Hardware-Secured Configuration and Two-Layer Attestation Architecture for Smart Sensors

Thomas Ulz, Thomas Pieber, Christian Steger[1]
Sarah Haas, Rainer Matischek, Holger Bock[2]

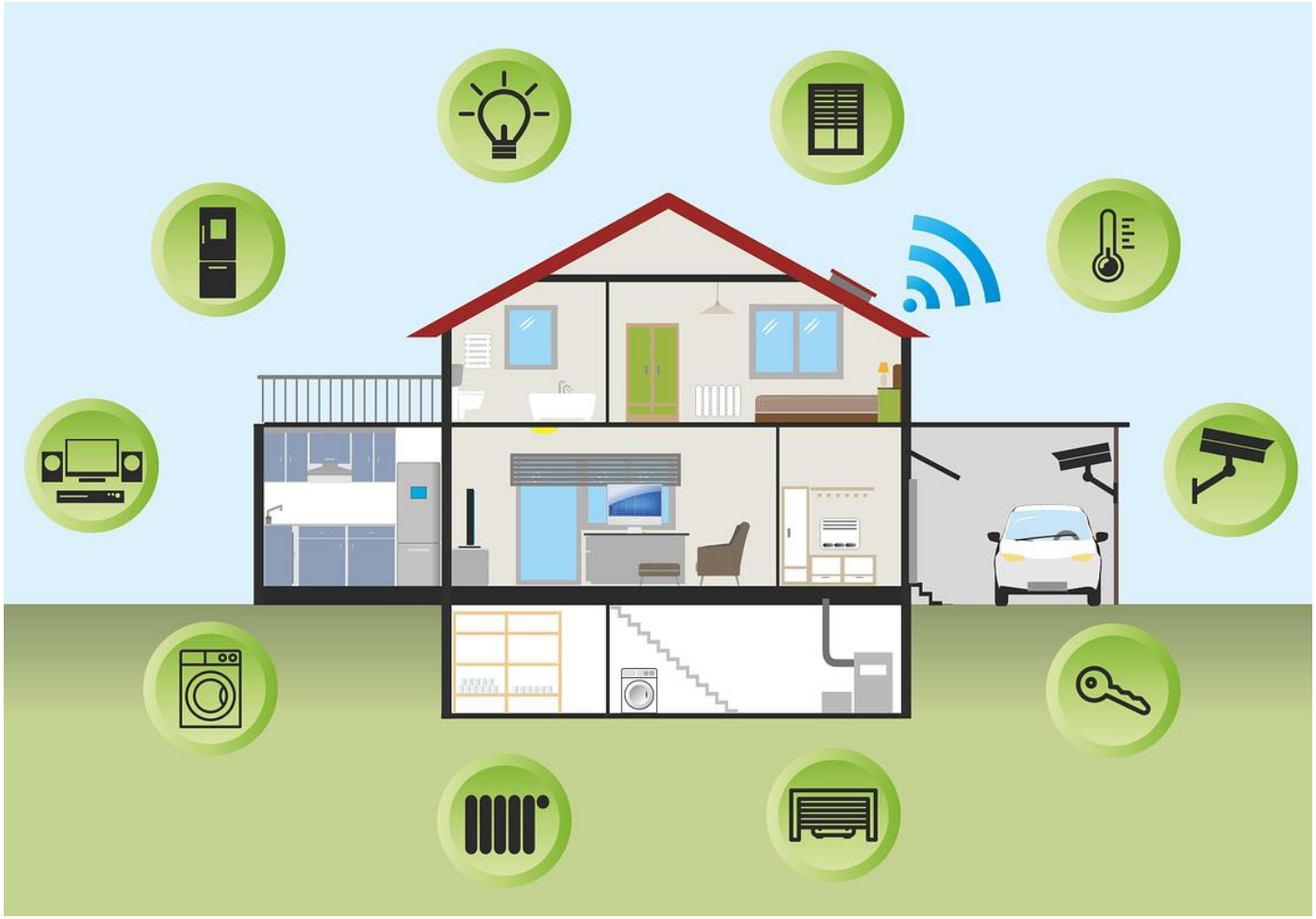
[1]Graz University of Technology
[2]Infineon Austria AG

