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

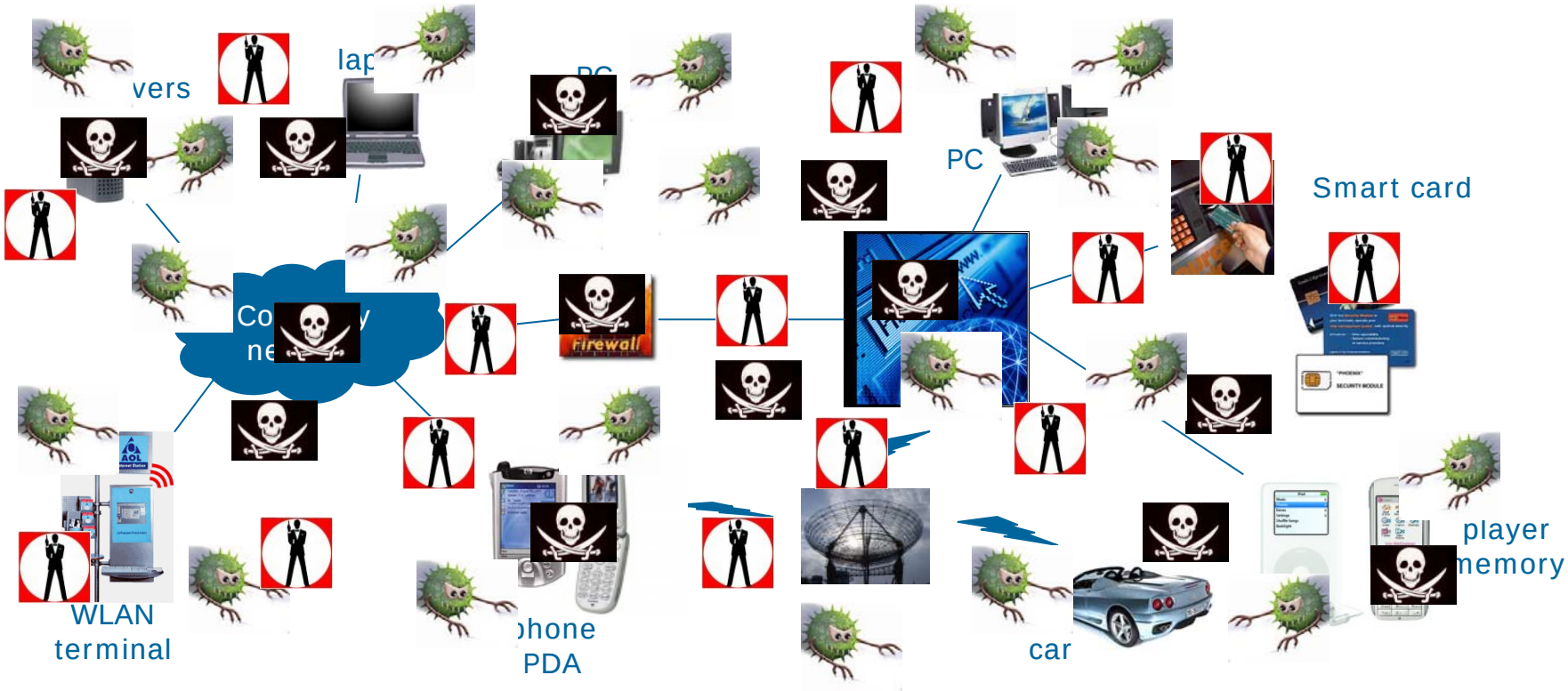
- Since 2006 I'm in charge of several courses
  - ➔ Digital systems design
  - ➔ Digital communication
  - ➔ Digital IC : FPGA, microprocessor
  - ➔ FPGA for DSP
  - ➔ FPGA for telecommunication
  - ➔ **Hardware security …**

- How to present and to give a good course focussing on hardware security?????

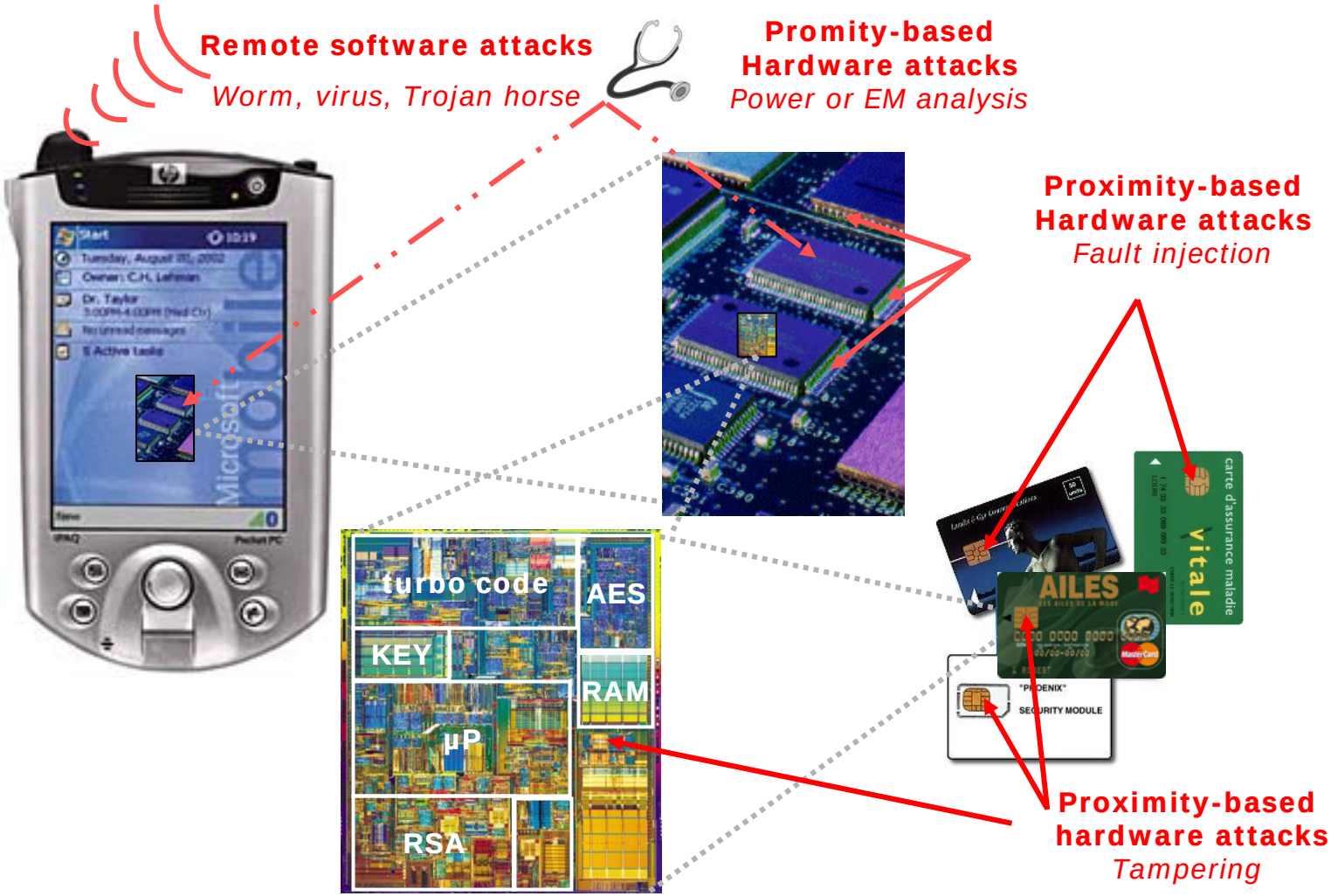
Outlines

- 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 …

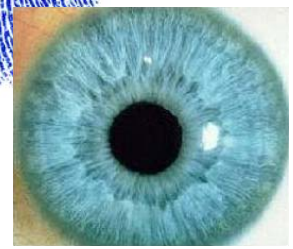
Welcome in a secure world???

