Volume 11, 2014 http://www.esecurity.ch/communications.html

Contents

1 Editorial

In 2014, we have seen quite a few security incidents that have attracted a lot of media attention: Heartbleed, Shockshell, and—more recently—POODLE. All three incidents have shown that IT security is a highly involved topic, and that todays IT systems and networks are highly exposed to distinct attacks with sometimes severe consequences.

- Heartbleed was caused by a bug in the OpenSSL implementation of the TLS Heartbeat extension specified in RFC 6520. Under certain circumstances, it allowed an adversary to read out the server's memory and to eventually find cryptographic keys. As such, the consequences of Heartbleed were devastating and the affected servers had to replace their keys. To make things worse, it was not easily decidable for a server administrator whether his or her system had been attacked successfully. This, in turn, meant that he or she had to replace the keys anyway (even if the system was not attacked or the attack was not successful).
- Shockshell was a vulnerability in the Bourne Again Shell (BASH) that is frequently used on Linux and Mac OS systems. The vulnerability is caused by the fact that variables can be defined as functions, and that arbitrary (and unchecked) code could be executed this way—sometimes even across network connections. The consequences of Shockshell were also devastating, but the attack could be mitigated by patching the affected systems. Also, any exploit could be detected by inspecting the respective log files.
- As its name suggests, POODLE[1] refers to a padding oracle attack that specifically exploits the padding used in SSL 3.0 (this padding is slightly different than the padding used in TLS). It is a rather sophisticated attack that requires an adversary who is able to insert chosen ciphertext on the client side. This can, for example, be achieved through active content (e.g., some JavaScript code), but the respective attack is difficult to mount. Fortunately, it is quite simple to mitigate the POODLE attack by simply disabling SSL 3.0. This is what is generally recommended and done today, and there is no serious disadvantage in doing so. TLS 1.0, 1.1, and 1.2, as well as the soon to be released version 1.3 all provide viable alternatives to SSL 3.0. But one should still be cautious, because there are many proxy servers that still support SSL 3.0 and there are many buggy implementations that use the SSL padding instead of the TLS one.

[1]The acronym is standing for "Padding Oracle dOwngraded Legacy Encryption".

All three incidents have also shown that theory and practice are inherently different when it comes to security. Or to put it in Albert Einstein's words:

> "In theory, theory and practice are the same. In practice, they are not."

This quote clearly illustrates the point that theoretical investigations about the security of a system and its practical resistance against specific attacks are different pairs of shoes. There are simply too many attacks to defend against, and—to make things worse—the attacks always get better and better (see the history of padding oracle attacks as an example to illustrate this point). This should always be kept in mind when one talks about the security properties of a particular system. The theoretical security of a system is only one side of the medal; the other side refers to its practical security, and this side is usually much more difficult to assess. Unfortunately, it is the one that counts at the end of the day.

2 News

Rolf Oppliger's new book entitled *Secure Messaging on the Internet* has been published and is now available in

the shelves of the bookstores (the book cover is illustrated above).[2] The book goes beyond what could be seen as a second edition of *Secure Messaging with PGP and S/MIME*—a book that was published 12 years ago. In fact, it broadens the scope significantly, and it addresses many additional topics related to secure messaging on the Internet, such as Web-based messaging, gateway solutions, certified mail, delivery platforms, and instant messaging. The aim is to draw a picture that is comprehensive and sufficiently complete when it comes to all aspects related to secure messaging on the Internet. It is hoped that this aim is fulfilled, and that the book serves its intended purpose for practitioners working in the field. If you have read the book, then we are interested in hearing about your reading experience, your thoughts, and your judgement. Please, feel free to send us any feedback about the book. This will be particularly important, if the book goes into a second edition (needless to say that we hope that this will be the case one day).