Outline

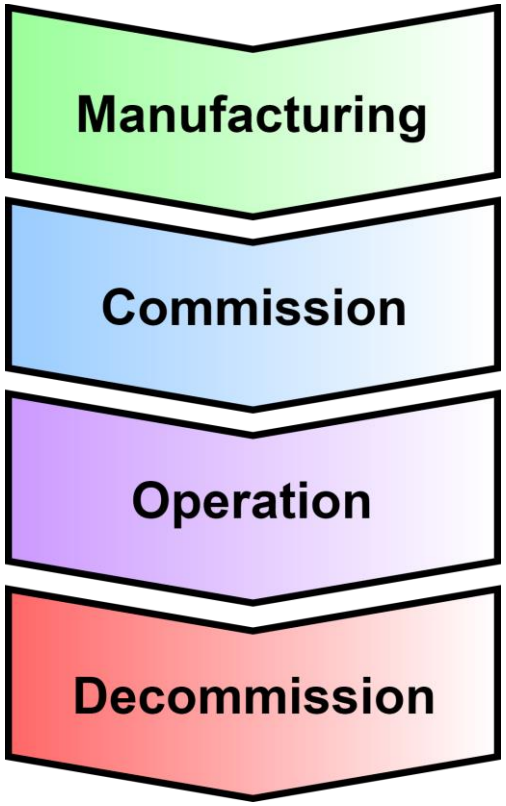
1. Motivation, State-of-the-art
2. Secured Configuration
    1. NFC-Interface
    2. Protocol
    3. System Model
3. Hardware Architecture
    1. Two-Layer Attestation
4. Evaluation
5. Conclusion and Future Work

Motivation – Industry 4.0 / Smart Homes

Motivation – Smart Homes



Motivation – Smart Sensor Configuration



- Initial manufacturer keys
- Initial configuration

- Device owner key update
- Specific configuration updates

- Recurrent configuration updates
- Reconfiguration for changing tasks

- Reconfiguration for resale
- Deletion of confidential data

Motivation – Requirements I/II

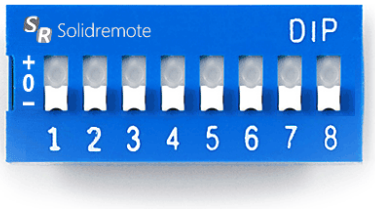
- Secured transfer of configuration data
  - Confidential information
- Tamper resistant
  - Stored data must be protected
- Easy and intuitive to use
  - Applied in industrial and smart home settings
- Attestation mechanism to verify correct config

Motivation – Requirements II/II

- Energy efficient
  - Smart sensors might be operated on battery power
- Configuration update without power source
  - E.g. during manufacturing of sensor

State-of-the-art

- Various configuration interfaces
  - Wired
  - Wireless (WiFi, Bluetooth, …)
  - Buttons, Displays, DIP Switches



- Often limited security considerations
- No arbitrary payloads but firmware, pairing info, …
- No attestation of applied configuration

Contributions

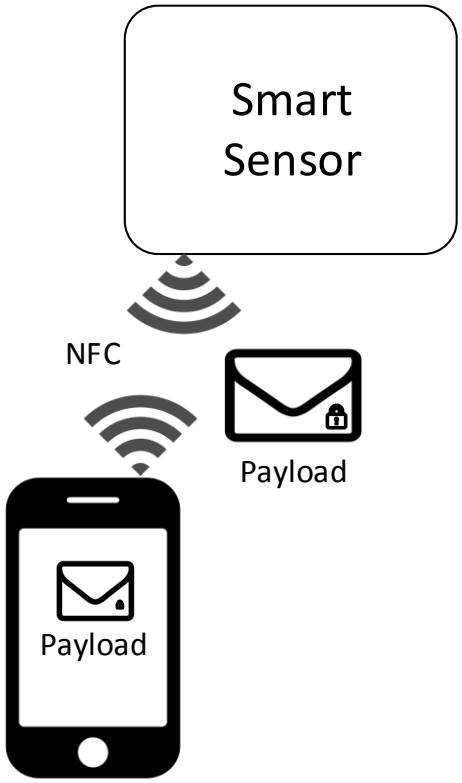
- Define a secured configuration interface
  - Easy and intuitive to use
  - Protocol and hardware
- Suitable for existing devices and new devices
- Show how our proposed architecture can be used for configuration attestation

