ERNW
providing security.

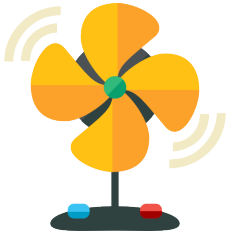
Update Management in the IoT, or: You Can't Update Hardware over the Air

Matthias Luft, mluft@ernw.de, @uchi_mata

Enno Rey, erey@ernw.de, @Enno_Insinuator

#IoT Will Change the World We Live In

Smart objects (hardware running software) will control:



- the air we breath

- physical properties/attributes of our household environments (doors, temperature, security against intruders)

- vital functions of our bodies

- the food we consume, in many ways

- the way we move from one place to another

ERNW
providing security.

"To Control Something" ... Has Two Meanings

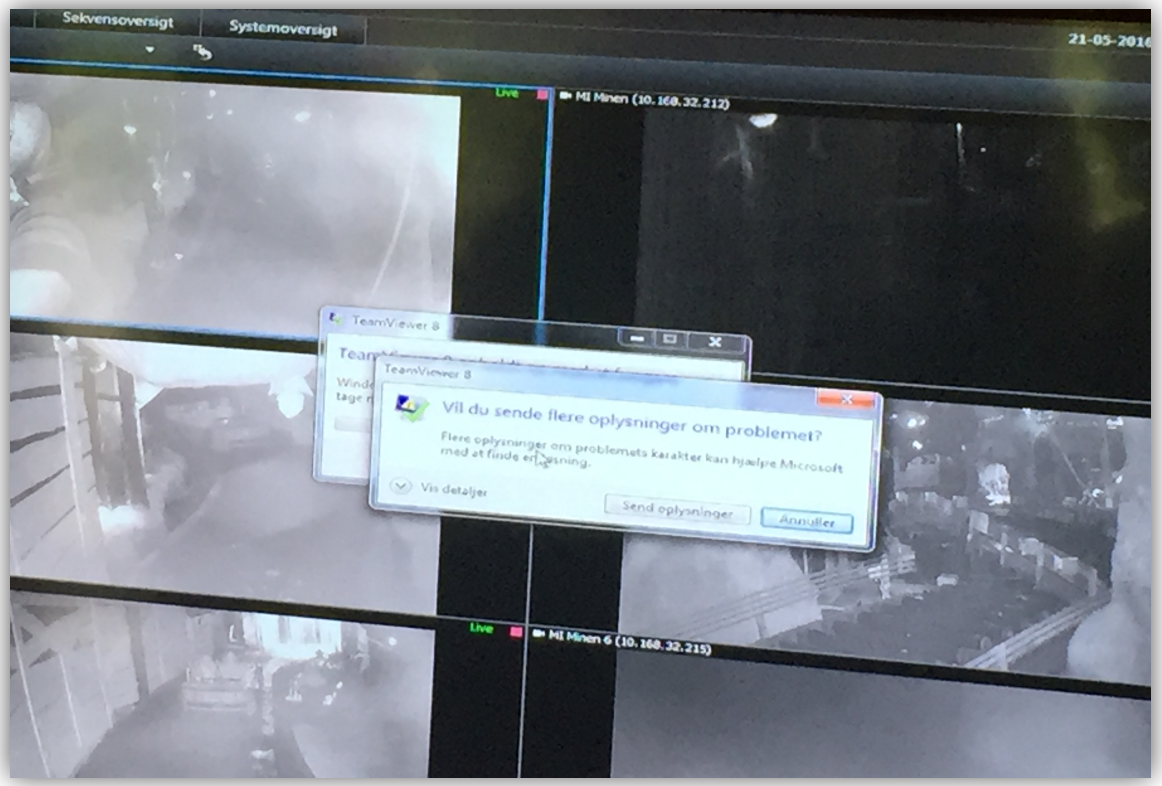
"(actively) **direct/steer** the actions or function of (something)"

&

"(provide ability to) **monitor and check** (the state of something)"

See also: https://www.insinuator.net/2016/09/to-control-something/

ERNW
providing security.



