



UNIONE EUROPEA  
Fondo sociale europeo



# Seminario "Hardware Security and Trust"

Prof. Paolo PRINETTO  
Politecnico di Torino

## Abstract

The seminar aims at presenting the main issues related with **Hardware Security** (i.e., dealing with (secret) data in hardware devices) and **Hardware Trust** (i.e., dealing with design and manufacturing of hardware devices). In particular we focus on potential threads that can occur though the overall device life cycle, including design, production, test, and dismissal. Several example of real threads and counterfeitings will be presented. The concept of **PUF - Physically Unclonable Functions** (i.e., built-in mechanisms that generate one stable different ID for each identically-manufactured device) will then be introduced. The main feature of **SEcube™**, an Open Security Platform, and some examples of usage of the platform in protecting critical infrastructures will be presented.

## Paolo PRINETTO

- 01.11.1990÷today: Full professor of Computer Engineering at the Dipartimento di Automatica e Informatica of the Politecnico di Torino.
- 2004÷today: Adjoin Professor of the University of Illinois at Chicago, IL (USA).
- Research activities mainly focused on *Hardware Security, Digital Systems Design & Test, System Dependability, ICT and Assistive Technologies for people with disabilities*
- 2018÷today: Director of the CINI Cybersecurity National Lab.
- 2013÷today: President of CINI: Consorzio Interuniversitario Nazionale per l'Informatica.
- 2012: Honored of the title "Doctor Honoris Causa" of the Technical University of Cluj-Napoca (Romania).
- 2010÷2014: Member of the Scientific Committee of the French "Centre National de la Recherche Scientifique" (CNRS).
- 2013÷today Vice-Chair of the IFIP (International Federation for Information Processing) Technical Committee TC 10 - Computer Systems Technology.
- 2000÷2003 Elected chair (and 1998-1999: Elected vice-chair) of the IEEE - Computer Society TTTC: Test Technology Technical Council.

Taranto, 25 settembre 2018 - ore 9.30  
Via Alcide De Gasperi – Q.re Paolo VI

AVVISO PUBBLICO N. 3/PAC/2017  
Piano di Azione e Coesione approvato con Decisione C(2016)1417 del 03/03/2016  
Azioni aggiuntive per il rafforzamento dei corsi di studio innovativi erogati dalle Università pugliesi  
Determinazione Dirigenziale n. 755/2017 – BURP n. 68/2017 del 15/06/2017  
CUP: H91117000110002  
Progetto SI – Sicurezza Informatica