

PASTIS 2010 : PAca Security Trends In embedded Systems

16th and 17th of June in Gardanne, France(13) :(Ecole des Mines de Saint-Etienne, Centre Microelectronique de Provence)

WORKSHOP

Security is a key component for information technologies and communication. It undoubtedly represents one of the main tools of its rise because it is the base to introduce confidence which is necessary for users. Among the security threats, vulnerability of electronic material that implements cryptography, for services of confidentiality, identification and authentication in particular, is perhaps the most important. Indeed, some unfaithful means, or attacks, on this material makes it possible to extract confidential information like encoding keys and thus to lower the performances of all the protected transmission chain of information. As the race engaged between the designer of secured circuits and systems and the evil-disposed people speeds up with the diversity of new systems, their opening and their multiplicity, it seems today a major stake in the security of the communication systems to improve hugely the tamper resistance of the components to these techniques of attack.

OBJECTIVES OF THE WORKSHOP

The main objective of these security days is to exchange around embedded security more precisely in experimental domain. Allowing to

- Share ideas.
- Identify security trends for the next 5 years.
- Exchange on advance practices in fault injection and side channel analysis.
- Define the future challenges in embedded security
- To initiate strong European cooperation

This workshop is strongly supported by "Secured Communicating Solutions" cluster and French funding organisation: ANR. It will be also the occasion to present our mutualised platform in security (Micropacks : <https://ssl.arcsis.org/cimpaca.html>). This platform lodges 6 different labs around security characterisation.

COVERED SUBJECTS

- Side channel attacks and countermeasures
- Fault attacks and countermeasures
- Hardware tamper resistance
- Tools and Methodologies
- Hardware architectures for public-key and secret key cryptographic algorithms
- Cryptographic processors and co-processors
- Hardware accelerators for security

Who should attend? People who are involved in:

- Secured design
- Cryptography
- Security Evaluation
- Secured characterisation
- Silicon manufacturing.
- CAD tools
- National and European experts in embedded security

IMPORTANT DATES

- May 31th 2010: Full paper / presentation / poster
- June 7th 2010 Final release (full paper or/and presentation)
- For PhDD student , you may submit poster

Materials have to be sent to: assia.tria@cea.fr

LOCATION

ENSMSE-CMP/SGC
880 avenue de Mimet,
13120 Gardanne.

REGISTRATION

Registration is free of charge but the number of attendees is limited. No on site registration!

Please fill in and send the [registration form](#) back by email to assia.tia@cea.fr

Accommodation and Travel Information will be available on request

Sergei SKOROBOGATOV (Cambridge university) : **Fault attacks on memories**

Geert-Jan SCHRIJEN (IntrinsicID) : **PUFs and Their Use for IP Protection**

Michael TUNSTALL (Bristol) : **Using Templates to Distinguish Multiplications from Squaring Operations**

Marc JOYE : **Highly regular algorithms and side-channel attacks**

Sylvain GUILLEY (ENST): **Combined countermeasures against perturbation & observation attacks**

Philippe NGUYEN (Secure IC): **Pinpointing the leakage of cryptographic circuits with an illustration on dual-rail logics**

Benoit FEIX (Inside contactless) : **Combined attacks**

Hamadou SERE (XLIM) : **Checking the Paths to Identify Control Flow Modification on Embedded Systems**

François VACHERAND (CEA-LETI)/ **Philippe LALEVEE** (ENSMSE) : **Contactless : Attacks and countermeasures**

Nathalie FEYT (CEA-CI Thales) : **Hard/Soft combined attacks : a research axe for the security.**

Amir-Pasha MIRBAHA (ENSMSE) : **Reproducible Single-Byte Laser Fault Injection**

Victor LOMNE (LIRMM) : **A Simulation Flow for Time Domain Magnetic Radiations of ICs**

Bruno ROBISSON (CEA-LETI) : **SOS/SOS**

Thanh-ha LE (Sagem) : **Different approaches to perform Mutual Information Analysis**

Yann LOISEL (MaximmIC) : **Can attacks on terminals chips inherit from smart cards attacks ?"**

Antoine REVERDY (Sector-technologies) : **Failure analysis techniques targeted for security investigations**

Olivier BENOIT/Jean-jacques DELORMES (Ingénico) : **Terminals Security & Solutions**

Alexandre BERZATI (CEA-LETI) : **Fault attacks on public key cryptosystems**

June 16	June 17
9h30-9h30 : WELCOM + Coffee	9h30-9h30 : WELCOM + Coffee
9h30-10h30 Sergei SKOROBOGATOV	9h30-10h30 : Geert-Jan SCHRIJEN
10h30-11h00 : Nathalie FEYT	10h30-11h00 : Olivier BENOIT
11h00-11h30: Sylvain GUILLEY	11h00-11h30 : Philippe NGUYEN
11h30-12h00: Marc JOYE	11h30-12h00: Amir Pasha MIRBAHA
12h00-12h30 : Hamadou SERE	12h00-12h30 : Antoine REVERDY/ Daniel ARIAS
12h30-14h00 ; LUNCH	12h30-14h00 ; LUNCH
14h00-14h30 : Alexandre BERZATI	14h00-14h30 : Victor LOMNE
14h30-15h00 : Michael TUNSTALL	14h30-15h00 : Bruno ROBISSON
15h00-15h30 : Thanh-ha LE	15h-15h30 : Yann LOISEL
15h30-16h00: François VACHERAND	15h30-16h00 : Benoit FEIX
16h00-16h30 Coffe Break	
16h30-17h30 Security labs visit	
19h30 social event	