J Cryptogr Eng (2017) 7:19–20
DOI 10.1007/s13389-016-0140-7

SPECIAL SECTION ON PROOFS 2015

Editorial about PROOFS 2015

Sylvain Guilley[1]

The goal of the International Workshop on Security Proofs for Embedded Systems (PROOFS) is to promote methodologies that increase the confidence level in the security of embedded systems. Formal methods for verification and safety are used in several related fields, such as software; however, the security of embedded systems, including cryptographic hardware and software, is often challenged by many attacks, particularly at the implementation level. Strategies to secure embedded systems are known, but they need to be implemented with care. The main objective of the PROOFS workshop is to bridge the gap between both topics and thus pave the way to verifiable *security by design* for embedded systems. The workshop is an opportunity for researchers of different fields to exchange on their work and also to present some innovative use cases and/or proofs of concept.

The fourth edition of the PROOFS workshop was held on Thursday September 17, 2015, at Saint-Malo, in France. As for all previous editions, PROOFS workshop is scheduled the day after Cryptographic Hardware and Embedded Systems (CHES), the flagship IACR conference on embedded systems security. The agenda of PROOFS 2015 has been aligned with the fourth workshop on secure hardware and security evaluation (TRUDEVICE), which has been held in parallel.

Interestingly, Saint-Malo was a particularly interesting and relevant location to host a security workshop. It is well protected city and was notorious for privateering (the "cité corsaire") in the past. Today the city is a major tourist destination, with many ancient, attractive buildings. Saint-Malo belongs to the French Brittany region, which is the home of the French excellence center for cybersecurity (the "PEC"—"Pôle d'Excellence Cyber"), an ecosystem where education institutes (graduate schools, universities, etc.), governmental organizations (defense procurement agency, cities, region, etc.) and companies (start-ups, SMEs, large corporations) collaborate to develop new cyber technologies.

The PROOFS workshop 2015 featured two invited talks:

- Jean-Louis Lanet (from INRIA, Rennes, France) gave a talk on the following topic: "black hat can also benefits from formal method."
- Pascal Cuoq (from TrustInSoft, Paris, France) talked about: "formal verification at the source level that execution time does not depends on secrets—inasmuch as this means anything."

The rest of the program included five contributed papers, selected out of eight submissions. The three best papers were offered a long slot (30 min each), and the other two papers were present in a smaller slot of 20 min. All these papers have been revised after the PROOFS workshop and improved notably to reflect the comments made by the audience in the *question and answer* session which followed the oral talks. After a second review process in the *Journal of Cryptographic Engineering*, the papers have all been accepted for publication. They appear in this special issue of the JCEN on PROOFS.

In order to increase social interaction within the PROOFS community, a welcome dinner is customarily organized on the eve of PROOFS. For PROOFS 2015, it took place at the nearby city Rennes, the capital of the region of Brittany.

The PROOFS workshop organizers are very indebted to the program committee for its hard work in reading, evaluat-

✉ Sylvain Guilley
sylvain.guilley@telecom-paristech.fr

[1] COMELEC Department, TELECOM-ParisTech, Institut MINES-TELECOM, 46 rue Barrault, 75634 Paris Cedex 13, France

ing and commenting the submissions. Each paper received at least three reviews. In total, the program committee produced 29 reviews, which brought some feedback to the authors of the submitted papers.

I would like to sincerely acknowledge the work of the program committee of PROOFS 2015, which was made up of: Naofumi Homma, Yongbin Zhou, Mehdi Tibouchi, Renaud Pacalet, Emmanuelle Encrenaz, François Dupressoir, Graham Steel, Alessandro Barenghi, Svetla Nikova, Marie-Laure Potet, Bruno Robisson, Chao Wang, Joan Daemen, Debdeep Mukhopadhyay, Loïc Correnson and Éliane Jaulmes. They were helped by seven sub-reviewers, I also thank a lot: Karine Heydemann, Durga Prasad Sahoo, Louis Dureuil, Guillaume Bouffard, Sikhar Patranabis and Rei Ueno.

Finally, I also thank the 40+ participants, who enjoyed the workshop in a nice conference room with a scenic view on the English Channel ("la Manche").

Sylvain Guilley,

Program chair of PROOFS 2015.