eSECURITY® communications

Volume 3, Issue 1, Spring 2006 http://www.esecurity.ch/communications.html

Contents

1 Editorial

In the last issue of eSECURITY communications we called the security of Internet banking in question, and we elaborated on the feasibility of man-in-the-middle (MITM) attacks. We also said that we are (hopefully) ready to reveal a pragmatic and efficient countermeasure to protect against MITM attacks in the next issue of eSECURITY communications. We are ready and we keep the promise in Section 2.2 of this issue. The technical terms for the countermeasure are *SSL/TLS session-aware user authentication* (TLS-SA) and *man-in-the-middle proof authentication* (MPA). It is joint work with Ralf Hauser (PrivaSphere AG) and David Basin (ETH Zürich). More recently, we have started a proof-of-concept implementation together with AdNovum Informatik AG (the results will be published later on).

Most experts agree that MITM attacks are real, that they will probably take place soon, and that they are very powerful (from the attacker's viewpoint). We already experienced a first taste when a phishing site employed a legitimate server certificate to spoof the Web site of the Mountain America Credit Union. The real site is at `www.mtnamerica.org`, whereas the phishing site employed a certificate for `www.mountain-america.com` and `www.mountain-america.net`. It does not come as a surprise that this phishing attack was very successful and we expect many more to take place in the future. In fact, phishing is getting more and more sophisticated and we slowly run out of time. We need a better understanding of both the problem and possible protection mechanisms against phishing and MITM attacks—TLS-SA and MPA is our contribution. We hope that it will be adopted by the industry.

We hope that you enjoy reading this issue of eSECURITY communications (with a special focus on SSL/TLS session-aware user authentication), and we are looking forward hearing from you and receiving your feedback, comments, and criticism.

2 News

There are news related to certified mail, SSL/TLS session-aware user authentication, and the previously announced eSECURITY Technology Assessment Program.

2.1 Certified Mail

In a recent paper[1] entitled "Some Common Attacks against Certified Email Protocols and the Countermeasures," a group of researchers from Singapore analyzed the fairness properties of two certified mail protocols proposed by Rolf Oppliger and Peter Stadlin, i.e., the basic certified mail protocol (BCMP) and the stateless certified mail protocol (SCMP). The paper elaborates on two weaknesses and vulnerabilities that can be exploited to circumvent the fairness properties of both protocols. While the first weakness and vulnerability is trivial to fix, the second weakness and vulnerability requires a minor modification of the message formats (in particular, the way dual signatures are constructed). The modification will be described in a follow-up paper.

More recently, Rolf Oppliger and Peter Stadlin have started to extend the BCMP in the sense that it can be used to provide temporal authentication (i.e., time-stamping) and non-repudiation of delivery services (in addition to non-repudiation of receipt services). This is ongoing work and will be reported elsewhere.

We think and firmly believe that certified mail services (in any form) will become more important in the future. Consequently, we think that tracking and non-repudiation services, such as [inca]Mail from the Swiss Postal Services, are valuable contributions to the e-commerce marketplace in Switzerland. We do, however, also think that there is room for alternative approaches and services.

2.2 SSL/TLS Session-aware User Authentication

Man-in-the-middle (MITM) attacks pose a serious threat to browser- and SSL/ TLS-based online applications, like Internet banking, and there are only a few technologies available to mitigate the risks. In [1], Rolf Oppliger, Ralf Hauser (PrivaSphere AG), and David Basin (ETH Zürich) introduced the notion of SSL/TLS session-aware user authentication to protect SSL/TLS-based online applications against MITM attacks. The main idea is to make the user authentication depend not only on the user's (secret) credentials, such as a password or personal identification number (PIN), but also on state information related to the SSL/TLS session in which the credentials are being transferred to the server. The rationale behind this idea is that the

[1] `http://www.i2r.a-star.edu.sg/icsd/staff/guilin/papers/CC05-CEM-revised.pdf`

server should have the possibility to determine whether the SSL/TLS session in which it receives the credentials is the same as the user employed when he sent out the credentials in the first place.