Outline

1. Motivation, State-of-the-art
2. Secured Configuration
    1. NFC-Interface
    2. Protocol
    3. System Model
3. Hardware Architecture
    1. Two-Layer Attestation
4. Evaluation
5. Conclusion and Future Work

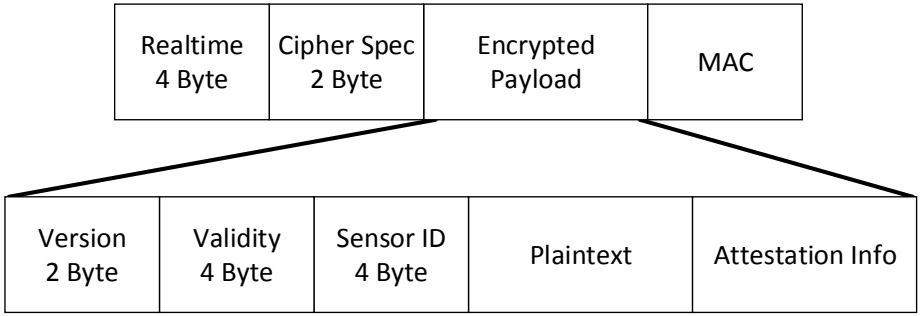
Secured Configuration – NFC Interface

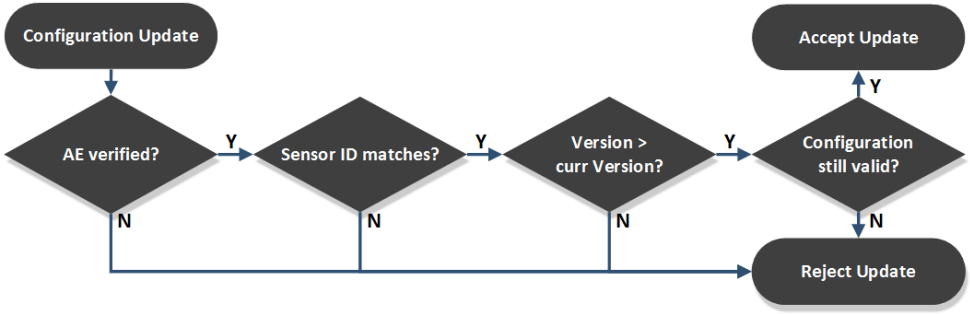
- Use NFC as configuration interface
  - Intuitive to use
  - Little interference compared to other technologies such as WiFi
    - NFC operates at 13.56 MHz
  - „Security by proximity“
    - Roughly 10cm, Eavesdropping 10m!
    - Configuration interface not accessible for remote attackers
    - But no security by protocol!



