
Volume 6, Issue 2, Fall 2009 http://www.esecurity.ch/communications.html

## Contents

**1 Editorial** **2**

**2 News** **2**
2.1 Upcoming Book . . . . . 2
2.2 Support of SSL/TLS . . . . . 2

**3 Publications** **3**

**4 Security Analyses** **3**
4.1 SecLookOn . . . . . 3
4.2 Cryptanalysis of AES-256 . . . . . 3

**5 Information Security and Privacy Books** **4**

**6 Announcements** **4**
6.1 University Lectures . . . . . 4
6.2 Courses . . . . . 4
6.3 Conferences and Workshops . . . . . 4

# 1 Editorial

At the rump session of this year's CRYPTO conference, Olivier Pereira gave a talk about the successful use of the Helios open-audit voting system for the election of the president of the University of Leuven (as reported, for example, in a USENIX EVT/WOTE '09 paper).[1] But in spite of Helios' theoretical security, Ivo Desmedt explained in the subsequent talk how the system can be compromised in practice.[2] In fact, Desmedt and his students have developed a Firefox plugin that exploits a buffer overflow vulnerability in the Adobe Acrobat Reader software to defeat the browser and to manipulate its behavior accordingly. As a result, the browser is able to modify ballots on the fly in a way that is invisible to the voters. This effectively undercuts the cryptographic security of the Helios system and implements a client-side attack. We have been warning against the feasibility of client-side attacks for a long time, and we hope that this proof-of-concept implementation now helps sensibilizing the public to the problem. Client-side attacks represent the Achilles' heel of remote Internet voting, and they are challenging to address and to protect against. We will continue our work in this area and report on the results in future issues of eSECURITY communications.

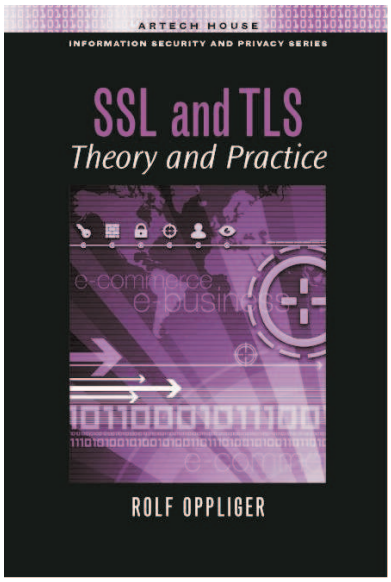
Anyway, we hope that you enjoy reading this issue of eSECURITY communications, and we are looking forward hearing from you and receiving your feedback, comments, or criticism.

# 2 News

We have news regarding an upcoming book on SSL/TLS and the support of these protocols for the Web site of eSECURITY Technologies Rolf Oppliger.

## 2.1 Upcoming Book

A new book of Rolf Oppliger entitled "SSL and TLS: Theory and Practice" (preliminary book cover is reproduced besides) is now in print and will be available early in October 2009. You may refer to the book's Web site[3] to get more information about the book and to pre-order it from Amazon. Needless to say that you can also buy the book directly from Artech House.




## 2.2 Support of SSL/TLS

SSL/TLS is the most widely deployed security technology in use today. Many Web sites support it to secure communications with their users and customers. This also applies to the Web site of eSECURITY Technologies Rolf Oppliger. This site is hosted by Hoststar Multimedia Networks AG, and this hosting provider has been supporting SSL/TLS since January 2009. If, for example, you connect to `http://secure.esecurity.ch`, then you are actually redirected to `https://www.esecurity.ch/Secure`, and access to this directory requires the prior establishment of an SSL/TLS session. As part of the SSL/TLS handshake, the server provides a server-side certificate. As of this writing, this certificate is an SSL wildcard certificate issued by the DigiCert[4] High Assurance CA-3 for `*.hoststar.ch`. So all Web sites hosted by Hoststar can either employ this certificate or have Hoststar retrieve and employ a specifically-crafted certificate for the hosted Web site and domain name. The first possibility is simple and straightforward, but it has the disadvantage that the domain name in the subject field of the certificate does not match the domain name of the Web site. In the case of `http://secure.esecurity.ch`, for example, the domain name of the certificate's subject field is `hoststar.ch`, whereas the domain name of

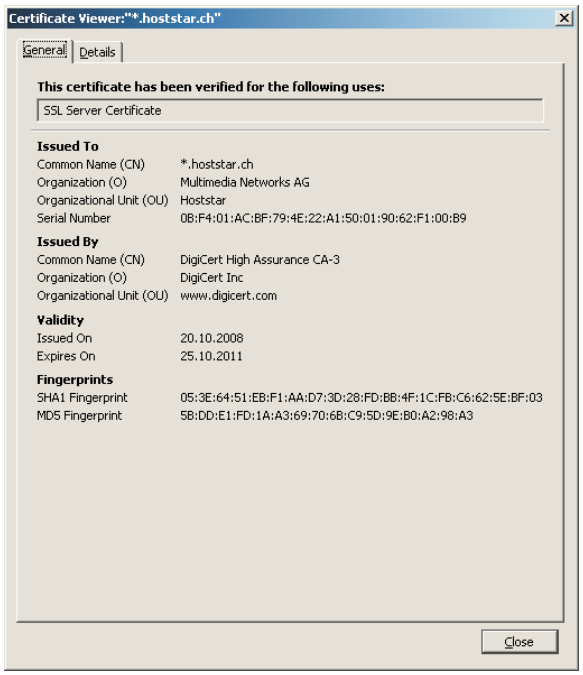
[1] `http://rump2009.cr.yp.to/29677b89667a5980158b1ab264d7a892.pdf`

