eSECURITY®
communications

Volume 6, Issue 1, Spring 2009 http://www.esecurity.ch/communications.html

Contents

1 Editorial

With regard to IT security, the last term has been relatively quiet. There have been some reported cases where security vulnerabities have been found and exploited, but none of these cases has been particularly spectacular or worrisome. Maybe most importantly, there has been a highly publicized case in which a group of international researchers has been able to exploit MD5 collisions to create a rogue CA certificate. This is theoretically interesting, but—as further addressed in Section 4.2—not really relevant in practice. The bottom line is that MD5 has finally come to its end, and that the ongoing competition of the U.S. National Institute of Standards and Technology (NIST) to standardize a new cryptographic hash function (preliminarily called SHA-3) is overdue. After the big success of the AES competition one decade ago, the SHA-3 competition seems to be successful again, as there are many submissions to choose from.[1] Furthermore, it seems that cryptographic primitives (i.e., algorithms and/or protocols) designed in dark rooms without public scrutiny are phased-out models, and that new cryptographic primitives are routinely designed and discussed in public. This general trend is certainly in line with Kerckhoffs' principle.

We hope that you enjoy reading this issue of eSECURITY communications, and we are looking forward hearing from you and receiving your feedback, comments, or criticism in one way or another.

2 News

In the last issue of eSECURITY communications, we announced the writing and publication of a new book about transport layer security in general, and the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols in particular. The book is scheduled to appear late in 2009 or early in 2010. It is preliminarily entitled "SSL/TLS: Theory and Practice," and it is structured in the following nine chapters:

1. Introduction
2. Cryptography Primer
3. Transport Layer Security
4. SSL Protocol
5. TLS Protocol
6. DTLS Protocol
7. Firewall Traversal
8. Public Key Certificates and PKI
9. Conclusions and Outlook

The foreword of the book will be provided by Taher ElGamal.[2] He is best known for the public key cryptosystem he developed and proposed 15 years ago. But he was also involved in the design of the first versions of the SSL protocol.

If you are interested in contributing in one way or another (e.g., review particular chapters), then please feel free to contact Rolf Oppliger. Any help is welcome and highly appreciated.

3 Publications

An article entitled "Internet Banking: Client-Side Attacks and Protection Mechanisms" (co-authored by Ruedi Rytz and Thomas Holderegger) has been accepted for publication in the prestigious *IEEE Computer* magazine (it will hopefully appear in the April or May 2009 issue). The article argues that—with the recent advent of client-side attacks—the security of Internet banking (and many other SSL/TLS-based applications) has come under fire, and that banks supporting Internet banking are challenged to implement more effective protection mechanisms. The article then reviews client-side attacks and corresponding protection mechanisms. More specifically, it adapts a distinction between offline credential-stealing, online channel-breaking, and content manipulation attacks, and it then overviews, discusses, and puts into perspective mechanisms that can be used to protect against them. The key findings are

- that currently available mechanisms are appropriate to protect against offline credential stealing attacks,
- that effective protection against online channel-breaking attacks requires the implementation of technologies to defeat man-in-the-middle (MITM) attacks, and
- that practical protection against content manipulation attacks requires the implementation of transaction authentication technologies.

The last trend is going on in the banking industry, and transaction authentication technologies are ideally complemented by technologies for transaction monitoring.

[1] `http://ehash.iaik.tugraz.at/wiki/SHA-3_submitters`

[2] `http://en.wikipedia.org/wiki/Taher_ElGamal`

4 Security Analyses

Let us say a few words about the SecLookOn authentication system (once again) and the MD5 collision exploit to generate a rogue CA certificate mentioned in the Editorial.

4.1 SecLookOn

In the last issues of eSECURITY Communications, we occasionally criticized the authentication system SecLookOn and the way it is brought to market. This critique is now supported by a security analysis done by Markus Steinkamp. The analysis is recommended reading for anybody interested in SecLookOn (or WebLookOn,[3] respectively). Please, feel free to contact Markus Steinkamp at `steimar@freenet.de` to get a copy of the analysis.

4.2 Rogue CA Certificates

A group of international researchers has shown at the 25th Chaos Communication Congress (25C3) how to exploit known vulnerabilities of the collision resistance property of MD5 to get a rogue CA certificate.[4] This certificate can be used, for example, to issue server certificates to mount large-scale phsishing attacks. In principle, the adversary has to construct two different certificate requests: one for a user certificate and one for a CA certificate. The contents of the certificate requests are constructed so that the data sets that are included in the certificates collide under MD5, meaning that both certificates have the same MD5 hash value and hence the same signature. If a trusted root CA then signs the user certificate, then this signature can also be used to issue the CA certificate without any further invocation of the trusted root CA. Because the certificate looks like being issued by the trusted root CA, it is going to be accepted by commonly used browsers without any user confirmation. This certainly yields a vulnerability or security protblem.

