Università degli Studi di Napoli Federico II

iteePhD information technology electrical engineering

DIETI UNINA

PhD student Erasmo La Montagna

Embedded Systems for Real-Time Applications

Tutor: Nicola Mazzocca

Cycle: XXXV

iteePhD information technology electrical engineering

My background

- MSc degree: Computer Engineering taken on 31 January 2019
- Research group: Seclab
- PhD started on 1 November 2019
- No Scholarship
- Currently working for Rete Ferroviaria Italiana (no company funded scholarship)

Research field of interest

- Hardware Security in modern Industrial Internet of Things systems
  - Challenges
    - Neglected Security Requirements
    - Limited Resources of embedded device
    - Chain of trust:
      - Secure Key Generation
      - Code Integrity Check
    - Mutual Authentication
  - Available technologies
    - Physical Unclonable Functions
    - Lightweight Encryption
    - Secure Crypto-processors (i.e. ARM TrustZone)
- Virtualization on embedded devices

Summary of study activities

- Conference attended (fully online):
  - 14th International Conference on the Quality of Information and Communications Technology (QUATIC 2021)
- Main focus on several fields of application of Physical Unclonable Functions
  - Physical Fingerprint and key generation (Fuzzy Extractor Algorithm)
  - Pseudo PUF: obtaining a strong PUF from a weak PUF
  - Real case scenario: authenticating nodes in a Power Delivery Network
  - Adopting a PUF as Root of Trust for the Virtual Machines running on a hypervisor
  - Secure boot
  - Use of virtualization on embedded devices
- Ad hoc PhD courses / schools:
  - Real-Time Embedded Systems for I4.0 and IIoT (Not Validated)
- Courses attended borrowed from MSc curricula:
  - Data Management (6 CFU)
- Seminars

Research activity: Overview (1/3)

- Problem
  - Decentralized key generation and identity management
  - Cryptographic primitives are complex to adopt due to IoT nodes’ limited power and computing capabilities
  - How strong can be the signatures derived from SRAM of commercial microcontrollers?

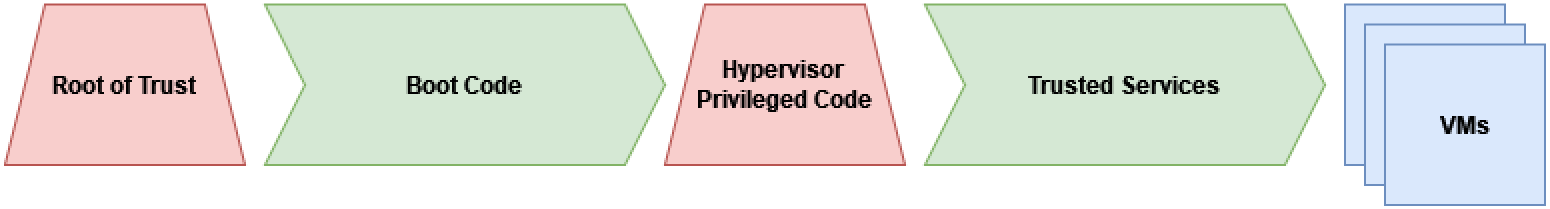
- Objective
  - Exploit SRAM-based PUF and provide security mechanisms and harden the device perimeter
  - Provide a design and a detailed evaluation of a PUF built on a non-custom circuit
  - Build a chain of trust on the microcontroller by means of secure boot procedure

- Methodology
  - Analyze SRAM response quality in terms of metrics such as uniqueness, stability, uniformity, bit-aliasing and entropy
  - Choose the optimal size for the Error Correction Code parameters

Research activity: Overview (2/3)

