



# How to Teach Hardware Security ?

*Lilian Bossuet, Guy Gogniat*

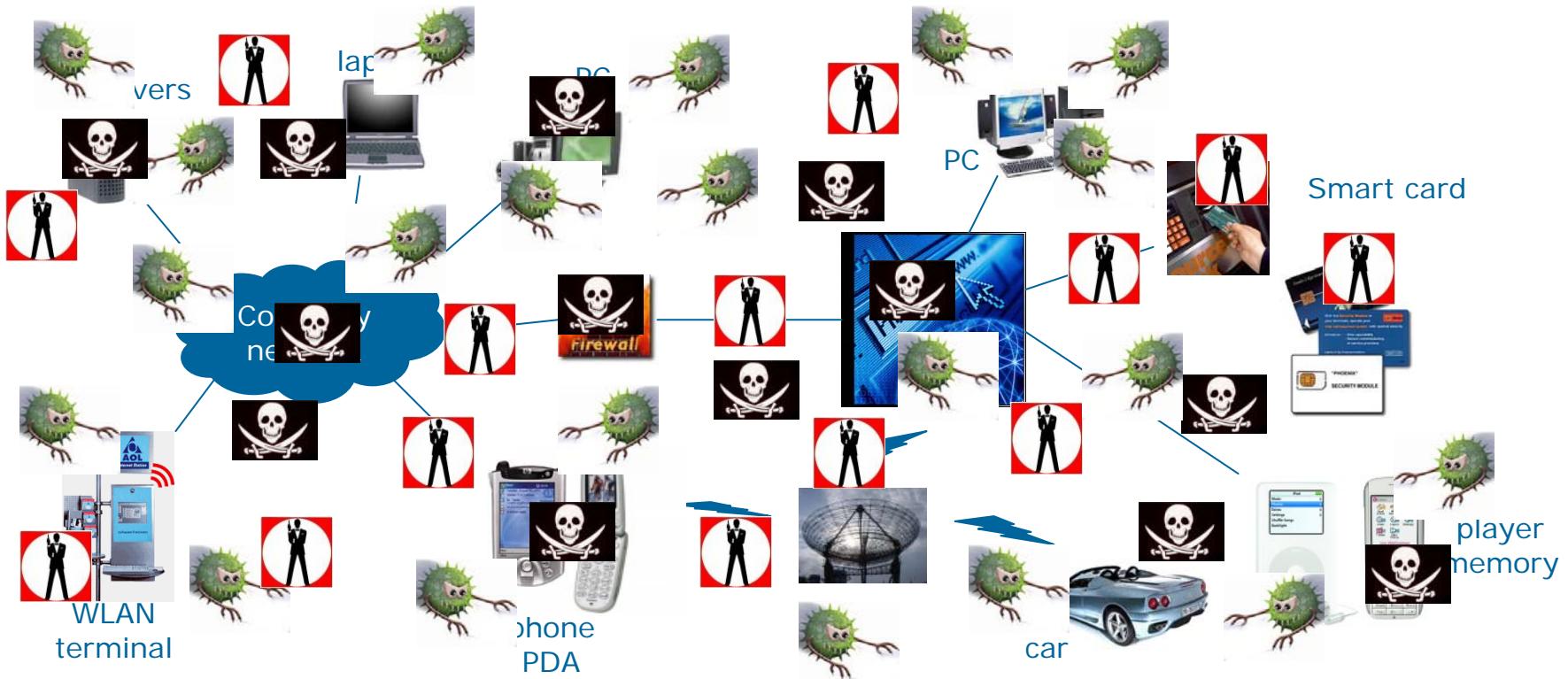
# In 2006, the story begins ...

- I had obtained a new position as an Associate Professor in an engineering school
  - ➔ Ecole Nationale Supérieure de l'Electronique, Informatique et Radiocommunication
- Since 2006 I'm in charge of several courses
  - ➔ Digital systems design
  - ➔ Digital communication
  - ➔ Digital IC : FPGA, microprocessor
  - ➔ FPGA for DSP
  - ➔ FPGA for telecommunication
  - ➔ **Hardware security ...**
- How to present and to give a good course focussing on hardware security?????

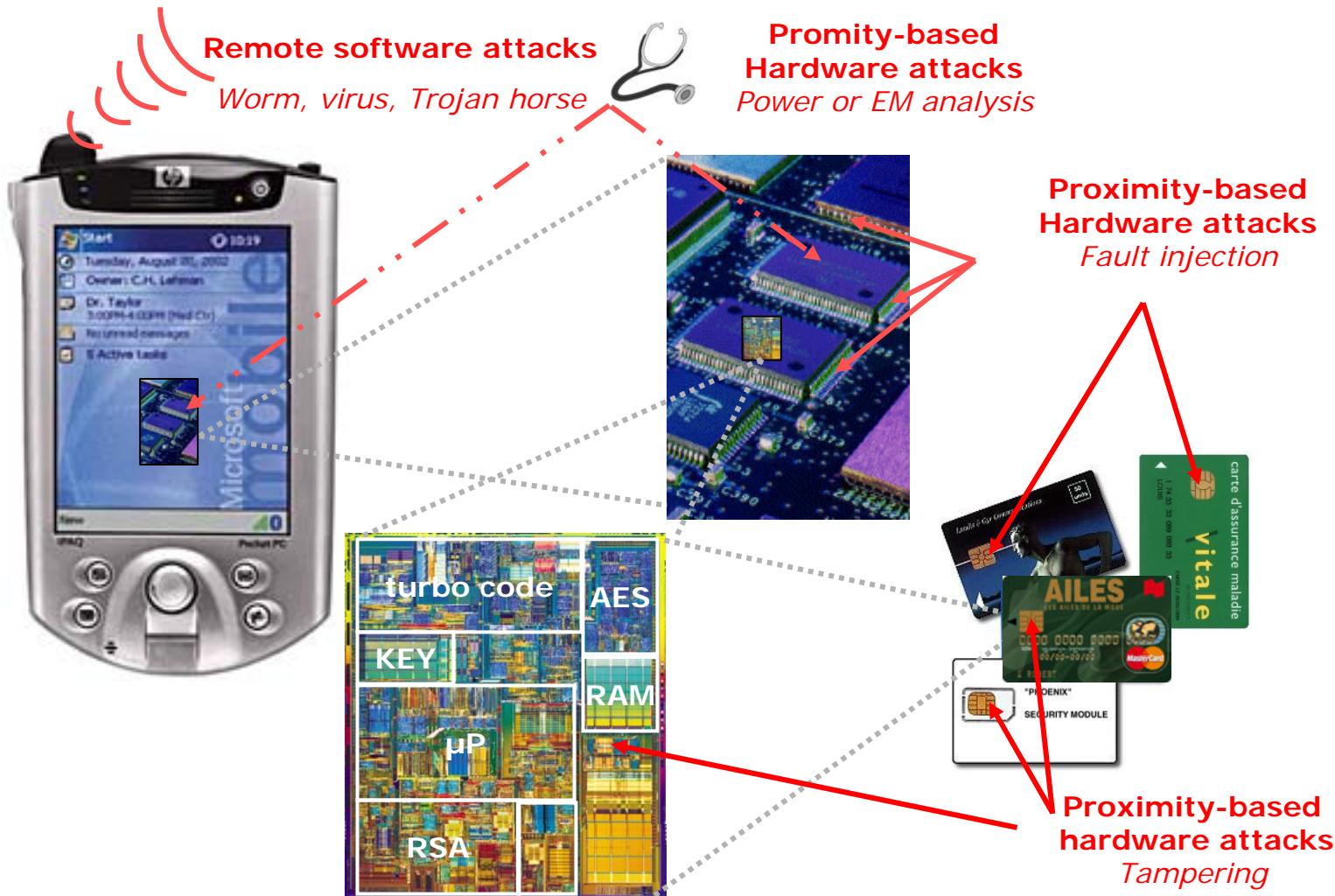
# Outlines

- The rise of hardware security
- How to dazzle students?
- An example of common emulation for teaching, the Bordeaux-Lorient project
- Now, what can we do?
- Conclusion & Discussion ...

