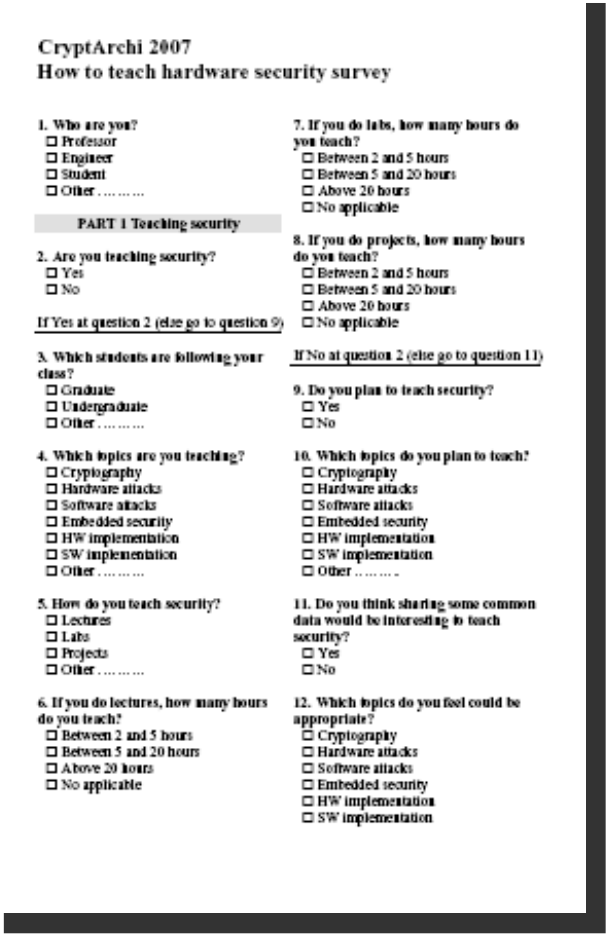
CryptArchi Web Site: A Collaborative Web site for Teaching Hardware Security

Bertrand Le Gal, Lilian Bossuet

Remember CryptArchi 2007

- A talk : How to teach hardware security ?
  - It was focus on teaching hardware security in University degree level
  - It had shown how it is difficult to teach hardware security
  - It had concluded to the need of a collaborative tool for teacher
- The contribution of CryptArchi participants
  - A short questionnaire about the way to teach hardware security
  - A good participation !
  - The results have shown the CryptArchi community interest for such collaborative tool.



CryptArchi 2007
How to teach hardware security survey

1. Who are you?
☐ Professor
☐ Engineer
☐ Student
☐ Other .....

PART 1 Teaching security

2. Are you teaching security?
☐ Yes
☐ No

If Yes at question 2 (else go to question 9)

3. Which students are following your class?
☐ Graduate
☐ Undergraduate
☐ Other .....

4. Which topics are you teaching?
☐ Cryptography
☐ Hardware attacks
☐ Software attacks
☐ Embedded security
☐ HW implementation
☐ SW implementation
☐ Other .....

5. How do you teach security?
☐ Lectures
☐ Labs
☐ Projects
☐ Other .....

6. If you do lectures, how many hours do you teach?
☐ Between 2 and 5 hours
☐ Between 5 and 20 hours
☐ Above 20 hours
☐ No applicable

7. If you do labs, how many hours do you teach?
☐ Between 2 and 5 hours
☐ Between 5 and 20 hours
☐ Above 20 hours
☐ No applicable

8. If you do projects, how many hours do you teach?
☐ Between 2 and 5 hours
☐ Between 5 and 20 hours
☐ Above 20 hours
☐ No applicable

If No at question 2 (else go to question 11)

9. Do you plan to teach security?
☐ Yes
☐ No

10. Which topics do you plan to teach?
☐ Cryptography
☐ Hardware attacks
☐ Software attacks
☐ Embedded security
☐ HW implementation
☐ SW implementation
☐ Other .....