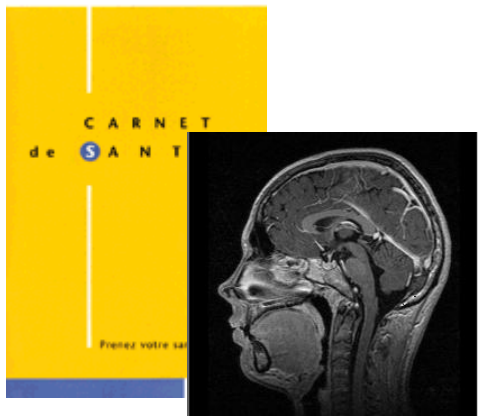


Attacks on embedded system



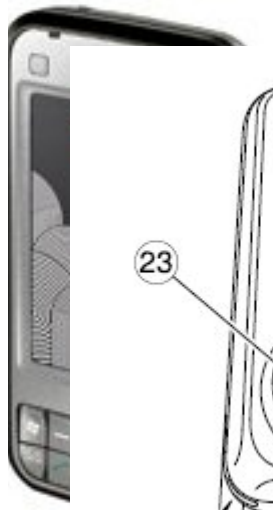
Many sensitive data will be embedded





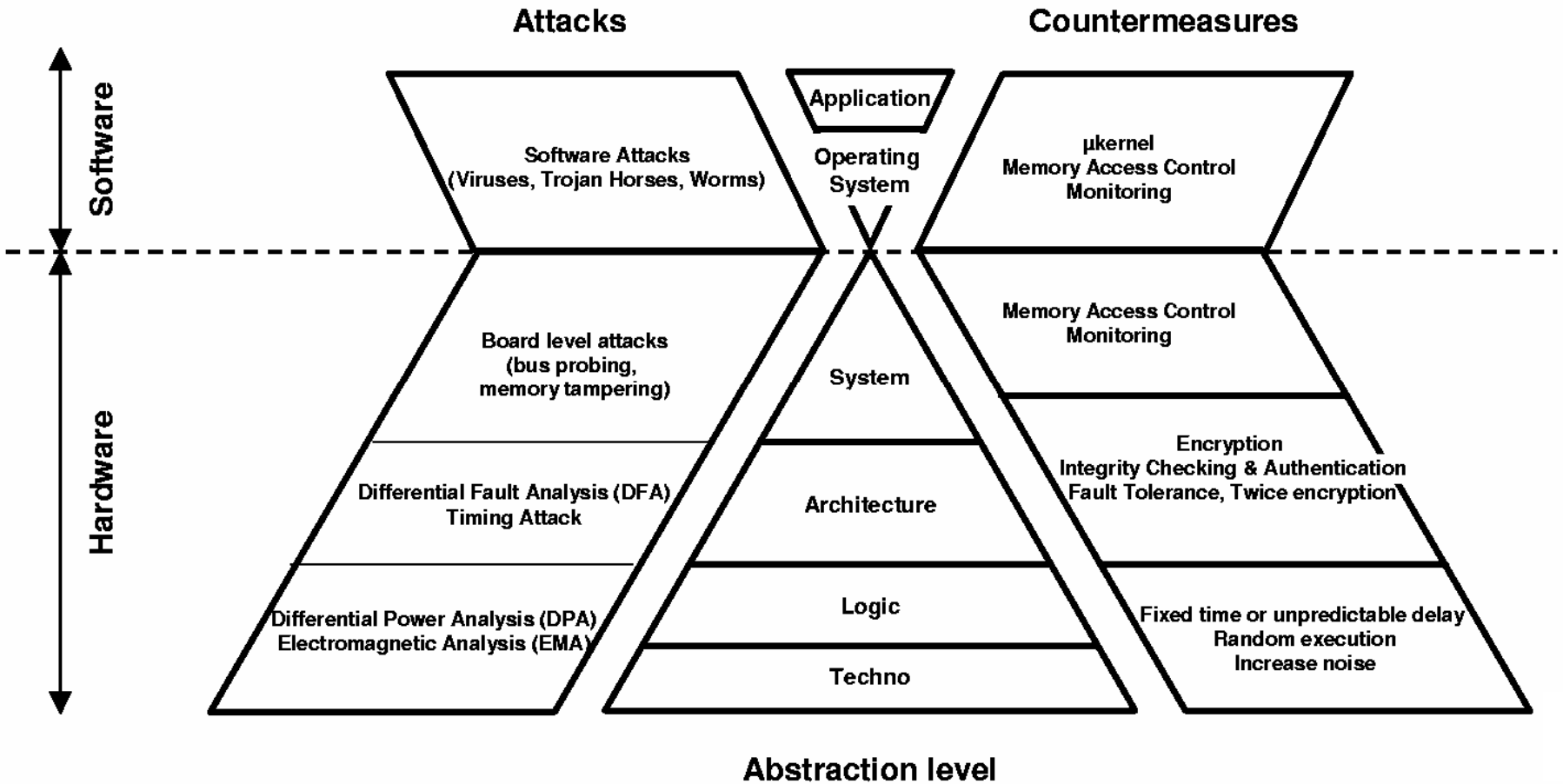
Exemple of available embedded biometric system

- Toshiba proposes a biometric ID authentication system embedded is 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

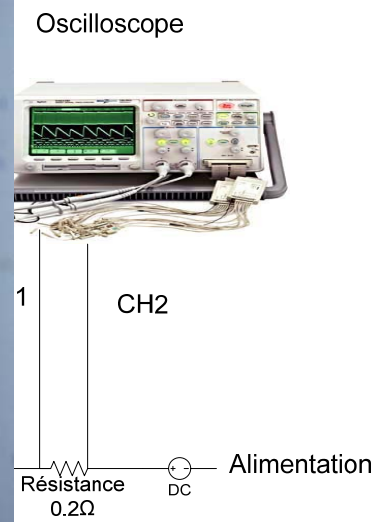
- The rise of hardware security
- **How to dazzle students?**
- An example of common emulation for teaching, the Bordeaux-Lorient project
- Now, what can we do?
- Conclusion & Discussion …

Embedded in a student brain …

- Students are not always excited to study …

- But there are enthusiasm t security syste

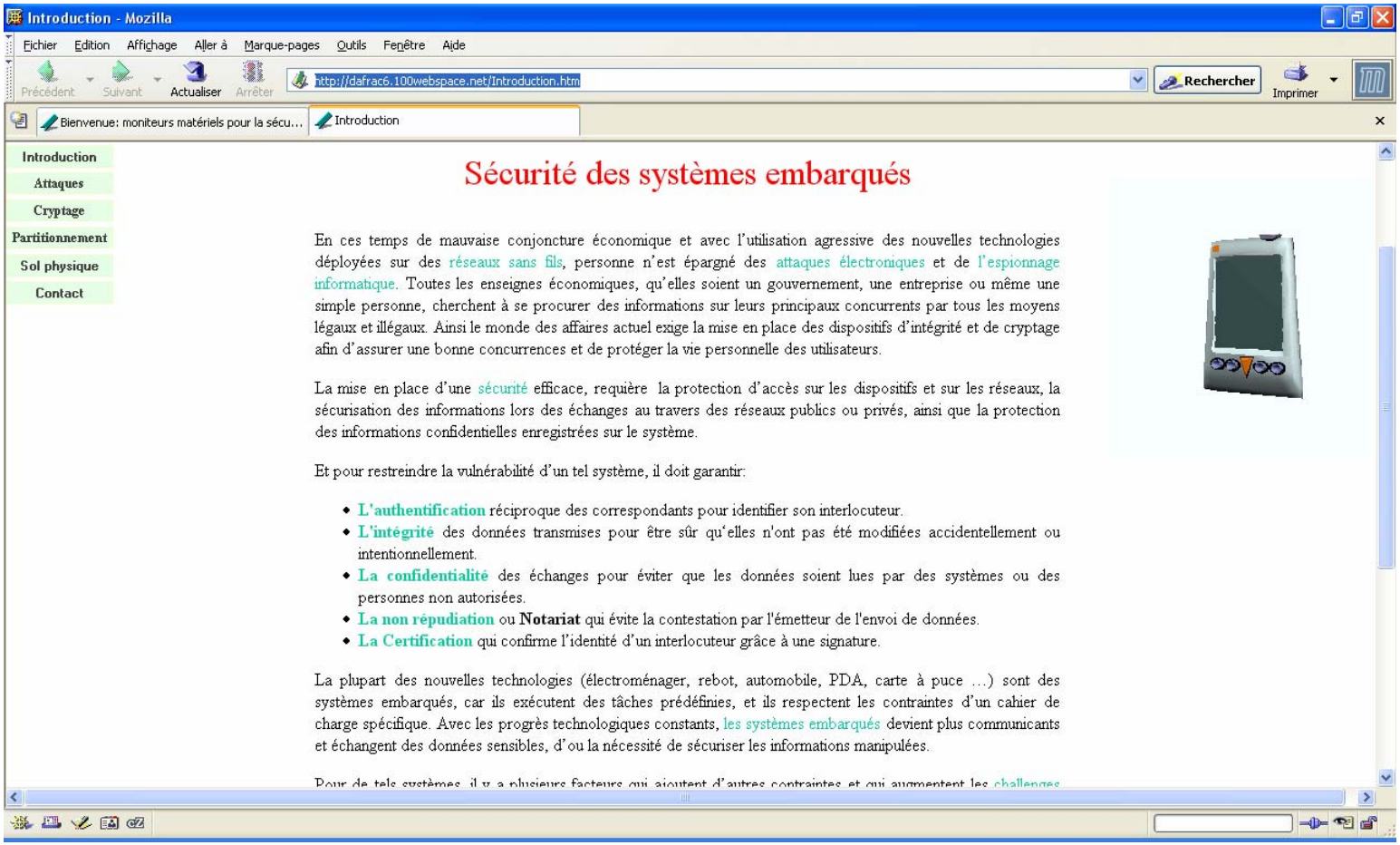
- Actually, it is job to interes security !



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



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

Example 2: Hardware Monitoring for System Security

http://monitor4security.free.fr/

University George Mason - Kris Gaj

- Student projects on Secure Telecommunications Systems

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

questionnaire