Volume 2, Issue 2, Fall 2005 http://www.esecurity.ch/communications.html

Contents

1 Editorial

Is Internet banking secure? Since we use SSL/TLS sessions with certificate-based server authentication and strong user authentication mechanisms (e.g., SecurID tokens or challenge-response mechanisms), we tend to answer in the affirmative. Unfortunately, this answer is too optimistic and it is worthwhile to have a closer look at the question we started with. Let's consider the following scenario: An attacker sets up a faked Web site (representing, for example, a bank), misleads the user to reveal his credentials to this site (using standard phishing techniques, including, for example, visual spoofing), and then misuses these credentials to spoof the user and act as a man-in-the-middle (MITM). The fact that the user authentication mechanism is strong does not really help if the attacker acts in real-time. We are very concerned about the feasibility of such attacks; they are simple to mount and likely to occur soon. Many customers of so-called "strong" user authentication mechanisms will painfully discover that the mechanisms they employ are not that strong, and—maybe even more importantly—that they are not qualified to protect users against MITM attacks in an SSL/TLS setting.

Against this background, eSECURITY Technologies Rolf Oppliger has teamed up with PrivaSphere AG to develop a pragmatic and efficient countermeasure to protect users against MITM attacks in an SSL/TLS setting. We are nailing down the details and we will (hopefully) be ready to present the countermeasure in the next issue of eSECURITY communications. If you are curious about it, then you may contact us towards the end of October 2005. We will then be ready to publicly discuss the topic.

2 News

Rolf Oppliger's new book entitled *Contemporary Cryptography* (ISBN 1-58053-348-5) was published by Artech House in April 2005. So far, the book has been well received on the marketplace. You may refer to the book's home page[1] to get more information or place an online order (with Amazon.com).

In summer 2005, Rolf Oppliger lectured on "Sicherheit in der Informationstechnik" at the University of Zürich. The slides are electronically available at the lecture's home page.[2] The lecture will be held annually and take place again in summer 2006.

On June 14, 2005, Rolf Oppliger gave an invited talk entited "Digital Signatures: From Theory to Practice" in the ZISC Information Security Colloquium. Abstract and slides are electronically available from the colloquium's Web site.[3] The talk was well attended and it was repeated on August 9, 2005, at the Swiss Federal Institute of Intellectual Property (coorganized by IAM Alumni and the Swiss Open Systems User Group /ch/open).

3 Publications

3.1 Refereed Articles

The refereed articles "IT Security: In Search of the Holy Grail" (to appear in *Communications of the ACM*) and "Privacy-enhancing Technologies for the World Wide Web" (to appear in *Computer Communications*, Vol. 28, No. 16, pp. 1791–1797) will be published soon. They were summarized in the last issue of eSECURITY communications.

Another refereed article entitled "Why Have Public Key Infrastructures Failed so far?" (co-authored by Javier Lopez and Günter Pernul) will be published in the *Internet Research* journal (Vol. 15, No. 5) in October 2005. The article overviews and discusses the technical, economical, legal, and social reasons why public key infrastructures have failed so far, summarizes the lessons learnt, and gives some expectations about the future development of the field.

3.2 Conference and Workshop Papers

The following conference and workshop papers have been published since the last issue of eSECURITY communications:

- A paper entitled "Classifying Public Key Certificates" (coauthored by Javier Lopez and Günther Pernul) appeared in the *Proceedings of the 2nd European PKI Workshop*. The workshop took place on June 30 - July 1, 2005, in Canterbury (UK), and the proceedings are published by Springer (LNCS 3545). The paper proposes a four-dimensional scheme that can be used to uniformly describe and classify public key certificates. The scheme distinguishes between (i) who owns a certificate, (ii) how the certificate owner

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

[2] `http://www.ifi.unizh.ch/~oppliger/Teaching/uni-zh-ifi-ss05.html`

[3] `http://www.zisc.ethz.ch/events/infseccolloquium2005`

is registered, (iii) on what medium the certificate (or the private key, respectively) is stored, and (iv) what type of functionality the certificate is intended to be used for.

