Defense-in-Depth for the Internet of Things

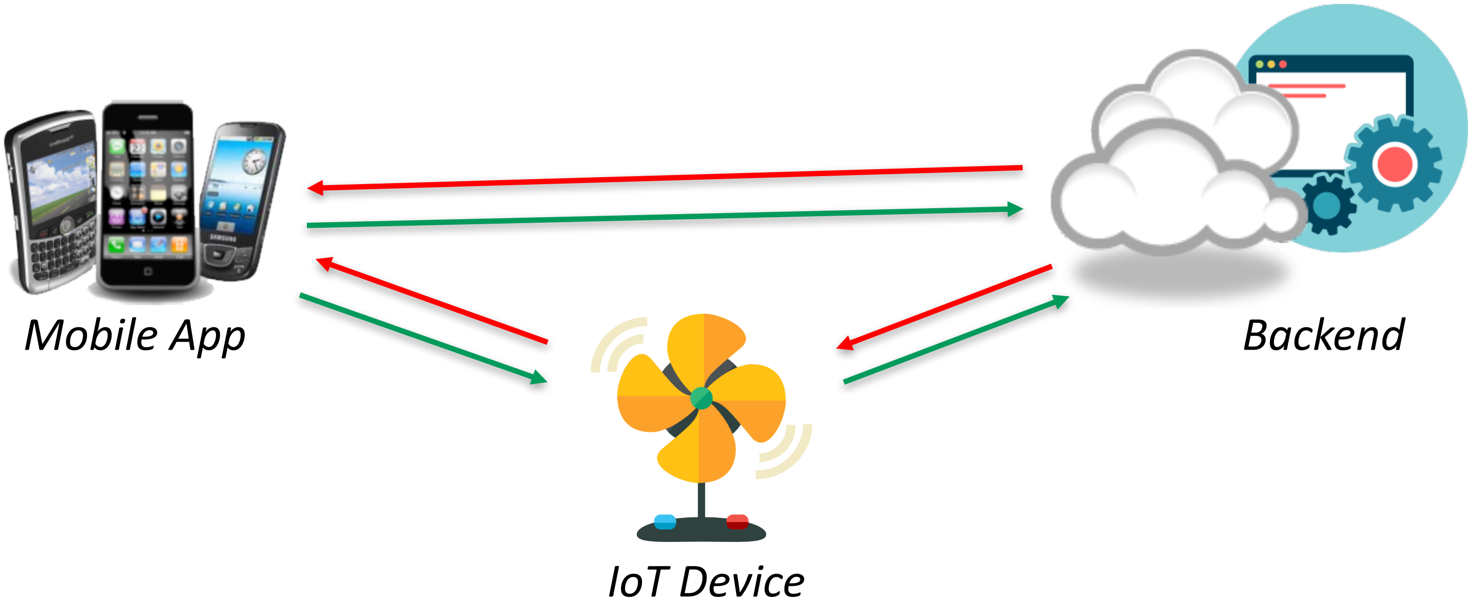
Kevin Schaller, kschaller@ernw.de

Internet of Things Areas

- Household environments
  - Doors
  - Temperature
  - Security against intruders
  - Smart Metering
  - Refrigerator/Coffee & Washing Machines/…
- Vital sensors
- Car systems
- …

ERNW
providing security.

Typical IoT Environment



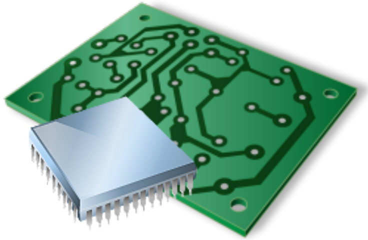
Mobile App

Backend

IoT Device

ERNW
providing security.

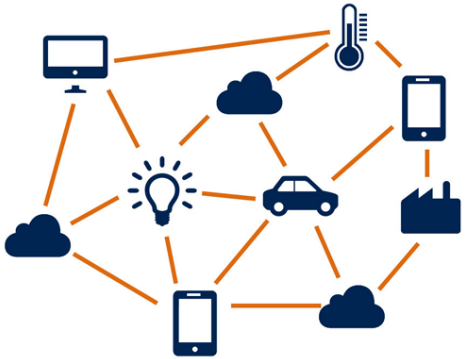
Security within the Internet of Things means:



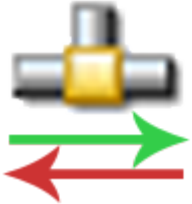
Hardware/Embedded Security

Mobile/App Security

Telco Security



IoT Security



Communication Security

Backend Security

ERNW
providing security.

Hardware/Embedded Security

- Resource Constraints
  - E.g. as for memory, computing power, power (batteries), network bandwidth, Trustzone, ...
- Physical Exposure
  - May be physically accessible by non-trustworthy parties, or (phys.) inaccessible by trusted parties
- Long lifespan
  - Some estimates up to 40 years

Mobile App Security

- Data storage/data avoidance
  - Don’t store sensitive data if not needed
  - If needed, store encrypted

- Authentication/authorization/session management
  - Sufficient algorithms/processes exist – use them!

- Handling of untrusted inputs
  - Client-side injection
  - Interprocess communication

- Refer to OWASP Top 10 Mobile

ERNW
providing security.

Backend Security

- Handling of untrusted inputs
  - SQL injection
  - Cross-site scripting
  - …
- Third-party library handling
  - Ensure most recent version of used libraries
- Sufficient access control concept
  - Huge amount of devices require a properly implemented separation of their respective spaces
- Refer to OWASP Top 10 Web

Communication Security

- Transport Layer Security (TLS) 1.1/1.2
- State-of-the-Art:
  - protocol versions (no SSLv2, SSLv3, ideally no TLSv1.0)
  - cipher suites (no DES, MD5, SHA1, RC4)
  - key lengths (no DH with 1024 bit, no symmetric encryption with < 128bit keys)
  - certificate validation
- If TLS cannot be used:
  - Don't Invent Super Crypto on your Own (DISCO)

Telco Security

- Setting up a rogue base station is no rocket science
  - Requires 2000 Euro and
  - some knowledge that can be easily gained
- Sensitive information (e.g. IMSI) has to be handled with care
  - Transport Layer Protection helps here
- If not needed: Avoid SMS parsing
  - Especially parsers are prone to vulnerabilities

ERNW
providing security.

Summary

- Security in the IoT comes with a challenge:
  - Security on multiple different layers
- But: Most aren't new – state-of-the-art solutions already exist for most of the technologies
- Sufficient transport layer protection is even more important
- Defense-in-Depth (=Multilayer Security) is required for a secure Internet of Things

Images/Icons credits: ERNW Icon Collection & Licensed Icons by Blazon Design Bureau