French Ministry Of Defense

Cedric BARBOIRON & Romain XU

Platform Expertise
Electronics & Embedded Systems Lab.

Monday September 12th 2011

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Outline

1. Introduction: Working for the French M.o.D.
2. Cedric
3. Romain

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Outline

1 Introduction: Working for the French M.o.D.

2 Cedric

3 Romain

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Introduction: Working for the French M.o.D.

A department of the Ministry of Defense dedicated to cryptographic applications, with differences w.r.t. academics & private companies:

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Introduction:
Working for the French M.o.D.

A department of the Ministry of Defense dedicated to cryptographic applications, with differences w.r.t. academics & private companies:

- non-commercial: all applications for internal usage only
  → direct contact with all end-users.
  → special purpose applications, optimal for a given problem.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Introduction: Working for the French M.o.D.

A department of the Ministry of Defense dedicated to cryptographic applications, with differences w.r.t. academics & private companies:

- non-commercial: all applications for internal usage only
  → direct contact with all end-users.
  → special purpose applications, optimal for a given problem.
- non-profitable: reduce budget issues when submitting a research project.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Introduction: Working for the French M.o.D.

A department of the Ministry of Defense dedicated to cryptographic applications, with differences w.r.t. academics & private companies:

- non-commercial: all applications for internal usage only
  → direct contact with all end-users.
  → special purpose applications, optimal for a given problem.
- non-profitable: reduce budget issues when submitting a research project.

Young & dynamic work environment.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Outline

1. Introduction: Working for the French M.o.D.
2. Cedric
3. Romain

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Platform Expertise Team

- Goals:
  - Detect cryptography in a software.
  - Check the correctness of the implementation.
- Missions:
  - Reverse-engineering of cryptographic algorithms.
  - Development of custom tools.
  - Lab-deployment of software or equipment.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Tools

- Executable Static Analysis
  - Some tools: IDA Pro, Metasm, ...
  - And custom scripts.
- Dynamic analysis of a binary
  - Custom kernel debugger.
  - Tracing tools.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Benefits of my formation

- Ability to understand crypto algorithms.
- System security knowledge.
- Awareness of possible flaws.

Outline

1. Introduction: Working for the French M.o.D.
2. Cedric
3. Romain
   - Electronics & Embedded Systems Lab
   - Cryptographic blocks on Hardware
   - Research field
   - Benefits from my formation

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Electronics & Embedded Systems Lab

Small but balanced team dedicated to the development of ComSec devices on FPGAs:

- hardware (6 pers.): VHDL coding, board design.
- software (6 pers.): embedded code, driver, user API, validations tools.
- maintenance (1 pers.).

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Cryptographic blocks on Hardware

Implementation of high-performance, re-usable crypto-blocks on FPGAs:

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Cryptographic blocks on Hardware

Implementation of high-performance, re-usable crypto-blocks on FPGAs:

- asymmetric cryptography: state-of-the-art modular multiplication on Elliptic Curve over $\mathbb{F}_p$ using RNS representation.
- symmetric cryptography: AES, XTEA, etc.
- on-the-fly memory encryption and integrity protection for an embedded processor.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Cryptographic blocks on Hardware

Implementation of high-performance, re-usable crypto-blocks on FPGAs:

- asymmetric cryptography: state-of-the-art modular multiplication on Elliptic Curve over $\mathbb{F}_p$ using RNS representation.
- symmetric cryptography: AES, XTEA, etc.
- on-the-fly memory encryption and integrity protection for an embedded processor.

with various constraints:

- countermeasures against side-channels attacks (SPA, DPA, fault-injection, etc) depending on the security model.
- area.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Research field

Collaboration with academics on recent topics:

- evaluation of TRNGs based on ring-oscillators.
- applications of *Physically Unclonable Functions* (PUF) for design protection and secure key storage.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Benefits from my formation

ENSIMAG

- introduction to FPGAs and VHDL coding.
- high-performance algorithmics.

Benefits from my formation

ENSIMAG

- introduction to FPGAs and VHDL coding.
- high-performance algorithmics.

SCCI

- mathematical background behind Cryptography.
- secure architectures & protocols.
- introduction to side-channel attacks.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Questions ?

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE