



www.emse.fr



Confiance et Privacy

Institut Henri Fayol / ISCOD



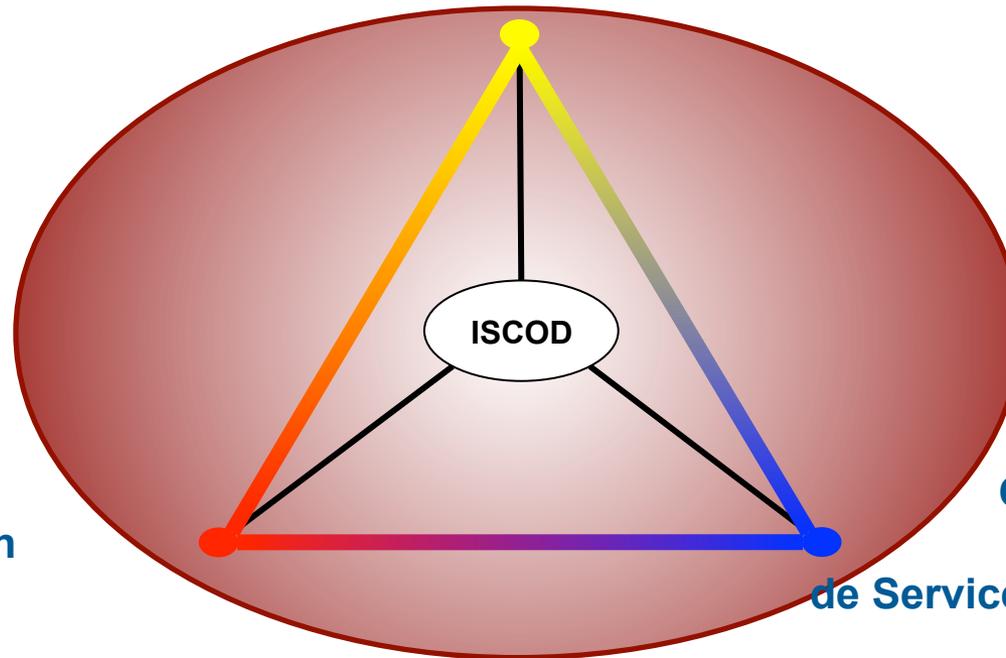


Thématiques scientifiques & Thématiques applicatives

Confiance & Privacy
dans la société numérique

Entreprises
Numériques

Conception
de
Systèmes
Complexes



Accès &
Représentation
de Contenus
Numériques

Coordination &
Adaptation
de Services Numériques

Permanents (2 PR, 7 MC)
MA Associé (1) PostDocs (2)
Doctorants (10)

Territoires et Villes
Intelligentes



Thème « Confiance & Privacy »

- La compréhension des mécanismes de confiance est devenue un problème important avec l'usage grandissant d'internet.
 - La confiance entre deux inconnus n'est pas établie *a priori*, il faut créer les moyens de son existence.
- Mots clefs : confiance mutuelle, négociation, *privacy*.



Une définition

- **Faire confiance, c'est accepter de prendre un risque.**
 - Cela n'a vraiment de sens que lorsque il est nécessaire de prendre une décision que l'on pourrait regretter.

Basée sur les travaux de Nikklas Luhmann.



Points importants

- **Décentralisation des différents aspects**
 - Les données, les politiques et la prise de décisions.
- **Source de la confiance**
 - Utilisation de toutes les informations disponibles : qualifications, réputation, recommandation, expérience personnelle, risque, coût, utilité, plaisir, désir...
- **Expression de la politique**
- **Respect de la vie privée (*privacy*)**



Travaux

- **Socialy Compliant Trust Management System.**
 - Dans le cadre des communautés virtuelles.
 - Gestion des politiques individuelles.
 - Gestion des politiques collectives.
 - Assurer la cohérence des décisions dans ce contexte.
 - Evolution des politiques.

Reda Yaich (thèse à soutenir en 2013)



Travaux (suite)

- **PrivaCIAS :**
respect de vie privée dans les réseaux sociaux décentralisés
 - Mécanismes non-intrusifs et extensibles
 - Théorie de l'intégrité contextuelle (Nissenbaum 04)
 - Application au partage de photos dans un réseau social :
 - Alarmes lorsque l'utilisateur ne respecte pas les politiques.
 - Empêcher la propagation des violations de la vies privée.
 - Punissions des contrevenants.
 - Démonstrateur Android (Ciortea 2011)

Yann Krupa (Thèse 2012)



Travaux (suite)

- **Négociation de la confiance dans un environnement ouvert**
 - La confiance s'établit tout au long de la transaction.
 - Satisfaction simultanée de la politique de toutes les parties en présence.
 - Basé sur l'observation des comportements.
 - Tire profit de l'expérience, du risque...
 - Approche logique : PP-LTL + Event Structure.

