SECURITY FEATURES FOR IOT DEVICES BASED ON RISC-V

Lukas Auer (AISEC), Christian Skubich (IIS/EAS), Matthias Hiller (AISEC)

RISC-V Activities Workshop 2019
SECURITY FEATURES FOR IOT DEVICES BASED ON RISC-V

- Internet of Things (IoT) Challenges
- Universal Sensor Platform (USeP)
- Security Architecture
  - Secure Boot
  - Key Management
  - Secure Update
  - Authenticated Watchdog Timer
Internet of Things (IoT) Challenges

- Internet of Things (IoT) is a booming market
  - Annual potential economic impact estimated between $3.9 trillion and $11.1 trillion by 2025

- High rate of adoption creates new challenges
  - Move towards edge computing → high CPU performance
  - Privacy and security concerns → keep data local
  - Low maintenance effort → low power consumption
  - Long life-span → security as fundamental design goal

Internet of Things (IoT) Challenges

- Dream IoT device has
  - High performance CPU subsystem
  - Low power consumption
  - Extensive security features

- These systems exist, but are custom high-volume products
  - Additional integration challenges from miniaturization
  - Not viable for small to medium enterprises
SECURITY FEATURES FOR IOT DEVICES BASED ON RISC-V

- Internet of Things (IoT) Challenges
- Universal Sensor Platform (USeP)
- Security Architecture
  - Secure Boot
  - Key Management
  - Secure Update
  - Authenticated Watchdog Timer
Universal Sensor Platform (USeP)

- Universal Sensor Platform (USeP) as solution for small to medium enterprises
  - Developed by several Fraunhofer Institutes

- 3D System-in-Package (3D-SiP) for the IoT market
  - Standardized, efficient processing subsystem based on RISC-V
  - Customizable selection of sensors and wireless interfaces

- SoC is manufactured in GLOBALFOUNDRIES’ 22FDX technology
Universal Sensor Platform (USeP)
Universal Sensor Platform (USeP)
SECURITY FEATURES FOR IOT DEVICES BASED ON RISC-V

- Internet of Things (IoT) Challenges
- Universal Sensor Platform (USeP)
- **Security Architecture**
  - Secure Boot
  - Key Management
  - Secure Update
  - Authenticated Watchdog Timer
Secure Boot

- Two software authorities
- Monotonic incrementing serial numbers to implement certificate revocation
  - Lowest accepted serial number is stored in internal non-volatile storage
Key Management

- Strong cryptographic keying material required to protect sensitive information

- Unique device secret stored in one-time programmable memory
  - Available to software once system state is determined to be secure
  - Access can be locked for the current power cycle

- Used to implement TCG’s Device Identifier Composition Engine (DICE)
Key Management

Unique Device Secret → Device Identity → Device Identity → Key CSR

First Software Stage → Second Software Stage → Third Software Stage
Secure Update

- Software vulnerabilities are difficult to avoid, a secure update mechanism is important
  - Update mechanism is implemented in software and protected by secure boot

- Software update mechanism alone is not sufficient
  - Configuration changes and updates must be pushed to devices
  - Failure to apply updates must be detected and recovery actions must be taken

- Additional control of device with the authenticated watchdog timer
  - Specified as part of Microsoft’s Cyber-Resilient Platform Program (CyReP)
Authenticated Watchdog Timer

- The typical watchdog timer
  - Resets the device once its internal timer has expired
  - Unless it is deferred beforehand by software

- The authenticated watchdog timer is similar, but with important differences
  - It cannot be disabled once enabled
  - It can only be deferred using deferral tickets send by an authenticated party
Authenticated Watchdog Timer

- Central management system sends deferral tickets

1. Update is distributed, failures are monitored
   1. Deferral tickets are sent to all good IoT devices
   2. Misbehaving devices are not sent deferral tickets
2. Misbehaving devices will deterministically reset
3. Early boot software is responsible for recovery

- Online and offline devices can be recovered within a predictable time frame
Authenticated Watchdog Timer

- The authentication protocol is based on hash chains
- Allows for efficient hardware implementation
- Concept of using hash chain for authentication is based on Lamport’s one-time password scheme [2]
  - Secure from an attacker eavesdropping on the communication
  - Passwords are difficult to guess, even with knowledge of previous passwords

Slide 16
© Fraunhofer

Authenticated Watchdog Timer – Setup

- The authentication protocol of the authenticated watchdog timer is based on T/Key [3]
- Authentication is split into two steps
  - Setup
  - Authentication

Authenticated Watchdog Timer – Authentication

Central Management System

Ticket n → ... → Ticket 3 → Ticket 2 → Ticket 1

Device

Received Ticket → Ticket 2 → Ticket 1
Conclusion

- Universal Sensor Platform (USeP) as solution for the IoT market
  - Highly integrated 3D System-in-Package (3D-SiP)
  - SoC manufactured in GLOBALFOUNDRIES’ 22FDX technology

- Integrated security features for the IoT market
  - Secure boot and update
  - Key Management
  - Authenticated Watchdog Timer

- Open-source activities
  - Improvements to U-Boot on RISC-V, currently adding SMP support