

**M2 GI (Univ. Grenoble Alpes)**

**Cours Cybersécurité**

**Un Tour d'horizon de la cybersécurité et de  
la cryptographie**

v2.00, Janvier 2017

Philippe Elbaz-Vincent



## Website of the course

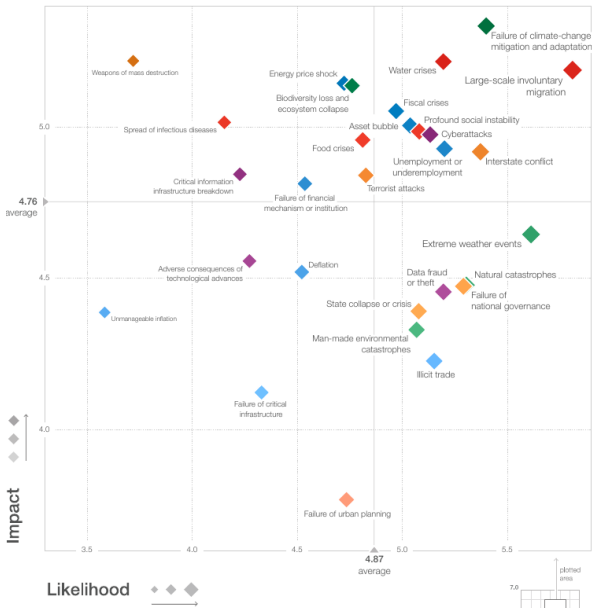
`http ://www-fourier.ujf-grenoble.fr/~pev/GI`

**login** : GI2016

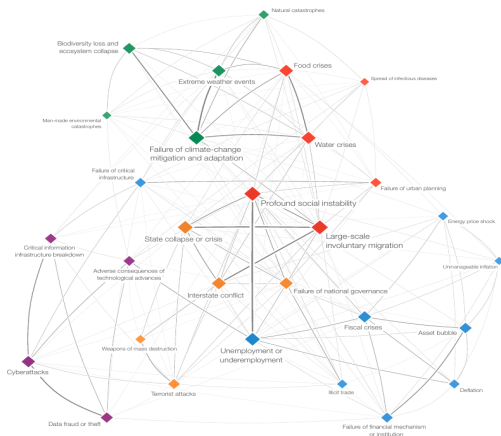
**passwd** : CyberGI2017Shannon



# Positionnement des cyberattaques en terme de risque



# Interdépendance entre «risques classiques» et «cyberattaques et vol de données»

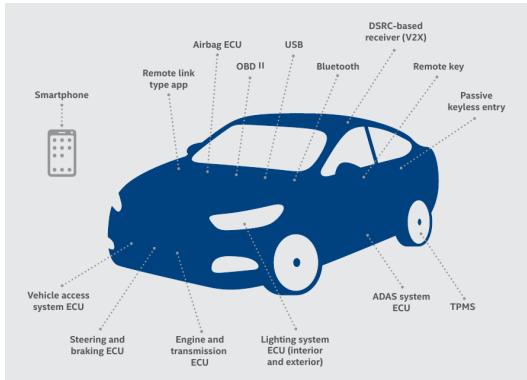


**(c) World Economic Forum 2016. The Global Risks Report 2016.  
11th Edition**

## Les enjeux

- Protection de la vie privée (protection de ses données personnelles, de ses identifiants, de son identité, de sa famille...),
- Protection de ses données professionnelles et des données sensibles (propriété intellectuel),
- Permettre une authentification (forte) des utilisateurs,
- Permettre des transactions financières,
- Protection de l'infrastructure informatique (interne et externalisée).

# La voiture comme exemple de risques cyberphysiques au quotidien



(c) McAfee Labs 2016

👉 220 millions de voitures connectées en 2020, 12% directement connectées à Internet, plus de 12 points d'entrée possible pour les attaques... !

# Attaques sur les infrastructures critiques



(c) SANS ICS et E-ISAC 2016, «Analysis of the Cyber Attack on the Ukrainian Power Grid», Mars 2016

☞ L'attaque s'est déployée de Mars 2015 à Décembre 2015 (date de la panne généralisée) !