Hoan Vu (thèse 2010)



Contacts

- « Confiance & Privacy » @ ISCOD/institut Henri Fayol
 - Olivier Boissier, Philippe Jaillon, Roland Jégou, Gauthier Picard, Xavier Serpaggi, Reda Yaich.

email : prénom.nom@emse.fr

<http://fayol.emse.fr/>



Méthodes INovantes pour l'Entreprise et la Société



<http://cmp.emse.fr/>

Center of Microelectronics in Provence

June 2013



“Designing, prototyping and integrating innovative and secure microelectronic technologies and devices”
“Pioneering microelectronics for applications in flexible electronics, secure hardware, bioelectronics and logistics”



Georges Charpak Campus
Gardanne



SAS Department (Secured Architectures & Systems)

CEA/EMSE joint team



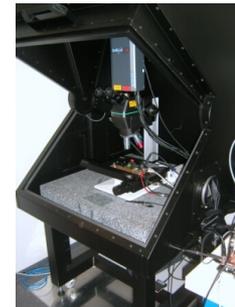
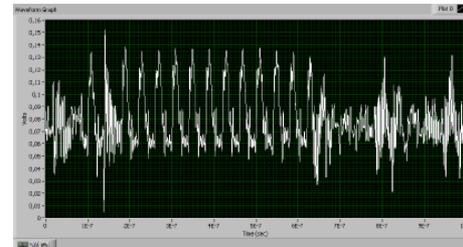
- **Head:** Assia Tria (CEA), Bruno Robisson (CEA)
- **Staff:** 26
 - 5 faculty members, 4 research engineers (CEA), 4 contract researchers, 1 engineer, 12 PhD students





Research axis

- Protect circuits (such as smart card) against physical attacks such as
 - Perturbation attacks (differential fault analysis, modification of algorithms, safe-errors, etc.)
 - Observation attacks (differential power/EM analysis)
- Ensure the secure integration of these circuits in complex systems,
- Design advanced cryptographic functions (elliptic curves, pairing, etc.)
- Design top of the art attacks tools and anticipate future attacks.





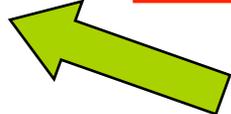
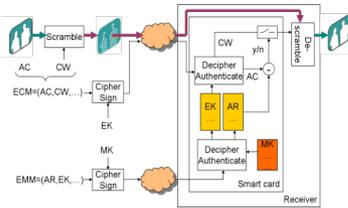
Approach

Physical cryptanalysis

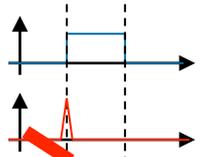
Security lab

Security characterization

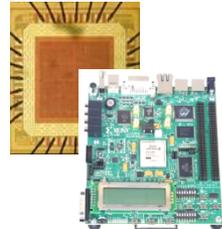
Specifications



Modeling

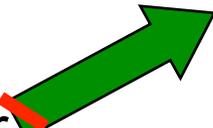
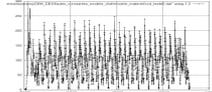
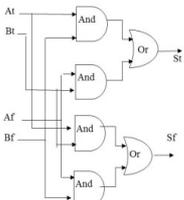


Circuits and prototypes



Protections

Add ons for CAO tool



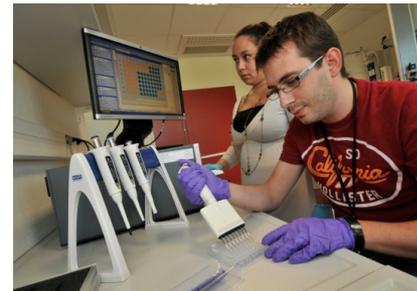
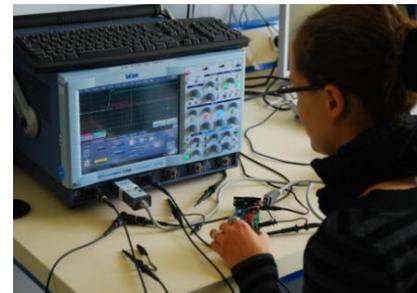
Design



Facilities



- **Collaborative R&D platform** (Micro-PackS platform)
 - 620 m² + 160 m² (2012)
 - 100 / 1000 / 10000 class
 - **Micropackaging prototyping line**
 - ✓ 300mm grinder, saw, wire bonders, pick & place, ...
 - **4 Inkjet printers**
 - ✓ MicroFab, Dimatix, Ceradrop, Jetpac
 - **Microfabrication**
 - ✓ Photolithography, PVD, RIE, ...
 - **Physical & electrical characterizations**
 - ✓ SEM, AFM, Raman, X-ray tomography, acoustic microscope, spectro ellipsometry, probe stations, I-V & C-V characterisation,....
- **Security Labs** (Micro-PackS platform)
 - **Attack benches: laser, DPA, EMA, ...**
- **Bioelectronics Labs**
 - **Biology labs including cell culture**
 - **Integration with microelectronic devices**





INSPIRING INNOVATION | INNOVANTE PAR TRADITION



FEDER - FSE





www.emse.fr



Merci de votre attention

