Università degli Studi di Napoli Federico II

itee PhD information technology electrical engineering

DIETI UNINA

Erasmo La Montagna

A PUF based authentication methodology for IIoT embedded safety critical systems

Tutor: Nicola Mazzocca

Cycle: XXXV

Year: 3rd

Background information

- 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)

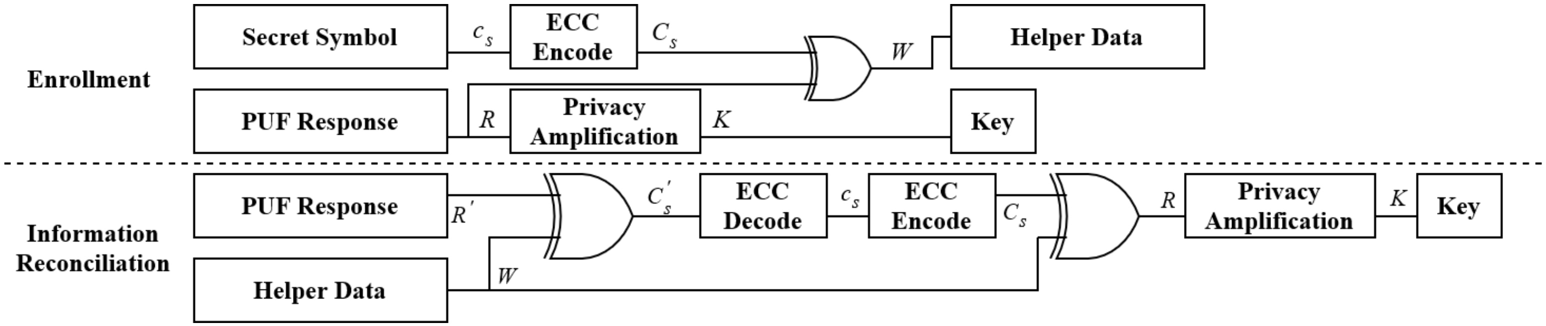
Summary of study activities

- 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:
  - Safety Critical Systems for Railway Traffic Management
  - Scientific Programming and Visualization with Python
  - Machine learning
  - Virtual Technologies and their Applications
  - Innovation Management, entrepreneurship and intellectual property
  - Real-Time Embedded Systems for I4.0 and IIoT (Not Validated)
- Courses attended borrowed from MSc curricula:
  - Big Data Analytics and Business Intelligence
  - Data Management (6 CFU)
- Seminars

Research areas

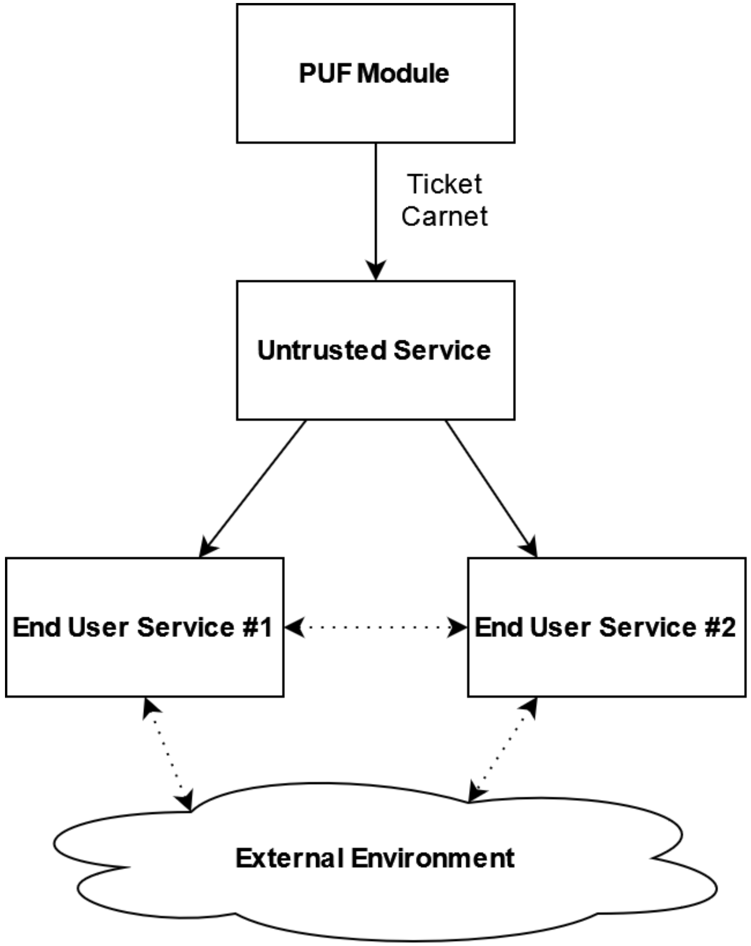
- Hardware Security in modern Industrial Internet of Things systems
  - Challenges
    - Neglected Security Requirements
    - Limited Resources of embedded device
    - Chain of trust:
      - Secure Key Generation
      - Code Integrity Check
    - Mutual Authentication
  - Available technologies
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