# Welcome in a secure world???



# Attacks on embedded system



# Many sensitive data will be embedded



## DALLET Dominique

Maître de conférences, département Télécommunications,  
responsable des stages industriels de 2e année au département  
Télécommunications

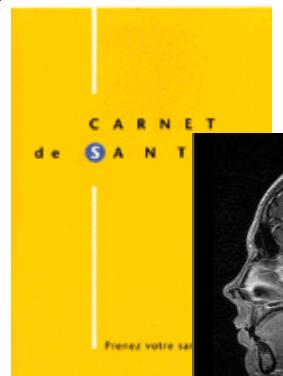
poste : 23 40      fax : 05 56 37 20 23      S 307

Dominique.Dallet@enseirb.fr

**IXL** Responsable de l'équipe Métrologie de la conversion  
de données

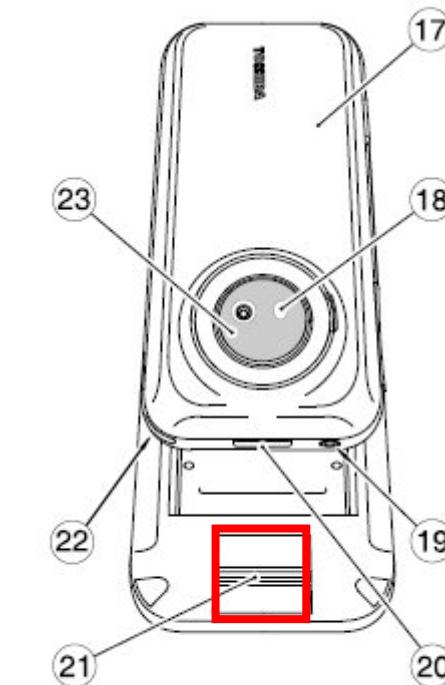
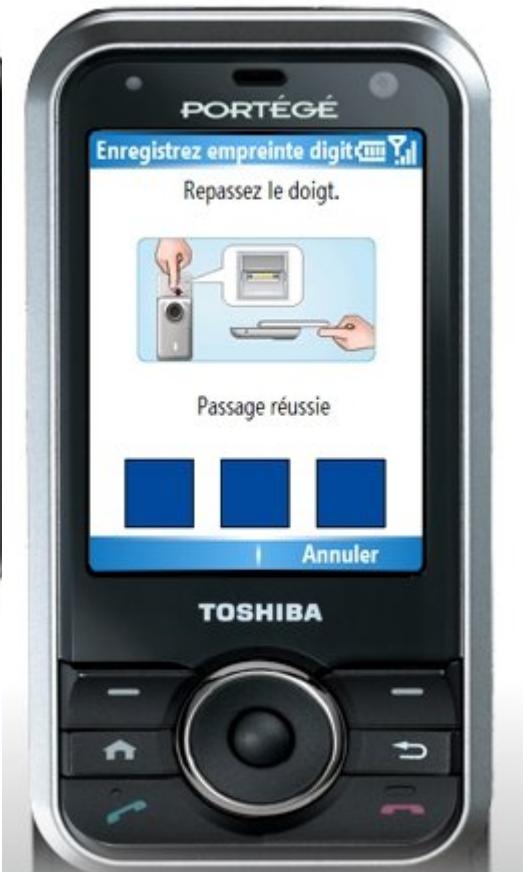
tél. 05 40 00 26 32      fax : 05 56 37 15 45