## Les catégories d'attaques

- Les attaques génériques de masses non ciblées (phishing, ramsonware, ...),
- Attaques ciblées économiques,
- Attaques ciblées idéologiques («hacktivistes», terroriste, «états»).

## Le problème des IoT...

- Des objets connectés disposant de puissances variées (e.g., une TV connecté utilise un CPU milieu de gamme, une machine à lavée un CPU bas de gamme)
- ...Mais capable de servir de serveurs de fichiers, de relai web ou de réseau de type «botnet»
- Des objets ne disposant en général d'aucune protection et donc facilement piratable...
- Des objets déployés massivement...(on anticipe plus de 20 milliards d'objets connectés à l'horizon 2020)
- **Ils sont déjà utilisés comme vecteurs d'attaques (notamment pour du DDOS) !**

# Exemple d'attaque ciblée simple : «Fraude au président ou FOVI»



(c) Police Nationale



Exemple le plus célèbre : Michelin 2014 pour 1,6 Millions d'euros !

## Comment se protéger ?

- Mise en place d'une infrastructure sécurisée (authentification des connexions et des accès numériques),
- Chiffrement des données sensibles (partitions, disques durs entiers ou fichiers) et des connexions,
- Filtrage du réseau et des composants logiciels (pare-feu, «anti-virus», détection logiciels malveillants, etc),
- Contrôle du réseau et des accès machines (détection d'intrusion, détection de cyberattaques,...),
- **Politique de sécurité des SI (y inclus utilisation de mot de passe robuste, protection des clefs numériques avec portefeuilles électroniques robuste, etc).**
- **Sensibilisation et Formation du personnel (robustesse face à l'ingénierie sociale).**

- ☞ Les méthodes cryptographiques sont incontournables...
- ☞ Les composants cryptographiques matériels sont en général plus robuste que les composants logiciels !

# La cryptographie usuelle repose sur des problématiques calculatoires

$n$	$2^n$	Ordre de grandeur
32	$2^{32}$	Nombre d'hommes sur Terre
46	$2^{46}$	Distance Terre-Soleil en millimètres
46	$2^{46}$	Nombre d'opérations effectuées en une journée à raison d'un milliard d'opérations par seconde (1GHz)
55	$2^{55}$	Nombre d'opérations effectuées en une année à raison d'un milliard d'opérations par seconde (1GHz)
82	$2^{82}$	Masse de la Terre en kilogrammes
90	$2^{90}$	Nombre d'opérations effectuées en 15 milliards d'années (âge de l'univers) à raison d'un milliard d'opérations par seconde (1GHz)
155	$2^{155}$	Nombre de molécules d'eau sur Terre
256	$2^{256}$	Nombre d'électrons dans l'univers

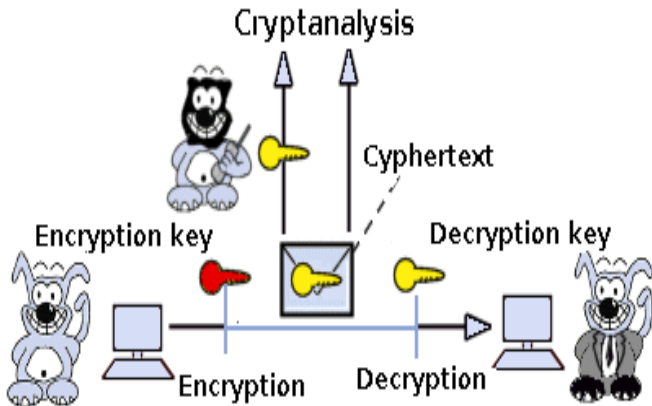
(c) ANSSI 2014 - Comparatif d'ordre de grandeur

👉 En pratique on mesure la robustesse d'une clef cryptographique (pour une méthode de chiffrement donnée) au nombre d'opérations nécessaires à retrouver cette clef avec le meilleur algorithme de «cassage». Cela donne un niveau de sécurité en bits qui sert d'étalon de dimensionnement !

# What is cryptography?

## **cryptography**

Principles, methods and technics which will ensure encryption (also called ciphering) and decryption (also called deciphering) of data in order to get confidentiality and authentication.