11. Do you think sharing some common data would be interesting to teach security?
☐ Yes
☐ No

12. Which topics do you feel could be appropriate?
☐ Cryptography
☐ Hardware attacks
☐ Software attacks
☐ Embedded security
☐ HW implementation
☐ SW implementation

Outlines

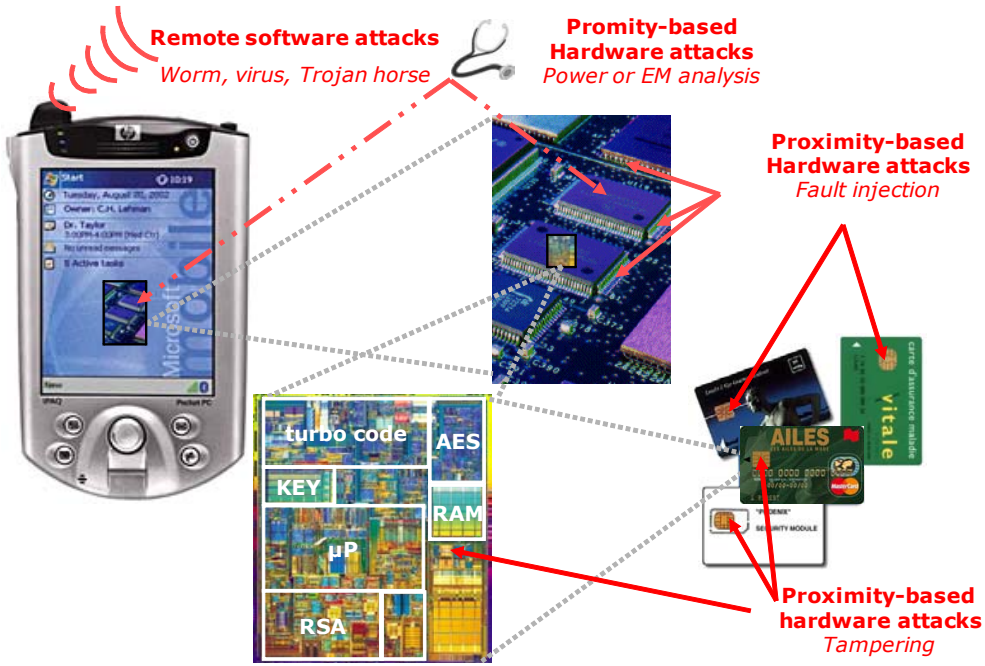
- Motivations and consultation results summary
- A proposition of collaborative web site
- Demonstration of CryptArchi Web Site
- Conclusion & Discussion …

Outlines

- **Motivations and consultation results summary**
- A proposition of collaborative web site
- Demonstration of CryptArchi Web Site
- Conclusion & Discussion …