dallet@ixl.fr



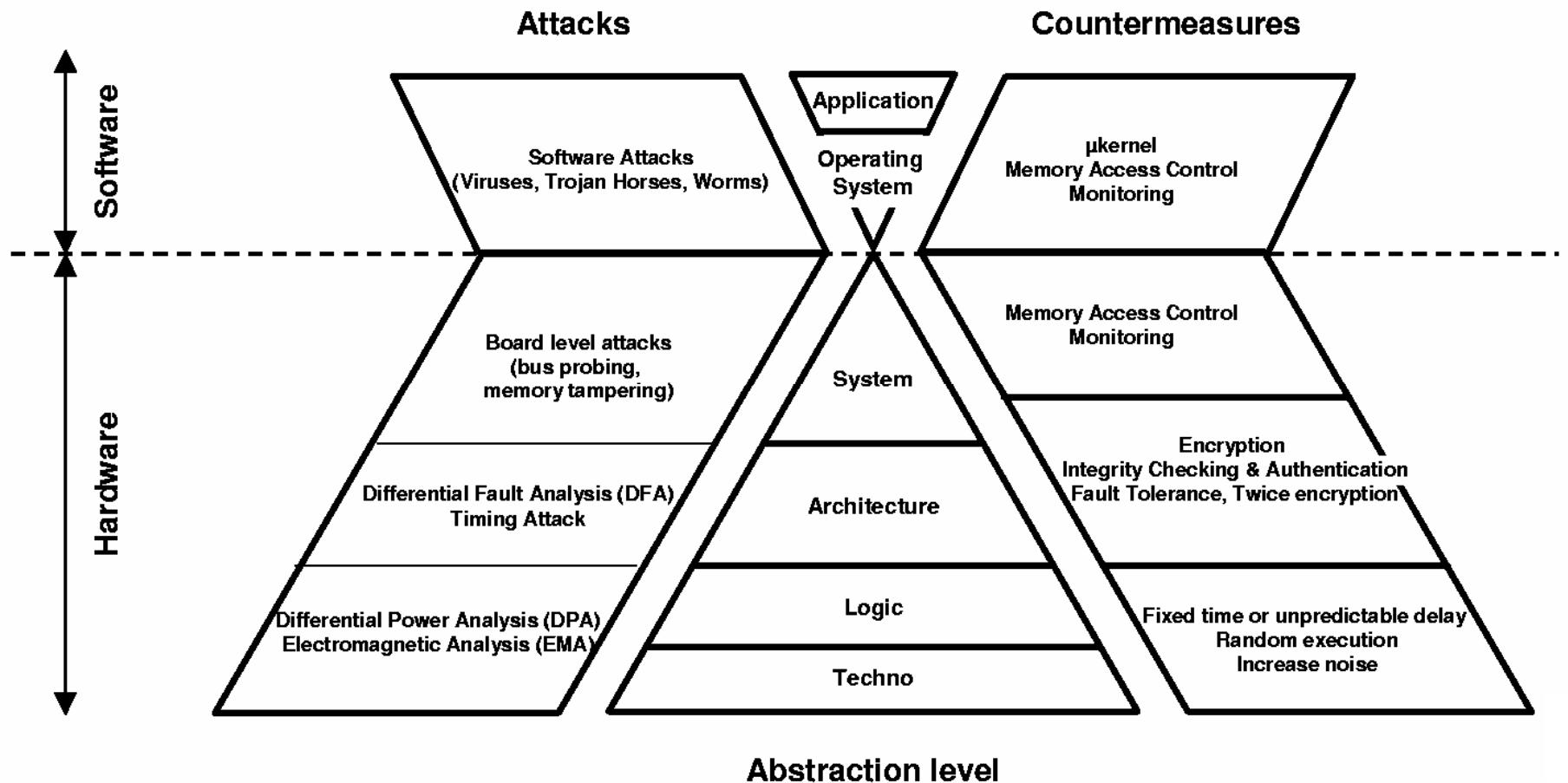
# Exemple of available embedded biometric system

- Toshiba proposes a biometric ID authentication system embedded in new smart phones G500 & G900
- The fingerprint scanner is on the back



# It is time to teach security for engineers

- Not only specialized on software security
- Good knowledge on software and hardware issues, embedded systems, digital systems design ...



# Outlines

- The rise of hardware security
- **How to dazzle students?**
- An example of common emulation for teaching, the Bordeaux-Lorient project
- Now, what can we do?
- Conclusion & Discussion ...