## Some historical bookmarks...



**Scytal** : VIth century b.c., Greece.

**Caesar** : shifting in the alphabet.

For instance, shifting of three letters on the right :

A	T	T	A	C	K	T	H	E	P	A	L	A	C	E
D	W	W	D	F	N	W	K	H	S	D	O	D	F	H

or one letter on the left :

I	B	M	W	N	T
H	A	L	V	M	S

# Enigma : The top model of the old fashion cryptography

**Enigma** : 1939–45, nazis WWII.





## Common points of the previous methods

The method (i.e. algorithm) used for the cipher is secret.

**Major disadvantage** : The method is not secret for the users.

☞ Kerchoffs' laws (19th century) :

*Main point : the security of a cipher should depend only on the key and not on the “method of ciphering”.*

## Democratisation of the secret.

## Some Terminology...

Our problematic will be often a “two player game”, say A and B. They want to exchange data on an open **transmission channel** (hence, it is possible to intercept data).

The goal is to describe, explain and analyse the methods (including concrete software or hardware implementations) for transforming an original message, that we will call **plaintext**, in an **equivalent** message such that the content is no longer readable. This process will be called **ciphering** and its inverse called **deciphering**. Such process will allow us to ensure **confidentiality** of the message. We will often call the ciphered message the **ciphertext**.

From a practical point of view, we will consider text only message (i.e. alphanumeric characters), but similar methods apply to general data (images, network frames, audio, video, etc).

## Terminology (continued)

A **cipher system** , also called **cryptosystem**, will denote the set of processes for encryption/decryption (the method, the algorithm and its implementation). We will speak of **cryptography** when we describe the concepts (an designs) of the cryptosystem. We will speak of **cryptanalysis** for denoting the science (and even the art !) of analysing a cryptosystem, in other word the methods for “breaking” the cryptosystem. The **cryptology** is the science (at the crossroad of mathematics, computer science, engineering and microelectronics) of cryptography and cryptanalyse.

We will often denote by  $M$  the plaintext,  $C$  the ciphertext,  $E$  the ciphering function and by  $D$  the deciphering function. We then have :

$$E(M) = C,$$

$$D(C) = M,$$

$$D(E(M)) = M.$$









## The four essential keywords of cryptography

In the “real life”, a cryptosystem should allow us to perform the following abilities :

- ❑ **Confidentiality** : it should be very difficult to break a message.
- ❑ **Authentication** : it should be possible for the receiver of a message to ensure the origin of the message. A third party should not be able to fake an identity.
- ❑ **Integrity** : the receiver should be able to ensure that the content has not been modified during the transmission. A third party should not be able to substitute part of a genuine message without being detected.
- ❑ **Non repudiation** : the sender (or the receiver) should not be able to deny the fact that he/she has sent (or received) a message.

**Remark** : As we can see, the three above constraints are of main importance from a law point of view.

## Today cryptography is everywhere...

- ❑ Military (and more generally governments security), and security of the companies,
- ❑ Banking system,   
- ❑ Internet (online shop, identification, incomes), 
- ❑ Mobile phones, electronic keys, GPS system (e.g., cars) 
- ❑ Pay-tv,
- ❑ Electronic National ID, health cards, 
- ❑ E-vote,
- ❑ DVD, Blue Ray, digital audio (some formats, e.g., WMA, AAC), 
- ❑ Games console (e.g., Xbox, Xbox360). 

## Algorithms and keys

An **algorithm of cryptography** (or cryptographic method) denotes the set of mathematical functions used for the ciphering and the deciphering. Such functions are usually viewed as a single function (or algorithm).

While in the prehistory of the cryptography, the security of a cryptosystem was solely based on the fact that the cryptographic method was secret. *It is only toward the end of the 19th century which was pointing out the fact that the security must not depend on the cryptographic method*

The articles of **Auguste Kerckhoffs** (« La cryptographie militaire », Journal des sciences militaires, vol. IX, pp. 5–38, Janvier 1883, pp. 161–191, Février 1883) set the background for modern cryptography



**Auguste Kerckhoffs 1835–1903**

## Kerkhoffs' Laws

Here are the (translation of the) six principles of practical cipher design of Kerckhoffs (originally for military cryptosystem) :

- ① The system should be, if not theoretically unbreakable, unbreakable in practice ;
- ② The design of a system should not require secrecy and compromise of the system should not inconvenience the correspondents ;
- ③ The key should be memorable without notes and should be easily changeable ;
- ④ The cryptograms should be transmittable by telegraph ;
- ⑤ The apparatus or documents should be portable and operable by a single person ;
- ⑥ The system should be easy, neither requiring knowledge of a long list of rules nor involving mental strain.

