Die Fakultät für Informatik an der Universität Wien lädt Sie herzlich ein zum

CS-Colloquium

Password-Hardened Encryption Services

mit Prof. Dr. Dominique Schröder (Friedrich-Alexander-Universität Erlangen-Nürnberg, Deutschland)

Wann? 3. Juli, ab 14:00 Uhr
Wo? Hörsaal 2 (HS2), Fakultät für Informatik
Währinger Straße 29
1090 Wien

Abstract

Passwords and access control remain the popular choice for protecting sensitive data stored online, despite their well-known vulnerability to brute-force attacks. A natural solution is to use encryption. Although standard practices of using encryption somewhat alleviate the problem, decryption is often needed for utility, and keeping the decryption key within reach is obviously dangerous. To address this seemingly unavoidable problem in data security, I propose password-hardened encryption (PHE). With the help of an external crypto server, a service provider can recover the user data encrypted by PHE only when an end user supplied a correct password. The crypto server has several important properties for practical purposes, such as being completely independent of the user's data and supporting key-rotation of their private keys, a proactive security mechanism mandated by the Payment Card Industry Data Security Standard (PCI DSS).

Bio

Dominique Schröder is a professor of computer science at Friedrich-Alexander-Universität Erlangen-Nürnberg where he holds the chair for Applied Cryptography. Before joining FAU, he was a tenured professor at Saarland University, a postdoctoral researcher at the University of Maryland, USA and he completed his Phd at the Technical University of Darmstadt. His research focuses on the development and analysis of cryptographic techniques, schemes and protocols that address a variety of IT security and privacy problems, such as password-based cryptography, privacy-preserving authentication, multi-party signatures, outsourced data and cryptocurrencies. This results received many international awards, such as the Intel Early Career Award.