the programm committee for the following events (again, in chronological order):

- 13th International Conference on Security and Cryptography (SECRYPT 2016), Lisbon (Portugal), July 26 – 28, 2016
- 15th Annual Information Security South Africa Conference (ISSA 2016), Johannesburg (South Africa), August 17 – 18, 2016
- 11th International Conference on Availability, Reliability and Security (ARES 2016), Salzburg (Austria), August 31 – September 2, 2016
- 13th International Conference on Trust, Privacy & Security in Digital Business (TrustBus 2016), held in conjunction with the 27th International Conference on Database and Expert Systems Applications (DEXA 2016), Porto (Portugal), September 5 – 8, 2016
- 4th International Symposium on Security in Computing and Communications (SSCC 2016), Jaipur (India), September 21 – 24, 2016
- 10th WISTP International Conference on Information Security Theory and Practice (WISTP 2016), Crete (Greece), September 26 – 27, 2016
- 21st European Symposium on Research in Computer Security (ESORICS 2016), Crete (Greece), September 26 – 30, 2016
- 9th International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage (SpaCCS 2016), Zhangjiajie (China), November 18 – 20, 2016

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 2017. A respective overview is available on the Internet[10] 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.

© 2016 eSECURITY Technologies Rolf Oppliger

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

[7] http://www.compass-security.com

[8] https://www.compass-security.com/services/security-trainings/kursinhalte-ssltls-security-lab/

[9] https://www.hacking-lab.com

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