Research results (1/3)



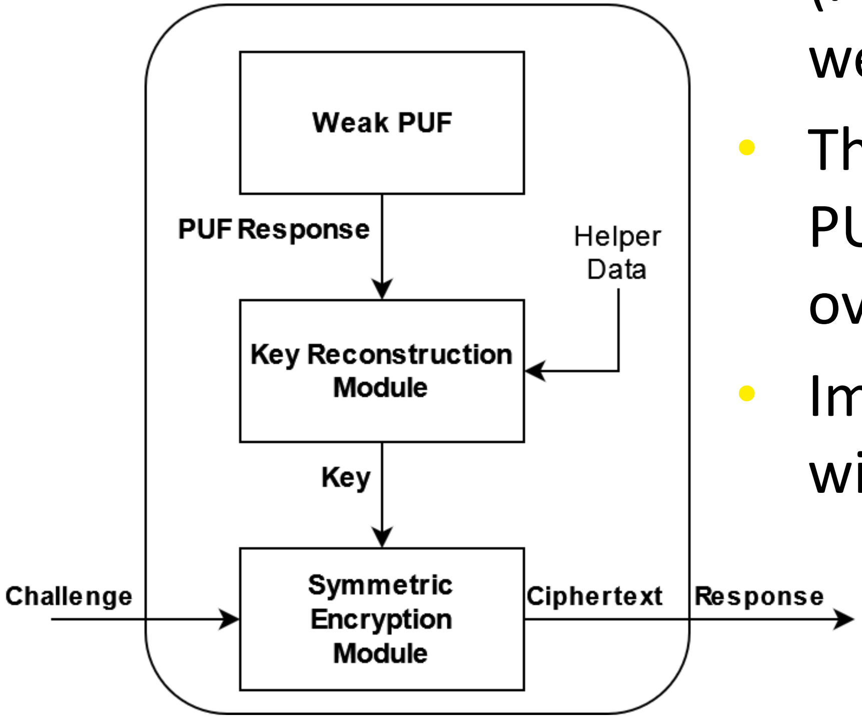
- A secure bootloader that extracts PUF responses from SRAM cells
- A PUF implementation that can be obtained also in a restrincted computing environment (small microcontrollers)
- Validates privileged code signed with the physical memory footprint of the device

Research results (2/3)



- Extended Phemap: a decentralized mutual authentication protocol
- A centralized trusted authentication service can delegate untrusted components that provides specific services
- A list of encrypted PUF responses is installed into the untrust services
- End Users benefits from several services based on virtual PUF responses

Research results (3/3)



- Design of a PUF-based architecture (Pseudo-PUF), obtained by combining a weak PUF and an encryption module
- The pseudo PUF behaves like a strong PUF while significantly reducing the overall footprint and cost
- Implements advanced security primitives with lower costs and resource demand

