SHCIS ’14 - 1st Workshop on Security in highly connected IT systems

Held in parallel with

11th International Conference on Trust, Privacy & Security in Digital Business - TrustBus 2014

http://dexa.org/trustbus2014

Munich, Germany

September 1-5, 2014

Modern society over the course of the past two decades developed an increasing dependency on their infrastructures in general, and on the availability and correct functionality of their IT systems in particular. While in the early days of the Internet revolution not many IT systems outside the academic world were directly connected to the Internet, the benefits of internetworking began to prevail by the end of the last millennium. Nowadays, all kinds of IT systems, from industrial control systems to nationwide sensor networks, from high-traffic business platforms to e-health applications, are connected to the Internet and thus, directly connected to each other. Such highly connected IT systems exhibit their very own peculiarities and need to be studied accordingly.

In this context, SHCIS’14 has two different, yet closely related goals. Firstly, the organizers of this workshop want to bring together IT security alliances and institutions with their global counterparts in order to strengthen collaboration and sharing of knowledge and research results between these entities. FORSEC (http://www.bayforsec.de/) and Secure Business Austria (http://www.sba-research.org) in particular, have committed themselves to participating in this workshop by providing members of the program committee as well as planning to contribute through participation and publications.

In addition to FORSEC and Secure Business Austria, we cordially invite participants from other national and international IT security alliances and institutions.

Secondly, SHCIS’14 aims to bring together IT security researchers and practitioners in the area of highly connected IT systems, with a strong emphasis on interdisciplinary aspects. The focus on the workshop is on diffusion of ongoing work and currently running research projects. Suggested topics are aligned along a cyclic IT security process for highly connected IT systems, consisting of the following phases:

- Preventive measures against attacks
- Defense against ongoing attacks
- Forensics and post-mortem examination of IT-security incidents

Suggested topics include, but are not limited to:

- Secure distributed architectures
- Secure mobile architectures
- Secure embedded systems
- Security in sensor networks
- Privacy
- Online trust
- Human factors in security and privacy
- Digital forensics

- Secure cloud computing
- Code obfuscation
- Security Economics
- Identity management
- Security through virtualization, security in virtualized environments
- Security in mobile computing
- Detection of security related anomalies

Relevant application areas include, but are not limited to:

- Virtualization platforms
- Smart grids, smart cities
- Social networks
- Big data

Workshop chairs

- Prof. Dr. Günther Pernul, Chair of Information Science I - Information Systems, University of Regensburg
- Prof. Dr. Guido Schryen, Department of Management Information Systems, University of Regensburg

Submission Guideline

Authors are invited to publish original and unpublished research that is not currently in a review process for other workshops, conferences or journals. Papers must be in English and formatted according to the IEEE Proceedings format (description available at http://www.computer.org/portal/web/cscps/formatting). Camera ready versions of the accepted papers must not exceed a length of 5 pages. At least one of the authors has to be attending the workshop to present the paper. All accepted papers will be published in the proceedings of DEXA'14 Workshops with IEEE CSP. Submissions will be handled electronically through https://confdriver.ifs.tuwien.ac.at/dexa2014. The site will be operating by mid February 2014.

Important dates

Submission of full papers: April 5, 2014
Notification of acceptance: April 14, 2014
Camera-ready copies due: May 31, 2014

Program committee

tba.