- A paper entitled "Effective Protection Against Phishing and Web Spoofing" (coauthored by Sebastian Gajek) appears in the *Proceedings of the 9th IFIP TC6 and TC11 Conference on Communications and Multimedia Security (CMS 2005)*. The conference will take place on September 19 - 21, 2005, in Salzburg (Austria), and the proceedings will be published by Springer (LNCS 3677). The paper summarizes, discusses, and evaluates the effectiveness of protection mechanisms against (large-scale) phishing and Web spoofing attacks.

The second paper was the starting point for the current research activities related to phishing, Web spoofing, and MITM attacks (as mentioned in the Editorial).

3.3 Other Articles

The following (German-speaking) article has been published since the last issue of eSECURITY communications:

- A German-speaking article entitled "Die Jagd nach dem heiligen Gral" appeared in *digma* (Vol. 5, No. 2, 2005, pp. 92–93). The article elaborates on an analogy to explain and put into perspective the task(s) of an information security officer.

Please, feel free to request a paper copy of one (or all) of the articles if you don't have access to the proper source(s). We invite you to discuss the articles and their contents with us.

4 Security Analyses

In the recent past, we have analyzed many technologies and mechanisms that are claimed to protect against phshing, Web spoofing, and MITM attacks (again, you may refer to the Editorial). As mentioned above, a first paper entitled "Effective Protection Against Phishing and Web Spoofing" will appear in the *Proceedings of the 9th IFIP TC6 and TC11 Conference on Communications and Multimedia Security (CMS 2005)*. Other papers are in the queue and will likely be published in the future.

5 Computer Security Series

Since the publication of the last issue of eSECURITY communications, the following books have been published in the computer security book series of Artech House:[4]

- Rolf Oppliger, *Contemporary Cryptography*, ISBN 1-58053-642-5, 2005, 510 pp.
- Thomas Hardjono and Lakshminath R. Dondeti, *Security in Wireless LANs und MANs*, ISBN 1-58053-755-3, 2005, 266 pp.

Furthermore, the following books are scheduled for 2006:

- Panagiotis Papadimitratos, *Securing the Internet Infrastructure*, ISBN 1-58053-852-5, scheduled for February 2006, approx. 301 pp.
- John Velissarios, *Identity, Security and Anonymity on the Internet*, ISBN 1-58053-822-3, scheduled for April 2006, approx. 400 pp.
- Anthony M. Rutkowski, *Lawful Interception and Access*, ISBN 1-58053-880-0, scheduled for June 2006, approx. 354 pp.

Including these titles, the computer security book series comprises 28 titles. As such, it is the largest book series devoted to computer security only.[5]

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 any of the Commissioning Editors (Tiina Ruonamaa or Wayne Yuhasz). The coordinates of these persons can be found on the series' home page. We are particularly interested in book proposals about new, upcoming, and leading-edge topics, such as privacy, RFID, anonymity and pseudonymity, identity management, or identity-based cryptography. It goes without saying that any other topic related to computer security is of interest to the series.

6 Outlook

6.1 Courses

We are currently in the process of planning and preparing an introductory course on contemporary cryptography (based on the book *Contemporary Cryptography*).

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

[5] The competing book series are itemized at `www.esecurity.ch/links.html#bookseries`.

The course will take place on December 5-7, 2005, in the Zürich area. Registration is open and a corresponding flyer can be downloaded from the eSECURITY EDUCATION CENTER's home page.[6] If you are interested in a specific topic (related to contemporary cryptography), then please let us know (so we can make sure that it is included in the course).

6.2 Conferences and Workshops

In addition to the conferences and workshops announed in the last issue of eSECURITY communications, Rolf Oppliger also serves as a member of the programm committee for the following conference in this year:

- 8th Annual Information Conference on Information Security and Cryptology (ICISC '05), Seoul, Korea, December 1 - 2, 2005

Furthermore, he will serve as a member of the programm committee for the following conferences and workshops to be held in 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

Please, feel free to register and attend any of these conferences and 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).

[6] www.esecurity.ch/Flyers/Kurs_Kryptographie_2005.pdf
[7] www.esecurity.ch