TeleTrusT
Pioneers in IT security.

TeleTrusT-interner Workshop

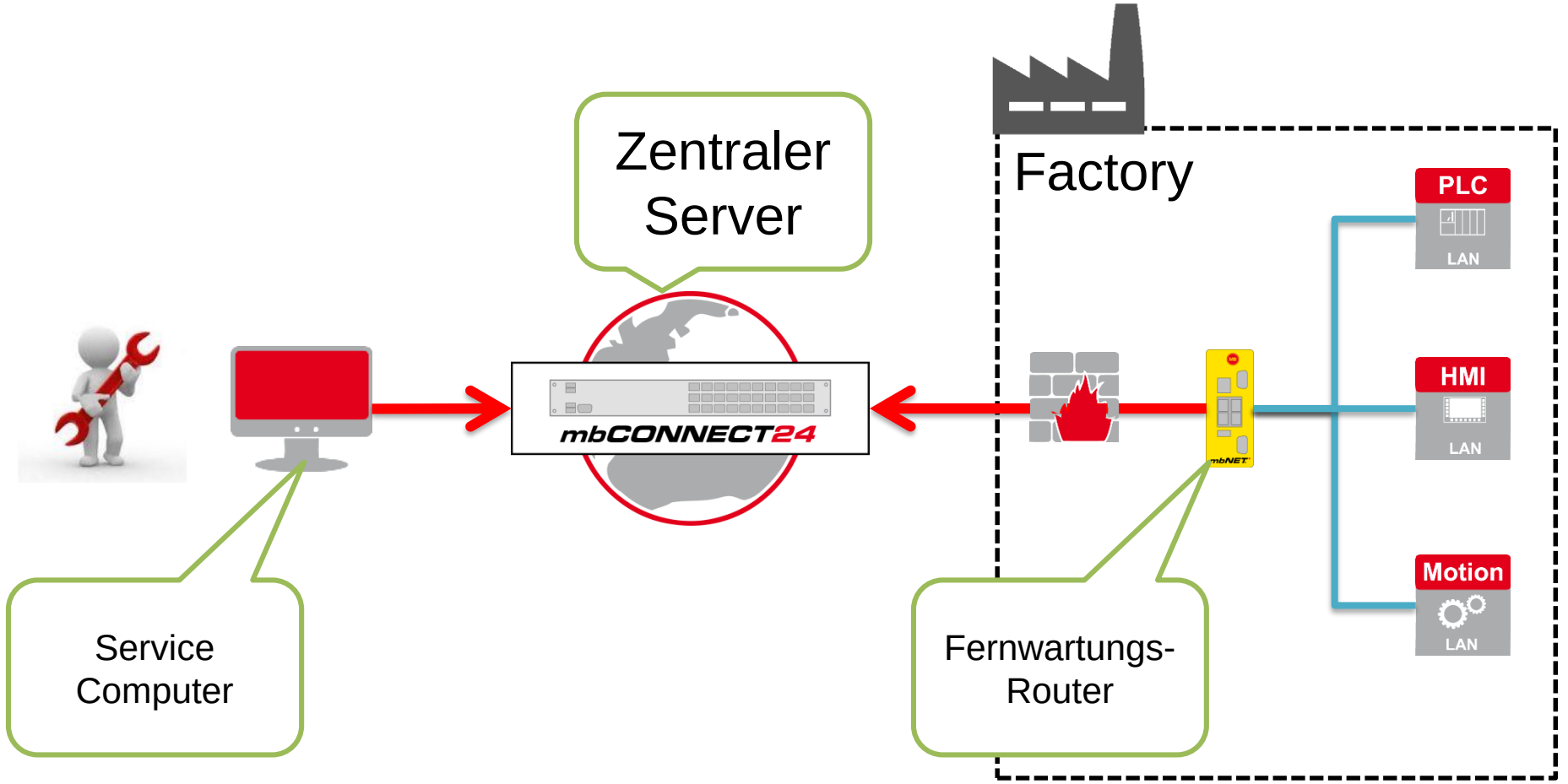
Berlin, 05./06.07.2018

Security By Design für IoT fängt schon beim Hardwaredesign an

Siegfried Müller,

MB Connect Line

Anwendungsfall Fernwartung in der Industrie



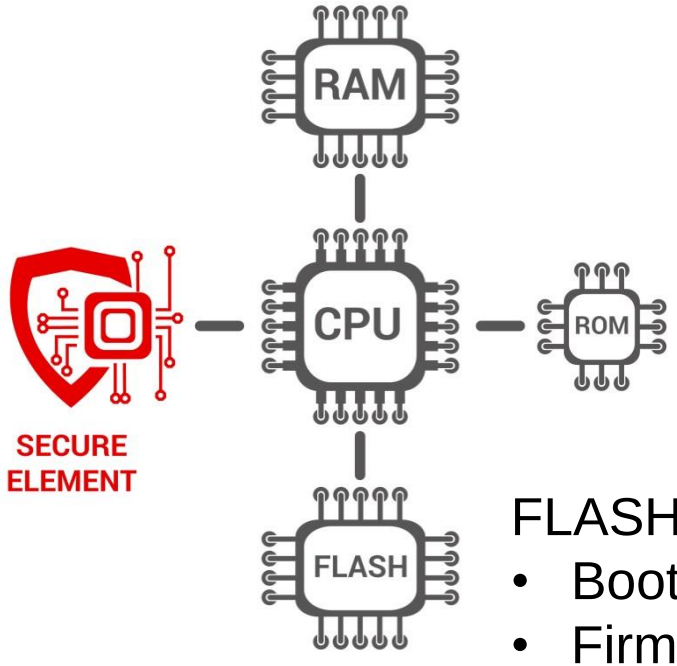
Anforderungen an einen industriellen Router

- Nur signierte Firmware akzeptieren
- Systemveränderungen unter Root sollen keine Auswirkungen nach ReBoot haben
- Benutzerspeicher verschlüsseln
- Hardware muss Software vertrauen
- Keine statischen "Geheimnisse" (Passwords, Keys, etc.) in der Firmware

Hardware Design

Secure Element:

Hardware-IC welches Schlüssel und Passwörter speichert. Es ist hardwarebasiert und von jedem anderen Prozess isoliert.

