Comparison of the Methods Used to Assess the Security of Smartcards and Information Systems

Pierre Girard, Jean-Luc Giraud

{Pierre.Girard, Jean-Luc.Giraud}@gemplus.com

Smart Card Security Conference

Tokyo, March 29-30, 2001

GEMPLUS

Introduction

- **Device/software performance is easy to quantify :**
  - **SpecInt ’xx, transaction/s, bandwitdh ...**
- **Device/software security level is hard to measure**
  - **A system seems secure until it is broken**
- **Nevertheless :**
  - **Customers want to assess what they buy**
  - **Manufacturers want to convince them with facts**

Outline

- **Classical flaws**
- **Evaluation of security assessment techniques :**
  - **Properties of good assessment techniques**
  - **Available assessment techniques**
- **Conclusion**

Classical flaws

- **Security through obscurity or snake oil**
  - **Netscape 4.5 mail password « ciphering » [1]**
- **Faulty design**
  - **Key length issue of the French « Carte Bancaire »**
- **Implementation shortcomings**
  - **Buffer overflows : 8 of the 17 1999-CERT advisories**
- **Back doors / deliberately introduced weaknesses**
  - **Exportable products are often suspicious [2]**

Security evaluation needs ...

- **Expertise**
- **Time**
- **Methodology**
- **Information**
- **Independence of the evaluator**

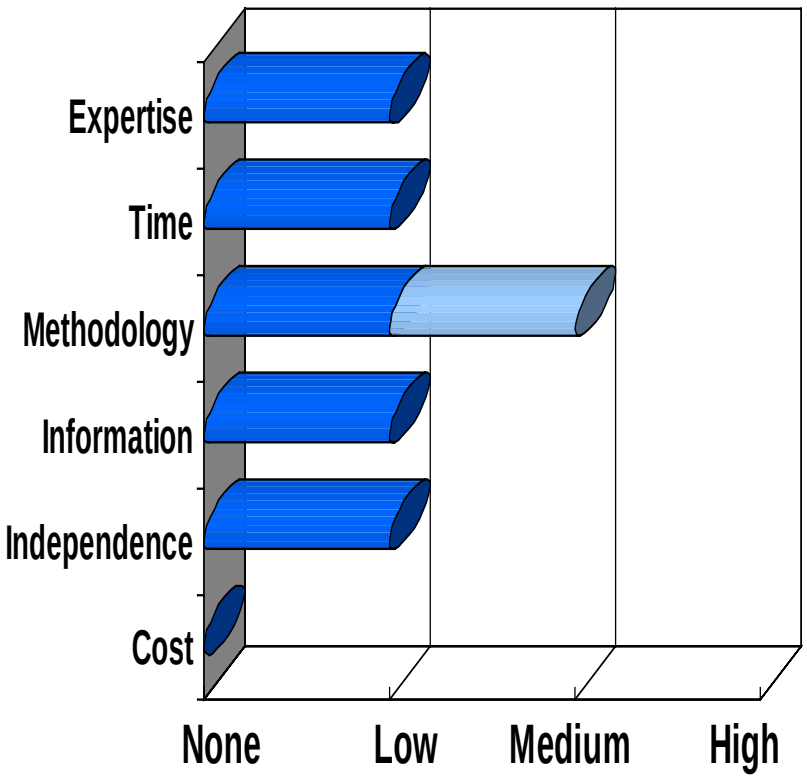
But should also be cost-effective

Compared Evaluation Methods

- **Comparative test of the press**
- **Evaluation by the customer**
- **Audit of the manufacturer and/or partnership with it**
- **Evaluation by a specialised third party**
- **Public challenge**
- **Public review**
- **ITSEC/Common Criteria**
- **Public formal proof**

