PANEL: THEORY OF IMPLEMENTATION SECURITY

Moderators:

Svetla Nikova, Vincent Rijmen

Ruggero Susella
Security Expert at STMicroelectronics, Italy

2017 – now	Manager of the Italian division of STMicroelectronics’ System Research and Applications Security R&D Team
2010 – 2017	Security Engineer at STMicroelectronics Advanced System Technology Security R&D Team
2007 – 2010	External Security Consultant at STMicroelectronics Advanced System Technology Security R&D Team
2007	MSc in Computer Science and Engineering at Politecnico di Milano (Technical Supervisor Guido Bertoni)

Our main activity is to contribute to the security of the company’s products (MCUs, PLC/BT modems, sensors, automotive, etc.):

- Security architecture definition
- Leading edge HW and SW cryptographic solutions
- Countermeasures against side channel and fault attacks
- Methodology for verification of countermeasures’ effectiveness during design and on silicon

Emmanuel Prouff

Deputy Head of the Embedded Security Lab at ANSSI, France

2017 – now Deputy Head of the Embedded Security Lab at ANSSI

2014 – now Associate Researcher at Sorbonne Université

2016 – 2017 Cryptography and Security Team Manager at Safran

2012 – 2016 Security Expert at ANSSI and Support to Common Criteria Evaluation at ANSSI

2008 – 2012 Cryptography & Security Research Manager at Oberthur Technologies

2004 – 2008 Researcher / Security Expert at Oberthur Technologies

Research areas: secure implementation of cryptographic algorithms and the security evaluation of embedded applications.

Ventzi Nikov, NXP Semiconductors
Technical Director in Innovation Center Crypto and Security

2004 – now Security Expert and Architect at Philips/NXP
2000 – 2002 Security Expert at ACUNIA

Areas:

- Secure implementations of cryptographic algorithms, countermeasures against SCA & FA
- Efficient implementations of cryptographic algorithms, low area/power/energy/latency

Topics:

- Industry perspective – efficient and balanced security approach vs all relevant attacks
- Provable vs. Practical Security, or Pro & Cons of provable secure designs
- How to efficiently test security of implementations, in particular TI provable designs
- Easier to first standardize the basics - Secret Sharing, MPC and TI

Junfeng Fan
Founder and CEO of Open Security Research, China

2014 – now CEO of Open Security Research (OSR)

2018 – now Guest master student supervisor at Tsinghua University

2013 – 2014 Lead of the hardware security lab of Nationz Technologies, China

2012 – 2013 Postdoc researcher, COSIC, KU Leuven

2007 – 2012 PhD student, COSIC, KU Leuven

Areas: secure implementation of cryptographic algorithms, security evaluation of embedded applications.

Topics:

- Chip industry feedback about “provable security” - It seems to be costly
- Do I need them if my chips were certified by CC EAL5+ already?
- Having a secure crypto component is nice - It would be even better if there is a way to design a “provably secure” system

Mike Hutter
Rambus Cryptography Research Division

2014-now Senior Principal Engineer & Tech Lead Crypto IP Cores
since 2016 Privatdozent (Applied Information Processing)
2011-2014 Post-doctoral researcher and lecturer at TU Graz (IAIK)
2008-2011 Lecturer and research assistant at TU Graz (IAIK), Austria

Areas: Side-channel Analysis, DPA Hardware Countermeasures, Fault Attacks, Embedded System Security & RFID/IoT

Topics:

- TI from an industry perspective: Provable vs. Practical Security: Pros & Cons of provable secure designs? Are practical tests/evaluations required/recommended and why?
- Practical Limitations: Customer-specific requirements (area, power, throughput, …). Attack space is broad – balance required to provide good protection (don’t forget weakest link)
- Requirements for quality of entropy for TI? How to test & standardize it?
- How to efficiently test security of TI implementations? TVLA testing, formal verification of TI gadgets, how to test compatibility requirements efficiently?

Nigel Smart
Professor at KU Leuven

- There is a strong link (in theory and practice) between TI and MPC
- Link is via secret sharing
- There is an ISO standard for secret sharing
  - *Relatively limited in scope*
- Would be good for NIST to also have a standard in secret sharing
- This would seem to be a pre-requisite for other standards in the area of TI and MPC
  - *Easier to standardize basic first*
  - *e.g. AES was done before the new modes etc*

- We can think of TI and MPC as changing protection boundaries
  - *In TI its now areas of a chip*
  - *In MPC its machines*
- What does this mean for traditional security standards based on physical boundaries which are easier to define?

Discussion Topics

- Certification of implementation methods
- Realistic adversary models for combined physical attacks
- Standardization of Threshold Crypto
- Provably secure countermeasures based on Threshold Crypto
- Quality of randomness
- Conclusions