eSECURITY®
communications

Volume 4, Issue 2, Fall 2007 http://www.esecurity.ch/communications.html

Contents

1 Editorial

Welcome to the fall 2007 issue of eSECURITY communications.

There is a famous anecdote about a bank robber who—being asked why he robs banks—answered with "because this is where the money is." At first sight, this answer seems obvious and trivial (maybe too trivial to be mentioned in the first place). But at second sight, the answer is still noteworthy, mainly because it is symptomatical for all security considerations related to electronic commerce: *if there is money, then there is also crime*, or—alternatively speaking—*crime follows money*. On the defense side, this insight suggests that one must take a differentiating view when one discusses and considers the use of security measures. Such measures only make sense, if they mitigate specific risks. If there is no risk, then it is useless to spend money on security measures in the first place. This risk-based approach to information security has started to take off in the last couple of years. Today, any disquisition of security technologies, mechanisms, and services should start with a threat model (i.e., a model that elaborates on the types of attacks one wants to protect against).

If crime follows money, then it is not suprising that organized crime has sights on Internet banking, and that all major banks are subject to phishing, pharming, Web spoofing, man-in-the-middle, and malware attacks. Note that these attacks do not address the server systems of the banks, but rather the client systems of their clientele. Consequently, the usefulness and effectiveness of Internet banking as a whole is up for discussion, and there are many conclusions one may draw. For example, one may question the use of commercial off-the shelf browsers (e.g., Microsoft Internet Explorer or Mozilla Firefox) for Internet banking. Maybe the use of proprietary (and more static) client software is advantageous from a security viewpoint. This argument can be discussed controversially. Taking the discussion one step further, one may even argue about the future of software-open computer systems for security-critical applications. The alternative would be software-controlled or even software-closed computer systems, such as the ones being discussed in the context of trusted computing. Such a discussion is beyond the aims and scope of eSECURITY communications, but we are still interested in knowing your thoughts. We invite you to write them down and submit them for possible publication in eSECURITY communications. We are interested in having a discussion about this important and practically influential topic.

In any case, 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.

2 News

In May 2007, Rolf Oppliger was appointed adjunct professor at the University of Zürich, Switzerland, where he will continue to lecture regularly on information technology (IT) security. The next lecture is scheduled for spring 2008 (cf. Section 6.2).

3 Publications

An overview article entitled "SSL/TLS Session-Aware User Authentication: A Lightweight Alternative to Client-Side Certificates" (co-authored by Ralf Hauser and David Basin) has been accepted for publication and will appear in a future issue of the *IEEE Computer* magazine. 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. Due to the large readership of the *IEEE Computer* magazine, we expect a serious discussion about TLS-SA taking place after the publication of the article. We will keep you informed.

4 Invited Talks and Panel Discussions

As a member of the technical program committee, Rolf Oppliger took part in the 4th International Conference on Trust, Privacy and Security in Digital Business (TrustBus '07[1]) held on September 3–7, 2007, in conjunction with the renowned 18th International Conference on Database and Expert Systems Applications (DEXA 2007) in Regensburg (Germany).

During the conference, Rolf Oppliger participated in a panel discussion entitled "Managing Digital Identities—Challenges and Opportunities." Other panel particpants included (in alphabetical order):

- Marco Casassa-Mont from HP Labs in Bristol (UK)

[1] `http://www.icsd.aegean.gr/trustbus07/`

- Eduardo B. Fernández from Florida Atlantic University (USA)
- Socrates Katsikas from the University of Piraeus (Greece)
- Alfred Kobsa from UC Irvine (USA)

The panel was chaired and moderated by Günther Pernul from the University of Regensburg (Germany).

Identity management is an important and very timely topic that is sometimes discussed controversially even within the information security community. The term *identity management* is still vaguely defined and comprises the management of entities, identities, identifiers, privileges and access rights, as well as identification cards.

- According to RFC 2828, the term *entity* refers to "an active element of a system—e.g., an automated process, a subsystem, a person or group of persons—that incorporates a specific set of capabilities." In a typical setting, entities represent persons or legal entities, such as companies or organizations.
- There are many definitions of the term *identity* that can be found in the literature. The greatest common denominator of all these definitions is that an identity refers to some set of qualities (or attributes) that make an entity unique and different from other entities. Alternatively speaking, it is the individual characteristics by which an entity is recognized or known in a specific community. Consequently, an entity may have several identities—depending on the context in which it resides—and each identity can be characterized by a set of attributes.
- Every identity (of an entity) may have one (or several) *identifier(s)* that refers (refer) to it. In the simplest case, an identifier is just a name, an employee number, a social security number, or something similar. In some situations, the identifier is unique; in other situations it is not.
- Every identity (of an entity) may have a set of *privileges* and *access rights* associated with it. While the identity is the basis for authentication, privileges and access rights are the basis for authorization. In theory, authentication and authorization can be conceptually separated. In practice, however, authentication and authorization are often combined and implemented in an authentication and authorization infrastructure (AAI), a privilege management infrastructure (PMI), or an infrastructure with some other name.