[2] `http://rump2009.cr.yp.to/1b884ce772d84af05f0f4b07bf019053.pdf`

[3] `http://books.esecurity.ch/ssltls.html`

[4] `www.digicert.com`

the Web site is `esecurity.ch`. This mismatch results in a pop-up window, in which the user is asked whether he or she really wants to accept the (invalid) certificate. In Firefox, for example, this may look as follows:




At this point, users are required to manually verify the certificate's fingerprint with a fingerprint value that is provided out-of-band (in this case, the proper value is `0x053e6451ebf1aad73d28fdbb4f1cfbc6625ebf03` for SHA-1 in hexadecimal notation). This verification step is not elegant, laborious, and often ignored in practice. The price to pay is susceptibility to Web spoofing and man-in-the-middle (MITM) attacks. This also applies to the Web site of eSECURITY Technologies Rolf Oppliger. So if you really want to be sure and protect yourself against MITM attacks, then you have to manually verify the certificate's fingerprint mentioned above (to make things more involved, you'd also have to verify that the pop-up window that displays the fingerprint is in fact genuine).

# 3 Publications

The article entitled "Internet Banking: Client-Side Attacks and Protection Mechanisms" (co-authored by Ruedi Rytz and Thomas Holderegger) finally appeared in the June 2009 issue of the *IEEE Computer* magazine. You may request a paper copy of the article if you don't have access to the magazine.

# 4 Security Analyses

We have a few comments to make about the SecLookOn authentication system (hopefully for the last time) and the cryptanalysis of the AES-256.

## 4.1 SecLookOn

In the last issues of eSECURITY communications, we have criticized the authentication system SecLookOn (or WebLookOn,[5] respectively) and the way it is brought to market a couple of times (the system really started to become a running gag). But instead of seriously discussing the points of criticism with us, the developer and promoter of the system, Helmut Schluderbacher of MERLINnovations & Consulting GmbH, threatened to sue us in a way that is neither friendly nor polite (to say the least). We have been involved in many security analyses in the past, but we have never met somebody acting as nervous and incorrigible as Mr. Schluderbacher. This is unfortunate, because information and IT security requires seriousness and respectability—two properties that cannot be easily attributed to Mr. Schluderbacher. We are still waiting for an excuse and stop commenting on SecLookOn.

## 4.2 Cryptanalysis of AES-256

The Advanced Encryption Standard (AES) is a standardized block cipher specified in Federal Information Processing Standard (FIPS) PUB 197.[6] There are 3 versions of the AES, i.e., AES-128, AES-192, and AES-256, that use different key lengths and number of rounds. Since the AES became a standard in 2001, it has received a lot of public scrutiny and has become a popular target to attack. The progress in its cryptanalysis has initially been very slow. Only recently, substantial progess has been made and a couple of papers have been published that explain how to apply related-key attacks against the longer-key versions of the AES, i.e., AES-192 and AES-256. AES-128 remains unaffected by these attacks. More specifically, AES-192 can be broken with a time complexity of $2^{176}$ (which is marginally better than $2^{192}$), but AES-256

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

[6] `http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf`

can be broken with a time complexity of $2^{119}$ (which is substantially better than $2^{256}$). Also, reduced versions of AES-192 and AES-256 can be broken with a time complexity that is feasible. For example, 11-round AES-256 can be broken with a time complexity of $2^{70}$, which is almost practical. It will be interesting to see if and how related-key attacks can be further improved to make the cryptanalysis of full AES (at least AES-256) feasible and practical.

# 5 Information Security and Privacy Books

As mentioned above, a new book entitled "SSL and TLS: Theory and Practice" will appear shortly in Artech House's information security and privacy series. Also, 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[7] for the coordinates of the Commissioning Editors).

# 6 Announcements

There are announcements to make regarding university lectures, courses, and conferences and workshops.

## 6.1 University Lectures

In spring 2010 (starting on February 22, 2009), Rolf Oppliger will again lecture at the University of Zürich on "Sicherheit in der Informationstechnik." The lecture that takes place annually is to provide a thorough introduction to information technology (IT) security. The lecture slides will be made electronically available at the lecture's home page[8] early in 2010.

## 6.2 Courses

On November 16–20, 2009, InfoGuard will host a seminar on contemporary cryptography. Four out of five days will be taught by Rolf Oppliger. If you are interested to attend, then you may request a flyer from InfoGuard or eSECURITY Technologies Rolf Oppliger (or you can download an electronic version). 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 such possibilities with you.

## 6.3 Conferences and Workshops

In addition to the conferences and workshops itemized in the last issue of eSECURITY communications, Rolf Oppliger served as a member of the programm committee for the 6th European Workshop on Public Key Services, Applications and Infrastructures (EuroPKI '09) that takes place in Pisa (Italy) on September 9–11, 2009. Again, the program of the workshop looks very promising.

With regard to 2010, Rolf Oppliger has committed to serve as a member of the programm committee for the following international conferences and workshops:

- 25th ACM Symposium on Applied Computing (SAC 2010), Technical Track on Privacy on the Web, Sierre (Switzerland), March 22–26, 2010
- 4th International Conference on Information Security and Assurance (ISA 2010), Uzbekistan, April 5 - 7, 2010
- 25th IFIP International Information Security Conference (IFIP SEC 2010), Brisbane (Australia), September 20–23, 2010

Other program committee memberships for 2010 will be announced in the next issue of eSECURITY communications.

# About the Company

eSECURITY Technologies Rolf Oppliger[9] 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.esecurity.ch/serieseditor.html

[8] http://www.esecurity.ch/Teaching/uni-zh-2010.shtml

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