Volume 9, Issue 2, Fall 2012 http://www.esecurity.ch/communications.html

Contents

1 Editorial

Cloud computing is a hot topic that is hyped in the media today. Contrary to what is claimed in marketing and promotional slogans, cloud computing is not something fundamentally new; it is rather a reincarnation of outsourcing, paired with the additional difficulty that a customer may not know where (i.e., in what data center and in what country) his or her data actually resides. This makes it very difficult to say something meaningful about the security of cloud computing.

From a bird's eye perspective, there are at least two problem areas that must be considered with care and taken into account:

1. The customer abandons control over his or her data, and this may, in turn, have some negative impact on data availability. If, for example, the legislation in the cloud service provider's home country changes, then it may happen that the customer is denied further access to his or her data. The fact that the customer has a contract is then meaningless (as in many other cases, too). It goes without saying that this is an extreme case, and yet it is one that is not entirely impossible.
2. Except in the special case of a storage cloud with transparent encryption and decryption mechanisms put in place, a cloud service provider can always access the data of its customers. It may be forbidden to do so, but it is still technically feasible. On the horizon, we see a technology known as fully homomorphic encryption (FHE) that may allow someday a cloud service provider to process data in encrypted form. But the technology is still in its infancy and must be improved considerably for practical use. So there is a long way to go.

Both problem areas directly lead to a question of trust. Does the customer trust the cloud service provider not to deny access to his or her data one day? Does he or she trust him or her not to look into (and misuse) the data? As was pointed out by Prof. em. Hans Geiger in a talk a few years ago,[1] the German notion of trust comes in two flavors: trust and confidence. What we need is confidence, but what we actually get most of the times is trust. This applies to many areas, including, for example, cloud computing. It is our job as security professionals to bring in the notion of confidence when it comes to security discussions related to cloud computing. Trust alone does not help and is at most an intermediate step. In the long term, we must find means and ways to establish confidence. This is key for a successful deployment of outsourcing and cloud computing.

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. You can have confidence that I take it seriously, so you don't need to trust me.

2 News

Starting next year, eSECURITY communications will be published annually and represent an activity report for the respective year. So the next issue of eSECURITY communications will hopefully appear towards the end of 2013.

3 Publications

In addition to a talk that Rolf Oppliger will give on October 17, 2012, he has also written an article with the same title, i.e., "Geld im digitalen Zeitalter: Eine Standortbestimmung." The article will be pusblished in a respective book early in 2013. If you are interested in the topic, then please feel free to ask for a preprint of the article.

For the latest issue of the readme alumni newsletter,[2] which is the bulletin of the Alumni Wirtschaftsinformatik Universität Zurich that appears twice a year, Rolf Oppliger has written a short article on the state of the art and some recent changes in e-Security. The bottom line is that eSecurity as a field of study has become interdisciplinary, and that the role of the human factor has generally been underestimated in the past.

[1] `http://www.hansgeiger.ch/wp-content/uploads/2009/02/banken_und_vertrauen_08_05_27.pdf`

[2] `http://www.alumni.ch/readme/readme_aktuell.shtml`

4 Information Security and Privacy Books

There are no new books published in the series, but there are a few books in the queue. Besides, the process of contracting new authors is going on. If you are working in the field and are interested to write and publish a book in the series, then you may contact either the Series Editor (Rolf Oppliger) or one of the Commissioning Editors (refer to the book series' home page[3] for the coordinates of the Commissioning Editors).

5 Announcements

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

5.1 University Lectures

In the spring semester of 2013, Rolf Oppliger will lecture on "Sicherheit in der Informationstechnik" at the University of Zurich. The lecture provides a comprehensive introduction to various topics related to information technology (IT) security. The slides will be made electronically available at the lecture's home page[4] (also accessible from outside the University of Zurich). Feel free to browse through the slides and provide feedback where appropriate. Any feedback is welcome and highly appreciated.

5.2 Courses

The Swiss companies InfoGuard[5] and CRYPTO[6] 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 (or Baar, respectively). In 2012, the last seminar is scheduled for November 12 - 16. The dates for 2013 will be announced shortly. If you are interested in attending any of these seminars, then you may request a flyer from InfoGuard or eSECURITY Technologies Rolf Oppliger (the flyer is also electronically available on the Internet[7]). Also, any of these companies can take and 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 always without any commitment for you.