As a consequence, a cryptographic method uses keys for ciphering and deciphering. We will then denote the functions  $E$  and  $D$  by  $E_{K_1}$  or  $D_{K_2}$ , or even  $E_K$  and  $D_K$  if the keys are identical. In general the possible number of keys is very (very) large (far more than the number of atoms in the Universe).

We will speak of **keys' space** for the set of all the possible keys.



## The two family of cryptosystems

- Symmetric cipher
- Asymmetric cipher

# Symmetric cipher

*We say that a cryptosystem is symmetric if the ciphering keys and the deciphering keys can be deduce from each other in polynomial time.*

In practice, the key used for the ciphering will be the same than the one used for the deciphering.

☞ The inconveniency of such system is that the sender and the receiver must have the same key before starting secure transmission. Furthermore, we need a key for each user of the system.

**The most known symmetric ciphers** : DES, triple-DES, AES, RC4, One-time-pad.

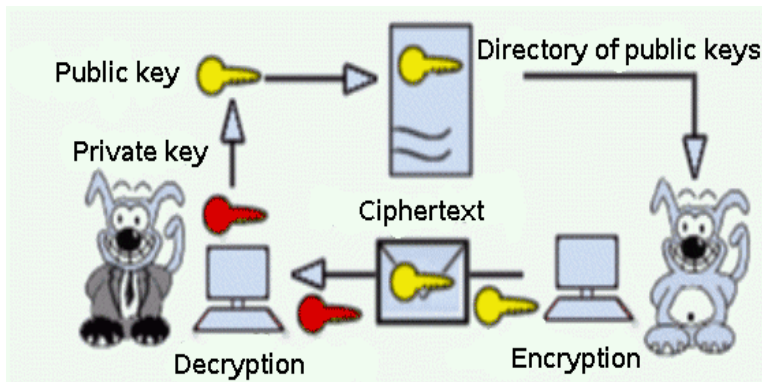
**Advantages** : ciphering is very fast.

## Asymmetric cipher (a.k.a. “public key cipher”)

Such ciphers use two different keys for ciphering and deciphering. In practice, we cannot recover the deciphering key from the ciphering key in polynomial time.

☞ we can give the cipher key.

We call the ciphering key the **public key** of the cryptosystem and the deciphering key the **private key**. The last one is secret.



The principle of public key cryptography has been introduced by Whitfield Diffie and Martin Hellman in 1976 (also done separately by Ralph Merkle).

Make use of *one-way function* (**public key**) with a trapdoor (**private key**).

☞ solve the problem of symmetric cryptography.

**Disadvantage** : 100 to 1000 (even more...) times slower than symmetric cryptography.

In practice, we mix both techniques (SSL, SSH, PGP for example).



Whitfield Diffie

*The fathers of public key cryptography...*



Martin Hellman

# Cryptanalysis

We distinguish four types of attacks :

- ❑ **Ciphertext-only attack** : The cryptanalyst has a serie of ciphertext, eventually ciphered with the same key. The goal is to find the plaintext for a large number of ciphertext, and eventually to retrieve the key (or the keys). Mathematically : We have  $C_i$  knowing that  $C_i = E_K(M_i)$  for  $i = 1, \dots, N$ , and we want to deduce  $M_{N+1}$  knowing  $C_{N+1}$ .
- ❑ **Known-plaintext attack** : The cryptanalyst has a set of plaintext with corresponding ciphertext. The problem is to retrieve the key from the data or an algorithm for the deciphering of any other ciphertext (ciphered with the same key). We know some fixed couples  $(M_i, C_i)$  with  $C_i = E_K(M_i)$  for  $i = 1, \dots, N$ , and we want to deduce either  $M_{N+1}$  knowing  $C_{N+1}$ , or  $K$ . Notice that in the case of a public key scheme we can make as much couples plaintext/ciphertext that we want.