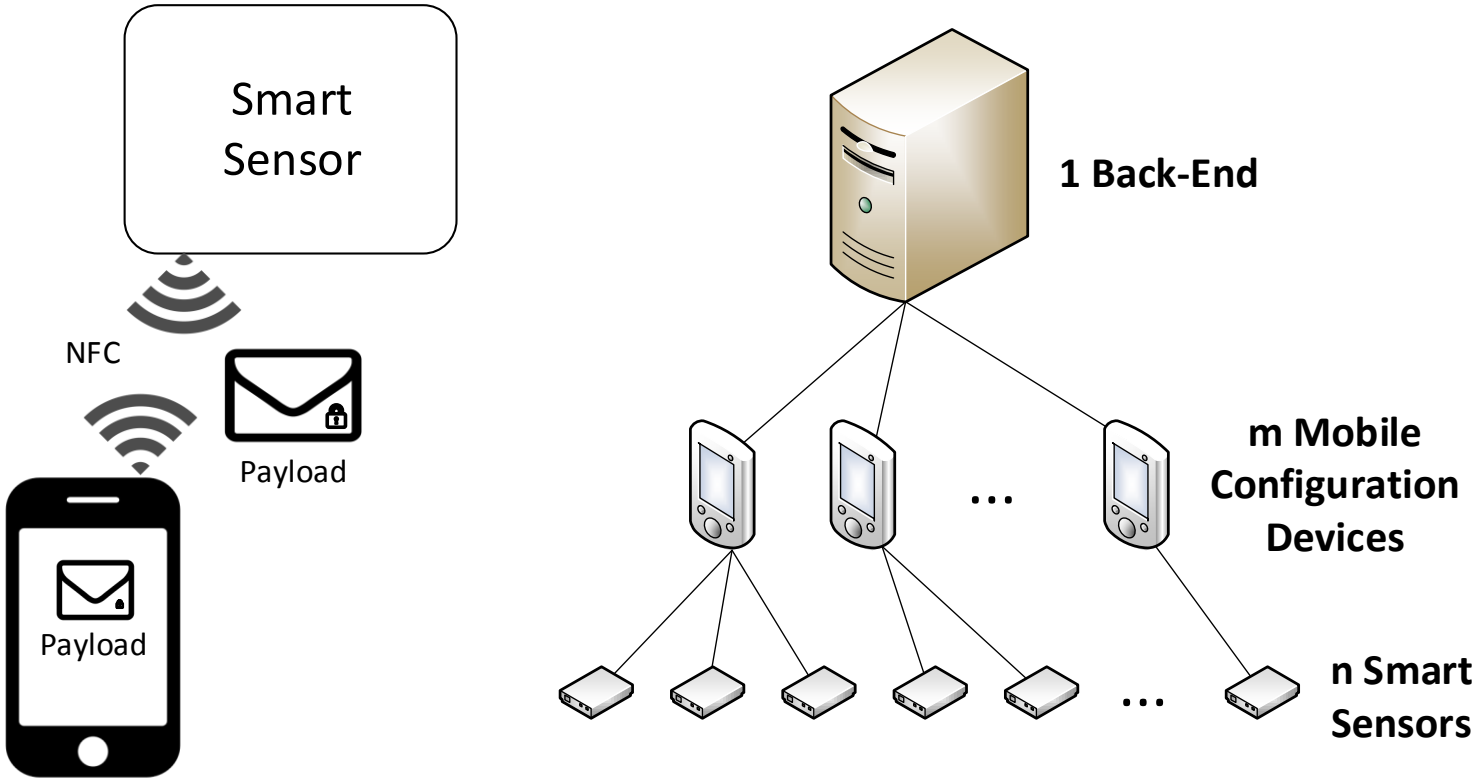
Secured Configuration – Protocol

- NDEF-based protocol for configuration transport
- Data protected by authenticated encryption
- „Ticket“ information to mitigate replay attacks





Secured Configuration – System Model

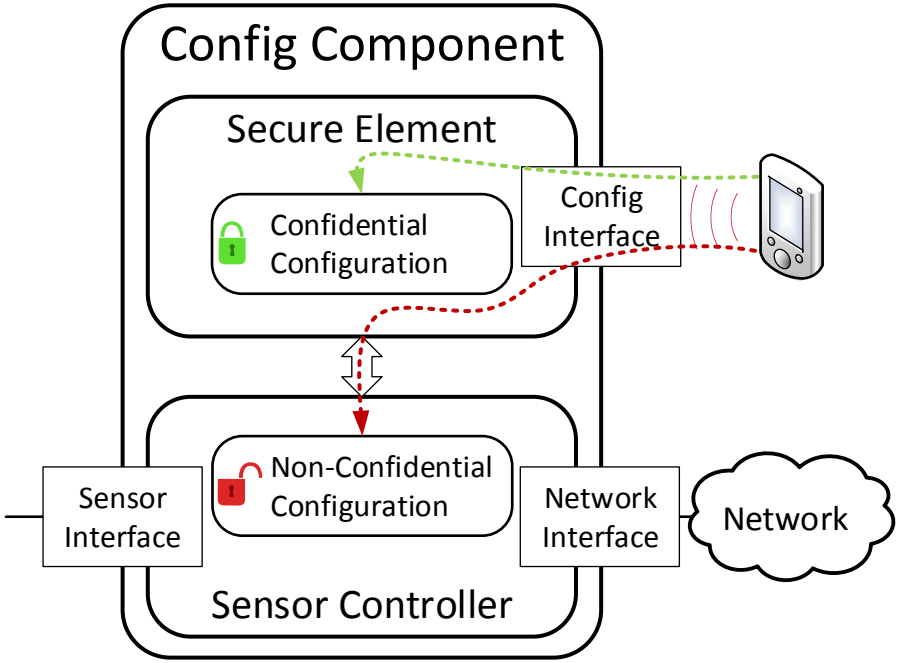


Outline

1. Motivation, State-of-the-art
2. Secured Configuration
   1. NFC-Interface
   2. Protocol
   3. System Model
3. Hardware Architecture
   1. Two-Layer Attestation
4. Evaluation
5. Conclusion and Future Work

