Volume 4, Issue 1, Spring 2007 http://www.esecurity.ch/communications.html

Contents

1 Editorial

An entity may have several identities. Take you as an example. You may have an identity with the state (as a citizen), an identity with your employer (as an employee), an identity with your financial institution (as a customer), and so on. Each identity is typically identified by an identifier (that may or may not be unique) and may be cerified in some way. For example, your ID card certifies your identity as a citizen, whereas your employee card certifies your identity as an employee. The numerous cards we usually carry with us in our wallets attest to the fact that we are multiple-identity entities. To make things worse, each identity may be coupled with a number of privileges that are relevant in a given context. And again, these privileges may be cerified in some way.

Against this background, *identity management* has to deal with entities, identities, identifiers, privileges, and certificates (not necessarily public key certificates). This is a broad and highly complex topic that goes beyond the issuance of electronic ID (eID) cards. In the recent past, identity management has become a hot topic in the industry, and there are multiple initiatives to provide Web-based identity management services on the Internet. Examples include Microsoft's Passport Network, the Liberty Alliance,[1] Shibboleth[2] (as part of the Internet 2 project), and OpenID.[3] With the release of Microsoft Vista, Microsoft has launched an identity metasystem and an implementation of an identity selector named *CardSpace* (formerly codenamed *InfoCard*). We think that CardSpace is a highly relevant technology that will have a deep impact on the way we think about identity management.

In this issue of eSECURITY communications, we have a closer look at Microsoft's identity metasystem and CardSpace from a security viewpoint. We hope that you enjoy reading it, and we are looking forward hearing from you and receiving your feedback, comments, or criticism.

2 News

Since November 2006, eSECURITY Technologies Rolf Oppliger has been participating in heise's "News for your site" program and has been providing security news from the heise security portal (in English). We are interested in hearing from you whether these news are actually useful for you—please, let us know.

[1] `www.projectliberty.org`
[2] `shibboleth.internet2.edu`
[3] `openid.net`

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. In either case, we kindly invite you to discuss the topics with us.

3.1 Refereed Articles

The article entitled "Providing Certified Mail Services on the Internet" was published in the *IEEE Security & Privacy* magazine (Vol. 5, No. 1, January/Februrary 2007, pp. 16–22). As mentioned in previous issues of eSECURITY communications, this introductory article overviews, discusses, puts into perspective, analyzes, and assesses the technologies that are available to provide certified mail services on the Internet.

The article entitled "IT Security: In Search of the Holy Grail" was published as a technical opinion in the *Communications of the ACM* (Vol. 50, No. 2, February 2007, pp. 96–98). In essence, the article argues that IT security is not a product or service problem, but rather an engineering and management problem (that must be addressed with an appropriate IT security process). The process must start with political, strategic, and architectural considerations, and may eventually lead to security architectures that are professionally designed, implemented, put in place, and enforced. This is in contrast to the trend in industry to replace architectural considerations with ad-hoc penetration testing.

Last but not least, the invited article "Certinyms-low-end certificates in large-scale computing environments" (co-authored by Ruedi Rytz) is still awaiting publication in the *Journal of Journal of Autonomic and Trusted Computing* (JoATC). It has long been argued that public key certificates with only poor identity verification of their holder are not useful to establish trust in large-scale computing environments, such as the Internet. In the article, we disagree and argue that low-end certificates—we call them certinyms—allow for a gradual build-up of trust among different parties. From a service provider's viewpoint, a certinym, by definition, 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 between the originator and the service provider in the long term.

