eSECURITY® communications

Volume 1, Issue 2, Fall 2004 http://www.esecurity.ch/communications.html

Contents

1 Editorial

Earlier this year, we presented the first issue of eSECURITY communications — the official newlsetter of eSECURITY Technologies Rolf Oppliger. The feedback we have received so far is overwhelmingly positive and very encouriging. So we continue our effort and come up with a second issue of eSECURITY communications. The result is in your hands (or on the screen of your computer system, respectively). We hope that you enjoy reading it, and we are looking forward hearing from you and receiving your feedback, comments, and criticism.

2 News

In June 2004, a company named eSecurity Solutions GmbH was registered in Aargau (CH-400.4.025.475-5). The company is independent from and has nothing in common with eSECURITY Technologies Rolf Oppliger.

In July 2004, eSECURITY Technologies Rolf Oppliger registered two alias domain names[1] (in addition to `esecurity.ch`). Consequently, the Web server of eSECURITY Technologies Rolf Oppliger is now available at one of the following URLs:

- `www.esecurity.ch`
- `www.rolf-oppliger.com`
- `www.rolf-oppliger.ch`

Furthermore, a new company flyer was designed and made available in August 2004. The flyer can either be ordered in printed form or downloaded electronically in Adobe's portable document format (PDF) from the company's Web site.[2] The flyer will also be distributed at conferences and other security-related events that take place in Switzerland and abroad.

3 Patents

Early in September 2004, eSECURITY Technologies Rolf Oppliger filed a Swiss patent application entitled "Verfahren zur Erhöhung der Sicherheit beim Einsatz von Streichlisten zur Benutzerauthentifizierung." As its name suggests, the application proposes a method to increase the security of currently used transaction authentication numbers (TANs). The idea is to physically protect a TAN list in a way that reading a TAN requires a physical act that can be detected easily at some later point in time. One possibility is to use a physical layer that hides the TANs, and that can easily be rasped away by the user (similar to lots in some lotteries).

If you are using a widely deployed TAN-based authentication system and want to increase its security without going to more involved technologies (e.g., one-time password systems, challenge-response systems, public key certificates, ...), then this method may be something to look at. Feel free to contact eSECURITY Technologies Rolf Oppliger in this matter.

[1] `rolf-oppliger.com` and `rolf-oppliger.ch`

[2] `www.esecurity.ch/Flyers/flyer.pdf`

4 Publications

The following articles have been published since the last issue of eSECURITY communications:

- An article entitled "Microsoft .NET Passport and identity management" appeared in the *Information Security Technical Report* (Vol. 9, No. 1, 2004, pp. 26–34). The article overviews, discusses, and puts into perspective the Microsoft .NET Passport single sign-in service, and addresses the question whether Microsoft .NET Passport provides an appropriate solution to the user authentication and authorization or identity management problem on the World Wide Web (WWW).
- An article (co-authored by Peter Stadlin) entitled "A Certified Mail System (CMS) for the Internet" appeared in *Computer Communications* (Vol. 27, No. 13, August 2004, pp. 1229–1235). The article proposes and describes a certified mail system (CMS) that can be used to provide certfied mail services on the Internet. The CMS employs an online TTP and uses dual signatures to cryptographically link the message keys to the messages that are certified. A patent application for the CMS was filed in July 2000.
- An article entitled "Certified Mail: The Next Challenge for Secure Messaging" appeared in *Communications of the ACM* (Vol. 47, No. 8, August 2004, pp. 75–79). The article argues that certified mail will become important in the future to provide non-repudiation of receipt services. Furthermore, it overviews, discusses, and puts into perspective technologies that can be used to provide such services on a large scale. As such, the article puts the above-mentioned article about the CMS into perspective.

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).

Furthermore, a paper (co-authored by J. Lopez, J.A. Montenegro, and G. Pernul) entitled "On a Taxonomy of Systems for Authentication and/or Authorization Services" appeared in the *Proceedings of the TERENA Networking Conference* that took place on June 7–10, 2004, in Rhodes (Greece). Both the paper and the slides used for the presentation are electronically available from the conference Web site.[3]

5 Security Analyses

As part of its consultancy services, eSECURITY Technologies Rolf Oppliger reviews, analyzes, evaluates, and puts into perspective security technologies, products, and services. Some exemplary results are briefly summarized next.