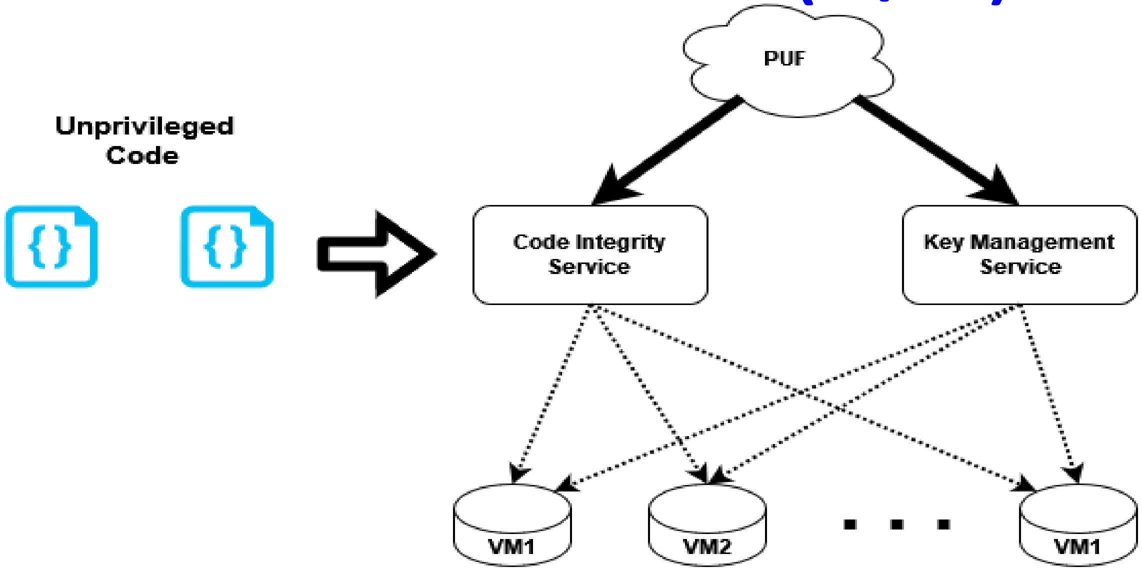
Research products

[P1]	M. Barbareschi, A. De Benedictis, E. La Montagna, A. Mazzeo, N. Mazzocca *A PUF-based mutual authentication scheme for cloud-edges IoT systems* **Future Generation Computer Systems** vol. 1439, pp. 246-261, 2019, DOI: 10.1016/ j.future.2019.06.012.
[P2]	M. Barbareschi, A. De Benedictis, E. La Montagna, A. Mazzeo, N. Mazzocca *PUF-Enabled Authentication-as-a-Service in Fog-IoT Systems* **International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises** Naples, Italy, Jun. 2019, pp. 58-63, Publisher, DOI: 10.1109/WETICE.2019.00020
[P3]	M. Barbareschi, S. Barone, A. Fezza, E. La Montagna *Enforcing Mutual Authentication and Confidentiality in Wireless Sensor Networks Using Physically Unclonable Functions: A Case Study* **International Conference on the Quality of Information and Communications Technology** Faro, Portugal, Sep. 2021, pp. 297-310, Publisher, DOI: 10.1007/978-3-030-85347-1_22
[P4]	M. Barbareschi, V. Casola, A. De Benedictis, E. La Montagna, N. Mazzocca, *On the Adoption of Physically Unclonable Functions to Secure IIoT Devices* **IEEE Transactions on Industrial Informatics** vol. 17 (11), pp. 7781-7790, 2021, DOI: 10.1109/TII.2021.3059656.

PhD thesis overview

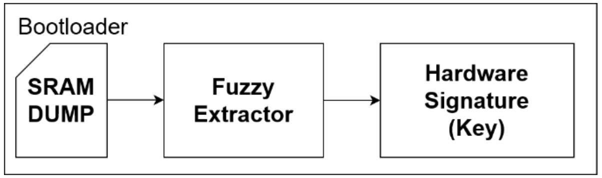
- IIoT systems involved in safety critical tasks must be subjected to Verification and Validation procedures before their deployment.
  - Use of virtualization can significantly reduce costs of certification
- IIoT networks relies on resource constrained devices which are exposed to physical manipulation.
  - These device are usually not equipped with a TPM
- Objective
  - Provide a Root of Trust based on PUFs that is suitable even for edge devices deployed in a safety critical system
- Methodology
  - Analysis of SRAM responses in terms of quality metrics (uniqueness, entropy, bit aliasing)
  - Designing of a low effort PUF module for COTS embedded devices
  - Provision of trusted services that rely on PUFs (i.e. code integrity check, key distribution and management) available to the VMs running on a hypervisor
  - Validation of performances and resilience against known attacks

