IoT Security

Christoph Klaaßen <cklaassen@ernw.de>

ERNW
providing security.

Agenda

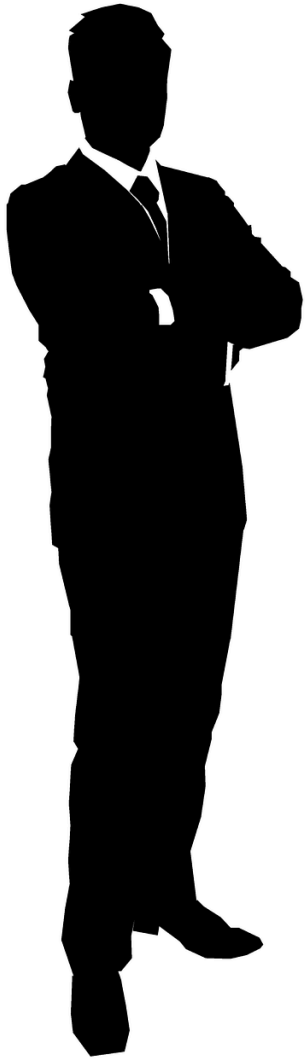
- About Me
- IoT Security Basics
- Case Studies

ERNW
providing security.

About Me

Christoph Klaaßen

- Senior Information Security Consultant
- Strategy, Architecture, Risk Management
- Private/Public Cloud and IoT



ERNW
providing security.

ERNW

- Established in 2001,
  all shares held by active employees
- Vendor-independent
- 70 employees, 48 FTE consultants
- Continuous growth in revenue/profits
  - No venture/equity capital, no external financial obligations of any kind
- Customers predominantly large/very large enterprises
  - Industry, telecommunications, finance, manufacturing, …

ERNW
providing security.

IoT – A ‘New’ Security Frontier

Remote Exploitation of an Unaltered Passenger Vehicle

Dr. Charlie Miller (cmiller@openrce.org)
Chris Valasek (cvalasek@gmail.com)

Hackers are hijacking smart building access systems to launch DDoS attacks

More than 2,300 building access systems can be hijacked due to a severe vulnerability left without a fix.

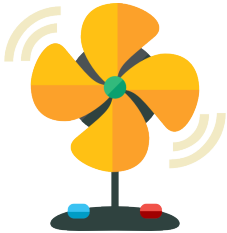
Ring Doorbell Flaw Opens Door to Spying

FDA confirms that St. Jude's cardiac devices can be hacked

ERNW
providing security.

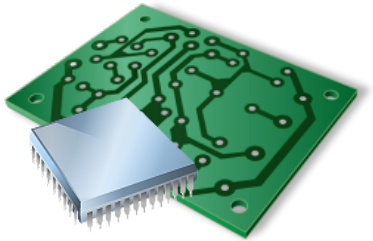
Internet of Things Areas

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



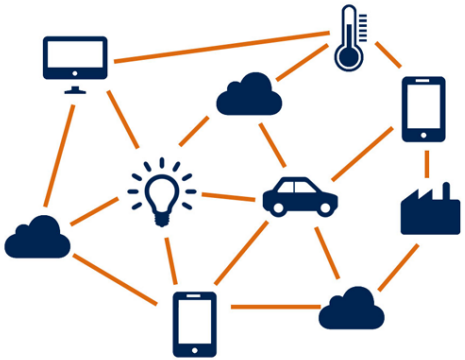
Security within the Internet of Things means:

Mobile/App Security

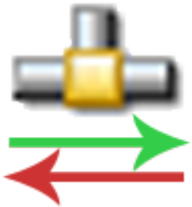


Hardware/Embedded Security

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

ERNW
providing security.

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
  - Inter-process 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

ERNW
providing security.

Communication Security

- Transport Layer Security (TLS) ~~1.1~~/1.2/1.3
- State-of-the-Art:
  - protocol versions (no SSLv2, SSLv3, ideally no TLSv1.0/1.1)
  - cipher suites (no DES, MD5, SHA1, RC4)
  - key lengths (no DH with 1024 bit, no symmetric encryption with < 128bit keys)
  - certificate validation, best case: certificate pinning

- If TLS cannot be used:
  - Don’t Invent Super Crypto on your Own (DISCO)

ERNW
providing security.

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 (does not apply to telco sec only)

ERNW
providing security.

Remark

- Remember: We’re an IT-Security Provider
- Confidentiality is one of our main objectives

