UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II

itee PhD
information technology
electrical engineering

DIETI UNINA

PhD Student
Erasmo La Montagna
Presentation Title

Tutor: Prof. Nicola Mazzocca

Cycle: XXXV

Year: 1

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
    - Secure Key Generation
    - Mutual Authentication
  - Available technologies
    - Physical Unclonable Functions
    - Lightweight Encryption
    - Secure Cryptoprocessors (i.e. ARM TrustZone)

Summary of study activities

- Research:
  - Main focus on several fields of application of Physical Unclonable Functions
    - Physical Fingerprint and key generation
    - Challenge-Response Mechanisms for mutual authentication
    - Design of new architectures that are easier to obtain on edge devices
- Ad hoc PhD courses / schools:
  - Safety Critical Systems for Railway Traffic Management
  - Scientific Programming and Visualization with Python
  - Virtual Technologies and their Applications
  - Innovation Management, entrepreneurship and intellectual property
- Courses attended borrowed from MSc curricula:
  - Big Data Analytics and Business Intelligence
- Seminars

Research activity: Overview (1/2)

- Problem:
  - Many industrial monitoring systems make use of a Wireless Sensor Network(WSN)
  - Devices are deployed in unattended environment
    - successful attack to a sensor node can cause damage far beyond the single device
- Objective
  - Focus on a case of study (Power Delivery Network)
  - Discuss the attack model of such application
  - Identify flaws and overhead of classic authentication and encryption
- Proposed contribution
  - A different approach that does not rely on key-exchange protocols and encryption
    - Propose and extension of PHEMAP
  - Evaluate security concerns and communication overhead

Research activity: Overview (2/2)

- PUF architectures may have an excessive footprint and/or they may be hard to embed within actual devices
- Objective
  - Design of a PUF-based architecture (Pseudo-PUF) that can be successfully adopted in the IIoT context
  - Meet the existing requirements in terms of cost and resource demand
- Proposed contribution
  - A combination of a weak PUF and a symmetric cypher
  - Analyze the overall quality of different Pseudo-PUF instances with respect quality metrics

Products

[P1]	Conference Paper • Authors: M. Barbareschi, S. Barone, A. Fezza, E. La Montagna • Title: *“Enforcing mutual authentication and confidentiality in Wireless Sensor Networks using Physically Unclonable Functions: a case study”* • Conference Name: ICTSS 2020 • Status: submitted
[P2]	Paper • Authors: M. Barbareschi, V. Casola, A. De Benedictis, E. La Montagna, N. Mazzocca • Title: “*Pseudo-PUF: an Encryption-Based Challenge/Response Mechanism to enforce security in IIOT embedded devices”* • Journal: IEEE Transactions on Industrial Informatics • Status: draft (submission deadline on 30 October)

I year credits

	Courses	Seminars	Research	Tutorship	Total
Bimonth 1	0	1.6	8.4	0	10
Bimonth 2	3.3	0.2	6.5	0	10
Bimonth 3	2	0.4	7.6	0	10
Bimonth 4	15	4.1	0.9	0	20
Bimonth 5	4	0	6	0	10
Bimonth 6	0	0	7	0	7
Total	24.3	6.3	36.4	0	
Expected	30 - 70	10 - 30	80 - 140	0 – 4.8	