- ❑ **Chosen–plaintext or Chosen–ciphertext attack (CCA)** : The cryptanalyst can choose the couples plaintext/ciphertext. This is a dangerous attack, as the cryptanalyst can use well crafted plaintext or ciphertext (with very specific format) and then get complementary data on the key.

*Illustration* : the vulnerability in SSL (with protocol RSA PKCS#1) found in 1998 was of the type “Chosen–ciphertext attack”.

- ❑ **Adaptative–Chosen–plaintext or Adaptative–Chosen–ciphertext attack** : It is a special case of the previous attack where the cryptanalyst can build pairs  $(C_{i+1}, M_{i+1})$  depending of the results at the step  $i$ .

## Security of Algorithms/Ciphers

In 1994, Lars Knudsen has proposed a classification for the “breaking” of a cryptosystem. This classification is the following and is useful in practice for the evaluation of cryptosystems :

- ➊ **Total break** : we can recover the key  $K$  such that  $C = D_K(M)$ .
- ➋ **Global deduction** : we can find an alternative algorithm for the deciphering without knowledge of the key (i.e., the algorithm gives  $D_K(C)$  without the knowledge of  $K$ ).
- ➌ **Local deduction** : we can find a plaintext from a ciphertext.
- ➍ **Partial deduction** : we can get partial information on the key or on the plaintext. For instance, we can know several bits of the key.

An algorithm is **unconditionnally secure**, if for any number of ciphertexts given to a cryptanalyst, there is not enough data for deducing the plaintext. In practice, we want cryptosystem hard to break even with a large computing power. It is what we called algorithms **computationally secure**. We formulate the complexity of breaking the algorithm by the number of (elementary) operations needed for the breaking. Currently, an algorithm using at least  $2^{80}$  (even  $2^{85}$ ...) operations is considered as “secure”.



## Difference between cryptography and steganography

The steganography is the art of hiding a text within a text without being seen. If we know the recipe for “the hiding”, we recover easily the text.

Currently, the most used steganographic method is via digital pictures ; we replace the least significant bit for each octet involved in the image (which usually encodes the color) by a bit of the text that we want hide. This type of change is almost invisible to the human eye.

For instance, in an album of 30 images with a resolution of  $1024 \times 768$ , we can hide a book of 300 pages.

## One-Time Pad

It is a commonly held misconception that every encryption method can be broken !

The One-Time pad is an example of such cipher. This cipher is of the type of “Vernam cipher”.

**The principle** : the key is a long list of **true random** characters that **we use only one time**. The ciphering is done by adding modulo 26 the plaintext to the key (i.e, the “one-time pad”) which should as long as the plaintext. Of course both the sender and the receiver should have the same pad.

☞ Claude Shannon proved that the one-time pad cipher is unbreakable, provided the key material is truly random, never reused, kept secret from all possible attackers, and of equal or greater length than the message.

For instance, if the plaintext is *ONETIMEPAD* and the pad is *TBFRGFARFMGQ*.

Then the ciphertext is *IPKLPSFHGQ*. Indeed,

$$\begin{aligned}O(15) + T(20) &= I(9) \pmod{26}, \\N(14) + B(2) &= P(16) \pmod{26}, \\&\vdots\end{aligned}$$

The problem of this method is that we need a huge quantity of true random characters which is difficult to provide.

## La problématique des tailles de clefs

Comparatif des tailles de clefs pour les chiffrements publics classiques en termes de «bits de sécurité»

bits of security	RSA key size	ECC key size
80	1024	160
112	2048	224
128	3072	256
256	15360	512

For ECC, the best known general attack (assuming well chosen parameters) is in  $O(\sqrt{n})$  where  $n$  is the order of the base point.

The above table should be understood as follows : given a line with  $k$  bits of security, an RSA key size of  $m$  bits and an ECC key size of  $n$  bits, it means that we need  $2^k$  operations in order to recover the RSA key of  $m$  bits or the ECC key of  $n$  bits.

## Quid de la taille de mes mots de passe ?

Le niveau de sécurité usuel est de 128 bits, une clef RSA 2048 bits (usuellement utilisée pour un certificat SSL pour une connexion web sécurisée) à une sécurité de 112 bits.

