Volume 5, Issue 2, Fall 2008 http://www.esecurity.ch/communications.html

Contents

1 Editorial

IT security teeters on a knife edge. If we consider the current situation regarding botnets, malware attacks, and infrastructural problems related to routing and DNS, we recognize that a professionalization of IT security is going on—both on the attacker and defender's side. To deal with today's attacks, the defenders (who are the information security professionals like you and me) need to have a deep understanding of technologies at various levels, ranging from operating system and networking issues to application and software development. There are so many ways to attack an Internet or Web-based application that the task of defending it has become upmost involved and tricky. The days of information security professionals sitting in their offices and writing checklists and cross-checking documents against these lists are definitively over. Today's information security professionals need to be much more proactive and responsive. They must team up with application developers and operators to come up with architectures and implementations that are as secure as possible for a given application context. Simply saying "no" or flooding application developers with directives are no longer valid options. Security—and in particular IT security—is a process that must start with a project and accompany it from the beginning to the end. The information security professional is the accompanist of the project leader—this literally calls for teamwork.

eSECURITY Technologies Rolf Oppliger has positioned itself to serve as a security architect for the digital world. As such, it tries to follow the principles stated above. If you lack an information security professional in your team, then we may fill this gap—at least, we can give it a try. The consolidated findings of some recent activities are summarized in this issue of eSECURITY communications. We hope that you enjoy reading it, and we are looking forward hearing from you and receiving your feedback, comments, or criticism.

2 News

Given the importance of the *Secure Sockets Layer* (SSL) and *Transport Layer Security* (TLS) protocols for e-commerce, e-business, e-government, or—more generally—e-∗ applications, Rolf Oppliger decided to write a new book about these protocols and to publish it in the information security and privacy book series of Artech House. The book is preliminarly titled "SSL and TLS: Theory and Practice," and its publication is tentatively scheduled for spring 2010. If you are interested in the topic, you are invited to provide input, i.e., issues that you would like to see addressed in the book. You may even go one step further and volunteer as a reviewer or proof-reader for the manuscript. Needless to say that any form of engagement and support is welcome and highly appreciated.

3 Publications

An article entitled "SSL/TLS Session-Aware User Authentication Revisited" (co-authored by Ralf Hauser and David Basin) was published in the *Computers & Security* journal (Vol. 27, Issues 3–4, May/June 2008, pp. 64–70). The article continues the line of research related to SSL/TLS session-aware user authentication (TLS-SA). More specifically, it starts with the TLS-SA implementation based on impersonal authentication tokens, and then presents a number of extensions, such as multi-institution tokens, possibilities for changing the PIN, and different ways of making several popular and widely deployed user authentication systems be SSL/TLS session-aware. The article provides another piece of the puzzle of making TLS-SA more practical and applicable.

A paper entitled "CAPTCHA-based Code Voting" (co-authored by Jörg Schwenk and Christoph Löhr) was presented by Christoph Löhr at the 3rd International Conference on Electronic Voting 2008 (EVOTE08) that took place in Bregenz (Austria) on August 6–9, 2008.[1] The paper was published in the conference proceedings. It starts with the insight that code voting provides an appropriate technology to address the secure platform problem of remote Internet voting, but that it is not particularly user-friendly. It then proposes the use of CAPTCHAs—an acronym standing for Completely Automated Public Turing tests to tell Computers and Humans Apart—to improve the user-friendliness of code voting, discusses the security of CAPTCHA-based code voting, and elaborates on a possible implementation. Unfortunately, the security of CAPTCHAs is not sufficiently well understood (cf. Section 4.1), and hence more basic research is needed to make CAPTCHA-based code voting a valid option for secure remote Internet voting.

A German article entitled "E-Voting auf unsicheren Client-Plattformen" appeared in the second issue of this year's *digma* magazine (Vol. 8, No. 2, June 2008, pp. 82–85). The article elaborates on the security of remote Internet voting in Switzerland. More specifically, it argues (i) that the attack vectors that currently

[1] `http://www.e-voting.cc/topics/conference2008`

affect Internet banking applications also apply to remote Internet voting and corresponding solutions, (ii) that code voting provides an appropriate technology to address the secure platform problem of remote Internet voting, and (iii) that technologies like CAPTCHA-based code voting may be used to simplify the user interface. The last point is particularly important, and considerably more research is needed to make the user interface as simple as possible. In fact, we think that the user interface is going to be a critical factor of success for any secure remote Internet voting technology.