- We will not disclose customer names in the following…

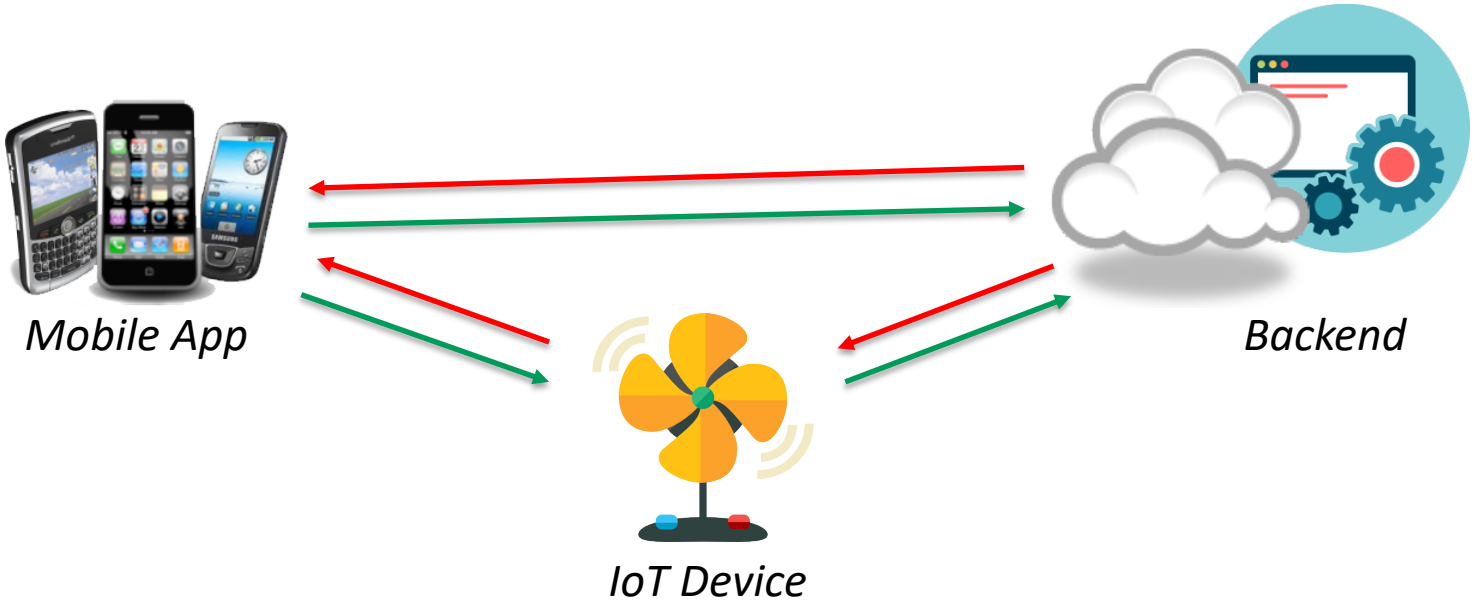
ERNW
providing security.

Case Study: Global Player for Smart Devices

- $COMPANY acquired the product from another vendor and wanted us to evaluate the overall security posture
- Scope: IoT device, mobile apps on Android & iOS, Cloud services, all communication channels → Whole IoT environment

ERNW
providing security.

Typical IoT Environment



ERNW
providing security.

Assessment went good, so far...

- ... Cloud services were mainly PaaS → Secure
- ... Mobile apps did not store confidential data → Data reduction
- … Most of the connections were secured according to current best practices (TLS 1.2) → Secure

- But: a git repository was found which revealed highly sensitive information (source code repo credentials)
- With the help of these credentials, the source code was retrieved and a white box assessment (code review) took place…

ERNW
providing security.

Result o

- Remote co … of the applicatio…
- Remote co … queue → Attacke… …ll (>5000) so…

ERNW
providing security.

Lessons Learned

- Even if parts of the environment are secure (Cloud, mobile apps, …), a security-in-depth approach has to be applied to all involved components
  - This also includes components of the development environment

- A minor vulnerability in ONE of the scripts can lead to a full compromise

ERNW
providing security.

Next Case: Asian Vendor of Medical Solutions

- Hospital Information System – active in numerous hospitals around the globe
  - Mobile apps for doctors
  - Azure cloud backend and Intune MDM
  - Multiple on-premise web services for handling of confidential data

ERNW
providing security.

Asian Vendor of Medical Solutions

- Penetration Test revealed:
  - Almost secure application layer – minor improvements possible
  - Setup in cloud infrastructure was not ideal – due to:
    - Missing authentication for administrative endpoints
    - Flat network – no segmentation/filtering

ERNW
providing security.

Car Manufacturer/OEM

- Cars are highly connected due to
  - Electronic Control Units (ECUs) everywhere
  - Multiple Internal Communication Channels (CAN, OABR, Embedded Simcards, etc.)
  - Multiple Outbound Channels like IP(v6), BT & BTLE, Local WiFi, GPS, DAB+, etc.

ERNW
providing security.

Car Manufacturer/Part Provider

- We took primarily a look at the external interfaces
  - Local WiFi was set up securely – almost no running services -> almost no attack surface
  - BT & BTLE interfaces were secured in terms of best practices, but chip firmware was flawed -> DoS vulnerability
  - GPS was impacted by GPS spoofing

ERNW
providing security.

Car Manufacturer/Part Provider

- GPS signal was used for time synchronization of some of the ECUs
- Due to higher prioritization of GPS than Internet/4G/… the time of some ECUs could be spoofed
- 19. January 2038 at 03:14:08 UTC 32bit signed integer unix stamp will overflow, resulting in a time travel into 1901

ERNW
providing security.

Car Manufacturer/Part Provider

- Now what's the problem when my car thinks it's in 1901?
  - The firmware reflashing service could be bypassed as now ALL old firmwares can be reflashed which can result in integrity change of crucial parts of the firmware
- Another big problem in automotive industry:
  - Patching of cars in the field is a real issue

ERNW
providing security.

Conclusion & Recommendations

- Security in the IoT comes with a challenge:
  - Security on multiple layers comprising the full product lifecycle
- But most challenges 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

ERNW
providing security.

Thank You for Your Attention!

cklaassen@ernw.de

@earl553

www.ernw.de

www.insinuator.net

ERNW
providing security.

Image Sources

- Icons made by Freepik from www.flaticon.com
- Pictures from www.troopers.de
- Meme from imgflip.com