PROOFS:
Security Proofs for Embedded Systems
— Call for Papers —

Copyright: Marco Mertens

Leuven, Belgium — Thursday, September 13rd, 2012.

Important dates

Diffusion of the CfP	**Thursday February 16th, 2012**
Submission deadline	**Sunday May 27th (~~6th~~), 2012**
Authors notification	**Sunday July 8th (~~1st~~), 2012**
Final version due	**Sunday July 29th, 2012**
PROOFS workshop venue	**Thursday September 13rd, 2012**

Scope

The security of firmware (software or hardware) is challenged by a wealth of recent implementation-level exploits, that bypass security mechanisms.

(i) Side-channel attacks:
- secret extraction,
- high-value design recovery.

(ii) Perturbation attacks:
- protocol alteration,
- control flow modification,
- type confusion,
- critical instruction skipping,
- TRNG forcing,
- side-channel attacks enhanced by fault injection techniques,
- attacks targeting the cryptographic modules (DFA, DBA, FSA, FIRE, safe-error attacks).

(iii) Invasive attacks:
- malicious alteration of the control flow (*e.g.* Trojan insertion),
- malicious alteration of the datapath (*e.g.* the bug attack on RSA),
- design edition by means of FIB.

Many efforts have been devoted in the past years on these issues (either for attack or defense) when applied to cryptography. However, their effectiveness on the whole firmware (and associated protections) is an almost open topic.

Formal methods are used to increase the confidence level in system designs. They are customarily used for safety and dependability testing. The focus of the PROOFS workshop is the study of formal methods applied at the design stage with a view to preventing implementation-level attacks. As analog devices (random number generation, physically unclonable functions, *etc.*) are involved in some protection schemes, their experimental security proof are also emerging as a hot topic. Thus the workshop welcomes contributions in the following fields:

- **modelization of the threat**,
- **protections, with their formal proof (at algorithmic or at code-level)**,
- **resilience approaches to side-channel attacks**,
- **resilience approaches to perturbation attacks**,
- **resilience approaches to invasive attacks**,
- **formal verification of embedded software, at source code or assembly level**,
- **formal verification of VLSI designs, at RTL or netlist-level**,
- **formal verification of hardware designs of crypto algorithms**,
- **formal techniques for malicious circuits detection in embedded system**,
- **return on experiment about common criteria certification at EAL6 or EAL7**.

We invite submissions of high-quality papers describing original research related to proofs for security. We will not accept any paper which, at the time of submission, is under review for or has already been published or accepted for publication in a journal or another conference. We encourage works in progress or original initiatives, even if some further developments would be needed. The submitted articles must be anonymous: they shall not mention the authors, or obvious references to them. The layout must comply with Springer LNCS format. The page limit is 16. Up to 12 pages of additional supporting information may be provided, but committee members will read this information at their discretion, so the paper should be intelligible and self-contained within the 16 page limit required for the camera-ready version. The submission website is: https://www.easychair.org/conferences/?conf=proofs2012.

Committees

Programme Committee

- Alessandro Barenghi, Politecnico di Milano, Italy.
- Gilles Barthe, Fundación IMDEA Software, Spain.
- Loïc Correnson, CEA LIST, France.
- Emmanuelle Encrenaz, LIP6, France.
- Naofumi Homma, Tohoku U., Japan.
- Éliane Jaulmes, ANSSI, France.
- Gerwin Klein, NICTA, Australia.
- Debdeep Mukhopadhyay, IIT Kharagpur, India.
- Svetla Nikova, K.U.Leuven, Belgium.
- Renaud Pacalet, TELECOM-ParisTech, France.
- Bruno Robisson, ENSMSE, France.
- Timothy Sherwood, UCSB, USA.
- Graham Steel, LSV, France.

Steering Committee

- Sylvain Guilley, TELECOM-ParisTech, France.
- Çetin Kaya Koç, UCSB, USA.
- David Naccache, ENS, France.
- Akashi Satoh, AIST, Japan.
- Werner Schindler, BSI, Germany.

Local Committee

- Jean-Luc Danger, TELECOM-ParisTech, France.
- Svetla Nikova, K.U.Leuven, Belgium.
- Ingrid Verbauwhede, K.U.Leuven, Belgium.