Providing Tamper-Secure SoC Updates through Reconfigurable Hardware

Franz-Josef Streit[1], Stefan Wildermann[1], Michael Pschyklenk[2] and Jürgen Teich[1]
franz-josef.streit@fau.de

[1]Hardware/Software Co-Design, Friedrich-Alexander University Erlangen-Nürnberg (FAU), Germany
[2]Schaeffler Technologies AG & Co. KG, Germany

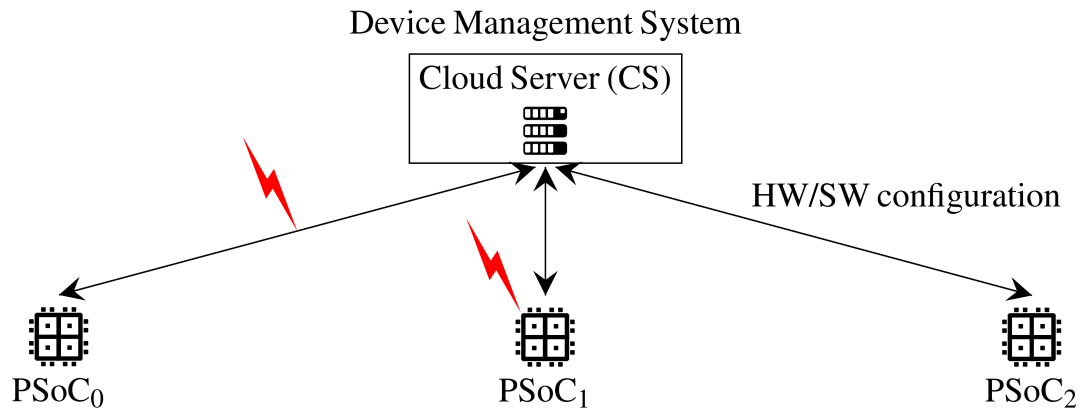
International Symposium on Applied Reconfigurable Computing (ARC)

June 29-30, 2021

Curious about IoT Device Security and Cryptographic Hardware?

Motivation

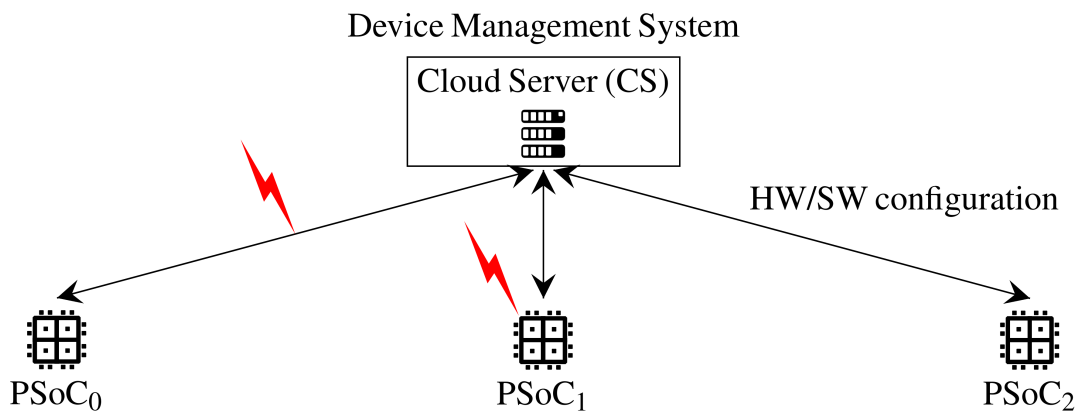
- Remote firmware updates guarantee secure deployment of IoT devices
- **Questions:**
  - How to secure the **confidentiality** of secret keys?
  - Still possible if the system's **software** is compromised?
- **Idea:**
  Entirely relying on **hardware-intrinsic secrets**
  → We propose a partial reconfigurable hardware design called
  Trusted Update Unit (TUU)



Curious about IoT Device Security and Cryptographic Hardware?

Motivation

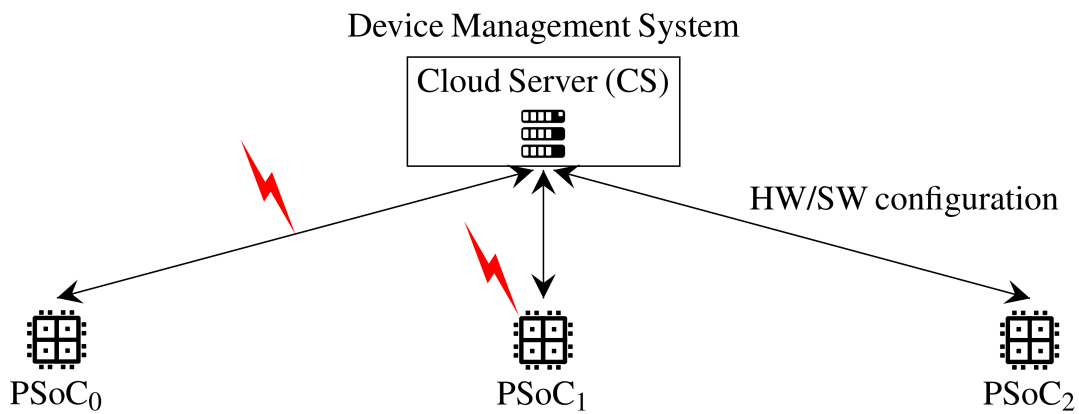
- Remote firmware updates guarantee secure deployment of IoT devices
- **Questions:**
  - How to secure the **confidentiality** of secret keys?
  - Still possible if the system's **software** is compromised?
- **Idea:**
  Entirely relying on **hardware-intrinsic secrets**
  → We propose a partial reconfigurable hardware design called
  Trusted Update Unit (TUU)