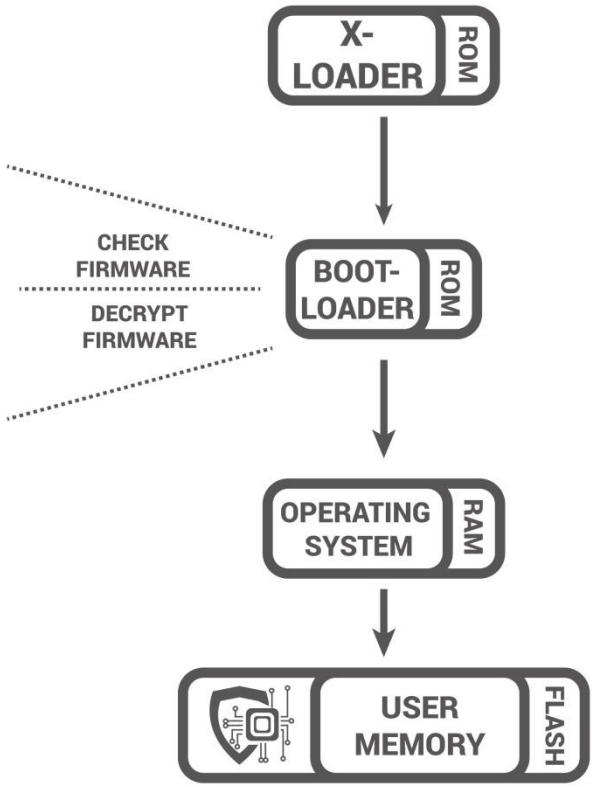


FLASH:
- Bootloader
- Firmware
- Benutzerspeicher

ROM:
- Bootloader
- MB Connect Line Certificate

FLASH:
- Firmware
- Benutzerspeicher

Boot-Prozess



1. X-Loader: ist nur im Read-Only-Memory vorhanden

2. Boot-Loader: Ist ebenfalls im ROM, zusammen mit dem Firmware-Zertifikat. Die Firmware selbst verschlüsselt und signiert mit dem MB Connect Line Zertifikat

3. Die Firmware wird vom FLASH entschlüsselt und in das RAM geladen. Jeder Boot enthält somit immer die Original-Firmware. Eventl. Änderungen im RAM sind nicht mehr vorhanden.

4. Das Betriebssystem wird im RAM ausgeführt

5. Der Benutzerspeicher ist einem CryptoContainer. Das Secure Element "öffnet" diesen nach dem Boot-Prozess.