Elektrotechnisches Kolloquium

der Bergischen Universität Wuppertal

Die Fakultät für Elektrotechnik, Informationstechnik und Medientechnik lädt zur Teilnahme an folgender Vortragsveranstaltung mit anschließender Diskussion ein:

Es spricht

Tobias Handirk, M.Sc.
Lehrstuhl für IT-Sicherheit und Kryptographie
Prof. Dr.-Ing. Tibor Jager

über das Thema

On Real-World Cryptographic Protocols for End-to-End Encrypted Backups and Key Confirmation

Inhalt:

The widespread use of the Internet and mobile devices has sparked a rapid growth in digital communication and, in turn, made the use of cryptography an integral part of everyday life, as countless applications are only enabled through the protection of confidentiality, integrity, and authenticity of sensitive data.

One particularly interesting application is instant messaging (IM), which is highly relevant due to its userbase spanning billions of people. The de facto security standard for IM is end-to-end encryption, meaning that no party except the sender and the intended recipient are able to read exchanged messages. While the security of the data in transit has received a lot of attention, the security of the data at rest has so far been somewhat neglected. In particular, a popular feature in IM applications are automated backups, which ensure that a user can recover their chat history if they lose their phone, however, their exact security guarantees are often unclear. In this talk, we analyze the security of the first backup protocol aiming at end-to-end encryption developed by WhatsApp in 2021, which protects the backup under some password chosen by the user. We show that by relying on a hardware security module, the protocol provides strong security guarantees for the chat histories even against a maliciously acting WhatsApp server.

T e r m i n: **06.11.2024, 12 Uhr**

O r t: Bergische Universität Wuppertal
Campus Freudenberg, FME, Loft Ebene 2