Volume 3, Issue 2, Fall 2006 http://www.esecurity.ch/communications.html

Contents

1 Editorial

In previous issues of eSECURITY communications, we repeatedly called the security of Internet banking in question and elaborated on the (theoretical) feasibility of man-in-the-middle (MITM) attacks. Meanwhile, the first MITM attacks occured in practice. In November 2005, a Swedish Internet bank fell victim to an MITM attack,[1] and on July 10, 2006, Brian Krebs reported in his Washington Post blog that an MITM attack had been launched against the U.S. Citibank.[2] In either case, the banks were using one-time password systems that were supposedely secure but proven to be the opposite. We are afraid that these attacks are not one-time events, and that we will see similar attacks occur in the future.

Against this background, mechanisms to protect SSL/TLS-based applications, such as Internet banking, against MITM attacks will become essential. The use of public key certificates on the client side provides an obvious solution to the problem. However, the deployment and rollout of a public key infrastructure (PKI) has turned out to be slow—certainly slower than it was originally anticipated. We therefore think that *SSL/TLS session-aware user authentication* (TLS-SA)—as proposed previously—provides an interesting lightweight alternative to the use of client-side certificates. TLS-SA is joint work with Ralf Hauser (PrivaSphere) and David Basin (ETH Zurich). Meanwhile, we have designed SSL/TLS session-aware solutions for almost all user authentication mechanisms and systems in use today.

In addition to TLS-SA, eSECURITY Technologies Rolf Oppliger has been (and is still) involved in a couple of other security-related projects. Some of them are reported 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

There is news related to a TLS-SA proof of concept implementation, certified mail, and Web hosting.

[1] `http://www.theregister.co.uk/2005/10/12/outlaw_phishing`

[2] `http://blog.washingtonpost.com/securityfix/006/07/citibank_phish_spoofs_2factor_1.html`

2.1 TLS-SA Proof of Concept Implementation

Earlier this year, AdNovum Informatik[3] prototyped TLS-SA in a proof of concept (PoC) implementation. The implementation employs challenge-response tokens from Vasco (i.e., Digipass 250 tokens) and a plugin for Microsoft Internet Explorer on the client side, as well as an adapted version of AdNovum's Nevis Web portal[4] on the server side.

A preliminary technical report describing the PoC implementation is available and can be downloaded from AdNovum's homepage.[5] A more mature version of the report is submitted for publication (the corresponding paper can be requested from eSECURITY Technologies Rolf Oppliger, PrivaSphere, or AdNovum). The results of the PoC implementation are promising, and we are looking into possibilities to integrate TLS-SA support into standard Web browsers and user authentication systems.

2.2 Certified Mail

In July 2006, Peter Stadlin and Rolf Oppliger were granted a Swiss patent entitled "Verfahren zur Erbringung von Empfangsbestätigungen für die Umsetzung von 'eingeschriebenen Nachrichten' in einem elektronischen Nachrichtenvermittlungssystem." The patent provides a mechanism and protocols to provide nonrepudiation services with proof of receipt (i.e., certified mail services) on the Internet.

In the same month, they also filed an application for a complementary patent entitled "Verfahren zur Erbringung von temporal authentifizierten Versand- und Empfangsbestätigungen in einem elektronischen Nachrichtenvermittlungssystem" (Swiss Patent Application No. 01196/06 filed on July 24, 2006). This patent application provides a scheme to additionally provide time-stamping and nonrepudiation services with proof of delivery.

We are currently looking into possibilities to provide and commercially deploy certified mail services on the Internet. Potential licensees are welcome to contact either of the inventors to discuss the terms and conditions of licensing agreements.

[3] `http://www.adnovum.ch`

[4] `http://www.nevis-web.com`

[5] `http://www.adnovum.ch/pdf/wps/wp_mitm_poc.pdf`

2.3 Web Hosting

In August 2006, eSECURITY Technologies Rolf Oppliger moved its Web site `www.esecurity.ch` from VTX Services[6] to Multimedia Networks (Hoststar[7]). Hoststar provides advanced features to protect e-mail message stores against spam mail. The aliases `rolf-oppliger.com` and `rolf-oppliger.ch` remain unaffected by this move.

3 Publications

There are a couple of publications that have appeared since the last issue of eSECURITY communications.

Most importantly, an 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) was published in the *Computer Communications* journal (Vol. 29, Issue 12, August 2006, pp. 2238–2246). This paper will be complemented by a series of follow-up papers that address specific aspects related to TLS-SA and the implementation thereof.

The two articles entitled "Providing Certified Mail Services on the Internet" and "Certinyms—low-end certificates in large-scale computing environments" are pending and awaiting publication. The same is true for a technical opinion column entitled "IT Security: In Search of the Holy Grail" that is scheduled to appear in the *Communications of the ACM* early in 2007.

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.

4 Security Analyses

In the last term, eSECURITY Technologies Rolf Oppliger has analyzed the security of Webmail, instant messaging, as well as Microsoft's identity metasystem and CardSpace (formerly codenamed InfoCard).