ERNW
providing security.

Relevant Properties of Smart Objects

- Resource Constraints
  - E.g. as for memory, computing power, power (batteries), network bandwidth, ...

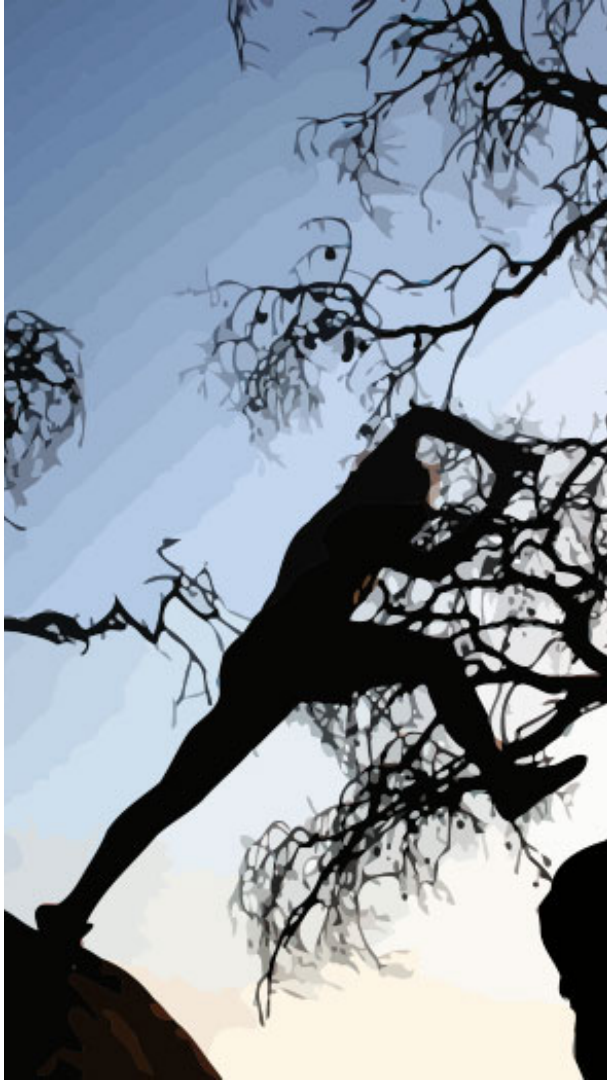
- Physical Exposure
  - May be physically accessible by non-trustworthy parties, or (phys.) inaccessible by trusted parties

- Long lifespan
  - Some estimates up to 40 years
- Unclear Ownership/Responsibilities?

ERNW
providing security.