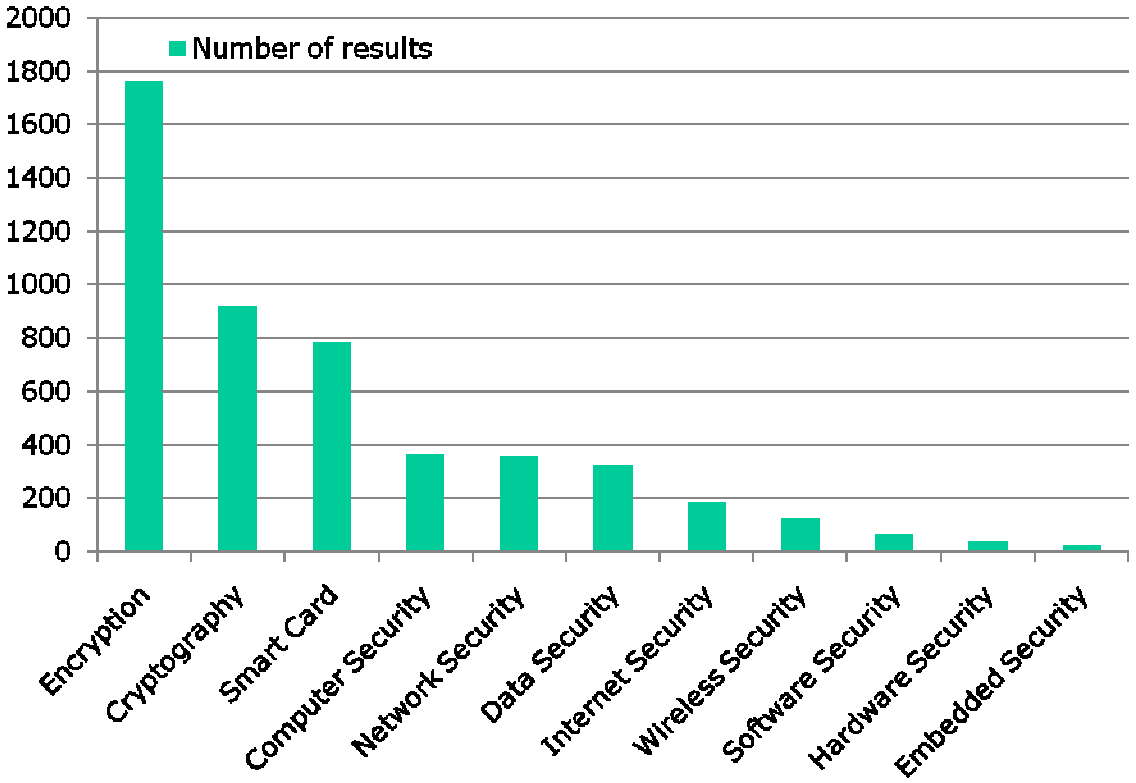
Attacks on Embedded System

- According to the embedded system threats
  - It is necessary to include teaching of embedded system security at University Degree Level for electrical engineering curriculum
  - Not only focuses on software security and crypto !
  - Take into account of hardware security (not only smart card !)



Find teaching information

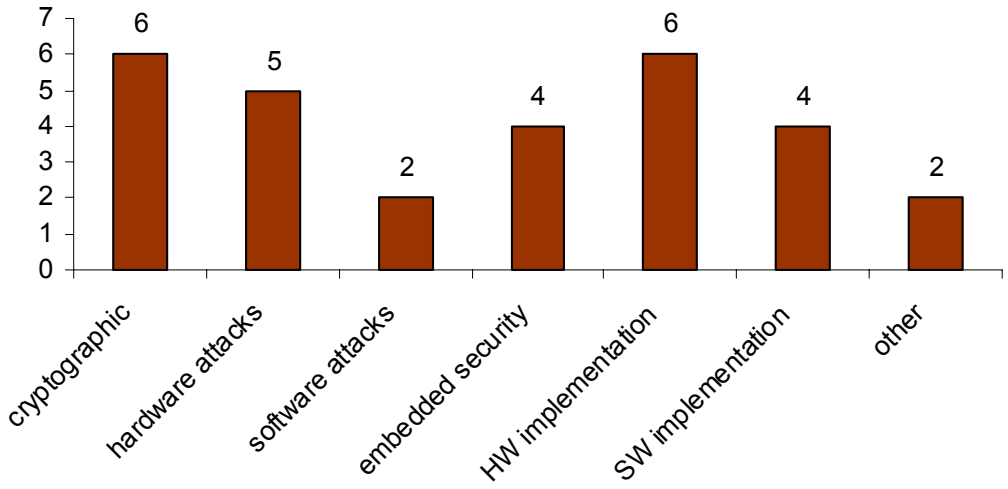
- Security book : a quick search on amazon.com
  - Search Criteria : professional & technical / Engineering / Electrical & Electronics
  - English language



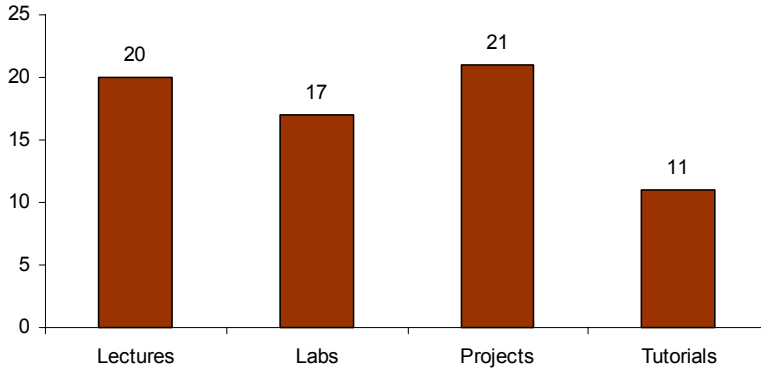
- Warning : numerous multiple results
- Historical security fields give more results: Encryption, Cryptography and Smart Card
- At the end : hardware and embedded security !

