Volume 5, Issue 1, Spring 2008 http://www.esecurity.ch/communications.html

Contents

1 Editorial

Remember the last issue of eSECURITY communications? We wanted to test the suitability of digital signatures for daily use, and we therefore digitally signed the e-mail message that actually delivered the newsletter using the S/MIME implementation of Microsoft Outlook Express and a digital certificate issued by Swisscom Solutions AG. The result of the experiment was not unexpected but still came as a surprise in its clearness: some recipients were not able to make use of digital signatures; other recipients could not verify them—most likely because the proper root CA certificate was missing in their local certificate store. The overall experience was disillusioning and approved the fact that digital signatures and certificates are not ready for prime time, and that there is still a long way to go. Part of the problem is related to the general theme of how users can be appropriately interfaced to cryptographic systems and applications. The other part of the problem is specifically related to the inherent complexity of digital signatures and certificates. Unlike handwritten signatures, the generation and verification of digital signatures requires and depends on a lot of hardware and software that must work and interoperate correctly. The resulting complexity is so huge that it is possible and even likely that some things will eventually go wrong.

With this issue of eSECURITY communications, we dare another experiment: we have generated a self-signed certificate using the open source software XCA,[1] and we have used the private signing key to digitally sign the PDF file that represents the newsletter using the Open eGov LocalSigner software.[2] Instead of digitlly signing the e-mail message that delivers the newsletter, we now digitally sign the document that represents the newsletter. We are very curious to learn whether this approach poses similar problems to the viability of digital signatures. If you see any advantages or disadvantages related to any of these use cases, then please let us know. We would like to have a (possibly ongoing) discussion about this topic.

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.

[1] `http://sourceforge.net/projects/xca`

[2] `https://www.e-service.admin.ch/wiki/display/suispublic/Open+eGov+LocalSigner`

2 Publications

An editorial entitled "Sicherheit auch in der Informatik — Jetzt gilt es ernst" appeared in a guidebook entitled "Schutz und Sicherheit" that was distributed as a supplement to the Tages-Anzeiger on December 20, 2007. The editorial argues that after many years spent on the theoretical foundations of computer security, things are now getting real and relevant in practice. The first application that has come under fire is Internet banking. The attacks mounted so far are effective and very powerful, and there is no simple solution in sight. The best available solution to protect Internet banking customers against malware-based attacks is to have them authenticate their transactions (in addition to user authentication). Unfortunately, this solution also changes the user behavior, and Internet banks therefore hesitate to introduce it on a large scale. This will probably change in the foreseeable future.

In addition to this editorial, a few other articles and papers about TLS-SA and e-voting were published recently.

2.1 TLS-SA

The article entitled "SSL/TLS Session-Aware User Authentication" (originally entitled "SSL/TLS Session-Aware User Authentication: A Lightweight Alternative to Client-Side Certificates" and co-authored by Ralf Hauser and David Basin) appeared in the March issue of the *IEEE Computer* magazine.[3] The article elaborates on the feasibility of man-in-the-middle (MITM) attacks in an SSL/TLS setting, surveys possible countermeasures, examines the rationale behind SSL/TLS session-aware (TLS-SA) user authentication as a lightweight alternative to client-side certificates, and overviews and discusses different possibilities for making user authentication mechanisms be SSL/TLS session-aware. The article is well-suited to provide an introduction to MITM attacks and TLS-SA.

A complementary but more advanced research article entitled "Protecting TLS-SA Implementations for the Challenge-Response Feature of EMV-CAP Against Challenge Collision Attacks" (co-authored by Ralf Hauser) appears in the first issue of John Wiley's *Security and Communication Networks* magazine.[4] The article argues that a TLS-SA implementation for the challenge-response (C/R) feature of the EMV Chip Authentication Program (CAP) is appropriate but sus-

[3] `http://doi.ieeecomputersociety.org/10.1109/MC.2008.98`

[4] `http://dx.doi.org/10.1002/sec.11`

ceptible to challenge collision attacks. It then picks challenge collision attacks out as a central theme, and elaborates on a possible protection mechanism. Assuming that the adversary has no access to the browser's graphical user interface (GUI) and cannot retrieve the EMV-CAP challenge accordingly, the level of protection against challenge collision attacks can be improved considerably by non-deterministically derivating the challenge from information related to the SSL/TLS session and using encryption to turn a challenge into a response. If the adversary has read access to the browser's GUI, then this approach is counterproductive, and if the adversary even has write access, then the use of EMV-CAP is insecure and problematic in the first place.