Update Management Challenges

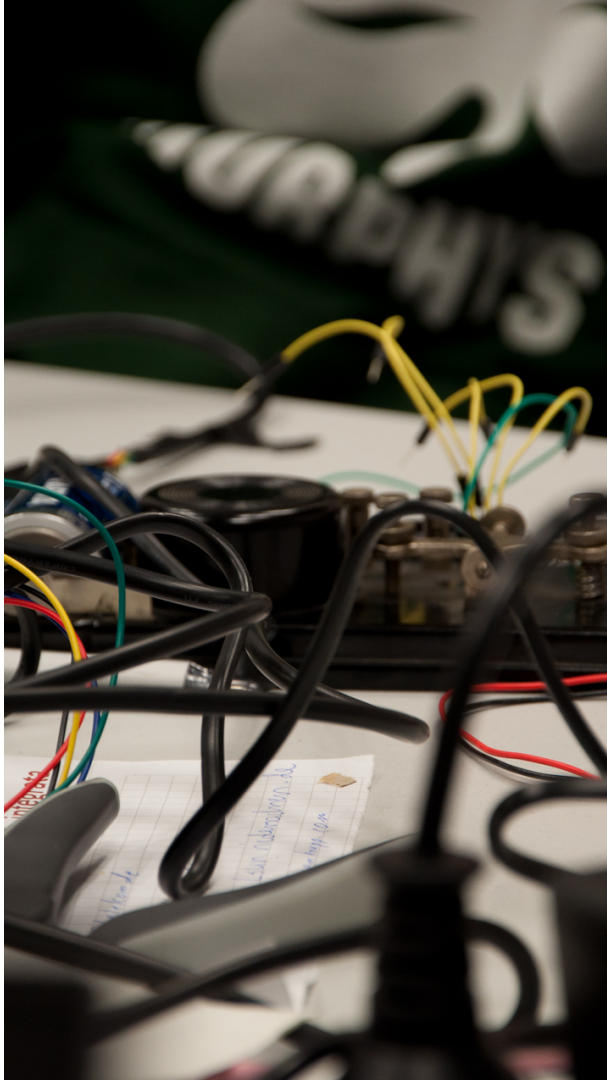
- Physical Exposure
- Root of Trust
- (Computing) Resources & Environment
- Warranty
- Certification
- Ownership & Responsibility
- Research, Disclosure, and Ethical Aspects



ERNW
providing security.

(Computing) Resources & Environment

- Storage: Updates may double the required storage space
- Reboots during updates
- Unknown network connectivity
- Version gaps



ERNW
providing security.

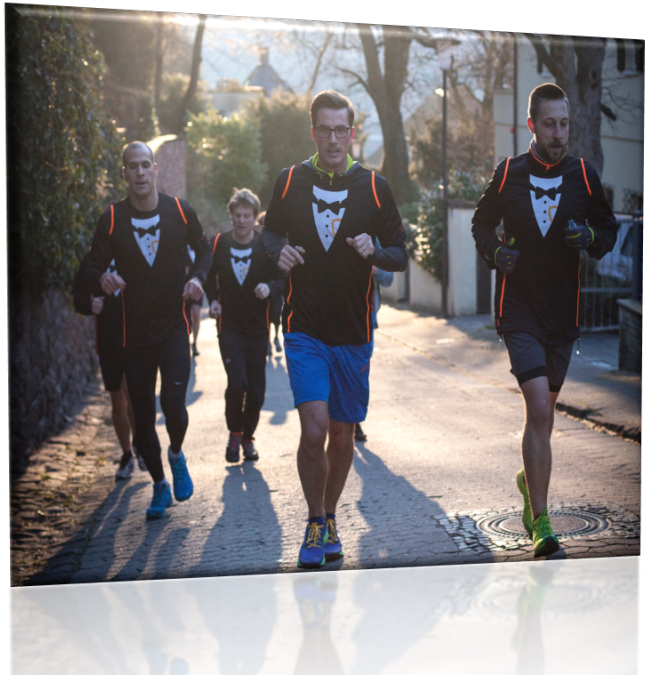
Certification

- Certain types of embedded devices require extensive verification and certification.
  - Often not a strong focus on IT security
- Certifications must allow fast response to discovered vulnerabilities
- For example, from [FDA]:

Software patches and updates are essential to the continued safe and effective performance of medical devices. Typically, FDA approval is not required before installing changes, updates, or patches that address cybersecurity issues

ERNW
providing security.

Research & Disclosure



- Vulnerability disclosure always had impact on society
- (More) Direct impact in a world with smart objects
- Vendors vs. (uninformed) end users

ERNW
providing security.

Summary

- First and foremost: Design your product for updates.
- Typical cryptographic measures should be applied
  - With a careful evaluation of resource consumption
- Extensive use of logical locking mechanisms
- Take environmental considerations into account
- Contribute to certification processes

ERNW
providing security.

References

- Cesar Cerrudo, Hacking US Traffic Control Systems
- FDA Safety Reminder on Cybersecurity
- Paper on Secure Firmware Updates
- Article on Embedded System Updates