PhD thesis (1/3)

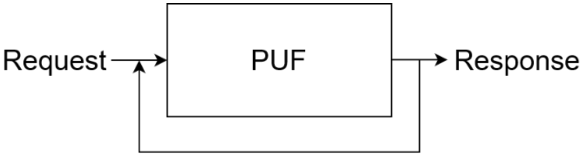


- A mixed criticality system architecture based on a hypervisor
- A PUF module provides root of trust for the entire system
- A safe boot loader extracts the hardware signature and authenticates the privileged code
- A mutual authentication protocol (Extended PHEMAP) generates authentication keys derived from PUF responses (key distribution and management) and delegate the authentication service

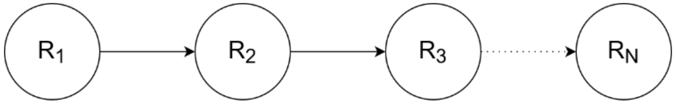
PhD thesis (2/3)



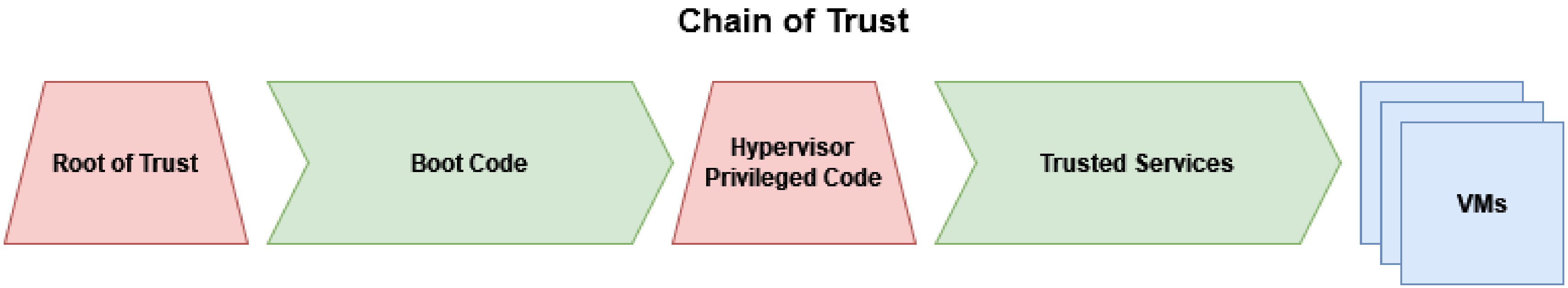
- The secure bootloader extracts the key from the SRAM response at power up
  - The key authenticates the hypervisor executable



- The PUF module, designed with the Pseudo PUF scheme, returns a unique response to a given request



- A privileged virtual machine manages the PUF module to construct authentication chains and issues authentication tickets for task specific services



PhD thesis (3/3)

- Pros:
  - A PUF circuite provides an unclonable hardware signature of the device. A similar approach relies on asymmetric encription and Endorsement keys
  - PUFs provide tamper evidence in case of manipulation
  - There is no need for asymmetric encryption nor key storage
- Cons:
  - PUF suffer from alteration provoked by extreme temperature

- The complexity of the PUF module is scalable:
  - Even a weak PUF (i.e., SRAM PUF one of the most available), can be enforced by mean of a symmetric cipher (Pseudo PUF) and behave like a strong PUF
  - There is no need for a custom architecture (i.e., FPGA, dedicated SoCs), just COTS microcontrollers
- Edge devices are mainly designed to operate industrial processes safely and reliably, but are not created with security in mind,
  - Neglected authentication, authorization and encryption requirements