Comparative tests of the Press

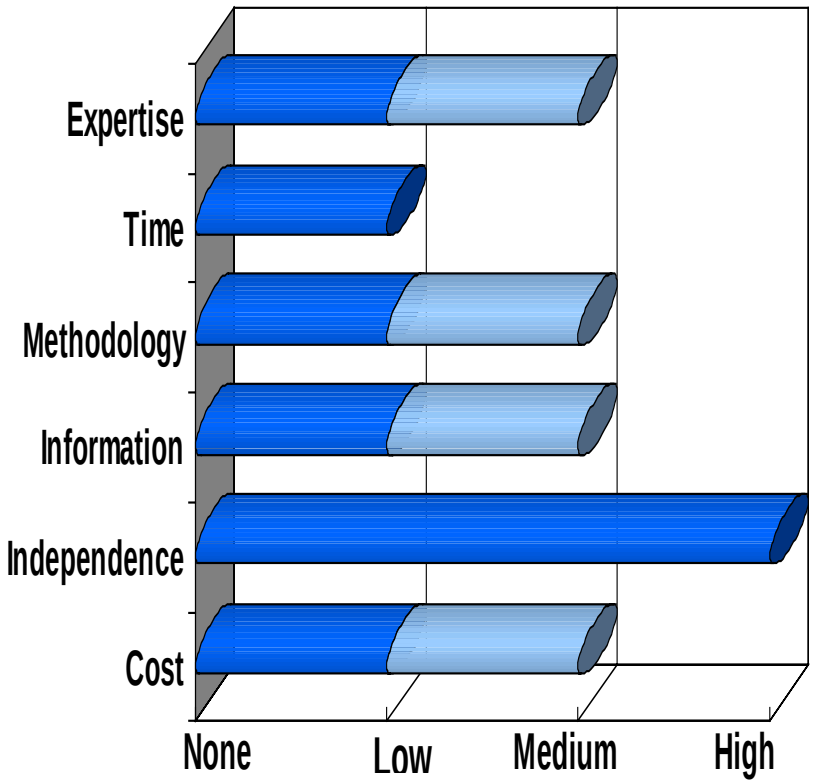
- **Evaluation based on functionalities**
- **Hardly detects any security problem**
- **No cost**



Detects :	Snake oil	Design	Implementation	Back door
	☐	☐	☐	☐

Evaluation by the customer

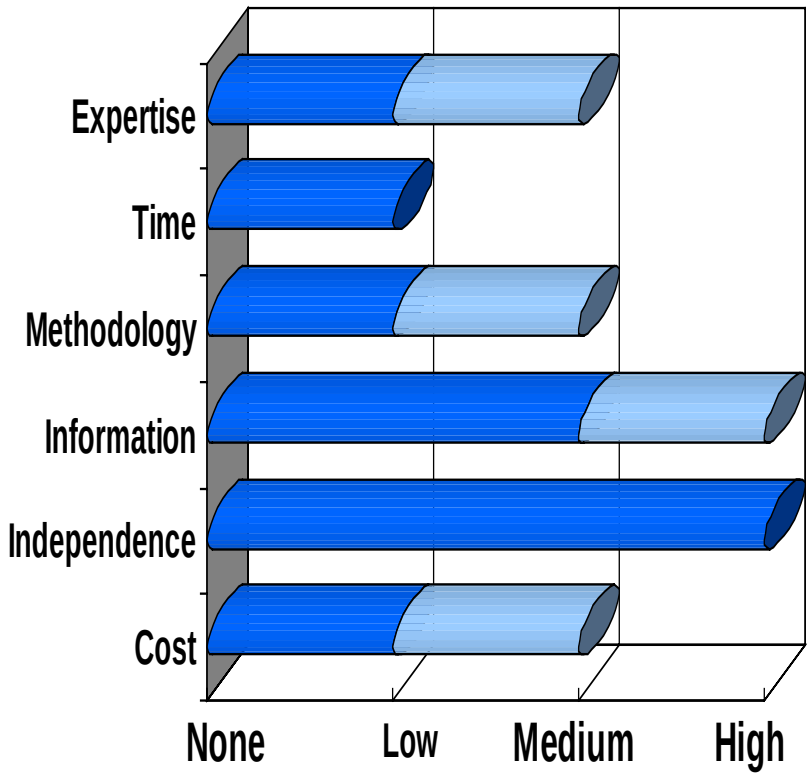
- **Need in-house experts**
- **Opposed to the current externalisation trend**



