Internet of Things
Security Standards

Ludwig Seitz
ludwig@sics.se
Why is IoT special?

- Massive deployments
  - Many simultaneous connections
  - Huge increase in data traffic
- Constrained devices (Sensors, Actuators)
  - 16 KB RAM, 128 KB Flash, battery-driven
- Low-Power Lossy Networks
  - 100 kbit/s, high packet loss (~ 20%)
  - Physical layer packet size limited (~ 100 bytes)
Why not standard security?

• Too much network traffic
  – Too many messages
    • TLS: 2 round trips
  – Too large messages
    • TLS certificates > 1 KB

• Too much RAM needed
  – Example: Minimal TLS ~ 4 KB

• Too large libraries required
  – Example: TLS has over 100 algorithm options
  → Standard security needs profiling
Current Scope

• Cooperation: ERICSSON & SICS

• Authentication
  – Who/What are you?

• Authorization
  – Who can do what?

• Communication security
  – Integrity, Confidentiality, Replay protection
Example A: Actuator

Client (C)

Request:
Set actuator to 5

Response:
changed

Actuator [Server (S)]

• S needs to know C is authorized
• C needs to know that the response is from S
• Communication needs to be protected
Example B: Sensors

- Access to sensor readings must be controlled
- Clients need to be able to verify the origin of a sensor reading and to detect replay or fraudulent messages
IoT standardization at IETF

- Internet Engineering Task Force
  - Standardizes e.g. HTTP, TCP, IP
- Divided in Working Groups
- Most relevant for IoT:
  - **ACE** (Authorization and Authentication in Constrained Environments)
  - **CoRE** (Constrained Restful Environments)
  - **COSE** (CBOR Object Signing & Encryption)
The ACE solution* : OAuth 2.0 profile for IoT

1. Authorization request

Client → Authorization Server

2. Access token

Client

3. request + token

Server

Rationale:
Authorization decision = heavyweight
Verify token = lightweight

* very much simplified
Other components

• Existing standards
  – CoAP (Constrained Application Protocol)
    • Similar to HTTP but for constrained devices
  – CBOR (Concise Binary Object Representation)
    • Similar to JSON but binary and more compact

• Work in progress
  – COSE (CBOR Object Signing and Encryption)
    • Securing CBOR objects
  – OSCoAP (Object Security for CoAP)
    • Using COSE to secure CoAP messages
Conclusions

• IoT is an important part of 5G,
• Important parts of IoT are constrained ...

... and need adapted security solutions

These are standardized **now**

SICS is a central part of it!