3 Publications

The article entitled "Certification Authorities under Attack: A Plea for Certificate Legitimation" was published in the *IEEE Internet Computing* magazine (Vol. 18, No. 1, January/February 2014, pp. 40–47). The abstract of the article reads as follows:

> "Several recent attacks against certification authorities (CAs) and fraudulently issued certificates have put the security and usefulness of the Internet public-key infrastructure (PKI) at stake. In this article, the author argues that such attacks are likely to occur repeatedly and that respective countermeasures must be designed, implemented, and put in place. In particular, he discusses two problem areas in which countermeasures are needed: certificate revocation and certificate authorization. Both areas are related and can be subsumed under the term *certificate legitimation*. The author introduces the notion of certificate legitimation, discusses some recent proposals, and outlines new areas of research and development."

As such, the article is in line with the latest developments in the PKI arena, such as DNS security (DNSSEC) and DNS-Based Authentication of Named Entities (DANE), public key pinning, Sovereign Keys (promoted by the Electronic Frontier Foundation),[3] Certificate Transparency (promoted by Google and a few other companies),[4] as well as notary and trust agility approaches, such as Perspectives,[5] Convergence,[6] and the Certificate Notary of the International Computer Science Institute (ICSI).[7] Taking into account all of these recent developments, it is likely and possible that future PKIs will look fundamentally different from what we know and usually work with today. This does not come as surprise, given the fact that we have tried to establish a PKI for the Internet for almost 20 years without any remarkable success. Instead of redoing the same mistakes over and over again, it is reasonable to try out other approaches.

4 Information Security and Privacy Books

Rolf Oppliger is still serving as the editor for Artech House's information security and privacy book series. The series is the eldest and by far the most comprehensive book series on information security and privacy. Since the beginning of this century, Artech House has published 39 titles in the series, covering most areas that are somehow related to information security and privacy. In addition to these titles, the following book is scheduled to appear in 2015:

- Amir Herzberg and Haya Shulman, *DNS Poisoning: Attacks and Defenses*

Also, Rolf Oppliger is currently updating his book entitled *SSL and TLS: Theory and Practice* (ISBN 978-1-59693-447-4) that was published in 2009. This relatively short update cycle has become necessary because many attacks against the SSL/TLS protocols and respective attack tools have appeared recently, such as BEAST, CRIME (including TIME and BREACH), and POODLE (as mentioned in the Editorial of this issue of eSECURITY communications). One of the intended purposes of the updated book is to fully explain, discuss, and put into perspective all of these nicely acronymed attacks and attack tools. It is planned that the second edition of *SSL and TLS: Theory and Prac-*

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

[3] `https://www.eff.org/de/sovereign-keys`

[4] `http://www.certificate-transparency.org`

[5] `http://perspectives-project.org`

[6] `http://convergence.io`

[7] `http://notary.icsi.berkeley.edu`

tice will be published and become available in the bookstores somewhen in late 2016. If you are interested in the topic, then you may get involved and overtake a more active role in the book publication process (e.g., by reviewing draft versions of the manuscript or some chapters thereof).

The process of contracting new authors is steadily going on. If you are working in the field and 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[8] for the coordinates of them).

5 Announcements

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

5.1 University Lectures

In the spring semester of 2014, Rolf Oppliger gave a lecture on "IT Security" at the University of Zurich. It was the first time the introductory lecture on IT security was given in English. Except from the language, only a few things have changed since the last few years. The lecture still provided a basic introduction into the (increasingly) broad field of IT security. The slides are electronically available at the lecture's homepage[9] (also accessible from outside the University of Zurich). Please, feel free to download the slides, have a look at them, and hopefully provide some feedback. It goes without saying that any feedback is weleome and highly appreciated.

In the upcoming spring semester of 2015, Rolf Oppliger will give an updated version of the lecture. Again, the slides will be made electronically available at the lecture's homepage[10] as soon as they are finished (hopefully early in 2015). The same invitation for feedback as mentioned above applies here.

5.2 Courses

The Swiss company CRYPTO AG[11] 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 2014, a respective seminar took place in October.

For 2015, the following seminars are tentatively scheduled:

- April 27 - May 1, 2015
- October 12 - 16, 2015

Feel free to register for and attend any of these seminars. They take place, if a sufficiently large number of attendees registers for them. So the decision whether a particular seminar takes place can usually be made only a few weeks ahead of the planned starting date.