# Embedded in a student brain ...

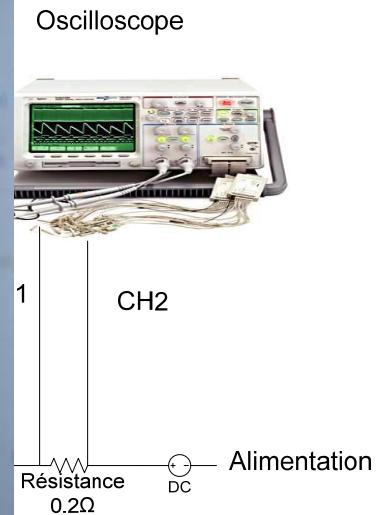
- Students are not always excited to study ...



- But there are enthusiasm to security system



- Actually, it is job to interest security !



# Some solutions ...

- Student projects: cryptographic core implementation
  - ➔ Performances competition: area, throughput, power
  - ➔ Example of George Mason University master students project by Kris Gaj
- Lab on attacks on AES in FPGA
  - ➔ SPA and DPA application
  - ➔ Development on actual countermeasures
- Bibliographical project
  - ➔ Short paper on state of the art
  - ➔ Web site
  - ➔ Example of University of South Brittany master students project by Guy Gogniat

# Example 1: Embedded System Security

The screenshot shows a Mozilla Firefox browser window with the title "Introduction - Mozilla". The address bar displays the URL <http://dafrac6.100webspace.net/Introduction.htm>. The main content area features a red header "Sécurité des systèmes embarqués". On the left, a sidebar menu includes "Introduction" (selected), "Attaques", "Cryptage", "Partitionnement", "Sot physique", and "Contact". The main text discusses the challenges of securing embedded systems due to economic factors and the widespread use of new technologies. It emphasizes the need for effective security measures like authentication, integrity, confidentiality, non-repudiation, and certification. A small image of a handheld device (PDA or smartphone) is shown on the right. At the bottom, a footer note mentions factors that add to the challenges of securing these systems.

Bienvenue: moniteurs matériels pour la sécu... Introduction

## Sécurité des systèmes embarqués

En ces temps de mauvaise conjoncture économique et avec l'utilisation agressive des nouvelles technologies déployées sur des réseaux sans fils, personne n'est épargné des attaques électroniques et de l'espionnage informatique. Toutes les enseignes économiques, qu'elles soient un gouvernement, une entreprise ou même une simple personne, cherchent à se procurer des informations sur leurs principaux concurrents par tous les moyens légaux et illégaux. Ainsi le monde des affaires actuel exige la mise en place des dispositifs d'intégrité et de cryptage afin d'assurer une bonne concurrence et de protéger la vie personnelle des utilisateurs.

La mise en place d'une sécurité efficace, requiert la protection d'accès sur les dispositifs et sur les réseaux, la sécurisation des informations lors des échanges au travers des réseaux publics ou privés, ainsi que la protection des informations confidentielles enregistrées sur le système.

Et pour restreindre la vulnérabilité d'un tel système, il doit garantir:

- L'**authentification** réciproque des correspondants pour identifier son interlocuteur.
- L'**intégrité** des données transmises pour être sûr qu'elles n'ont pas été modifiées accidentellement ou intentionnellement.
- La **confidentialité** des échanges pour éviter que les données soient lues par des systèmes ou des personnes non autorisées.
- La **non répudiation** ou **Notariat** qui évite la contestation par l'émetteur de l'envoi de données.
- La **Certification** qui confirme l'identité d'un interlocuteur grâce à une signature.

La plupart des nouvelles technologies (électroménager, robot, automobile, PDA, carte à puce ...) sont des systèmes embarqués, car ils exécutent des tâches prédefinies, et ils respectent les contraintes d'un cahier de charge spécifique. Avec les progrès technologiques constants, les **systèmes embarqués** devient plus communicants et échangent des données sensibles, d'où la nécessité de sécuriser les informations manipulées.

Pour de tels systèmes, il y a plusieurs facteurs qui ajoutent d'autres contraintes et qui augmentent les **challenges**.