3.2 Conference and Workshop Papers

A research paper entitled "A Proof of Concept Implementation of SSL/TLS Session-Aware User Authentication (TLS-SA)" (co-authored by Ralf Hauser, David Basin, Aldo Rodenhaeuser, and Bruno Kaiser) was published in the *Proceedings of the 15th GI/ITG Conference on "Kommunikation in Verteilten Systemen" (KiVS '07)*. The conference took place on February 26 – March 2, 2007, in Berne (Switzerland), and the paper was presented by Rolf Oppliger. It elaborates on a proof of concept implementation of TLS-SA—a technological approach introduced in previous issues of eSECURITY communications. We think that TLS-SA fills a gap between the use of public key certificates on the client side and currently deployed user authentication mechanisms. Most importantly, it allows for the continued use of legacy two-factor authentication devices while still providing protection against man-in-the-middle (MITM) attacks.

Also, an industry track paper entitled "Security of Microsoft's Identity Metasystem and CardSpace" (co-authored by Sebastian Gajek and Ralf Hauser) was published in the industry track proceedings of KiVS '07. The paper was also presented by Rolf Oppliger. As its name suggests, the paper elaborates on the security of Microsoft's identity metasystem and CardSpace (cf. Editorial and Section 4). In contrast to its important role on the marketplace, there are comparably few studies about the topic (this has not changed the last couple of months).

4 Security Analysis

As part of its .NET initiative, Microsoft developed and tried to deploy a Web-based single sign-in (SSI) service called *Passport Network* (formerly known as *.NET Passport*). The security of the Passport Network has been thoroughly analyzed and a couple of vulnerabilities and problems have been identified. The deployment of Passport Network has turned out to be slow, certainly slower than it was originally anticipated. Even Microsoft is using it only to secure access to a few MSN services, such as Messenger and Hotmail.

Meanwhile, identity management has become a hot topic, and several technologies to manage (digital) identities have been developed and partly deployed (cf. Editorial of this issue of eSECURITY communications). To complement these technologies, Microsoft has designed and proposed an identity metasystem that is user-centric and consistent with open Web services (WS-∗) standards. The metasystem is based on the *laws of identity* that were proposed, debated, and refined through an open dialogue. They codify a set of fundamental principles to which any universally adopted identity management architecture should conform. As such, they also provide the architectural basis for Microsoft's identity metasystem and implementations thereof.

In general, there are several possibilities to implement Microsoft's identity metasystem. The user interface of the metasystem is an identity selector that allows a user to select and use a specific digital identity in a given context. There are a few implementations of such an identity selector. Most importantly, Microsoft has implemented an identity selector that is part of Windows Communications Foundation (WCF) of the .NET Framework 3.0. The implementation was codenamed *InfoCard* and later renamed *CardSpace* (mainly because the name "Infocard" is protected with a trademark). The term "InfoCard" ist still used to refer to a visual representation of a digital identity in CardSpace. Anyway, CardSpace represents the interface users notice when they work with Microsoft's identity metasystem and implementation. Any application running on a Windows system with .NET Framework 3.0 can invoke and make use of CardSpace. In a Web-based environment, for example, this applies to Microsoft Internet Explorer 7. As a matter of fact, Microsoft Internet Explorer 7 will probably be the first place for users to come in contact with Microsoft's identity metasystem and CardSpace. Note, however, that any WCF application—or, even more generally, any application that implements the WS-∗ standards—can employ and make use of CardSpace.

Due to the fact that Microsoft Internet Explorer is widely deployed and has a large market share, we expect Microsoft's identity metasystem and implementation (and hence CardSpace-based authentication) to become widely deployed on the Internet. This is particularly true for subjects that self-assert security tokens. There is good and bad news:

- The good news is that CardSpace-based authentication will simplify authentication and authorization for Web-based services and applications considerably (both from an application developer and user's viewpoint).
- The bad news is that CardSpace will also become a popular target to attack. In fact, it is possible and very likely that design or implementation shortcomings, weaknesses, or vulnerabilities will be discovered and exploited. It is, for example,

possible to mount MITM attacks, if the MITM is located between the subject and its identity provider.

