Cryptologie et confiance numérique

Louis Goubin

Université de Versailles-St-Quentin-en-Yvelines

Groupe « Droit et numérique »

Mardi 7 mars 2017

Qu'est-ce que la sécurité ?

- Dans le « vieux monde »
  - Confidentialité : courrier postal, messagers
  - Intégrité : sceaux
  - Authenticité : signatures manuscrites
  - Anonymat : élections
- Dans le cyberespace
  - monde de formalisme
  - monde virtuel
  - les canaux de communication sont supposés vulnérables
  - les données sont copiables indéfiniment et sans erreur
- La sécurité numérique, et en particulier la cryptologie, ont pour but de « compenser » la vulnérabilité des données et des canaux de communications

Logical Security is an Abstraction

- Attacker exchanges messages with the system:
  - Known messages: passive adversary (eavesdropping)
  - (Adaptively) chosen messages: active adversary
- Uses these messages to defeat security goals:
  - Confidentiality: e-mails, card numbers, voice, …
  - Integrity: software downloading, …
  - Authenticity: access control, digital signature, …
  - Anonymity: anonymous payment, e-vote, …
  - …

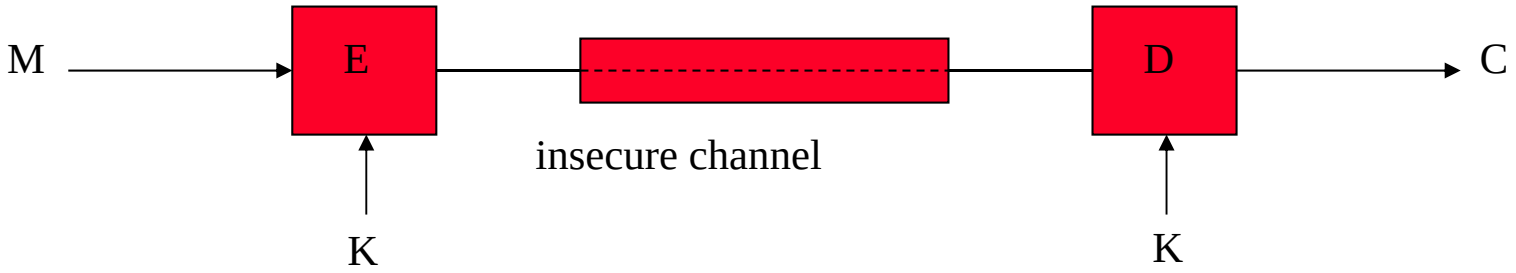
Security at the cryptographic level

- Cryptographic algorithms = Basic security components
  - Encryption, signature, authentication, …
  - Highly based on mathematics: probability, combinatorics, coding theory, number theory, lattice reduction, finite fields, (hyper)elliptic curves, algebraic geometry, graphs…
  - Secret = Key (*Kerckhoff's principle*, 1883)
  - Attacks use cryptanalytic techniques
  - (Partial) proofs of security, assuming the difficulty of some mathematical problem (complexity theory)

Security at the protocol level

- Procotols = On a network, supposed to be hostile
  - Intruders can read, modify and delete traffic, may take control of one or more network principals.
  - Often non-intuitive attacks:
    - Basic attacks: use basic functionalities, in any arbitrary order.
    - More complex attacks: also use subtle properties of the cryptographic algorithms, or statistical analysis of traffic…
  - Proofs of security for protocols:
    - Mathematical/logical model of system & requirements
    - Effective procedure to verify proof (formal methods).

