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

CS-Colloquium

Resilient and Privacy-aware Networks - From Tracking to Intrusion Detection and Response

mit Prof. Dr. Mathias Fischer (Universität Hamburg, Deutschland)

Wann? 3. Juli, ab 09:00 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

Mathias Fischer is an assistant professor at the University Hamburg since September 2016. Before that, he was an assistant professor at the Westfälische Wilhelms-Universität Münster (2015-16), a Postdoc at the International Computer Science Institute (ICSI) / UC Berkeley (2014-15), and Postdoc at the Center for Advanced Security Research Darmstadt (CASED) / TU Darmstadt from (2012-14). His research interests encompass IT and network security, network monitoring, privacy, and botnets. Mathias received a PhD in 2012 and a diploma in computer science in 2008, both from TU Ilmenau.