4.1 Webmail

Many companies and organizations have a policy in place that prohibits the use of Webmail. Some of them even try to technically enforce the prohibition (by using, for example, URL filtering mechanisms).

eSECURITY Technologies Rolf Oppliger has analyzed the security implications of Webmail and its usage in a corporate environment. From a security viewpoint, the major problem related to Webmail is that it allows users to bypass virus protection and content screening mechanisms that are otherwise applied to SMTP data streams. If there were similar technologies put in place to control HTTP(S) data streams, then there would hardly be any security argument against the usage of Webmail (as long as SMTP data traffic is allowed to flow in and out of a corporate network). Since there are now such technologies available on the market,[8] the remaining arguments in favor of prohibition are economic ones and arguments related to user guidance. Both are valid but not directly related to security.

4.2 Instant Messaging

In the U.S., we observe a strong trend towards the professional use of synchronous messaging services like instant messaging. It is possible and very likely that we will see a similar trend in Europe, and that synchronous messaging services will become important communication media in future business environments. We already see this trend in the context of push-based messaging services, like Research in Motion's Blackberry or Microsoft's ActiveSync.

eSECURITY Technologies Rolf Oppliger has analyzed the security implications of instant messaging and its usage in a corporate environment. The normal use of instant messaging requires specific ports to be opened on the firewall. This is dangerous and not recommended (especially if one considers the fact that most instant messaging protocols are proprietary and have not been subject to public scrutiny). Instead, it seems more appropriate to use either security appliances that control instant messaging data traffic at the firewall level or Web-based instant messaging. Web-based instant messaging applications, in turn, are based on a new programming paradigm named AJAX (Asynchronous JavaScript and XML). Unfortunately, the security implications of AJAX are still poorly understood and it is therefore too early to tell whether AJAX- and Web-based instant messaging will meet the professional security expectations.

[6] `http://www.vtx.ch`

[7] `http://www.hoststar.ch`

[8] Examples include products from Akonix, CipherTrust, and FaceTime, as well as managed services from Postini.

4.3 Microsoft's Identity Metasystem and CardSpace

Microsoft has designed and proposed an identity metasystem that is user-centric and consistent with open Web services (WS-∗) standards. An implementation of the metasystem is, for example, available in Windows Vista's Windows Communications Foundation (WCF) of .NET Framework 3.0. The implementation interfaces to the user by providing an identity selector (i.e., CardSpace) that visually represents digital identities (i.e., InfoCards) that are available and from which the user can choose from in a given context. Various applications can make use of the identity selector, including, for example, Microsoft Internet Explorer 7. Consequently, it is possible and very likely that Microsoft's identity metasystem and CardSpace will become widely deployed on the Internet and attractive targets to attack.

Against this background, Sebastian Gajek (Ruhr-University Bochum), Ralf Hauser (PrivaSphere), and Rolf Oppliger have analyzed the security of Microsoft's identity metasystem and CardSpace. The findings are positive in the sense that the architectural design looks fine, and that no additional vulnerability has been identified (in addition to the vulnerabilities that are specific to the technologies in use). If you are interested in the security analysis, then you may contact one of the authors.

5 Book 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 available in the series (3 additional titles being scheduled).

More recently, the aims and scope of the series has been redefined, and the title of the series has been changed from *Computer Security* to *Information Security and Privacy*. This new title should better reflect the new (and refined) aims and scope of the series. We hope that you like the new title, and that you continue to show interest in the books published in the series. If you have particular suggestions or proposals (related to topics that should be addressed by future books), then please let us know.

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

6 Outlook

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

6.1 University Lectures

On February 12–14, 2007, Rolf Oppliger will lecture at the Georg-August-University in Göttingen (Germany) on cryptography.[10] The lecture will be based on the book *Contemporary Cryptography* (ISBN 1-58053-642-5) and a set of corresponding slides that are available from the book's homepage.[11]

In summer 2007, Rolf Oppliger will again lecture at the University of Zurich (Switzerland) on "Sicherheit in der Informationstechnik." The details of the lecture will be published soon, and the lecture slides will be made available on the lecture's homepage.

6.2 Courses

All courses on contemporary cryptography hosted by Swiss Infosec have been postponed to 2007. We will keep you informed.

On October 2–6 and November 20–24, InfoGuard[12] will host an English-speaking seminar on contemporary cryptography in Zug, Switzerland. Rolf Oppliger will be the seminar instructor for 4 (out of 5) days.

Ralf Hauser, David Basin, and Rolf Oppliger are currently in the process of planning a security-related course that will be held at the ETH Zurich early next year. The details of the course will be announced later this year.

6.3 Conferences and Workshops

In addition to the conferences and workshops itemized in the last issue of eSECURITY communications, Rolf Oppliger serves as a member of the programm committee for the following conferences in 2006:

- 2nd International Conference on Signal-Image Technology & Internet-Based Systems (SITIS

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

[10] `http://www.informatik.uni-goettingen.de/studies/courses/special/krypto/`

[11] `http://books.esecurity.ch/cryptography.html`

[12] `http://www.infoguard.ch`

'06), Track II - Web-Based Information Technologies & Distributed Systems, Hammamet (Tunisia), December 17–21, 2006

- International Conference on Systems and Networks Communications (ICSNC 2006), Miniconference on Security Systems (SESYS 2006), Tahiti (French Polynesia), November 2–4, 2006

The program committee appointments of Rolf Oppliger for the year 2007 will be reported in the next issue of eSECURITY communications.

About the Company

eSECURITY Technologies Rolf Oppliger[13] 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).

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