<http://dafrac6.100webspace.net/Introduction.htm>

# Example 2: Hardware Monitoring for System Security

The screenshot shows a Mozilla Firefox browser window with the following details:

- Title Bar:** Bienvenue: moniteurs matériels pour la sécurité des systèmes embarqués - Mozilla
- Menu Bar:** Fichier, Edition, Affichage, Aller à, Marque-pages, Outils, Fenêtre, Aide
- Toolbar:** Précédent, Suivant, Actualiser, Arrêter, http://monitor4security.free.fr/, Rechercher, Imprimer
- Content Area:**
  - Logo:** UBS logo (University of Bretagne-Sud)
  - Title:** Moniteurs matériels pour la sécurité des systèmes embarqués
  - Text:** Anthony Barreteau et Régis Lebreton, étudiants en dernière année du Master Recherche MARS (Microtechnologies Architecture Réseaux & Systèmes) à l'université Bretagne-Sud de Lorient, vous présentent leurs travaux (état de l'art) sur les moniteurs matériels destinés à sécuriser les systèmes embarqués. Ce site est en complément de la soutenance qui ce déroulera le 18 janvier 2007 à l'INSA de Rennes, en collaboration avec l'INSA, SUPELEC de Rennes, l'ENST Brest, ainsi que les laboratoires de recherches IETR et le LESTER.
  - Section I- PRESENTATION DES SYSTEMES EMBARQUES:**
    - Definition:** Un système embarqué est un système électronique qui est complètement intégré au système qu'il contrôle. Il est soumis à diverses contraintes (surface, autonomie, puissance de calcul).
    - Domaines d'applications:**
      - Transport: automobile, aéronautique ...
      - Astronautique: fusée, satellite ...
      - Militaire: missile...
      - Télécommunication: téléphone portable...
- Right Side:** L.E.S.T.E.R. logo (Laboratoire d'Électronique des Systèmes Temps Réel) with flags of various countries.
- Bottom Right:** Image of an Airbus A380 aircraft.

<http://monitor4security.free.fr/>

# University George Mason - Kris Gaj

## ■ Student projects on Secure Telecommunications Systems

The screenshot shows a Mozilla Firefox browser window with the following details:

- Title Bar:** ECE 746 Secure Telecommunication Systems - Mozilla Firefox
- Menu Bar:** Fichier, Édition, Affichage, Historique, Marque-pages, Outils, ?
- Address Bar:** http://ece.gmu.edu/courses/ECE746/
- Toolbar:** Back, Forward, Stop, Home, Refresh, Stop, Google search bar.
- Page Content:**
  - Header:** ECE 746, Secure Telecommunication Systems, Fall 2006, Wednesdays, 4:30-7:10 PM, Robinson Hall A, room 249.
  - Instructor:** Kris Gaj, kgaj@gmu.edu
  - TA:** Chang Shu, cshu@gmu.edu
  - Announcements:** Final Project Presentations, Dec. 18, 2006; Project Presentations and Final Reports - Fall 2006.
  - Navigation:** Lecture, Viewgraphs, Project, Lab, Literature, Homework, Exams, Web Resources.
- Status Bar:** Terminé

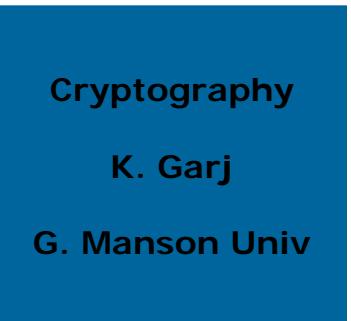
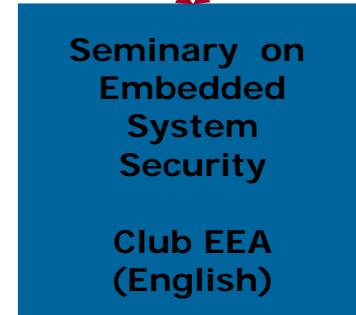
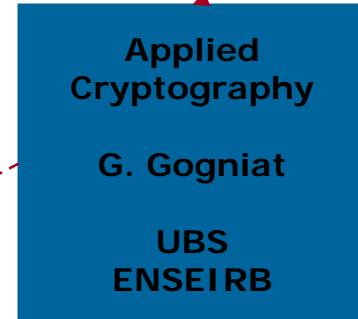
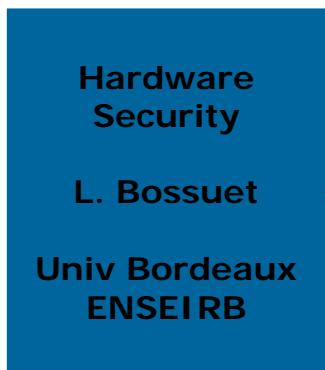
<http://ece.gmu.edu/courses/ECE746/>