Symmetric Cryptography



- Same key for encryption and decryption
  - ➔ Secret key cryptography
- Examples in conventional cryptography:
  - Data Encryption Standard (DES): NBS 1976
  - Advanced Encryption Standard (AES): NIST 2001
  - Kasumi: SAGE 199903

Asymmetric Cryptography

- Seminal idea: the encryption key can be made public ➔ Public key cryptography
  - Merkle's puzzle system (1975)
  - Diffie-Hellman key exchange protocol (1976)
  - Rivest-Shamir-Adleman public key encryption scheme: RSA (1977)
- Based on the existence of intrinsically difficult mathematical problems (complexity theory)

Authentication Protocols

- Idea: (interactive) proof of knowledge of a secret key
  - With an asymmetric encryption scheme
  - Better: do not reveal any information about the secret itself ➔ Zero-knowledge [Goldwasser-Micali-Rackoff, 1985]
- Examples:
  - Knowledge of factorization: Fiat-Shamir (1986), Guillou-Quisquater (1988, 2000)
  - Knowledge of discrete logarithm: Schnorr (1989), Giraud-Poupard-Stern (1998)

Signature Protocols

- Prove the identity of the author of a message (➔ non-repudiation).
  - With an asymmetric encryption scheme
  - Better: transform interactive proof of knowledge into non-interactive proof
- Examples:
  - RSA FDH, RSA PSS (PKCS#1 v2.1)
  - Schnorr signature scheme
  - ElGamal signature scheme
  - DSA signature scheme

Quelle confiance ?

- W. Pieters, *Verifiability of electronic voting*
  - In: Gutwirth, S., Poullet, Y., De Hert, P. (eds.) *Data Protection in a Profiled World*, pp. 323–334. Springer, Netherlands (2010)
  - *"When computing scientists speak about electronic voting, it is often in terms of trust. But there are two contradictory statements. First, they argue that it should not be necessary to trust e-voting systems, which would be the case if they are provably secure. Second, for an e-voting system to be successful, the public must trust it."*
  - *"When we unravel the confusing concept of trust, we find that there are two quite different meanings: relying on something that one does not understand and does not really choose (**confidence**), or relying on something that one does understand and has consciously chosen (**trust**). The distinction is due to the German sociologist Niklas Luhmann."*

La confiance ne peut pas être uniquement numérique

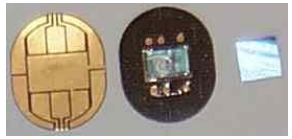
- C'est une illusion de croire que tout est réglé à l'intérieur de ce monde numérique.
- La sécurité informatique ne peut être vue uniquement comme un problème interne au monde numérique.
- On fait toujours -de manière implicite- des hypothèses sur la confiance en des choses extérieures au strict monde numérique :
  - Le monde physique ressurgit
  - La confiance n'est pas magique
  - Les aspects humains de la confiance

Le monde physique ressurgit

- Confiance dans les lois de la physique
  - Mécanique quantique pour générer de l'aléa (qui est nécessaire pour obtenir de bonnes clés cryptographiques) : on doit faire réintervenir la physique (y compris la mécanique quantique)
  - La crypto suppose en général l'existence de problèmes "difficiles" à résoudre (théorie de l'information (Shannon) vs théorie de la complexité), notion qui s'appuie sur la technologie électronique, la loi de Moore. Cf aussi question des ordinateurs quantiques.
  - Fiabilité du hardware (cf attaques par injection de fautes)
  - Validité du modèle de la machine de Turing : en fait il ne reflète qu'une partie de la réalité, les calculs ne sont pas une notion éthérée, il s'agit d'électrons qui circulent dans des fils, d'où des fuites physiques d'information, et les attaques "side-channel"

