Welcome to PROOFS!

PROOFS: “Security Proofs for Embedded Systems”

Introduction to the fourth workshop

Presentation Outline

1. Goal of PROOFS

2. Practical Aspects
   - Program
   - Invited Talks
   - Contributed Talks
   - Proceedings

Presentation Outline

1. Goal of PROOFS

2. Practical Aspects
   - Program
   - Invited Talks
   - Contributed Talks
   - Proceedings

What we intend to do:

- **For designers**: get more *confidence* in
  - security-oriented designs;
  - security-oriented CAD tools;
- **For evaluators**: do independent tests / attacks.

Presentation Outline

1. Goal of PROOFS

2. Practical Aspects
   - Program
   - Invited Talks
   - Contributed Talks
   - Proceedings

Program of the Day

- Overview
  - Two invited talks
  - Five contributed talks (3 regular, 2 short)

Invited talks

1. Jean-Louis LANET (INRIA):
   - “*Black hat can also benefits from formal method*”
2. Pascal CUOQ (TrustInSoft):
   - “*Formal verification at the source level that execution time does not depends on secrets — inasmuch as this means anything*”

Contributed talks (regular)

1. Shoei Nashimoto, Naofumi Homma, Yu-Ichi Hayashi and Takafumi Aoki:
    - “*Buffer Overflow Attack with Multiple Fault Injection and a Proven Countermeasure*”
2. Bruno Robisson, Michel Agoyan, Patrick Soquet, Sébastien Le-Henaff, Franck Wajsbürt, Pirouz Bazargan-Sabet and Guillaume Phan:
    - “*Smart Security Management in Secure Devices*”
3. Florian Lugou, Ludovic Apvrille and Aurélien Francillon:
    - “*Toward a Methodology for Unified Verification of Hardware/Software Co-designs*”

Contributed talks (short)

1. Sabine Azzi, Bruno Barras, Maria Christofi and David Vigilant:
   - "*Using Linear Codes as a Fault Countermeasure for Nonlinear Operations: Application to AES and Formal Verification*"
2. Laurent Sauvage, Tarik Graba and Thibault Porteboeuf:
   - "*Multi-Level Formal Verification, a New Approach Against Fault Injection Attack*"

- 8 submissions
- 16 PC members

Proceedings

- Soft copies can be downloaded from the website: http://www.proofs-workshop.org/program.html.

Login: `proofs2015` Password: `pwd_4_proofs2015`

- We would like the put presentation slides online
- Contributed talks can be revised and submitted for a JCEN special section on PROOFS

Journal of
Cryptographic
Engineering

wifi

- Network: CHES
- Password: ches2015