2.2 E-Voting

A German article entitled "Anonymes E-Voting" appears in this year's first issue of the *digma* magazine. The article argues that blind signatures are theoretically fine to support anonymous e-voting, but that in practice covert channels can be used to easily circumvent and byepass the anonymity protection. Unfortunately, there are many possibilities to implement covert channels, and hence providing evidence for the anonymity of a particular e-voting solution requires a thorough analysis of the solution. This is laborious and costly, and hence the missing incentive may provide a problem in a real setting.

A paper entitled "Protecting Code Voting Against Vote Selling" (co-authored by Jörg Schwenk and Jörg Helbach) will be presented at the GI Conference on "Sicherheit, Schutz und Zuverlssigkeit" (Sicherheit 2008) to be held on April 2–4, 2008, in Saarbrücken (Germany). The paper will appear in the conference proceedings published by Springer. The paper starts from the insight that code voting is an appropriate technology to address the secure platform problem of remote Internet voting. It then elaborate on the susceptibility of code voting to vote selling, argues that the situation is comparable to all-postal voting, and overviews and puts up for discussion some organizational and procedural protection measures—recast ballots, multiple code sheets, and powerful voting credentials. The measures are to sap the incentive to sell (or buy) votes and hence to protect code voting against vote selling. Finally, the paper argues in favor of a clear separation of voter authorization and vote casting and discusses possibilities to do so.

3 Security Analyses

In the recent past, we have studied the set of problems related to Internet banking security, and we have analyzed some technologies that may be used to (partly) solve the problems.

3.1 Internet Banking

With the recent advent of client-side attacks, the security of Internet banking (and other SSL/TLS-based e-commerce applications) has come under fire and banks supporting Internet banking are challenged to implement more effective protection mechanisms and countermeasures. Against this background, Rolf Oppliger has teamed up with Ruedi Rytz and Thomas Holderegger to more specifically analyze the attacks and possible countermeasures. The draft of a first paper is available. It elaborates on client-side attacks and distinguishes between

- Offline credential-stealing,
- Online channel-breaking, and
- Content manipulation attacks.

Based on this distinction, it overviews, discusses, and puts into perspective countermeasures that can be used to protect against these attacks. At the bottom line, the paper argues that currently available measures are appropriate to protect against some offline credential-stealing attacks, that effective protection against online channel-breaking attacks is possible but requires the implementation of technologies to defeat man-in-the-middle (MITM) attacks (e.g., TLS-SA), and that practical protection against content manipulation attacks requires the implementation of technologies to authenticate the transactions (in addition to the users who initiate the transactions). Consequently, we expect many transaction authentication systems be developed and brought to market soon. In either case, we think that effective protection of Internet banking requires an accurate and careful transaction monitoring. Fortunately, banks have a lot of experience in this area.

If this topic is of interest to you, then please free to ask for the draft paper and optionally discuss it with us.

3.2 SecLookOn

A new visual authentication and authorization system called SecLookOn[5] has received broad press coverage.

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

The system was developed by Helmut Schluderbacher and it is marketed by MERLINnovations & Consulting GmbH. The system is funny to use and comes along with an even more funny security analysis. It basically argues that there are so many possibilities to combine the images and derive codes from them that the system is secure. This line of argumentation is overly simplistic and dangerous. It is in fact the same line of argumentation that made the Germans believe that the Enigma was secure in World War II. In spite of the fact that the encryption device had a huge key space, its ciphertexts were routinely (and secretly) broken by the British secret service. Having a sufficiently large key space is a necessary but usually not sufficient requirement for an encryption system to be secure. This also applies to other cryptographic systems. Given a system that is secure if the adversary chooses the most difficult way to attack the system (e.g., mount a brute-force attack) does not necessarily mean that it is secure in a real-world setting. An adversary who is slightly more intelligent would try to find other vulnerabilities and mount corresponding attacks.

If a security system comes along without a security analysis that addresses only the simplest and most straightforward ways to attack it, then one should be suspicious—this rule of thumb is general and does not only apply to authentication systems. Today, we know more and can do better than the Germans in World War II. We must consider different possibilities to attack the system and we must argue about the likelihood to mount the corresponding attacks. Many systems can be broken easily if certain things cannot be assumed. Remember, for example, the PaTHword system outlined and briefly analyzed in a previous issue of eSECURITY communications (Vol. 1, Issue 2, Fall 2004, Section 5.3). The security of this system can be broken easily if the adversary knows or has physical access to a PaTHword card. This can be achieved easily, and hence the attack is relevant and worrisome in practice. We expect similar vulnerabilities and corresponding possibilities to attack SecLookOn to exist—at least we have few incentive to believe the opposite. The promoters of SecLookOn should at least provide some evidence that other attacks than brute-force are not likely to exist or difficult to find.