- If the two sessions are the same, then there is probably no MITM involved.
- If the two sessions are different, then something abnormal is taking place. It is likely that a MITM is located between the user's client system and the server.

Using SSL/TLS session-aware (TLS-SA) user authentication, the user authenticates himself by providing a user authentication code (UAC) that depends on both the credentials and the SSL/TLS session (in particular, information from the SSL/TLS session state). A MITM who gets hold of the UAC can no longer misuse it by simply retransmitting it. The key point is that the UAC is bound to a particular SSL/TLS session, and if the UAC is submitted on another session, then the server can easily recognize this fact and drop the session. As such, SSL/TLS session-aware user authentication provides a lightweight alternative to the deployment and rollout of a public key infrastructure (PKI) to protect against MITM attacks.

There are a number of possibilities to implement SSL/TLS session-aware user authentication. In [1], it is argued (i) that software-based implementations are inherently vulnerable, (ii) that one should therefore pursue hardware-based implementations in the first place, and (iii) that a particularly promising possibility is the use of hardware tokens, preferrably in the form of impersonal authentication tokens. In [2], the scope is broadened and possibilities to implement (parts of) SSL/TLS session-aware user authentication in software are also considered (together with the security implications of doing this). This also includes possibilities to make 2- and 3-factor approaches, such as one-time password (OTP) and challenge-response systems, be SSL/TLS session-aware.

A proof of concept of TLS-SA is currently being implemented by AdNovum Informatik AG [3]. On the client side, the implementation comprises a plugin for Microsoft Internet Explorer and Vasco challenge-response tokens. On the server side, the implementation comprises two components from AdNovum's Nevis framework. We note that a few modifications in the user interface of standard browsers would simplify the implementation (and use) of SSL/TLS session-aware user authentication considerably. These modifications are overviewed and discussed in a position paper for a W3C workshop that is taking place in New York City [4].

[1] Oppliger, R., Hauser, R., and D. Basin, "SSL/TLS Session-Aware User Authentication—Or How to Effectively Thwart the Man-in-the-Middle," *Computer Communications*, to appear

[2] Oppliger, R., Hauser, R., and D. Basin, "SSL/TLS Session-Aware User Authentication Revisited," in preparation

[3] Oppliger, R., Hauser, R., Basin, D., Rodenhaeuser, A., and B. Kaiser, "A Proof of concept Implementation of SSL/TLS Session-Aware User Authentication," in preparation

[4] Oppliger, R., Hauser, R., and D. Basin, "Browser Enhancements to Support SSL/TLS Session-Aware User Authentication," Position paper, W3C Workshop on Transparency and Usability of Web Authentication, March 15-16, 2006, New York, USA, http://www.w3.org/2005/Security/usability-ws/papers/

2.3 eSECURITY Technology Assessment Program

In 2004, we launched the eSECURITY Technology Assessment program. The aim of the program is to provide independent and vendor-neutral assessments of upcoming and leading-edge information security technologies and techniques. Unfortunately, we have not been able to find sufficiently many sponsors, supporters, and subscribers in the past two years, and hence we have to abandon the program at the current point in time. We still think that the program is valuable, and hence the program may eventually be revived at some point in the future.

3 Publications

There are a couple of publications that have been published since the last issue of eSECURITY communications. Please, feel free to request a paper copy of one (or all) of the publications if you don't have access to the proper source(s). In either case, we kindly invite you to discuss the publications with us.

3.1 Refereed Articles

The articles entitled "Privacy-enhancing technologies for the world wide web" and "Why Have Public Key

Infrastructures Failed so far?" (co-authored by Javier Lopez and Günter Pernul) were published in *Computer Communications* (Vol. 28, Issue 16, pp. 1791–1797, 2005) and *Internet Research* (Vol. 15, No. 5, pp. 544–556, 2005).