Curious about IoT Device Security and Cryptographic Hardware?

Motivation

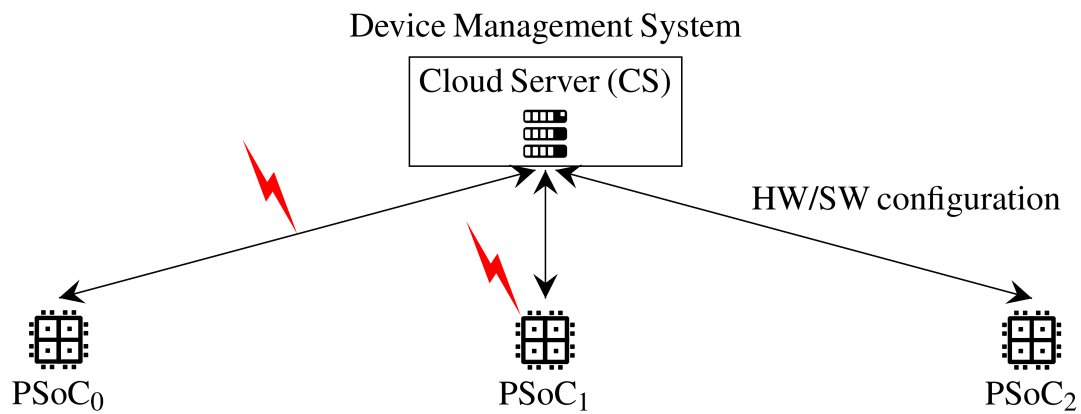
- Remote firmware updates guarantee secure deployment of IoT devices
- **Questions:**
  - How to secure the **confidentiality** of secret keys?
  - Still possible if the system's **software** is compromised?
- **Idea:**
  Entirely relying on **hardware-intrinsic secrets**
  → We propose a partial reconfigurable hardware design called
  Trusted Update Unit (TUU)



Curious about IoT Device Security and Cryptographic Hardware?

Motivation

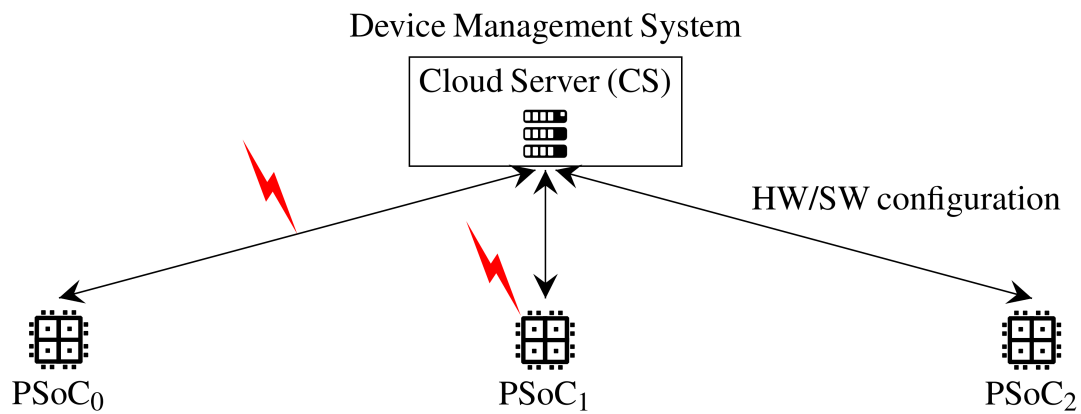
- Remote firmware updates guarantee secure deployment of IoT devices
- **Questions:**
  - How to secure the **confidentiality** of secret keys?
  - Still possible if the system's **software** is compromised?
- **Idea:**
  Entirely relying on **hardware-intrinsic secrets**
  → We propose a partial reconfigurable hardware design called
  Trusted Update Unit (TUU)



Curious about IoT Device Security and Cryptographic Hardware?

Motivation

- Remote firmware updates guarantee secure deployment of IoT devices
- **Questions:**
  - How to secure the **confidentiality** of secret keys?
  - Still possible if the system's **software** is compromised?
- **Idea:**
  Entirely relying on **hardware-intrinsic secrets**
  $\rightarrow$ We propose a partial reconfigurable hardware design called
  Trusted Update Unit (TUU)



Thank you!

Hope to see you in the interactive poster session!