4 Information Security and Privacy Books

Since the publication of the last issue of eSECURITY communications, the following books have been published in the information security and privacy book series of Artech House:

- Edward J. Coyne and John M. Davis, *Role Engineering for Enterprise Security Management*, ISBN 978-1-59693-218-0, 2007.
- Martin Luther, *Introduction to Identity-Based Encryption*, ISBN 978-1-59693-238-8, 2008.

Role based access controls (RBAC) and identity-based encryption (IBE) are hotly debated topics today. The advantages of RBAC are mostly undisputed, whereas the advantages of IBE are controversially discussed in the industry.

Furthermore, the following boos are scheduled to be published later in 2008:

- Ari Takanen and Jared DeMott, *Fuzzing for Software Security: Robustness Testing for Quality Assurance and Vulnerability Discovery*, ISBN 978-1-59693-214-2, scheduled for May 2008, approx. 230 pp.
- Javier Lopez, Steven Furnell, Sokratis Katsikas, and Ahmed Patel (Eds.), *Securing Information and Communication Systems: Principles, Technologies and Applications*, ISBN 978-1-59693-228-9, scheduled for May 2008, approx. 370 pp.
- C. Warren Axelrod, Jennifer Bayuk, and Daniel Schutzer, *Handbook of Information Security and Privacy*, ISBN-10 1-59693-190-6, scheduled for November 2008, approx. 395 pp.

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[6] for the coordinates of the Commissioning Editors).

5 Announcements

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

5.1 University Lectures

In spring 2008 (since February 18, 2008), Rolf Oppliger lectures at the University of Zürich on "Sicherheit in der Informationstechnik." The lecture provides a thorough introduction to various security issues related to

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

information technology (IT). The lecture slides are electronically available on the lecture's home page.[7] The lecture will be held annually and is supposed to take place again in spring 2009.

5.2 Courses

On January 25, 2008, David Basin, Ralf Hauser, and Rolf Oppliger taught a one-day compact course on "Secure Messaging in Theory and Practice" at the ETH Zürich.[8] The course mainly focused on S/MIME and PGP/OpenPGP, as well as many related issues, such as digital certificates and trust management, proxy- and gateway-based messaging, Web-based messaging, and certified mail. As of this writing, it is not clear whether (and if yes when) the course will be repeated in the future.

In 2008, InfoGuard will host three courses on contemporary cryptography (based on Rolf Oppliger's book *Contemporary Cryptography*). Four out of five days will be taught by Rolf Oppliger. The course will be held in English and take place in Zug. The dates are as follows:

- April 21–25
- June 23–27
- November 24–28

If you are interested in the course, then you may request a flyer from InfoGuard or eSECURITY Technologies Rolf Oppliger.

Also, if you are interested to host a course on various aspects related to contemporary cryptography, then please feel free to contact eSECURITY Technologies Rolf Oppliger without commitment. We look forward to discuss the possibilities with you.

5.3 Conferences and Workshops

In 2008, Rolf Oppliger serves as a member of the programm committee for the following conferences and workshops:

- 3rd International Conference on Systems and Networks Communications (ICSNC 2008), Sliema (Malta), October 26–31, 2008
- 4th International Conference on Information Assurance and Security (IAS 2008), Naples (Italy), September 8–10, 2008
- 9th International Conference on Electronic Commerce and Web Technologies (EC-Web '08) held in conjunction with the 19th International Conference on Database and Expert Systems Applications (DEXA 2008), Turin (Italy), September 1–5, 2008
- 5th International Conference on Trust, Privacy and Security in Digital Business (TrustBus '08) held in conjunction with the 19th International Conference on Database and Expert Systems Applications (DEXA 2008), Turin (Italy), September 1–5, 2008
- International Conference on Security and Cryptography (SECRYPT 2008), Porto (Portugal), July 26–29, 2008
- 5th European PKI Workshop: Theory and Practice (EuroPKI '08), Trondheim (Norway), June 16–17, 2008
- 2nd Workshop in Information Security Theory and Practices (WISTP 2008), Sevilla (Spain), May 13–16, 2008

The conferences and workshops look promising, and it would be a pleasure to personally meet you at any of them.

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/Teaching/uni-zh-2008.shtml`

[8] `http://www.inf.ethz.ch/education/continuing/compact_courses/details/index`cid=46?

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