The above-mentioned article entitled "SSL/TLS Session-Aware User Authentication—Or How to Effectively Thwart the Man-in-the-Middle" (co-authored by Ralf Hauser and David Basin) has been accepted for publication in the *Computer Communications* journal. It will appear later this year.

An article entitled "Providing Certified Mail Services on the Internet" has been accepted for publication in the *IEEE Security & Privacy* magazine. The article overviews, discusses, puts into perspective, analyzes, and assesses the technologies that are available to provide certified mail services on the Internet.

Last but not least, an invited article "Certinyms-low-end certificates in large-scale computing environments" will be published in the *Journal of Journal of Autonomic and Trusted Computing* (JoATC). The article starts with the popular argument that public key certificates with only poor identity verification of its holder are not useful to establish trust in large-scale computing environments, such as the Internet. In contrast to this argument, the article argues that low-end certificates—so-called certinyms—allow for a gradual build-up of trust among different parties. From a service provider's viewpoint, a certinym, by default, cannot be used to authenticate its holder; it can, however, be used to link different service requests to the same originator, and hence allow for the establishment of a trust relationship in the long term. Furthermore, the article gives several examples of Internet applications that would benefit from the availability and wide deployment of certinyms.

3.2 Conference and Workshop Papers

A position paper entitled "Browser Enhancements to Support SSL/TLS Session-Aware User Authentication" (coauthored by Ralf Hauser and David Basin) is electronically published on the home page at the W3C Workshop on Transparency and Usability of Web Authentication that takes place on March 15-16, 2006, in New York City. In short, the paper suggests three browser enhancements that simplify the implementation of MITM-resistant authentication with minimum changes to the SSL/TLS protocol stacks in use.

3.3 Other Articles

A (German-speaking) article entitled "MITM-Angriffe: Phishing in Echtzeit" appears in *digma* (Vol. 6, No. 1, 2006). The overview article elaborates on SSL/TLS session-aware user authentication on a relatively high level of abstraction. As such, it may serve as an appetizer for the more technical papers and articles mentioned above.

4 Security Analyses

In the context of our work on SSL/TLS session-aware user authentication, we have analyzed several technologies that claim to protect users against MITM attacks. Most importantly, we have looked into a patent-pending technology developed and proposed by RSA Security, Inc. The technology is described in a technology backgrounder entitled "Enhancing One-Time Passwords for Protection Against Real-Time Phishing Attacks" (available from RSA Security, Inc.).

The basic idea is to employ a trusted piece of software—a so-called Password Protection Module (PPM)—that utilizes password hashing to generate a passcode that is unique for the user and the application A in question. More specifically, the user is to invoke the PPM via a reserved control sequence and to enter his the password P_t (at time t) into the PPM (if the password is static, then $P_t = P$ is constant). The PPM, in turn, determines the application identifier ID_A and uses a cryptographic hash function h to generate a hashed passcode

$$P_{A,t} = h(ID_A, P_t).$$

The PPM then provides the hash passcode $P_{A,t}$ to the requesting application server, where it is verified. If the verification suceeds, then the application server returns a confirmation code

$$C_{A,t} = h'(ID_A, P_t)$$

to the PPM (where h' represents another cryptographic hash function). Finally, the PPM verifies $C_{A,t}$ and informs the user about the authenticity of the application server.

We think that the use of a PPM protects the user against attacks that try to reconstruct (or reuse) the user password in one way or another. For example, it seems to be computatonally infeasible to construct password $P_{B,t}$ from $P_{A,t}$ for another application B (instead of A). The use of a PPM, however, does not protect against MITM attacks. If the MITM operates

in real time (and is able to spoof the application server in the sense that the user thinks he's talking to the application server), then the MITM can simply forward $P_{A,t}$ and forget about $C_{A,t}$. Furthermore, instead of providing $C_{A,t}$ to the user's PPM, he can provide an error message (claiming that some network connection problem has occured).

