Dipl.-Ing. Dr. Thomas Länger
Département des systèmes d'information (ISI)
Université de Lausanne (UNIL) thomas.laenger@unil.ch

Dipl.-Inform. M.Sc. Info.-Security Henrich C. Pöhls
Institute of IT-Security and Security Law (ISL)
Universität Passau hp@sec.uni-passau.de

Abstract for a presentation at the TA16 conference 30.5.2016

Enhancing "Smart Services" with cryptography for the benefit of the individual end user

The Internet of Things, and its use in all kinds of "Smart Services" is just another manifestation of the ongoing embracement of our physical and informational world by information and communication technologies. Smart Services could be just another area of application adding end user convenience and benefit, while at the same time providing the desperately needed market growth and new opportunities for different economic sectors. But on the other side, these new technologies belong to the latest alarming trends feeding the virtually bottomless information repositories hidden behind the opaque veils of storage and computing clouds with still more personal and private data of individuals—to be accumulated, related, processed and assessed with Big Data technologies for commercialisation by data brokers and exploitation by surveillance organisations.

With its intended pervasiveness and penetration into areas which previously were strictly private for the individual, the wave of Smart Services constitutes a major threat to individuals' privacy, and with its dedicated relation to the physical world also to the individuals' physical security and safety. Related risks include technical risks, governance and control risks, and especially a huge set of data protection and privacy risks. These risks are currently addressed by organisational measures, like best practices and service level agreements—but such instruments are often insufficient because they rely on the benevolence of the data processor and neither can strict adherence be effectively controlled nor can violations thereof be proven by the individual or data subject.

To mitigate that developing security and privacy disaster, and to reinstate governance and control on behalf of the data subject or end user, the European integrated research project PRISMACLOUD ("Privacy and Security Maintaining Services in the Cloud", Feb 2015-Aug 2018) of the Horizon 2020 research programme proposes the application of recent cryptographic techniques. Goal is to provide effective end-to-end security and privacy, and to technically enforce the desired security and privacy properties in three critical areas: (i) Data storage in the cloud, (ii) user privacy protection and data minimisation and (iii) authentication of stored and processed data. Secret sharing technology facilitates secure data storage in the public cloud without requiring a complex cryptographic key management on the user side. Smart Services can be equipped with anonymous credentials to facilitate non-identifiable and untrackable service use and minimisation of private data exposure. Efficient data anonymisation technologies can provide an effective protection against linking data to individuals. Specific malleable signatures protect the authenticity of data handed to smart services for processing, while at the same time enabling the user to effectively blank out information which is not crucial for the service and may be exploited beyond the intended use of the service.

In the center of the presentation stand nine newly developed cloud security patterns, describing recurring situations in the virtual worlds of clouds and Smart Services where security and privacy is at risk for end users, and an assessment of the potential impact of applying in these situations the mentioned cutting-edge privacy and security technologies for effectively increasing end user security and privacy.

+++