5.3 Tutorials

On December 3, 2012, Rolf Oppliger will give a full-day tutorial (M5) on contemporary cryptography at the Annual Computer Security Applications Conference (ACSAC[8]) that will take place in Orlando, Florida. The tutorial announcement is as follows:

> Cryptography is a key technology to secure the Internet applications we build, use, and depend on in daily life. Due to a lot of research and development activities in the past 40 years, cryptography is a broad field of study with many aspects that are inherently difficult to understand. In this course, we overview, discuss, and put into perspective the various cryptographic systems in use today. This includes unkeyed cryptosystems in terms of one-way function, cryptographic hash functions, and random bit generators; secret key cryptosystems in terms of symmetric encryption systems, message authentication systems, and pseudorandom bit generators; as well as public key cryptosystems in terms of asymmetric encryption systems, digital signature systems, and key establishment protocols. The aim is to provide a basic understanding of the advantages and disadvantages of the various systems, without going too deep into algorithmic details.

The tutorial has the following outline (the values in square brackets refer to the amount of time available for presentation):

1. Introduction [20 min]
2. Cryptographic Systems [20 min]
3. One-Way Functions [20 min]

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

[4] http://www.esecurity.ch/Teaching/uni-zh-2013.shtml

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

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

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

[8] http://www.acsac.org

4. Cryptographic Hash Functions [20 min]
5. Random Bit Generators [15 min]
6. Symmetric Encryption Systems [45 min]
7. Message Authentication Systems [20 min]
8. Pseudorandom Bit Generators [15 min]
9. Pseudorandom Functions [10 min]
10. Asymmetric Encryption Systems [45 hour]
11. Digital Signature Systems [45 hour]
12. Key Establishment [20 min]
13. Entity Authentication [20 min]
14. Secure Multi-Party Computation [15 min]
15. Key Management [15 min]
16. Conclusions and Outlook [15 min]

It would be great if you could make it for both the tutorial and the technical program of ACSAC. Rolf Oppliger will also attend the technical program, so this may be a good opportunity to meet in person.

5.4 Invited Talks

On August 29, 2012, Rolf Oppliger gave an invited talk at the 17th Symposium on Privacy and Security that took place at ETH Zurich. The focus of the talk was on security in outsourcing and cloud security in general, and the role of trust (and confidence), in particular. Again, the security professional's job is to replace trust with confidence where possible and appropriate. This point was well received by the audience of the symposium.

As already announced in the last issue of eSECURITY communications, Rolf Oppliger will also give an invited talk on October 17, 2012, at the University of Zurich. The title of the talk will be "Geld im digitalen Zeitalter: Eine Standortbestimmung," and—as this title suggests—it is aimed at providing a general overview about the notion, role, and state-of-the-art of money in the digital age. The talk will take place in the main building of the University of Zurich (Rämistrasse 71) and will start at 18:15. It is scheduled for 45 minutes with an additional 30 minutes time slot for questions and points to discuss. Further information about the talk will be announced on the Web site of the organizing organisation.[9] You are cordially invited to attend the event (no registration is required) and to challenge the speaker in the discussion (or afterwards).

[9] `http://www.pdverein.uzh.ch/aktuell/ringvorlesungen.html`

5.5 Conferences and Workshops

In addition to the 2012 conferences and workshops mentioned in the last issue of eSECURITY communications, Rolf Oppliger serves as a member of the programm committee for the following events (in reverse chronological order):

- 4th IEEE International Conference on Cloud Computing and Science (IEEE CloudCom 2012), Security and Privacy Track, Taipei (Taiwan), December 3 - 6, 2012
- 15th International Conference on Information Security and Cryptology (ICISC 2012), Seoul (Korea), November 28 - 30, 2012
- 8th International Conference on Information Assurance and Security (IAS 2012), São Carlos (Brazil), November 21 - 23, 2012

The events are recommended to attend and learn more about the current state-of-the-art in cryptography and IT security. But contrary to ACSAC, Rolf Oppliger has no plans to attend these events, so do not expect to meet him in person there.

About the Company

eSECURITY Technologies Rolf Oppliger[10] 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.

[10] `http://www.esecurity.ch`