Need of collaborative tools to share teaching documents

- That is the CryptArchi 2007 consultation result :
  - CryptArchi Community teaching topics



  - CryptArchi Community had thought that a collaborative WEB site would be appropriate to share teaching resources



Outlines

- Motivations and consultation results summary
- **A proposition of collaborative web site**
- Demonstration of CryptArchi Web Site
- Conclusion & Discussion …

CryptArchi Web Site

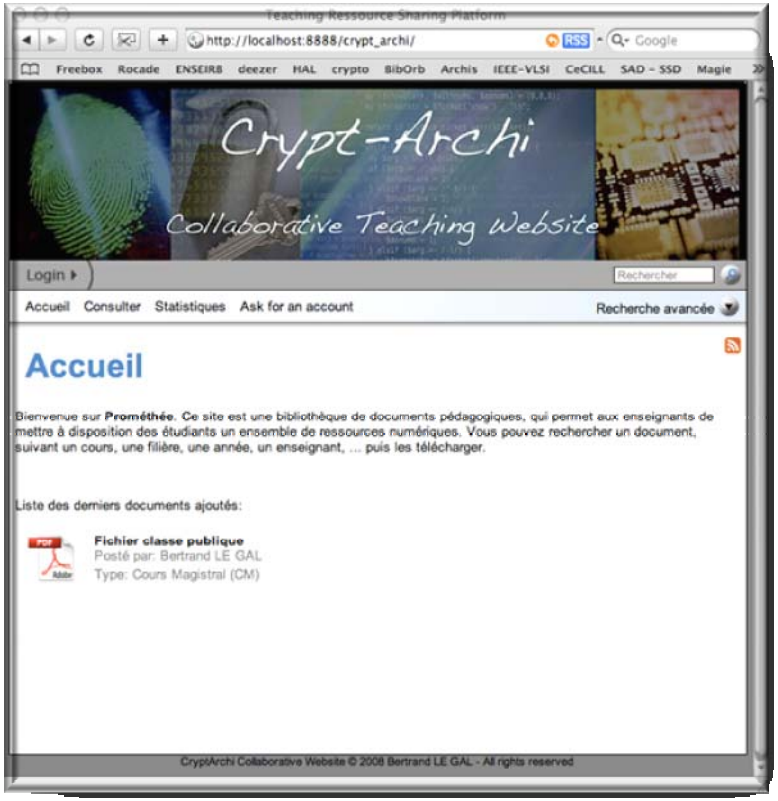
- CryptArchi Community is larger and larger
  - France, Slovakia, Czech Republic, Germany, United Kingdom, Belgium, The Netherlands, Poland, USA
  - A web site is the best way to easily share documentation
- Two user status with different rights on document access:
- Teacher (active contributor and reader)
  - Full access to free and restricted documents
  - Rights to add (or modify) document on web site
  - Teacher status need web site administrator confirmation (it can take a little time to obtain authorization).
- Student (simple reader)
  - Restricted access rights to some documents (no reading of restricted document)
  - No rights to submit or change document on the web site data base
  - Student status is free and directly given without administrator confirmation

CryptArchi Web Site

- Type of Document in the Web site data base
  - Lectures
  - Practical Lab
  - Exercise
  - Tutorial (research seminar, current trends …)
  - Others (PhD Thesis, Master Thesis, Students report ?)
- Application WEB developer's : Bertrand Le Gal
  - Page code: HTML
  - Page make-up: CSS
  - User friendly interface code: Java Script
  - Application Web code: PHP
  - Data base: MySQL
  - License : GPL
  - RSS syndication

CryptArchi Web Site

http://www.enseirb.fr/~legal/crypt_archi/



Outlines

- Motivations and consultation results summary
- A proposition of collaborative web site
- **Demonstration of CryptArchi Web Site**
- Conclusion & Discussion …

Outlines

- Motivations and consultation results summary
- A proposition of collaborative web site
- Demonstration of CryptArchi Web Site
- **Conclusion & Discussion …**

Conclusion & Discussion

- We propose to CryptArchi Community an user friendly and easy to use web site to share teaching documentations about embedded system security
  - Lecture, practical lab documentation, project, research seminar (tutorials, current trends …)
  - A large area of teaching topics :
    - Hardware security
    - Embedded security
    - Security for computer science
    - Cryptography
    - *All the CryptArchi Community takes an interest …*

- Idea : an special session on education for future CryptArchi workshop ?
  - Show of practical lab project about security
  - Experience of teaching security
  - Presentation of University Degree Curriculum

CryptArchi Web Site: A Collaborative Web site for Teaching Hardware Security

Bertrand Le Gal, Lilian Bossuet

THANK YOU !!!