HASLab
HIGH-ASSURANCE SOFTWARE LABORATORY

Cryptography and Information Security

Hugo Pacheco
INESC TEC / HASLab

24 October 2018

INESCTEC

What are we?

- INESC => HASLab => Crypto+InfoSec
- Minimize the vulnerability of each software component from **hostile attacks** to computer systems by providing them with structures and **cryptographic protocols**, whose security properties are **formally proven**.

Who are we?

- **Professors**
  - Manuel Bernardo Barbosa - mbb@dcc.fc.up.pt
  - José Bacelar Almeida - jba@di.uminho.pt
  - José Manuel Valença - jmvalenca@di.uminho.pt
- **Post-Docs**
  - Hugo Pacheco - hugo.p.pacheco@inesctec.pt
  - Bernardo Portela - blfp@inesctec.pt
  - João Marco Silva - joao.marco@inesctec.pt
- **Docs**
  - Óscar Pereira - oscar.f.pereira@inesctec.pt
  - Tiago Oliveira - tiago.f.oliveira@inesctec.pt
  - Vítor Pereira - vitor.parreira.pereira@inesctec.pt

Hot Topics

- Secure Multi-party Computation
- High-Speed Cryptography
- Formal Verification
- Trusted Hardware
- Theoretical Cryptography

Projects

- 🇪🇺
  - PRACTICE (secure cloud framework) (FINISHED)
    - https://practice-project.eu/
  - SafeCloud (re-architect cloud infrastructures)
    - http://www.safecloud-project.eu/
  - LightKone (lightweight secure computation for edge networks)
    - https://www.lightkone.eu/
- 🇵🇹
  - SMILES (smart mobility; high-speed/high assurance crypto code)
  - NanoSTIMA (health care; secure data sanitization; secure SQL databases)
  - CloudSetup (secure cloud-based streaming services)

Overview

- Our **applied** research has two main focus:
  - Cloud-related techniques
  - IoT-related techniques
- Our **core** research focuses on:
  - designing new cryptographic protocols
  - formal verification of cryptographic code
- We also do some **consulting** for national agencies and multinational companies

Opportunities

- If you want to **know** more…
- Please contact **me** or one of our **team** members
- We will be **glad** to discuss some ideas and have you in our **team**
- Financial situation is comfortable, so there is room for **new applications**!

HIGH-ASSURANCE
SOFTWARE LABORATORY

IMPROVING PRACTICE THROUGH THEORY