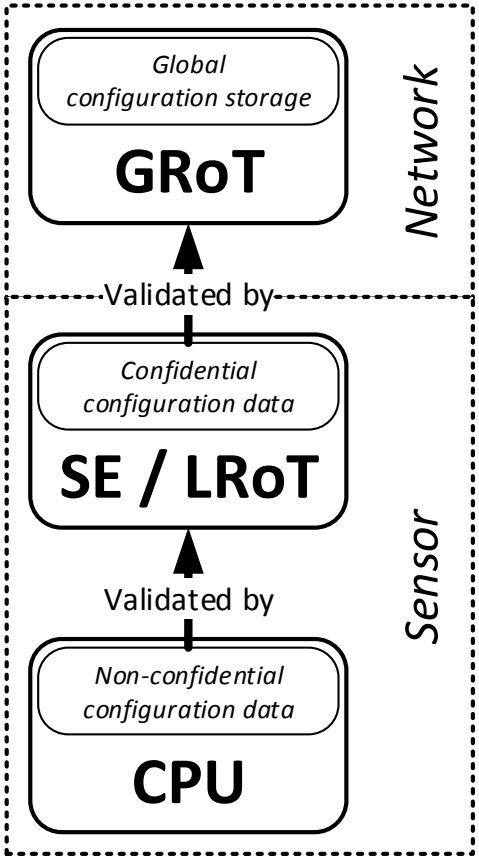
Hardware Architecture

- Component split into two worlds
  - Secured world
  - Normal world
- Security by isolation
- Secure Element
  - Storage
  - Cryptographic Operations



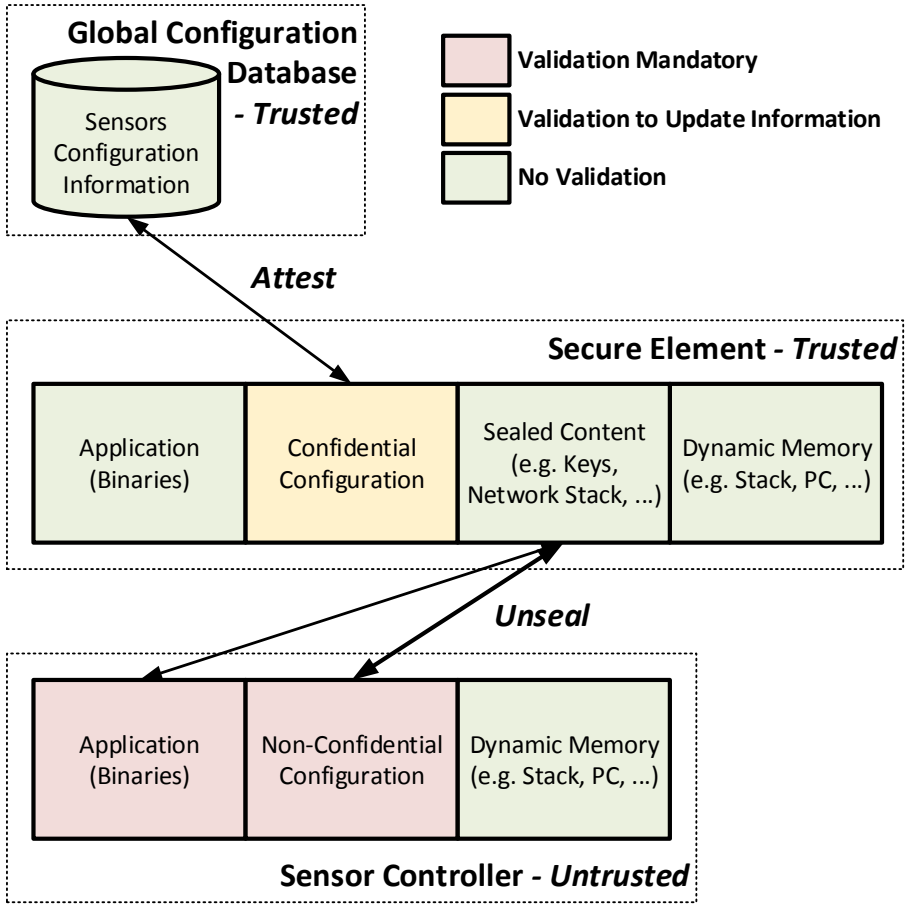
Configuration Attestation / Validation

- Based on hardware architecture
  - Local Root of Trust (LRoT) in any Smart Sensor
- Based on system architecture
  - Global Root of Trust (GRoT) given by global configuration storage present in system model