Detects :	Snake oil	Design	Implementation	Back door
	☑	☑	☐	☐

Manufacturer audit and/or partnership

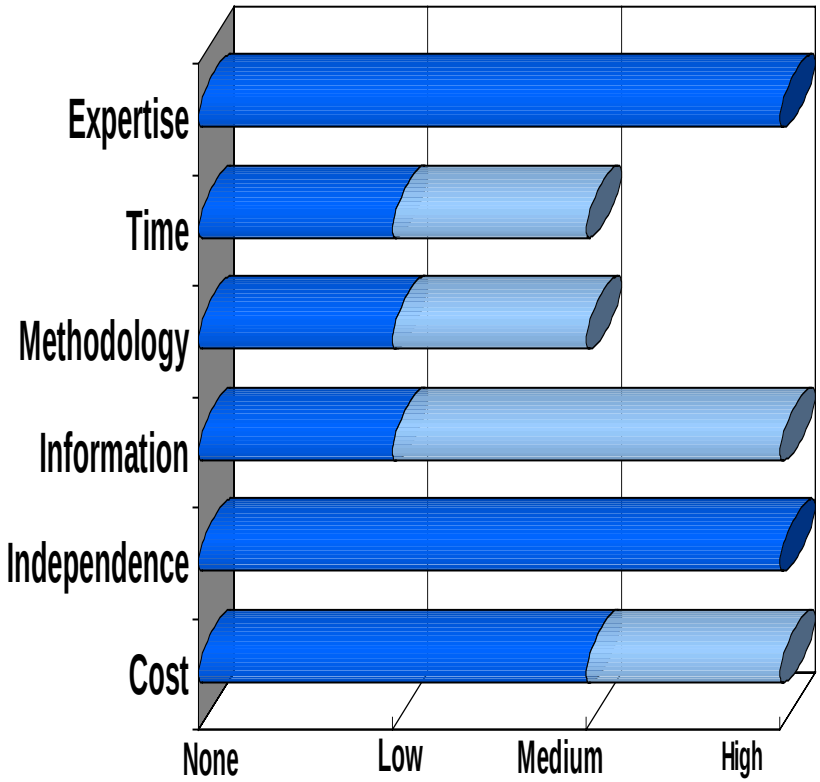
- **Conceivable only for major customers**



Detects :	Snake oil	Design	Implementation	Back door
	☑	☑	☑	☑ ☐

Evaluation by a specialised third party

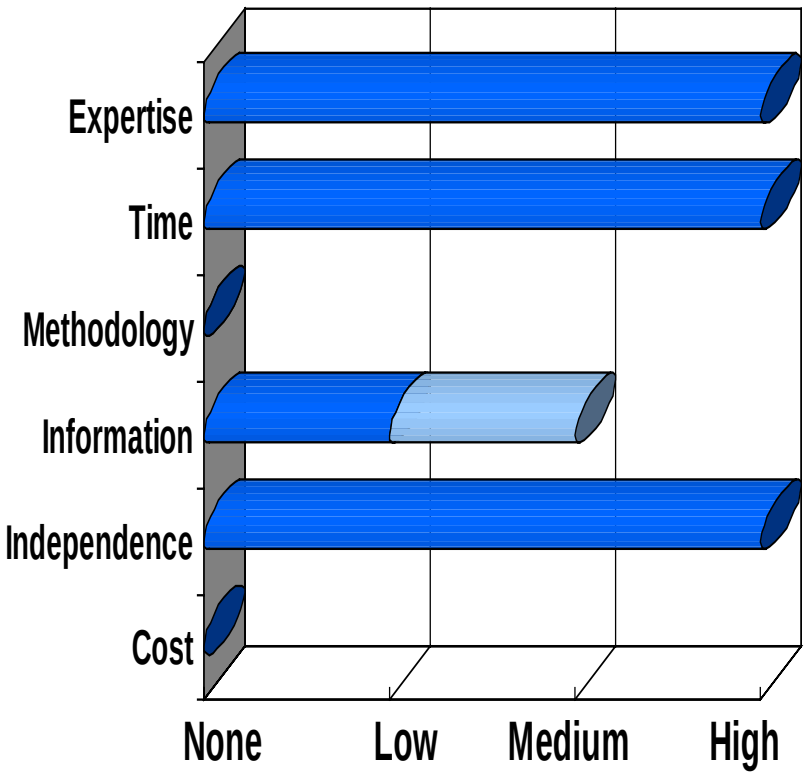
- **2 philosophies:**
  - **Consultants**
  - **Laboratories**
- **Real specialists are spare**