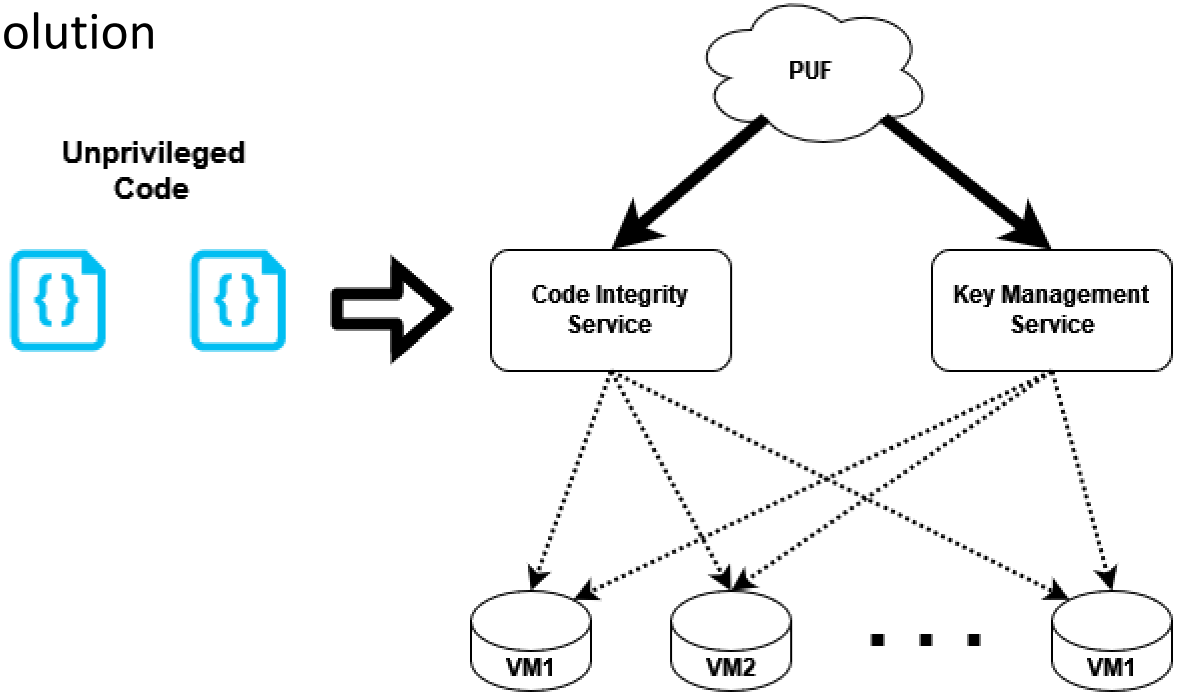
- Problem
  - Several CPU architectures intensively involved in the embedded world (e.g. ARMv7-A and ARMv8-A) offer support to the virtualization layer
  - Reliability and security of embedded systems would benefit from spatial and temporal isolation
  - The hypervisor layer would be the only high-privileged code to execute on the platform
- Objective
  - Design a RISC-V based architecture that endorses a dedicated PUF IPCore
  - The PUF module and the boot code provide the root of trust for the hypervisor layer
  - The virtualization layer satisfies the CIA triad (Confidentiality, Integrity, Authentication) by providing cryptography primitives *as-a-service* to virtual machines

Chain of Trust



Research activity: Overview (3/3)

- Proposed Solution



- The Code Integrity Service guardantees the Chain of Trust starting from the Boot code to user unprivileged code
- The Key Management Service generates and distributes symmetric and asymmetric encryption keys for the VMs

Products

[P1]	Scientific Paper: • Title: *On the Adoption of Physically Unclonable Functions to Secure IIoT Devices* • Authors: M. Barbareschi, V. Casola, A. De Benedictis, E. La Montagna, N. Mazzocca • Journal: IEEE Transactions on Industrial Informatics • Current Status: Published
[P2]	Conference Paper: • Title: *Enforcing mutual authentication and confidentiality in Wireless Sensor Networks using Physically Unclonable Functions: a case study* • Authors: M. Barbareschi, E. La Montagna, S. Barone, A. Fezza • Conference Name: 14th International Conference on the Quality of Information and Communications Technology – QUATIC 2021 • Current Status: Published