5.1 PGP Universal

Some years ago, the term "secure messaging" was synonymously used to refer to end-to-end e-mail security standards, such as S/MIME and PGP (or OpenPGP, respectively).[4] This has changed considerably. Nowadays, people often talk about secure messaging when they actually refer to proxy-based and/or gateway-based solutions. The main advantage of such a solution is that it neither requires public key certificates for all users, nor does it require all users to be aware of the security technologies used in the first place. As a consequence, these solutions are usually simple(r) to deploy, especially on a large scale.

There are several proxy-based and/or gateway-based solutions available today. Most of them support all standards that are relevant for secure messaging, including S/MIME and OpenPGP. For example, PGP Universal is a solution that has been developed by PGP Corporation[5] and is being marketed by several companies in Switzerland, such as Omicron Electronics GmbH.[6]

The use of PGP Universal (or a comparable product) is recommended for companies and organizations that want to secure their e-mail traffic with external partners. In this case, the PGP Universal server can be operated in external mode to act as a secure messaging gateway. Internal e-mail traffic is not affected in this configuration. In some cases, it may make sense to operate an additional PGP Universal server in internal mode. In this case, the internal e-mail traffic is secured, as well. The question whether PGP Universal should be operated externally and/or internally must be answered individually. eSECURITY Technologies Rolf Oppliger is able to provide corresponding consultancy services.

5.2 PrivaSphere

PrivaSphere[7] is a Swiss company that provides secure messaging and trust management services. Most importantly, it provides data confidentialty services for e-mail (it does not provide non-repudiation services). The PrivaSphere software was developed entirely in Switzerland and is based on open source software components.

eSECURITY Technologies Rolf Oppliger considers PrivaSphere to be a serious competitor in the field of Web-based secure messaging and trust management services and solutions. The "secure contact me" feature of PrivaSphere is particularly useful, since it allows anybody to contact and send a cryptographically protected message to a system subscriber. If, for example, you want to securely contact eSECURITY Technologies Rolf Oppliger and send a corresponding e-mail message using the "secure contact me" feature, you may look at the Contact Information section of the company's Web site[8] and drop a message there. In short, the message will be encrypted on the PrivaSphere server using Rolf Oppliger's public PGP key.

5.3 PaTHword

PaTHword is a graphical password management system developed by the Swiss company CryptMe GmbH.[9] In this system, every user gets a PaTHword card that he or she can use to generate and retrieve randomly-looking passwords (using a keyword and a graphical pattern). Refer to the company's Web site for a full description of the PaTHword system.

The idea of using graphical patterns to generate and retrieve randomly-looking passwords looks promising and is in fact seductive (it is usually simpler for human beings to memorize graphical patterns than it

[3] `www.terena.nl/conferences/tnc2004/`

[4] In 2001, Rolf Oppliger published a book entitled *Secure Messaging with PGP and S/MIME* with Artech House (ISBN 1-58053-161-X).

[5] `www.pgp.com`

[6] `www.omicron.ch`

[7] `www.privasphere.com`

[8] `www.esecurity.ch/contact.html`

[9] `www.cryptme.ch`

is to memorize specific words). The passwords that are generated look random and seem to have good random properties (i.e., they are hard to guess).

The major disadvantage of the system is that it makes the inherently independent passwords of a user dependent from the user's PaTHword card (or a copy thereof), the user's keyword (that is typically only two characters long), and the user's graphical pattern. Consequently, if an adversary has a copy of a user's PaTHword card and has captured one password generated with the card (for example, by eavesropping on the network traffic), he or she has good odds to correctly determine all passwords of that user. Consequently, the security of the PaTHword system critically depends on the inability of the adversary to make a copy of the user's PaTHword card. This assumption is strong, and eSECURITY Technologies Rolf Oppliger considers it to be too strong to be made for all practical puposes. Consequently, eSECURITY Technologies Rolf Oppliger does not recommend the use of the PaTHword system (or a similar graphical password management system) at least in its current form.

6 Computer Security Series

Since the publication of the last issue of eSECURITY communications, Tim Pitts has left Artech House and the Commissioning Editor's job has been split between Julie Lancashire (responsible for Europe, Middle East, Africa, and Asia) and Wayne Yuhasz (responsible for the United States, Canada, South America, and Australia).

Jose Nazario's book entitled "Defense and Detection Strategies Against Internet Worms" (ISBN 1-58053-537-2, 2003) is currently the bestselling title in the series.

A new book entitled "Bluetooth Security" has been published (ISBN 1-58053-504-6) in the series. The book has been written by Christian Gehrmann, Joakim Persson, and Ben Smeets, and focuses entirely on security aspects of Bluetooth. Due to the fact that Bluetooth security is a hot topic, the book has taken off well.