When people talk about identity management, they often mix up the terms itemized above with the notion of an *identification card* (*ID card*). In the physical world, people are using and are accustomed to the use of ID cards. In essence, an ID card attests for the legitimacy of an identity (or its attributes, respectively). There are ID cards for all kinds of purposes: passports and ID cards issued by the state, employee cards issued by companies, membership and customer cards issued by all kinds of organizations and companies, student cards issued by universities, and so on. In spite of the fact that multiple-use ID cards are technically feasible, most ID cards in use today are single-use, meaning that they serve one single purpose or application. There may be many reasons for this fact—an important reason is certainly the fact that an ID card is also to serve customer relationship (so ID card-issuing organizations are reserved in sharing the cards with other organizations). The omnipresence of single-use ID cards results in wallets that are filled with all sorts of cards. We know the problem from daily life, and hence we decide on a case-to-case basis which card to employ in a given context. In the latest issue of eSECURITY communications (Volume 4, Issue 1, Spring 2007), we elaborated on Microsoft's identity metasystem and the CardSpace implementation thereof. CardSpace tries to mimic the real-world experience with multiple ID cards serving different purposes.

In his panel position statement, Rolf Oppliger stressed the point that it is important to specifiy what one is really referring to when one is talking about identity management. There are different viewpoints and perspectives on the topic. For example, from a technology perspective there are many authentication and authorization technologies that can be used to manage identities. Some are based on the Kerberos authentication system (one could call them 1^{st} generation technologies), some are based on digital certificates and public key infrastructures (one could call them 2^{nd} generation technologies), and some are based on Web-based single sign-on (SSO) services (one could call them 3^{rd} generation technologies). There was in fact consensus among the panelists that there are many technologies available, but that there are also organizational, procedural, and legal issues to resolve before the technologies can be deployed on a large scale.

5 Review Activities

In addition to the conferences and workshops itemized in the last issue of eSECURITY communications, Rolf

Oppliger served as a member of the programm committee for the 2nd International Conference on Systems and Networks Communications (ICSNC '07) that took place on August 25–31, 2007, in Cap Esterel (France).

More recently, Rolf Oppliger was appointed Associate Editor of a new and upcoming John Wiley & Sons journal entitled *Security and Communication Networks* (SCN).[2] We are confident of turning the journal into recommended reading for any professional working on network security. The first issue of the journal will appear in 2008. If you are interested in writing a paper for possible publication in the SCN, then please feel free to contact Rolf Oppliger or any other member of the editiorial board.

6 Teaching Activities

The eSECURITY EDUCATION CENTER[3] has a break, but Rolf Oppliger still continues to teach courses and seminars and to lecture at universities.

6.1 Seminar on Cryptography

On behalf of InfoGuard AG[4] and Crypto AG[5], Rolf Oppliger taught an international seminar on *Contemporary Cryptography* on June 25–29, 2007. The seminar is based on Rolf Oppliger's book with the same title. It provides an overview and introduction to the current state-of-the-art in cryptography. The seminar is held in English and usually takes place in Zug. The next seminar is scheduled for November 26–30, 2007. If you are interested to participate, then you may register or request a flyer from InfoGuard, Crypto, or eSECURITY Technologies Rolf Oppliger.

In 2008, the seminar on *Contemporary Cryptography* is provisorily scheduled for April 21–25, June 23–27, and November 24–28. It would give us great pleasure to meet you there.

6.2 University Lectures

In spring 2008 (starting on February 18, 2008), Rolf Oppliger will lecture at the University of Zürich on information technology security (the original title of the lecture is "Sicherheit in der Informationstechnik"). Note that the lecture will henceforth take place in the spring semester (instead of the summer semester). The slides are being revised and will be made electronically available on the lecture's home page[6] soon. The final examn of the lecture will take place on May 26, 2008.

7 Book Series

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

- Edward Humphreys, *Implementing the ISO/IEC 27000 Information Security Management System Standard*, ISBN-10 1596931728, ISBN-13 978-1596931725, 2007.

With the increasing importance of ISO 27000-compliant information security management systems (ISMS), we think that this book hits the market in the right time. Also, Ted is one of the leading persons in the ISO 27000 community, so it is partiucularly interesting and stimulating to hear (or rather read) what he has to say about the topic.

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

About the Company

eSECURITY Technologies Rolf Oppliger[8] 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).

[2] http://www.interscience.wiley.com/journal/security

[3] http://www.esecurity.ch/education.html

[4] http://www.infoguard.ch

[5] http://www.crypto.ch

[6] www.esecurity.ch/Teaching/uni-zh-2008.shtml

[7] www.esecurity.ch/serieseditor.html

[8] www.esecurity.ch