From a theoretical viewpoint, the research result is interesting, because it demonstrates for the first time the feasibility of a collision attack that exploits the vulnerabilities of the collision resistance property of MD5 that has been known since 2004. From a practical viewpoint, however, the result is less spectacular, mainly because only a few CAs still use MD5. This trend to move away from MD5 to SHA-1 or even more collision-resistant hash functions (in particular SHA-2 or even SHA-3) will continue and get stronger in the future. But it is also important to note that the collision resistance property of the hash function in use is not the only Achilles' heel of using public key certificates. Many actual attacks use no certificate or a false certificate, or even exploit the fact that users routinely click through interactive dialogues. These attacks are less expensive but not necessarily less effective.

[3] `http://www.weblookon.com`

[4] `http://www.win.tue.nl/hashclash/rogue-ca/`

5 Information Security and Privacy Books

As of this writing, the following title is about to be published in Artech House's information security and privacy book series:

- C. Warren Axelrod, Jennifer Bayuk, and Daniel Schutzer (Eds.), *Enterprise Information Security and Privacy*, ISBN 978-1-59693-190-9, scheduled for March 2009, approx. 260 pp.

The upcoming book on SSL/TLS was already mentioned in Section 2. Furthermore, the process of contracting new authors is going on. If you are interested in writing and publishing a book in the series, then you may contact either the Series Editor (Rolf Oppliger) or a Commissioning Editors (refer to the book series' home page[5] for the coordinates of the Commissioning Editors).

6 Announcements

There are a couple of announcements to make regarding university lectures, courses, invited talks, and conferences and workshops.

6.1 University Lectures

In spring 2009 (starting on February 16, 2009), Rolf Oppliger lectures at the University of Zürich on "Sicherheit in der Informationstechnik." The lecture takes place annually and provides a thorough introduction to information technology (IT) security. The lecture slides are electronically available at the lecture's home page.[6]

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

[6] `http://www.esecurity.ch/Teaching/uni-zh-2009.shtml`

6.2 Courses

This year, InfoGuard will host three courses on contemporary cryptography. Four out of five days will be taught by Rolf Oppliger. The courses will be held in English and take place in Zug. The dates are as follows:

- April 27–May 1, 2009
- June 22–26, 2009
- November 16–20, 2009

If you are interested to attend any of these courses, then you may request a flyer from InfoGuard or eSECURITY Technologies Rolf Oppliger (or you can download an electronic version of the flyer[7]). Either company can also answer questions related to the course.

Furthermore, if you are interested to host a course on contemporary cryptography or any other topic related to IT security, then please feel free to contact eSECURITY Technologies Rolf Oppliger without any commitment. We are looking forward discussing the possibilities with you.

6.3 Invited Talks

The Swiss E-Voting Competence Center[8] is organizing a workshop on the status of e-voting in Switzerland that will take place on June 5, 2009, at the Schloss Münchenwiler near Murten.[9] Rolf Oppliger is invited to give a talk about the challenges related to client security. The talk will be held in German and is preliminarily entitled "Der Client als Achillesferse beim Remote Internet Voting." The slides of the talk will be electronically available from the Web site of the Swiss E-Voting Competence Center.

6.4 Conferences and Workshops

In 2009, Rolf Oppliger will serve as a member of the programm committee for the following international conferences and workshops:

- International Conference on Security Technology (SecTech 2009), Jeju Island (Korea), December 10–12, 2009
- 12th Information Conference on Information Security and Cryptology (ICISC 2009), Seoul (Korea), December 2 - 4, 2009
- 4rd International Conference on Systems and Networks Communications (ICSNC 2009), Porto (Portugal), September 20–25, 2009
- 3rd Workshop in Information Security Theory and Practices (WISTP 2009), Bruxelles (Belgium), September 2–4, 2009
- 6th International Conference on Trust, Privacy and Security in Digital Business (TrustBus '09) held in conjunction with the 20th International Conference on Database and Expert Systems Applications (DEXA 2009), Linz (Austria), August 31–September 4, 2009
- 10th Workshop of Information Security and Applications (WISA 2009), Jeju Island (Korea), August 25–27, 2009
- 5th International Conference on Information Assurance and Security (IAS 2009), Xi'an (China), August 18–20, 2009
- International Conference on Security and Cryptography (SECRYPT 2009), Milan (Italy), July 7–10, 2009
- 24th IFIP International Information Security Conference (IFIP SEC 2009), Pafos (Cyprus), May 18–20, 2009
- 9th International Conference on Information Management (Wirtschaftsinformatik 2009), Track 21: Security , Vienna (Austria), February 25–27, 2009

It goes without saying that the conferences and workshops are recommended events to attend and learn more about the current state-of-the-art in cryptography and IT security.

About the Company

eSECURITY Technologies Rolf Oppliger[10] 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 is located in Gümligen near Berne (Switzerland).

[7] http://www.infoguard.ch/docs/dokumente/IG_1wEdu_ConCry_e.pdf

[8] http://www.e-voting-cc.ch

[9] http://www.e-voting-cc.ch/ws2009

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