We provide a preliminary security analysis in the KiVS '07 industry track paper mentioned above. We show that most security problems related to Microsoft's Passport Network have been resolved and mitigated with CardSpace. The major problems that remain are related to public key certificates and the domain name system (DNS). These problems, however, are inherent to most identity management solutions in use today.

5 Information Security and Privacy Series

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

- David F. Ferraiolo, D. Richard Kuhn, and Ramaswamy Chandramouli, *Role-based Access Controls, 2nd Edition*, ISBN-10 1596931132, 2007, 418 pp.

Furthermore, the following 3 titles are scheduled to be published later in 2007:

- Edward Humphreys, *A Guide to ISO/IEC 27000 Information Security Management*, ISBN-10 1596931728, scheduled for July 2007, approx. 200 pp.
- Panagiotis Papadimitratos, *Securing the Internet Infrastructure*, ISBN-10 1580538525, scheduled for December 2007, approx. 301 pp.
- John Velissarios, *Identity, Security and Anonymity on the Internet*, ISBN-10 1580538223, scheduled for December 2007, approx. 400 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 Editors (refer to the book series' home page[4] for the coordinates of the Commissioning Editors).

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

6 Announcements

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

6.1 University Lectures

In February 2007, Rolf Oppliger gave a 3-day lecture on cryptography at the Insitute for Informatics of the Georg-August-Universität Göttingen. The slides are electronically available on the book's home page.[5] Also, the lecture was video-taped and the corresponding files are available on the lecture's home page.[6] Note, however, that the freely available LECTURNITY player is required to view the lecture. The examn to this lecture took place on March 6, 2007.

In summer 2007 (starting on March 19, 2006), Rolf Oppliger lectures at the University of Zürich on "Sicherheit in der Informationstechnik." The slides are electronically available on the lecture's home page.[7] The examn will take place on June 18, 2007. The lecture will be held annually and is supposed to take place again in summer 2008.

6.2 Courses

On March 5, 2007, David Basin, Ralf Hauser, and Rolf Oppliger taught a one-day course on "Securing Online Applications" at the ETH Zürich. The course was attended by several representatives mainly from industry.

In 2007, InfoGuard will host three courses on contemporary cryptography (based on Rolf Oppliger's book *Contemporary Cryptography*). Four out of five days will be taught by Rolf Oppliger. The course will be held in English and take place in Zug. The dates are as follows:

- April 23 - 27
- June 25 - 29
- November 26 - 30

If you are interested in the course, then you may request a flyer from InfoGuard or eSECURITY Technologies Rolf Oppliger.

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

[6] `user.informatik.uni-goettingen.de/~oppliger/`

[7] `www.esecurity.ch/Teaching/uni-zh-ifi-ss07.shtml`

6.3 Conferences and Workshops

In 2007, Rolf Oppliger serves as a member of the programm committee for the following conferences:

- 4th European PKI Workshop: Theory and Practice (EuroPKI '07), Mallorca (Spain), June 28 - 30, 2007
- International Conference on Security and Cryptography (SECRYPT 2007), Barcelona (Spain), July 28 - 31, 2007
- International Security Symposium on Information Assurance and Security (IAS '07), Manchester (UK), August 29 - 30, 2007
- 4th International Conference on Trust, Privacy and Security in Digital Business (TrustBus '07) held in conjunction with the 18th International Conference on Database and Expert Systems Applications (DEXA 2007), Regensburg (Germany), September 3 - 7, 2007
- 8th International Conference on Electronic Commerce and Web Technologies (EC-Web '07) held in conjunction with the 18th International Conference on Database and Expert Systems Applications (DEXA 2007), Regensburg (Germany), September 3 - 7, 2007
- International Association of Science and Technology for Development (IASTED) International Conference on Communication, Network, and Information Security (CNIS 2007), Berkeley, CA (USA), September 24 - 26, 2007
- 10th International Conference on Information Security and Cryptology (ICISC '07), Seoul (Korea), November 29 - 30, 2007

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

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).

[8] `www.esecurity.ch`