eSECURITY® communications

Volume 8, Issue 1, Spring 2011 http://www.esecurity.ch/communications.html

Contents

1 Editorial

Last year's big (security) event was the Stuxnet worm that hit process control systems mainly in Iranian nuclear plants. The event made press headlines in almost all newspapers around the globe. This is surprising taking into account the spare information that is available today about its origin, i.e., who created the worm and for what purpose? We see a lot of speculation, but we hardly see any real evidence. Due to the sophistication of the worm, for example, some people argue that governmental forces must have been involved in the creation of the worm. Also, it is commonly believed that the creators of the Stuxnet worm had had a lot of inside information. Interestingly, the original infections were caused by compromised USB sticks that were physically distributed. Once inside a nuclear plant, the worm employed "normal" self-replication techniques for further propagation.

It is hoped that in a few years from now, we will know the true story about Stuxnet. In the meantime, we can only draw some conclusions and itemize respective key findings:

- The malware threat is real and can target any infrastructure, even a critical one.
- Insiders represent the real enemies.
- No fruit is hanging so high that a determined enemy would not be able to reach it.

The bottom line is that anybody and any infrastructure can be victimized by todays cybercriminals. This is worrisome and calls for countermeasures. Most importantly, we now have a documented case that calls for more security in supervisory control and data acquisition (SCADA) systems used in industry.

In spite of this pessimistic insight, I hope that you enjoy reading this issue of eSECURITY communications, and I am looking forward hearing from you and receiving your feedback, comments, or criticism in one way or another.

R. Opplig

I am the author of this document
Qualified signed by Rolf Oppliger
Muri b. Bern, Switzerland, March 4, 2011

2 News

Since January 1, 2011, Rolf Oppliger is a member of the editorial board of the prestigious IEEE *Computer* magazine.[1] In this position, he is responsible for publications in the security and privacy area. A special issue on security and privacy in an online world is scheduled for this year's September issue. A respective Call for Papers has been officially released and is now available online.[2]

eSECURITY Technologies Rolf Oppliger is clearing its store room and sells spare copies of Rolf Oppliger's books.[3] Feel free to contact us if you have any particular interest or if want to get more information about this opportunity.

3 Publications

Due to the publication of *Contemporary Cryptography, Second Edition* (scheduled for May or June 2011), Rolf Oppliger has not been able to publish any paper or article in the recent past.

4 Information Security and Privacy Books

Earlier this year, a new book entitled *Identity Management: Concepts, Technologies, and Systems* was published in Artech House's information security and privacy series (ISBN 978-1-60807-039-8). The book is authored by Elisa Bertino (Purdue University) and Kenji Takahashi (NTT). It provides a comprehensive overview about many aspects related to identity management. As such, it addresses a timely and very important topic, and is recommended reading for anybody working in the field.

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 Editor (refer to the book series' home page[4] for the coordinates of the Commissioning Editors).

[1] http://www.computer.org/portal/web/computer/

[2] http://www.computer.org/portal/web/computingnow/cocfp9

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

[4] http://www.esecurity.ch/serieseditor.html

5 Announcements

There are a few announcements to make regarding university lectures, courses, invited talks, as well as conferences and workshops.

5.1 University Lectures

On February 21, 2011, Rolf Oppliger started this year's lecture on "Sicherheit in der Informationstechnik" at the University of Zürich in Switzerland. The lecture takes place annually and provides a thorough introduction to various topics related to information technology (IT) security. The topics addressed are as follows:

- Introduction
- Cryptographic foundations
- Cryptographic systems (overview)
- Authentication
- Authorization and access control models
- Software anomalies and manipluations
- Evaluation and certification
- Trusted computing
- Communication and network security
- Firewall technologies
- Cryptographic security protocols
- Intrusion detection and prevention systems
- Digital signature legislation
- PKI and identity management
- Privacy and privacy-enhancing technologies

At the end of the lecture, there is room for timely (and hopefully controversial) topics, such as the security of Internet banking, e-voting, or voice over IP (VoIP) security. The slides are electronically available at the lecture's home page.[5] The final exam will take place on June 6, 2011. If you are interested to attend the lecture without passing the exam, then you may contact the secretary of the Department of Informatics at the University of Zürich.

