Welcome to PROOFS!

PROOFS:
“Security Proofs for Embedded Systems”

Introduction to the workshop

Presentation Outline

1. Goal of PROOFS
   - Security Calls for Quality
   - Bridge the gap between theoretical computer science and practical security
2. What are the Challenges?
   - Many Needs
   - Many Actors
   - Many Notions
   - Many TRLs
3. Practical Aspects
   - Program
   - Invited Talks
   - Contributed Talks
   - Proceedings

Presentation Outline

1. Goal of PROOFS
   - Security Calls for Quality
   - Bridge the gap between theoretical computer science and practical security
2. What are the Challenges?
   - Many Needs
   - Many Actors
   - Many Notions
   - Many TRLs
3. Practical Aspects
   - Program
   - Invited Talks
   - Contributed Talks
   - Proceedings

Security Calls for Quality

Formal methods at the rescue of implementation-level counter-measures

- Give more confidence in the protections (*i.e.* dual-rail, masking, leakage/fault- resilience, *etc.*)
  - require a formalization, hence a consistant description of the system (to have a chance to start with relevent specifications already)
  - allow a systematic check for common mistakes
- Accompany the development flow
  - enable early capture of crucial security aspects
  - feature tests for non-regression

From Theory to Practice

Theoretical Computer Science

- Has applied successfully formal methods to safety-critical systems
- Has developed efficient tools (model checkers, theorem provers, *etc.*)
- Already knows *templates* to solve problems

Practical Security

- Targets the implementation, hence *how* it is done is as relevant as *what* is done
- Models are difficult to setup, because they are either *too loose* or *too strict*

Presentation Outline

1. Goal of PROOFS
   - Security Calls for Quality
   - Bridge the gap between theoretical computer science and practical security
2. What are the Challenges?
   - Many Needs
   - Many Actors
   - Many Notions
   - Many TRLs
3. Practical Aspects
   - Program
   - Invited Talks
   - Contributed Talks
   - Proceedings

Many Needs

- Certification:
  - Common Criteria, `SPM`, `FSP` and `TDS`
  - FIPS, now ISO/IEC 17825 (following FIPS 140-3)
  - Related events: ”Workshop on Provable Security against Physical Attacks”;
  - ISO/IEC N10801_NWIP Standard, called “Cryptographic algorithms and security mechanisms conformance testing”.
- The academic community of side-channels has grown a lot, but in practice fault/alteration attacks are extremely powerful and thus of industrial importance.
  - Semi-invasive and invasive attacks also deserve formal treatment!

Many Actors

- “Functional designers”:
  - want to make correct designs
- “Security designers”:
  - want to be sure their protections are viable
- “Certifiers”:
  - want to assess an implementation

Many Notions

Proven methods, in cryptography, cover many concepts. We talk about security proofs in all those topics:

- Zero-knowledge protocols
- Proofs of cryptographic mechanisms, by reduction (for signature schemes, for instance)
- Proofs of cryptographic protocols: Dolev-Yao model, computational model, *etc.*
  - *e.g.* CertiCrypt or CryptoVerif in the computational model;
  - *e.g.* ProVerif or Avispa in the formal model.
- Formal security policies proofs in CC (Z, ACL2, Isabelle, B)
- Formal side-channel analysis (IT, “frameworks”, *etc.*)
- “Provable Security for Physical Cryptography”, by K. Pietrzak.
- Formal fault analysis (coverage rate, infective computations, fault-resiliency, *etc.*)
- Physical models for randomness assessment, PUF uniquity...

Many TRLs

Many Technological Readiness Levels

- Easy examples: OK
- Complete security policy: more difficult

Varied Interactions

- No bug found: formal methods are useless?
- One bug found: “the hard task is to fix it”

Presentation Outline

1. Goal of PROOFS
   - Security Calls for Quality
   - Bridge the gap between theoretical computer science and practical security
2. What are the Challenges?
   - Many Needs
   - Many Actors
   - Many Notions
   - Many TRLs
3. Practical Aspects
   - Program
   - Invited Talks
   - Contributed Talks
   - Proceedings

Program of the Day

- Overview
  - Three invited talks
  - Three contributed talks
  - One round-table
- The program is also in your booklet, at page 8.

Invited talks

1. Werner Schindler
   - “*Understanding the reasons for the side-channel leakage is indispensable for secure design*”
2. Naofumi Homma
   - “*Toward Formal Design of Cryptographic Processors Based on Galois Field Arithmetic*”
3. Graham Steel
   - “*Analysing Cryptographic Hardware Interfaces with Tookan*”

Contributed talks

1. Sébastien Briais, Sylvain Guilley and Jean-Luc Danger, Secure-IC and TELECOM-ParisTech
   - “*A formal study of two physical countermeasures against side channel attacks*”
2. Mark Brown, RedPhoneSecurity.com
   - “*Toward A Taxonomy of Communications Security Models*”
3. Maria Christofi, Boutheina Chetali, Louis Goubin and David Vigilant, Gemalto, Trusted Labs, University of Versailles Saint Quentin-en-Yvelines
   - “*Formal verification of an implementation of CRT-RSA Vigilant’s algorithm*”

- 5 submissions
- each is evaluated by 3 PC members
- 4 PC members if one PC member is co-author

EasyChair
conference system

Round-Table

Panelists

1. Werner Schindler, BSI and CASED, Germany
   - Responsible for the certifications in Germany.
2. Toru Hashimoto, IPA, Japan
   - Hardware evaluation, for CC and JCMVP.
3. Graham Steel, LSV, France
   - Security of cryptographic tokens.

Covered topics

- How to make formal proofs more widely used?
- How to break the ice between theoricians and practitioners?

Proceedings

- Hard copies are available in your conference bags
- Soft copies can be downloaded from the website:
  - http://www.proofs-workshop.org/proceedings/PROOFS_cover.pdf
  - Login proofs2012
  - Password ....password_4_proofs2012
- Our goal is to have formal proceedings
- Two options (not defined yet):
  1. Post-proceedings
  2. Joint volume, that gathers PROOFS 2012 & 2013