If you are interested to host a course on contemporary cryptography or any other topic related to lT security 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 without any commitment for you.

5.3 Invited Talks

On April 11, 2014, Rolf Oppliger gave an invited talk entitled *Information Security: Key Concepts and Common Misconceptions* at the Imperial College in London (UK).[12] The talk was hosted by Proff. Chris Hankin and Michael Huth. It was originally announced as follows:

> "Information security is a timely and increasingly important topic and field of study that is heavily investigated both in theory and practice. But in spite of this huge effort, we are still far away from being secure in our information society. There are key concepts related to information security that are valid and help in practice, but there are also many common misconceptions in place.These misconceptions are particularly dangerous, because they obfuscate the situation and may (mis)lead information security officers and other executives to make wrong decisions or do the wrong things. In this talk, we provide a bird's eye view of information security, and we try to clearly distinguish between the key concepts (that

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

[9] http://www.esecurity.ch/Teaching/uni-zh-2014.shtml

[10] http://www.esecurity.ch/Teaching/uni-zh-2015.shtml

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

[12] http://www3.imperial.ac.uk/newsandeventspggrp/imperialcollege/engineering/computing/eventssummary/event_27-3-2014-12-41-33

work) and the common misconceptions (that don't work). As the market for information security products and services proliferates, we strongly believe that being able to make such a distinction is getting more and more important and is key to the success of any information security professional."

As such, the talk elaborated on the fundamentals of IT security, which are still not very well understood in the field. The talk was well attended by an impressing number of faculty members and students from both the Imperial College and the Royal Holloway University of London. It also led to an interesting and intellectually stimulating discussion regarding risk management after the talk. It is hoped that the discussion will be continued electronically.

5.4 Conferences and Workshops

In 2014, Rolf Oppliger served as a member of the programm committee for the following events (in chronological order):

- 11th Annual IEEE Consumer Communications & Networking Conference (CCNC 2014), Technical Track on Security, Privacy and Content Protection, Las Vegas (USA), January 10 - 13, 2014
- 10th International Conference on Information Security Practice and Experience (ISPEC 2014), Fuzhou (China), May 13 - 15, 2014
- 13th Annual Information Security South Africa Conference (ISSA 2014), Sandton Johannesburg (South Africa), August 13 - 15, 2014
- 11th International Conference on Security and Cryptography (SECRYPT 2014), Vienna (Austria), August 28 - 30, 2014
- 11th International Conference on Trust, Privacy & Security in Digital Business (TrustBus 2014), held in conjunction with the 25th International Conference on Database and Expert Systems Applications (DEXA 2014), Munich (Germany), September 1 - 5, 2014
- 9th International Conference on Availability, Reliability and Security (ARES 2014), Fribourg (Switzerland), September 8 - 12, 2014
- 10th International Conference on Information Assurance and Security (IAS 2014), Okinawa (Japan), November 27 - 30, 2014
- 17th International Conference on Information Security and Cryptology (ICISC 2014), Seoul (South Korea), December 3 - 5, 2014

Also, Rolf Oppliger has already agreed to serve as a member of the programm committee for the following events that take place in 2015 (again, in chronological order):

- 12th Annual IEEE Consumer Communications & Networking Conference (CCNC 2015), Las Vegas (USA), January 9 - 12, 2015
- 12th International Conference on Wirtschaftsinformatik (WI 2015), Track 8: Data Privacy and Security, Osnabrück (Germany), March 4 - 6, 2015
- 14th Annual Information Security South Africa Conference (ISSA 2015), Johannesburg (South Africa), August 12 - 14, 2015
- 20th European Symposium on Research in Computer Security (ESORICS 2015), Vienna (Austria), September 21 - 25, 2015

More involvements in programm committees for 2015 will be announced on the respective Web site[13] as soon as they are confirmed.

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 (IT) security. The company is registered in the commercial register of Bern-Mittelland (CH-035.1.023.622-7) and located in Muri b. Bern.

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