5.2 Courses

InfoGuard AG and CRYPTO AG regularly host a seminar on contemporary cryptography, in which four out of five days are taught by Rolf Oppliger. The seminars are held in English and take place in Zug. The dates are tentatively scheduled as follows:

- May 16–20, 2011
- September 19–23, 2011
- November 14–18, 2011

If you are interested in attending any of these seminars, then you may request a flyer from InfoGuard AG or eSECURITY Technologies Rolf Oppliger. The flyer is electronically available on the Internet.[6] Either of these companies can also answer questions related to the seminar.

If you are interested to host a course on contemporary cryptography or any other topic related to IT security in your organization, then please feel free to contact eSECURITY Technologies Rolf Oppliger. We are looking forward discussing the respective possibilities with you. Needless to say that such a discussion is without any commitment for you.

5.3 Invited Talks

On February 9 (Day 1), March 15 (Day 2), and April 7 (Day 3), 2011, the Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud (HEIG-VD[7]) hosts this year's IT Security Days. The second day will focus entirely on Web security, and Rolf Oppliger will give a talk entitled *SSL/TLS and Web Application (In-)Security.* The abstract of the talk is as follows:

> The terms SSL and TLS are omnipresent in todays expert discussions about Web application security. The term SSL refers to a transport layer security protocol that was developed in the 1990s to cryptographically protect data transferred by Internet applications, whereas the term TLS refers to the successive (and meanwhile standardized) security protocol. Hence, SSL/TLS provides a cryptographic solution for many security problems. But it is not a panacea, meaning that there remain problems in the way SSL/TLS is invoked as well as problems that cannot be solved cryptographically in the first place (e.g., the malware or secure platform problem). In this talk, we give a brief introduction to SSL/TLS, put the technology into perspective, explain how it can be used to secure Web applications, discuss where it is overrated,

[5] `http://www.esecurity.ch/Teaching/uni-zh-2011.shtml`

[6] `http://www.esecurity.ch/Flyers/CCC_brochure.pdf`

[7] `http://www.heig-vd.ch`

and elaborate on some of its limitations and shortcomings. The bottom line is that Web application security remains a challenge, even if the use of SSL/TLS is widely deployed.

Please, feel free to register for the event and attend the talk accordingly. Further information is available online.[8]The slides used for the talk will also be made electronically available after the event.

5.4 Conferences and Workshops

In addition to CCNC 2011, IFIP SEC 2011 (note that this year's conference will take place in Lucerne) and ICSNC 2011 (as announced in the last issue of eSECURITY communications), Rolf Oppliger will serve as a member of the programm committee for the following international conferences and workshops to be held this year (in chronological order):

- International Conference on Security and Cryptography (SECRYPT 2011), Seville (Spain), July 18 - 21, 2011
- 9th Annual Conference on Privacy, Security and Trust (PST 2011), Montreal (Canada), July 19 - 21, 2011
- 10th Annual Information Security South Africa Conference (ISSA 2011), South Africa, August 15 - 17, 2011
- 8th International Conference on Trust, Privacy and Security in Digital Business (TrustBus 2011) held in conjunction with the 22nd International Conference on Database and Expert Systems Applications (DEXA 2011), Toulouse (France), August 29 - September 2, 2011
- 7th International Conference on Information Assurance and Security (IAS 2011), Malacca (Malaysia), December 5 - 8, 2011

It goes without saying that the conferences and workshops are recommended events to attend and learn more about the current state-of-the-art in cryptography and IT security.

About the Company

eSECURITY Technologies Rolf Oppliger[9] 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 located in Muri b. Bern.

© 2011 eSECURITY Technologies Rolf Oppliger

[8] http://securitydays.heig-vd.ch

[9] http://www.esecurity.ch