Configuration Attestation / Validation

- Non-Confidential data
  - Binary attestation
  - Property based attestation
  - „Seal“ network access
- Confidential data
  - Stored in trusted SE
  - Only validation by GRoT to verify update



Design Decisions

- SE over TPM
  - Provides same functionality as TPM
  - Low power consumption (used in smartcards)
  - In addition
    - NFC interface
    - Can be powered through NFC interface
    - Trusted execution environment
- By „sealing“ network access
  - Malicious smart sensor is isolated
  - If data received: sensor and data is trustworthy

Outline

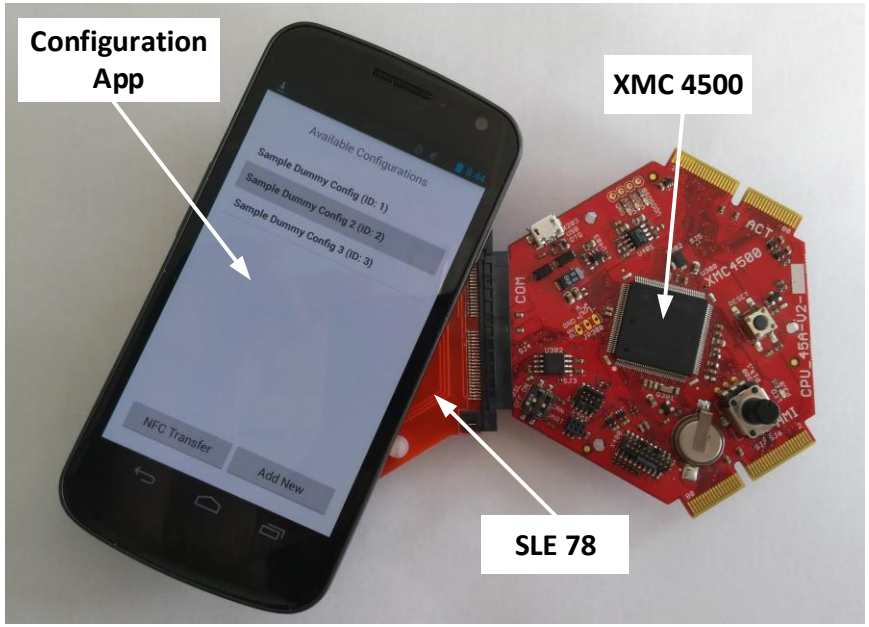
1. Motivation, State-of-the-art
2. Secured Configuration
    1. NFC-Interface
    2. Protocol
    3. System Model
3. Hardware Architecture
    1. Two-Layer Attestation
4. Evaluation
5. Conclusion and Future Work