Detects :	Snake oil	Design	Implementation	Back door
	☑	☑	☑	☑ ☐

Public challenge

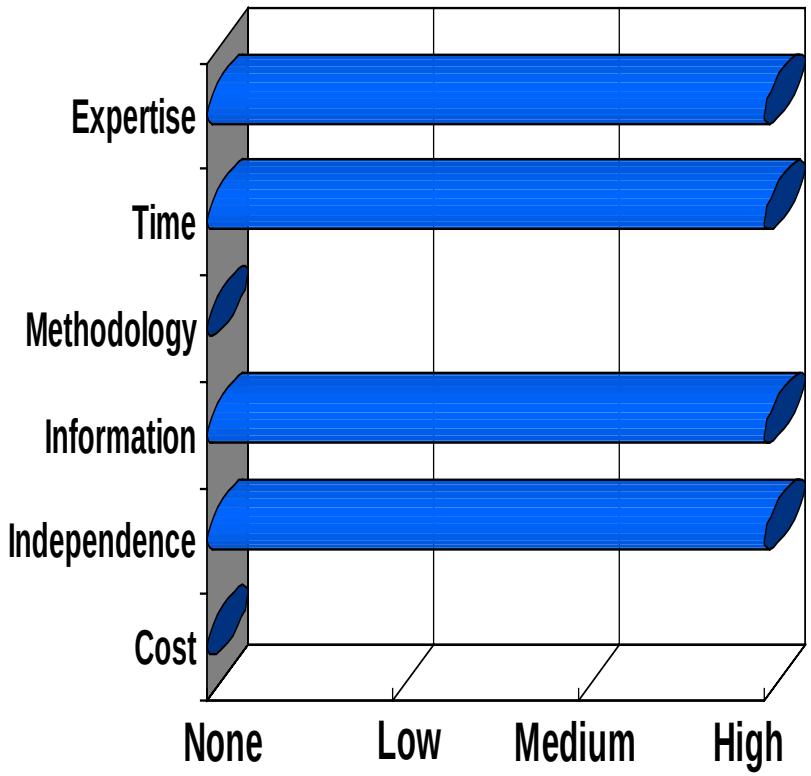
- Need to be attractive
- Black box evaluation
- Double edged sword for manufacturers
- Examples
  - RSA challenges [3]
  - R. Moreno's challenge [4]



Detects :	Snake oil	Design	Implementation	Back door
	☑	☑	☑ ☐	☐

Public review

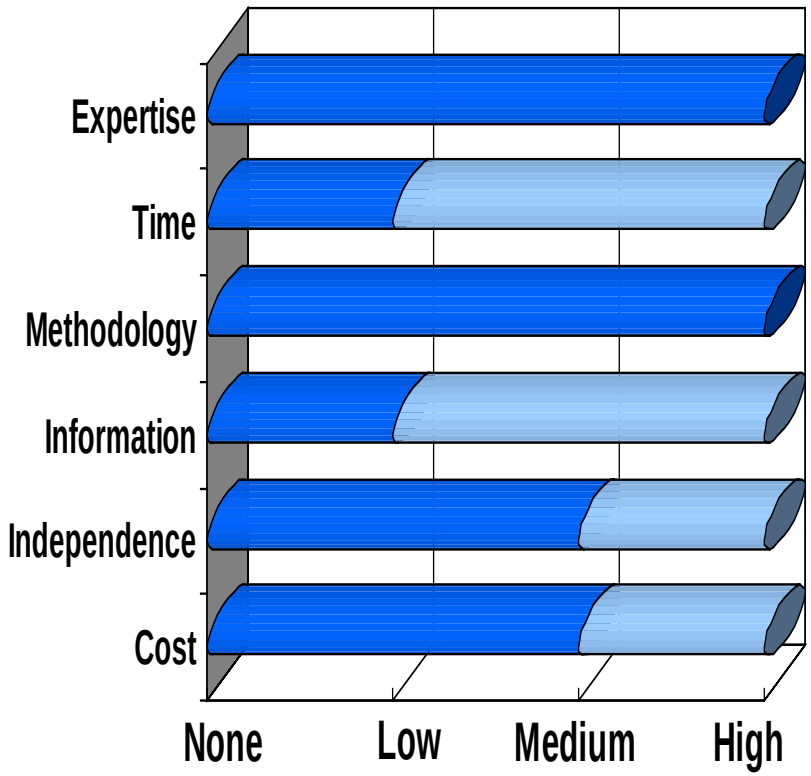
- **Need to be attractive**
- **White box evaluation : leakage of manufacturer technologies**
- **Double edged sword for manufacturers**
- **Definitive solution for paranoids**
- **Examples : AES [5], Linux, Java 2 platform, PGP, SDMI**