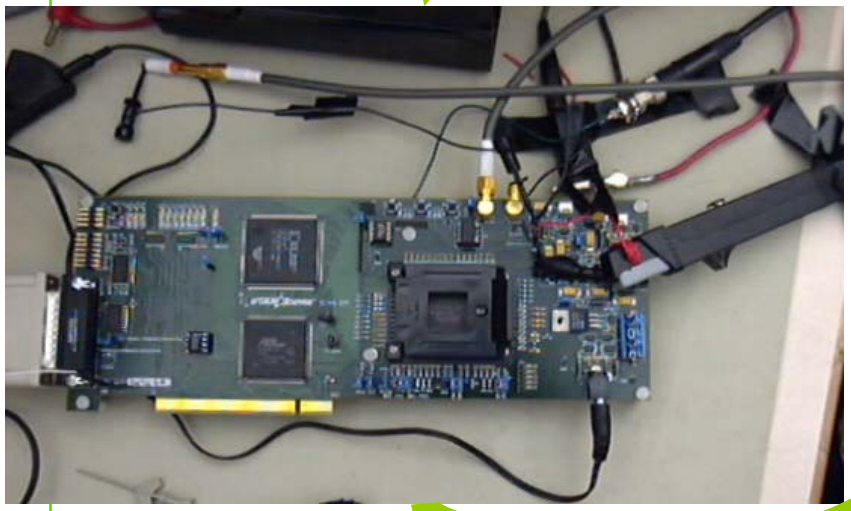
Physical Security

- More general security model: use the physical aspects of computation.
- Potential threat for any embedded system (especially smart cards)
- Invasive vs Non-invasive Attacks



  - Invasive attack ➔ depackaging the chip to get direct access to its components (*e.g.* connecting a wire on a data bus to eavesdrop the transfered data)
  - Non-invasive attack ➔ only exploits externally available information (running time, power consumption, …)

Hardware comes into the game…



14

Passive vs Active Attacks

- Passive attacks: simply observe the card's behaviour during its processing, without disturbing it:
  - Measures execution time (timing attack), power consumption (SPA, DPA), electromagnetic radiation (EM), …
  - Even remote systems: SSL [Boneh & Brumley, 2003]
- Active attacks: tamper with the card's proper functioning
  - Modify physical environment: Voltage, Clock, Temperature, Radiations, Light, Eddy current, …
  - Fault injection on cryptographic algorithms (DFA), virtual machines [Govindavajhala & Appel, 2003], …

La confiance n'est pas magique

- La confiance elle-même ne peut pas être "endogène" au monde numérique
  - rêve de Diffie-Hellman avec l'invention de la cryptographie asymétrique (1976) : créer une communication sécurisée entre Alice et Bob qui ne se sont jamais concertés auparavant.
  - en regardant de plus près, cela ne marche pas (attaques "man-in-the-middle")
  - d'où nécessité de faire confiance soit à une autorité (certificats, PKI = chaîne de confiance), soit à la majorité (*e.g.* blockchain)

Les aspects humains de la confiance (1)

- La confiance au sens de la psychologie/sociologie
  - Confiance en général dans la technologie (exemple du vote électronique)
  - Confiance dans les mathématiciens : un problème difficile, comme la factorisation, est-il difficile parce que beaucoup de mathématiciens l'étudient (cf principe de Kerckoffs) ou au contraire parce que personne ne le regarde (cf boutade de James Massey) ?
  - Confiance dans la cryptographie (les "preuves de sécurité" ont parfois révélé leurs faiblesses, soit à cause d'erreurs dans la preuve, soit parce qu'elles se placent dans un modèle inadéquat)

Les aspects humains de la confiance (2)

- La confiance au sens de la psychologie/sociologie (suite)
  - Confiance dans les développeurs (présence éventuelle de bugs, utilisation de méthodes formelles)
  - Confiance dans les organismes de standardisation (ISO, NIST, ETSI, etc) : cf mécanisme malicieux Dual_EC_DRBG introduit par la NSA à l'ISO, pb de l'implication des experts
  - Confiance dans la privacy (perception variable de ce que cela recouvre) : e.g. mécanismes d'authentification, zero-knowledge, attribute-based cryptography

Et le droit ? (3)

- Quelques pistes :
  - la cryptographie peut sembler définir de façon intrinsèque ce qui peut être fait ou pas par Alice, Bob, etc, ce qui peut donner l'impression qu'on n'a plus besoin du droit (cf Lawrence Lessig : "Code is the law"), mais ce n'est pas vrai.
  - les DRM (Digital Right Management) : les solutions techniques ne font pas tout !
  - responsabilité juridique : autorités de confiance pour les PKI (en lien par exemple avec la signature électronique) = chaînes légales de confiance ?
  - responsabilité (y compris juridique) des fournisseurs de solutions/produits de sécurité. En cas de vol de données, de fraude due à un défaut de conception, d'usurpation d'identité, etc.
  - schémas de certification (exemple : certification critères communs : ANSSI, Laboratoires CESTI, etc)