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

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

über das Thema

Construction and Security Analysis of 0-RTT Protocols

Inhalt:

Key establishment protocols are the foundation of secure communication on the Internet. Over the past years, reducing the latency while maintaining a protocol's security guarantees has become a major design goal of modern key establishment protocols. Striving for low latency in key establishment protocols gave rise to zero round-trip time (0-RTT) protocols, which allow to send cryptographically protected application data (0-RTT data) without prior need to execute an interactive and latency-incurring handshake protocol. Prominent examples are Google's QUIC protocol and the recently standardized TLS 1.3 0-RTT mode, which are used by millions of users per day.

One of the major challenges when designing 0-RTT protocols is to guarantee forward security for the 0-RTT data. Forward security ensures that compromise of a communicating party does not impact security of past communications. However, the lack of interactivity in 0-RTT protocols renders it difficult to achieve forward security for the 0-RTT data. Only recently, novel techniques to overcome this challenge have been discovered.

In this talk, we present novel techniques to achieve forward security for the 0-RTT data. Specifically, we investigate how forward security for the 0-RTT data can be achieved in the TLS 1.3 0-RTT mode. This yields the first efficient 0-RTT protocol that provides forward security for the 0-RTT data and can immediately be deployed in practice without modifications to the TLS 1.3 standard.

T e r m i n : **01. Juli 2020, 14:00 Uhr**

O r t : via Zoom; Meeting-ID: 946 0970 2508, Passwort: 8r$zSN@Q