A U S H A N G

FREIE UNIVERSITÄT BERLIN

Fachbereich Mathematik und Informatik

Promotionsbüro, Arnimallee 14, 14195 Berlin

D I S P U T A T I O N

Freitag, 11. April 2025, 16:00 Uhr

Ort: Seminarraum 006

(Fachbereich Mathematik und Informatik, Takustr. 9, 14195 Berlin)

Disputation über die Doktorarbeit von

Khan Mehedi Al Reaz

Thema der Dissertation:

Wireless Channel Based Security Protocols for IoT Devices

Thema der Disputation:

Proximity-aware Mutual Password Agreement Protocol for Wi-Fi Devices using Physical Layer Security

Die Arbeit wurde unter der Betreuung von **Prof. Dr.-Ing. G. Wunder** durchgeführt.

Abstract: The growing adoption of Wi-Fi-connected IoT devices, such as smart TVs and home monitoring systems, presents security challenges due to their limited computational resources. While WPA3 enhances Wi-Fi security, its reliance on public-key cryptography (PKC) raises concerns about post-quantum resilience, and its Diffie-Hellman (DH) key exchange requires large key sizes (≥3072 bits for 128-bit security), which can be impractical for resource-constrained devices. To address this, we propose ComPass, a proximity-aware password agreement protocol that leverages wireless channel phase randomness to establish shared secrets without user-generated passwords. ComPass generates high-entropy keys (128, 192, or 256 bits) with minimal overhead, making it efficient for Wi-Fi networks with heterogeneous device capabilities. This talk will cover ComPass's design, implementation on OpenWrt devices, integration with WPA2/3, and security evaluation, demonstrating its feasibility in mitigating password-based vulnerabilities in IoT ecosystems.

Die Disputation besteht aus dem o. g. Vortrag, danach der Vorstellung der Dissertation einschließlich jeweils anschließenden Aussprachen.

Interessierte werden hiermit herzlich eingeladen

Der Vorsitzende der Promotionskommission
Prof. Dr.-Ing. G. Wunder