4 Security Analyses

In the last issue of eSECURITY communications (Vol. 5, Issue 1, Spring 2008), we briefly introduced the SecLookOn authentication system and criticized the line of argumentation regarding security and resistance to attacks. We argued that simply enumerating the number of possible keys and assuming that an adversary is as stupid as to run through all of them is simply not sufficient. You may be familar with the game *Master Mind*: instead of running through all possibilities and doing an exhaustive search, players routinely make conclusions from past tries and narrow down the set of all remaining possibilities accordingly. We expect similar strategies to work against SecLookOn.

The story continues: Instead of going back to the drawing table and more thoroughly analyzing the security of the system, MERLINnovations & Consulting GmbH (i.e., the company that actually markets SecLookOn) has announced a "Hack The Key!" contest.[2] As its name suggests, the aim of the contest is to find a valid SecLookOn key until October 10, 2008. Among all valid submissions, a contract free 3G iPhone will be drawn. Again, we think that the approach taken by MERLINnovations & Consulting GmbH to promote SecLookOn is deceptive. There is no need to run a contest as long as the system that is subject to the contest is not sufficiently well investigated and understood. We therefore expect the system to survive the contest (also because the incentive to participate in the contest is sufficiently small). But we still doubt that the system will survive a more determined attack by somebody who is going for more than a contract free 3G iPhone. The better testbed would be a theoretical analysis based on a reasonably precise specification of the system that the protocols it employs. Only if such an analysis provided convincing arguments for the security of the system, would it make sense to go one step further and run a competition. Hence, there is a long way to go and we expect the SecLookOn story to be continued.

More seriously, there are a few remarks regarding the security of CAPTCHA-based code voting and recently occuring DNS cache poisoning attacks.

4.1 CAPTCHA-based Code Voting

A preliminary security analysis of CAPTCHA-based code voting is given in Section 5 of the paper presented at EVOTE08 (cf. Section 3). Roughly speaking, the paper argues that the security of CAPTCHAs[3] is inherited to CAPTCHA-based code voting, but that there remain two problems to be addressed:

1. CAPTCHA-based code voting must be made resistant against man-in-the-middle (MITM) attacks;
2. Care must be taken so CAPTCHAs are not solved in a distributed way.

The first problem can be solved, for example, using TLS-SA or a similar approach. The second problem is more worrisome. Note, for example, that it is rumoured that Google Mail accounts are systematically being created in a distributed way (e.g., the CAPTCHAs to solve are presented to visitors of pornographic sites). This rumour is very realistic, given the low costs of human labour in some countries like China.

In addition to these problems, there are two additional points to consider.

- First, textual CAPTCHAs are usually assumed to be secure in the sense that the adversary is not able to read out the text (that is arbitrary but encoded in the CAPTCHA). In the case of CAPTCHA-based code voting, however, the text to read out is not arbitrary—it refers to one of the voter's options (e.g., "Yes" or "No" in the case of a vote or a candidate name in the case of an election). To distinguish the CAPTCHAs that refer to these options is usually simpler than to read out arbitrary text. Consequently, the notion of *CAPTCHA indistinguishability* may be useful to formalize this point: If an adversary who is given two known texts and two CAPTCHAs referring to these texts is not able or cannot say which CAPTCHA refers to which text with a probability substantially better than

[2] `http://www.seclookon.com/seclookon/contest.asp`

[3] Keep in mind, however, that the security of CAPTCHAs is put into question troday.

guessing (i.e., 0.5), then the CAPTCHAs are indistinguishable.

- Second, it is important to assume an adversary who is not able to entirely keep under surveillance the voter and his or her computer system. If the adversary could systematically monitor the voter, then he or she would be able to guess the option chosen by the voter and eventually change it.

There is more work to be done regarding the first point (e.g., introduing and formalizing the notion of CAPTCHA indistinguishability). The second point, in turn, leads to a specific threats model and a "natural" bound for the security that can be achieved with CAPTCHA-based code voting. It is mainly a political question, whether such a bound is acceptable in a real-world setting.