# Outlines

- The rise of hardware security
- How to dazzle students?
- **An example of common emulation for teaching, the Bordeaux-Lorient project**
- Now, what can we do ?
- Conclusion & Discussion ...

# Course history

To give is not to loose !!!!



# Embedded system security course or seminar

## ■ Outlines

- ➔ Introduction to Security (software aspects)
- ➔ Data Confidentiality, Integrity and Availability
- ➔ Applied Cryptography
- ➔ Introduction to Embedded System, Security aspects
- ➔ Attacks on Embedded Systems –Case Study: DPA on AES in FPGA
- ➔ Countermeasures (from system to technological level)
- ➔ Reconfigurable Hardware System for Security
- ➔ Case Study: FPGA Bitstream Encryption
- ➔ Presentation of Research Works (Hardware Secure Architecture)
- ➔ Hardware Programmable System for Security (Example of TPM)
- ➔ Presentation of Research Works (Software Secure System)

**Software Security**

**Cryptographic**

**Embedded System**

**Security**

**Reconfigurable Hardware**

**with Security**

**Programmable System**

**with Security**

# Embedded system security course evolution ...

- Will be integrated in the course?

- ➔ Explore mathematical background: Groups, Rings, and Field
- ➔ Some aspects of software security
- ➔ IPP: IP protection (IP soft to IP hard)
- ➔ Network and telecommunication security (applied to embedded system)
- ➔ Biometric aspects: Applications, systems ....
- ➔ Applications of security (smart card ...)
- ➔ ....

# Outlines

- The rise of hardware security
- How to dazzle students?
- An example of common emulation for teaching, the Bordeaux-Lorient project
- **Now, what can we do?**
- Conclusion & Discussion ...

# Proposition...

- A web site for teachers and students (reminder : to give is not to loose)
- A Summer school on embedded system security
- A handbook on embedded system security ?

# Web site?

- Open access / restrictive access (both) to crypt'archi community?
- Contain
  - ➔ Courses
  - ➔ Lab
  - ➔ Exams
  - ➔ Documents
    - Survey
    - Standard
    - Presentations and articles
  - ➔ List of reference books
  - ➔ Link
- E-learning
  - ➔ Video stream
  - ➔ ...

# Summer school on embedded system security

- ENSEIRB is ready to welcome a summer school on embedded system security
- All aspects have to be shown (not only hardware)
  - ➔ Applied Cryptography
  - ➔ Software security focussing on embedded system OS, smart card ...
  - ➔ Hardware security for embedded systems, attacks and countermeasures
  - ➔ Bioware aspect?
  - ➔ Very open ...
- Need to find sponsors !

# Handbook on embedded system security

- Contain?
  - ➔ Essential to know for a master student ...
- Outlines?
- Who will be interesting to write a chapter?
- Editor?

# Outlines

- The rise of hardware security
- How to dazzle students?
- An example of common emulation for teaching, the Bordeaux-Lorient project
- Now, what can we do?
- **Conclusion & discussion ...**

# So, how to teach hardware security ?

- We have shown that it is a very interesting topic for students
- But it is really a large space of teaching !
- So, we need to merge our work to be efficient
- We need to propose new tools to improve this teaching domain





# How to Teach Hardware Security ?

## Thank You

*Lilian Bossuet, Guy Gogniat*

*[lilian.bossuet@ims-bordeaux.fr](mailto:lilian.bossuet@ims-bordeaux.fr)  
[guy.gogniat@univ-ubs.fr](mailto:guy.gogniat@univ-ubs.fr)*

*[questionnaire](#)*