In summary, we think that the use of a PPM is inappropriate to protect users against the powerful MITM attack we have in mind, and—maybe even more importantly and worrisome—that PPMs are very difficult to deploy.

5 Computer Security Series

Since the publication of the last issue of eSECURITY communications, no additional book has been published in the computer security book series of Artech House. There are currently 25 titles in the series. The following 3 titles are scheduled for this year:

- Panagiotis Papadimitratos, *Securing the Internet Infrastructure*, ISBN 1-58053-852-5
- John Velissarios, *Identity, Security and Anonymity on the Internet*, ISBN 1-58053-822-3
- Anthony M. Rutkowski, *Lawful Interception and Access*, ISBN 1-58053-880-0

The process of contracting new and promising 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[2] for the coordinates of the Commissioning Editors).

6 Outlook

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

6.1 University Lectures

In summer 2006 (starting on April 3, 2006), Rolf Oppliger will lecture at the University of Zürich on "Sicherheit in der Informationstechnik." The slides are electronically available on the lecture's home page.[3] The lecture will be held annually and is supposed to take place again in summer 2007.

6.2 Courses

We are currently in the process of planning and preparing an introductory course on contemporary cryptography (based on Rolf Oppliger's book *Contemporary Cryptography*). The course will last 3 days and will be hosted by Swiss Infosec AG.[4] It is scheduled to take place twice in 2006 (May 15–17 and September 11–13). The course will be announced by Swiss Infosec AG (you may also refer to the eSECURITY EDUCATION CENTER and the corresponding home page[5] to get the latest information).

In either case, the course slides will be made publicly available. A preliminary draft version of the slides is already available at the book's home page.[6] Any feedback or comment is welcome and highly appreciated. This is particularly true for people who want to use the slides to teach courses or lectures on contemporary cryptography.

6.3 Conferences and Workshops

In 2006, Rolf Oppliger serves as a member of the programm committee for the following conferences:

- Multikonferenz Wirtschaftsinformatik (MKWI 2006) IT-Security Track, Passau (Germany), February 20 - 22, 2006
- 20th IEEE International Conference on Advanced Information Networking and Applications (AINA 2006), Vienna, Austria, April 18 - 20, 2006
- 4th International Conference on Applied Cryptography and Network Security (ACNS 2006), Singapore, June 6 - 9, 2006
- 1st Conference on Advances in Computer Security and Forensics (ACSF), Liverpool (UK), July 13 - 14, 2006
- International Conference on Security and Cryptography (SECRYPT 2006), Setbal (Portugal), August 7 - 10, 2006
- 9th Information Security Conference (ISC '06), Island of Samos (Greece), August 30 - September 2, 2006
- 7th International Conference on Electronic Commerce and Web Technologies (EC-Web '06) held in conjunction with the 17th International Conference on Database and Expert Systems

[2] `www.esecurity.ch/serieseditor.html`

[3] `www.ifi.unizh.ch/~oppliger/Teaching/uni-zh-ifi-ss06.html`

[4] `www.infosec.ch`

[5] `www.esecurity.ch/education.html`

[6] `www.esecurity.ch/Books/cryptography.html`

Applications (DEXA 2006), Krakov (Poland), September 4 - 8, 2006

- 3rd International Conference on Trust, Privacy and Security in Digital Business (TrustBus '06) held in conjunction with the 17th International Conference on Database and Expert Systems Applications (DEXA 2006), Krakov (Poland), September 4 - 8, 2006
- International Association of Science and Technology for Development (IASTED) International Conference on Communication, Network, and Information Security (CNIS 2006), Cambridge, Massachusetts, USA, October 9 - 11, 2006
- 9th Annual International Conference on Information Security and Cryptology (ICISC '06), Busan (Korea), November 30 - December 1, 2006

It would be a pleasure to meet you at any of these conferences or workshops.

About the Company

eSECURITY Technologies Rolf Oppliger[7] 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] `www.esecurity.ch`