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

Montag, 3. Juni 2024, 14:00 Uhr

Ort: WebEx

Disputation über die Doktorarbeit von

Peter Kietzmann

Thema der Dissertation:

On Information-centric Resiliency and System-level Security in Constrained, Wireless Communication

Thema der Disputation:

Practical Challenges, Requirements, and Solutions to Security in the Low-end IoT

Die Arbeit wurde unter der Betreuung von **Prof. Dr. M. Wählisch** durchgeführt.

Abstract: The Internet of Things (IoT) interconnects numerous embedded devices, but the resource constraints of battery driven nodes pose challenges to robust and secure networking. Guided by RFC7744, this presentation begins with a motivation of the top most IoT challenges: Connectivity and security.

Implementation vulnerabilities are one big threat to security, and the increasing number of common vulnerability exposures (CVEs) raises the question of how to mitigate those. Security depends on the usability of the cryptographic interface, e.g., to avoid programming errors. A conflict arises between the IoT device constraints and the demands of cryptography, which must adhere to Internet security standards while remaining computationally feasible for battery driven nodes. Therefore, modern platforms provide crypto-accelerators, but the necessity for low-level code interaction on heterogeneous devices hinder usability. This presentation highlights the potential of crypto-hardware performance, advocating for an OS-level abstraction layer to streamline the integration of a configurable crypto-subsystem.

Moreover, random numbers are critical for security, yet their generation still leads to vulnerabilities, which this presentation tries to illuminate. Real randomness relies on unpredictable physical processes, but not all platforms provide interfacing to random hardware. This presentation introduces the concept of SRAM PUFs (Pyhsical Unclonable Functions), a promising solution that utilizes intrinsic device variations to provide entropy and unpredictable secrets without additional hardware requirements.

The presentation concludes with remarks on real-world challenges, and emphasizes the role of a mature software toolkit in providing essential building blocks for developing a secure Internet of Things.

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. M. Wählisch