4.2 DNS Cache Poisoning

The *Domain Name System* (DNS) is at the core of the Internet. If it fails or gets compromised, then the entire Internet (and all of its applications) is at stake. It is therefore not surprising that people periodically come up with new ways of attacking the DNS. Some of these attacks are not particularly worrisome, but others are. Shortly before this year's Black Hat conference, for example, Dan Kaminsky announced that he had found new ways to mount DNS cache poisoning attacks. The attacks exploit vulnerabilities announced by the US-CERT in Vulnerability Note VU#800113 entitled "Multiple DNS implementations vulnerable to cache poisoning" published on July 8, 2008.[4] There are basically three vulnerabilities mentioned in this note:

- Too short query ID (QID) fields that leads to an insufficiently large QID space;
- Possibility of having multiple outstanding DNS requests;
- Use of fixed source ports for generating DNS queries.

Taking advantage of these vulnerabilities, Kaminsky found ways to poison a DNS cache by providing faked additional resource records that are in-bailiwick. Because of the shortness and poor pseudorandomness of the QIDs, the fixed source port numbers of the requesting DNS resolvers (typically udp/53), and the fact that multiple responses can be provided and sent to a requesting DNS resolver, a DNS cache can be poisoned in a matter of seconds or minutes. Consequently, the attacks are fairly powerful and most vendors have provided patches for their products. Most of these patches modify the way source ports are chosen for DNS queries and/or improve the pseudorandomness quality of the generated QID values. In either case, the adversary has to try out more possibilities until he or she finds a correct DNS response that can poison the corresponding DNS cache.

In the long term, it is commonly agreed that *DNS Security* (DNSSEC) as specified by the IETF (cf. RFCs 4033–4035) is required to provide better protection against DNS cache poisoning and related attacks. Unfortunately, the deployment of DNSSEC on a large-scale is far away from being trivial, and hence the deployment rate of DNSSEC has turned out to be slow (certainly slower than originally anticipated). In fact, there is a long way to go until DNSSEC will be routinely used in practice.

5 Information Security and Privacy Books

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

- 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, 2008, 289 pp.
- Ari Takanen, Jared D. DeMott, and Charles Miller, *Fuzzing for Software Security Testing and Quality Assurance*, ISBN 978-1-59693-214-2, 2008, 230 pp.

The first book is used as lecture notes for the Intensive Programme on Information and Communication Systems Security (IPICS) schools.[5] Originally, IPICS started as an ERASMUS Intensive Programme activity. Meanwhile, IPICS summer schools have been held in several places around Europe (1998 in Vienna, 1999 and 2005 in Chios, 2000 in Stockholm, 2001 and 2002 in Samos, 2003 in Malaga, 2004 in Graz, 2006 in Leuven, 2007 in Glamorgan, and this year in Regensburg). For almost a decade IPICS has also been held as a winter school at the University of Oulu, Finland.

[4] `http://www.kb.cert.org/vuls/id/800113`

[5] `http://www.ipics-school.eu`

Furthermore, the following book is scheduled to be published later this year:

- 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 Editor (refer to the book series' home page[6] for the coordinates of the Commissioning Editors). We are open for new topics that are relevant for information security or privacy professionals.

6 Announcements

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

6.1 University Lectures

In spring 2009, Rolf Oppliger will lecture at the University of Zürich on "Sicherheit in der Informationstechnik." Again, the lecture is going to provide a thorough introduction to various issues related to IT security. The lecture slides are electronically available on the lecture's home page.[7]

6.2 Courses

In 2008, InfoGuard hosts three seminars on contemporary cryptography (based on Rolf Oppliger's book *Contemporary Cryptography*). The seminars are usually held in English and take place in Zug, which is located in the center of Switzerland. Two out of three seminars have already taken place and have been successful. There is one remaining seminar to take place on November 24–28, 2008. If you are interested in attending the seminar, then you may request further information or a flyer from InfoGuard or eSECURITY Technologies Rolf Oppliger. An electronic version of the flyer can also be downloaded from the Internet.[8]

The seminars will also take place in 2009. The preliminary dates are as follows:

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

Make a reservation as soon as possible, if you are able to attend any of these seminars.

6.3 Conferences and Workshops

In addition to the conferences and workshops mentioned in the last issue of eSECURITY communications issue, Rolf Oppliger has agreed to serve as a member of the programm committee for the following conference in 2008:

- 11th International Conference on Information Security and Cryptology (ICISC '08), Seoul (Korea), December 4–5, 2008

For the year 2009, Rolf Oppliger has agreed to serve as a member of the programm committee for the following conferences:

- 5th International Conference on Information Assurance and Security (IAS 2009), Xi'an (China), August 18–20, 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

Other programm committee memberships for 2009 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).

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

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

[8] http://www.esecurity.ch/Flyers/CC_Seminar_2008.pdf

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