Evaluation

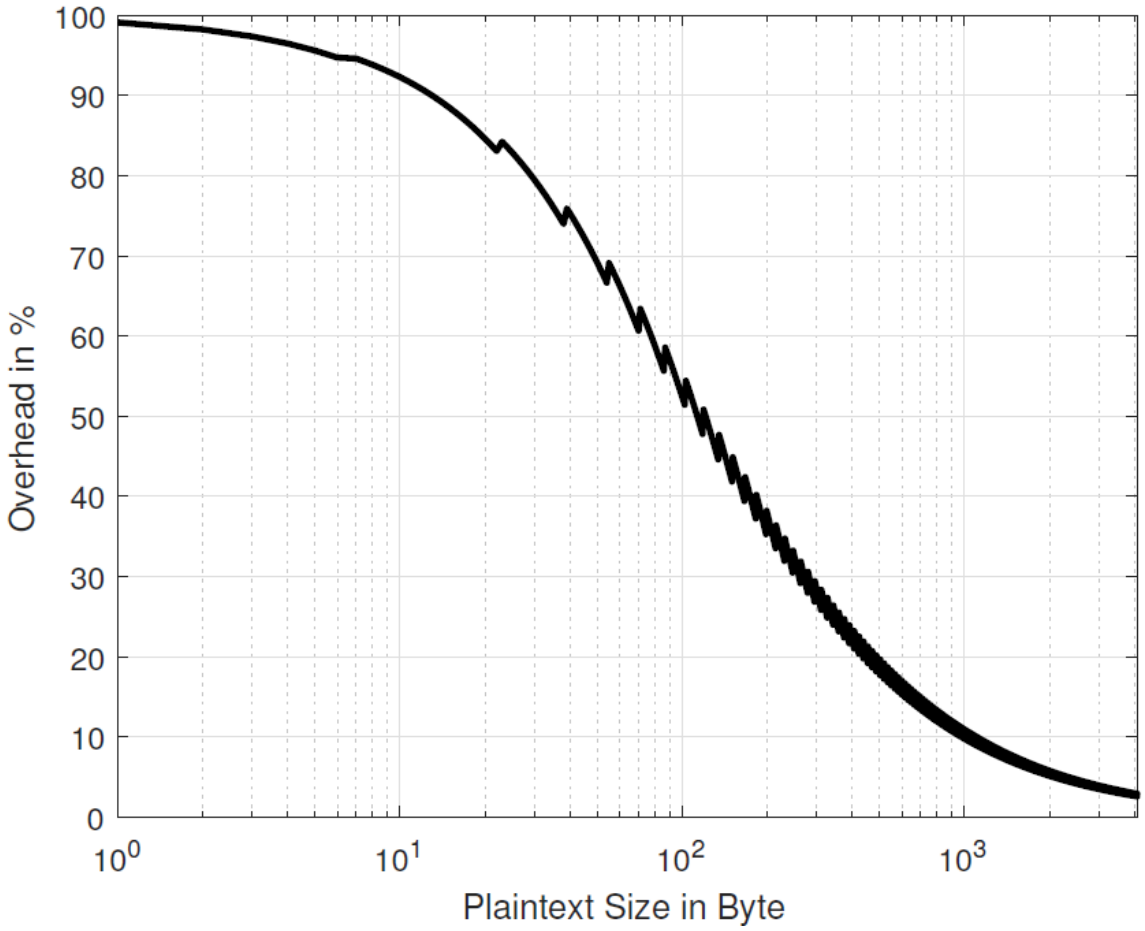
- Feasibility: Prototypical implementation
- Performance: Timing measurements
- Security improvements: Threat analysis

Evaluation – Prototype

- Infineon components
  - XMC4500
  - SLE78
- Android smartphone
- Performance
  - 5-10 parameters
  - 200ms
  - Similar to TLS over WiFi on Raspberry PI3



Evaluation – Protocol Overhead by Security



Evaluation – Threat Analysis

- Not exhaustive, most important threats identified
- Overall 8 threats identified that are mitigated by countermeasures implemented in our approach
- Mitigated: malicious configuration updates, replay attacks, DoS attacks (using configuration interface), and physical attacks

Evaluation – Threat Analysis

- Malicious updates, replay attacks
  - Mitigated by protocol
- Malicious configuration or software
  - Mitigated by attestation
- Remote attacks
  - Mitigated by only allowing updates via NFC
- Adversary with physical access to smart sensor
  - Mitigated by using tamper resistant SE

Outline

1. Motivation, State-of-the-art
2. Secured Configuration
    1. NFC-Interface
    2. Protocol
    3. System Model
3. Hardware Architecture
    1. Two-Layer Attestation
4. Evaluation
5. Conclusion and Future Work

Conclusion and Future Work

- Secured and easy-to-use configuration approach
  - Suitable for confidential and non-confidential data
- Can be retrofit into existing sensors and new devices
- Configuration solution is „attestation aware“
  - Attestation is considered in data transfer protocol
- 8 potential threats mitigated by our approach
- Future work: further investigate methods for granting or denying network access to smart sensors

Acknowledgements IoSense

This project has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement No 692480. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Germany, Netherlands, Spain, Austria, Belgium, Slovakia.

ECSEL Joint Undertaking
Electronic Components and Systems for European Leadership

IoSense is funded by the Austrian Federal Ministry of Transport, Innovation and Technology (BMVIT) under the program "ICT of the Future" between May 2016 and April 2019. More information: https://iktderzukunft.at/en/

bmvit
Austrian Ministry for Transport, Innovation and Technology

Questions?

Thank you!