The list of scheduled books has changed a little bit. As of August 2004, the following seven books are scheduled for publication:

1. Axelrod, C.W., *Outsourcing Information Security*, ISBN 1-58053-531-3, scheduled for September 2004, approx. 272 pp.
2. Dent, A.W., and C.J. Mitchell, *User's Guide to Cryptography and Standards*, ISBN 1-58053-530-5, scheduled for October 2004, approx. 370 pp.
3. Caloyannides, M.A., *Privacy Protection and Computer Forensics, Second Edition*, ISBN 1-58053-830-4, scheduled for October 2004, approx. 350 pp.
4. Papadimitratos, P., *Securing the Internet Infrastructure*, ISBN 1-58053-852-5, scheduled for May 2005, approx. 301 pp.
5. Oppliger, R., *Contemporary Cryptography*, ISBN 1-58053-642-5, scheduled for May 2005, approx. 500 pp.
6. Hardjono, T., and L.R. Dondeti, *Security in Wireless LANs und MANs*, ISBN 1-58053-755-3, scheduled for June 2005, approx. 306 pp.
7. Rutkowski, A.M., *Lawful Interception and Access*, ISBN 1-58053-880-0, scheduled for June 2005, approx. 354 pp.

Including these titles, the computer security book series now comprises 27 titles. As such, it is the largest book series devoted to computer security only.[10]

The process of contracting new and promising authors is ongoing. If you interested in writing and publishing a book in the series you may contact either the Series Editor (Rolf Oppliger) or any of the Commissioning Editors (Julie Lancashire or Wayne Yuhasz). The coordinates of these persons can be found on the series' home page.

7 Recommended Reading

eSECURITY Technologies Rolf Oppliger recommends several books on cryptography (all of them are available for purchase in the eSECURITY BOOKSTORE).[11] Among these books, the following four titles are particularly recommended reading for self-study, to teach classes, or to give lectures about contemporary cryptography:

1. Delfs, H., and H. Knebl, *Introduction to Cryptography: Principles and Applications*, ISBN 3540422781, Springer, 2002
2. Mao, W., *Modern Cryptography: Theory and Practice*, ISBN 0130669431, Prentice Hall PTR, Upper Saddle River, NJ, 2003
3. Smart, N., *Cryptography, An Introduction*, ISBN 0077099877, McGraw-Hill, 2002

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

[11] `www.esecurity.ch/bookstore.htm#cryptography`

4. Stinson, D., *Cryptography: Theory and Practice, Second Edition*, ISBN 1584882069, Chapman & Hall/CRC, 2002

In addition, Rolf Oppliger's book entitled *Contemporary Cryptography* will nicely complement these titles (it is hoped). As mentioned above, the book is scheduled to appear in May 2005.

8 Outlook

Let's finish up this issue of eSECURITY communications with some remarks regarding university lectures, courses, and invited talks.

8.1 University Lectures

The university lecture entitled "Sicherheit in der Informationstechnik" will be repeated at the University of Zürich in spring and summer 2005. Again, the slides will be made are electronically available at he lecture's home page (announced later).

8.2 Courses

The previously announced course entitled "Informatiksicherheit: Grundlagen und Umsetzung in der Praxis" is postponed to 2005.

Also in 2005, an introductory course on contemporary cryptography will take place and be hosted by the eSECURITY EDUCATION CENTER.

Both courses will be held in German and address theoretical and practical aspects. The details will be announced at some later point in time (the announcements will be repeated in the next issue of eSECURITY communications).

8.3 Invited Talks

On September 1, 2004, Rolf Oppliger gave a talk entitled "Internet Banking — Aktuelle Bedrohungen und Risiken" at a PKI meeting organized by the Trüb AG located in Aarau. In the talk, it was argued that that phishing is an electronic form of social engineering, and that it is very difficult to design and come up with technologies that protect against this form of attack. Contrary to what one would say intuitively, protection against phishing requires complementary server authentication methods (in addition to the certificate-based authentication method currently employed by the SSL/TLS protocol). If you are interested in the topic, you may request the slides of the talk.

On October 26, 2004, Rolf Oppliger will give a talk entitled "Digitale Dokumente: Alte und neue Herausforderungen sowie Lösungsansätze" at the "Tagung für Informatik und Recht." The talk will elaborate on the (security) problems related to digital objects and the evidence they provide. The talk will be made available on the conference Web site.[12] In the meantime, you may contact eSECURITY Technologies Rolf Oppliger for a preliminary version thereof.

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).

[12] `www.rechtsinformatik.ch/`
[13] `www.esecurity.ch`