Detects :	Snake oil	Design	Implementation	Back door
	☑	☑	☑	☑

ITSEC/Common Criteria

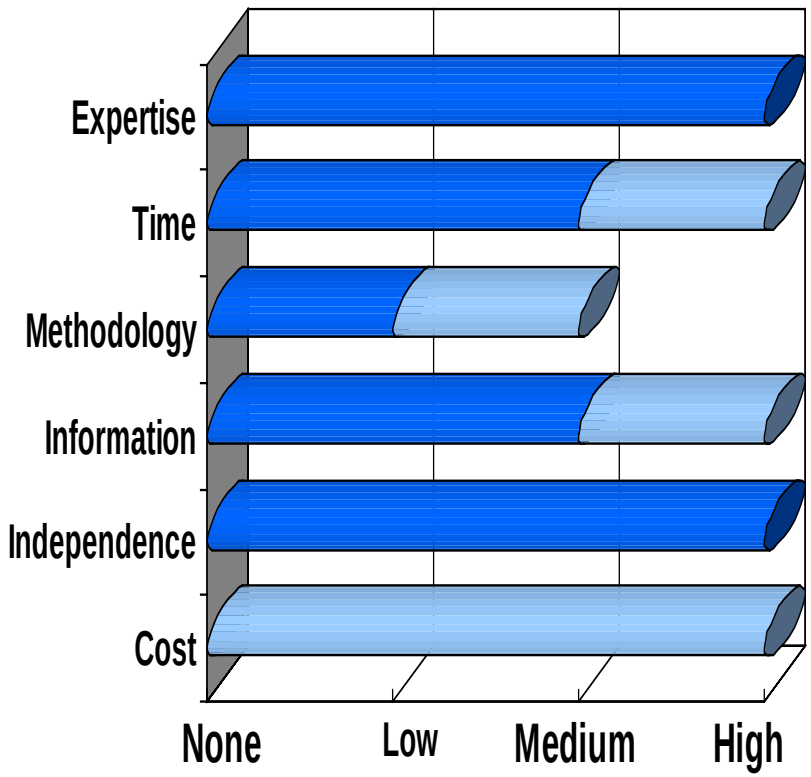
- **Great variability according to the evaluation level**
- **Beware of the content of the Security Target / Protection Profile**
- **May use formal methods for high evaluation level**



Detects :	Snake oil	Design	Implementation	Back door
	☑	☑	☑ ☐	☑ ☐

Public formal proof

- **Released by :**
  - **The manufacturer**
  - **A third party**
- **Beware of the proof level :**
  - **Specification**
  - **Design**
  - **Code generation**
- **Examples**
  - **Academic work on Java**
  - **Gemplus work on Javacard firewall [6]**



Detects :	Snake oil	Design	Implementation	Back door
	☑	☑	☑ ☐	☑ ☐

Conclusion for customers

- **Security requires periodic re-evaluation**
- **Buying without in-house security experts is risky**
- **Always take into account the results but ALSO the evaluation method**

Conclusion for manufacturers

- **State clearly what has been evaluated and how**
- **Using well established technology can reduce evaluation costs**
- **Choose your evaluation method according to your market segment**

References

[1] « Netscape 4.5 vulnerability », Alexey Pavlov, Bugtrack mailing list, Message-ID: <370CE37B.2A066C20 @uic.nnov.ru>, Apr 08 1999

[2] « Back Doors, Export, and the NSA », Bruce Schneier, CRYPTO-GRAM, February 15, 1999

[3] « Cryptographic Challenges », RSA Labs, http://www.rsasecurity.com/rsalabs/challenges/

[4] « Carte à puce: Roland Moreno offre un million de francs », Dépêche AFP, 13/03/2000

[5] « Advanced Encryption Standard », NIST, http://csrc.nist.gov/encryption/aes/

[6] « Formal Model and Implementation of the Java Card Dynamic Security Policy », Stéphanie Motré, AFADL2000, http://www-lsr.imag.fr/afadl2000/Programme/Articles/motre.doc