Keys for Secure Smartphone Communication

KIT Project SOKEN Focuses on Automatic Exchange of Keys among Mobile End Devices along Real Social Networks

SOKEN distributes safety keys via radio in the social network (Figure: Christoph Strieks).

Tap-proof communication via the smartphone today requires encoding. For this purpose, a secret key has to be generated and exchanged prior to communication. The KIT Cryptography and Security Working Group headed by Professor Jörn Müller-Quade works on technologies transmitting such keys securely along a chain of persons known to each other. The SOKEN (Social Key Exchange Network) project uses daily encounters for this purpose. Via an application, a safety key is generated and distributed further to friends or relations when passing by. This method is the basis of secure communication, even if the communication partners have not met in reality.

Secure encoding requires secure keys. Instead of generating these keys with special methods via the internet, for instance, KIT researchers propose to automatically generate them during personal encounters and to pass them on from smartphone to smartphone. The keys are remodified at every encounter, such that a message can only be read by both conversation partners. “When using these keys exchanged via personal encounters, tapping is much more

Monika Landgraf
Chief Press Officer

Kaiserstraße 12
76131 Karlsruhe, Germany
Phone: +49 721 608-47414
Fax: +49 721 608-43658
E-mail: presse@kit.edu

For further information, please contact:

Sebastian Schäfer
Department of Informatics – Public Relations
Phone: +49 721 608-44344
Fax: +49 721 608-4177
E-mail: sebastian.schaefer@kit.edu

difficult. An attacker must have corrupted one of the devices in the chain in order to know the key. When combining this method with today's technologies, the expenditure required for mass surveillance is increased considerably," Professor Jörn Müller-Quade, Head of the KIT Cryptography and Security Working Group, explains.

Key Exchange in Social Networks

Key exchange follows the social network of its users: Only those who encounter in reality do exchange the keys. In this way, keys are passed on from friends to friends of friends, and so on. Thanks to these friendships, even not so close friends can communicate in a securely encoded manner. The more common friends two users have, the higher is the probablility of smartphones infected by specialized viruses or trojans being no longer able to calculate the key used for communication in a chain.

"Our simulations have shown that even in case of many infected smartphones, large parts of the communication processes are protected reliably against tapping," Dirk Achenbach, another member of the group, adds.

This is due to the fact that the system generates a new key whenever a new encounter of two persons takes place. If only one of these keys reaches the recipient via a path without an infected smartphone, subsequent communication is secure. In the own social network, keys may be exchanged constantly with long-term security. A group of students has already developed a prototype in the seminar "Praxis der Software-Entwicklung" (Practice of Software Development) offered by the Department of Informatics. Professor Müller-Quade, however, cannot estimate when such a system will be available on the market.

Tips for IT Security: Anti-Prism Party on February 12, 2014

According to Müller-Quade, anybody should think about how own communication channels can be protected against attacks and data theft. "At the moment, there is no 100% safety. But with a few means, everyone of us can contribute to making the work of data thieves much more difficult." To present these often simple and cost-free means, the working group, together with the Karlsruhe IT Security Initiative (KA-IT-SI) and the Center for Art and Media (ZKM), Karlsruhe, will organize an encoding party on February 12, 2014. During the party, various options for digital self-protection will be presented and explained.

Information on the party: http://www.anti-prism-party.de/

Karlsruhe Institute of Technology (KIT) is a public corporation according to the legislation of the state of Baden-Württemberg. It fulfills the mission of a university and the mission of a national research center of the Helmholtz Association. Research activities focus on energy, the natural and built environment as well as on society and technology and cover the whole range extending from fundamental aspects to application. With about 9000 employees, including nearly 6000 staff members in the science and education sector, and 24000 students, KIT is one of the biggest research and education institutions in Europe. Work of KIT is based on the knowledge triangle of research, teaching, and innovation.

This press release is available on the internet at www.kit.edu.

The figure of printing quality may be downloaded under www.kit.edu or requested by mail to presse@kit.edu or phone +49 721 608-4 7414. The figure may be used in the context given above exclusively.