Sous l'hypothèse que le chiffrement du mot de passe se fait en «temps rapide» et que l'on utilise 80 caractères alphanumériques et spéciaux pour sa construction, nous avons la table de correspondance suivante :

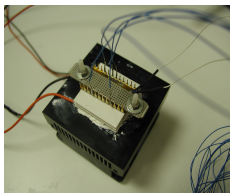
bits de sécurité	taille du mot de passe (nb de carac.)
80	13
112	18
128	21
256	41

**Conclusion :** Dans l'état actuel de la plupart des logiciels, si vous utilisez moins de 13 caractères quoi qu'il arrive, alors il est préférable d'attaquer votre portefeuille électronique que de casser vos clefs cryptographiques !

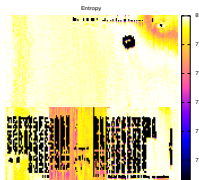
les mécanismes cryptographiques doivent être protégés contre les attaques physiques

Modification of the functioning parameters :

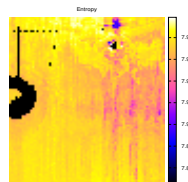
- Voltage/Power variations,
- Clocks perturbations,
- Extreme temperature,
- Fault injection (Laser beams, EM, Alpha ray, Gamma ray, etc),
- Whatever you can imagine...



Temperature perturbation  
(On a smartcard chip)



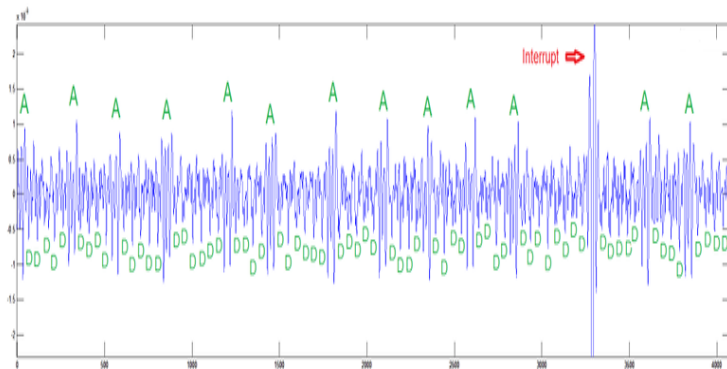
Laser perturbation  
(On a full CPU)



Focused Laser Perturbation  
(localized on the RNG of the CPU)

## Mais les implémentations cryptographiques dans les systèmes embarqués peuvent aussi être vulnérables

Genkin, Pachmanov, Pipman, Tromer and Yarom have shown (2016) that modern cryptographic software on mobile phones, implementing the ECDSA digital signature algorithm, may inadvertently expose its secret keys through physical side channels (with even a low cost attack) :



## Les vulnérabilités dans les logiciels : première source pour le cybercriminel

- OpenSSL (2014) : une vulnérabilité (aka «Heartbleed») dans le code d'OpenSSL (présente depuis plusieurs années!) permettait de récupérer des données sensibles coté client ou serveur.
- Distribution Linux Debian (2008) : le générateur de nombres aléatoires d'OpenSSL était devenu prédictible suite à un correctif (sic!).
- Dropbox (2011,2012,2013) : vulnérabilité dans l'authentification utilisée dans Dropbox, **vol de données clients via le piratage du compte d'un employé**, possibilité de vols de fichiers et d'infection/propagation de malware en utilisant Dropbox!
- PS3 (2010) : vulnérabilité dans le générateur de nombres aléatoires (erreur de programmation!).



## L'écosystème du cybercriminel

L'avènement du Darknet, initialement conçu (essentiellement par les USA et l'EU) pour permettre la liberté d'expression dans les pays où le pouvoir contrôle l'accès à l'information et a permis le développement de mouvements politiques «contestataires» au moyen-orient et en orient, a été mis a profit par la cybercriminalité.

- Réseau anonymisé et complètement décentralisé (pas d'autorité de contrôle telle que l'ICANN).
  - Possibilité de non tracabilité des logs (via des VPN anonymes).
  - Aucunes autorités de régulations (liberté d'expression «totale» pour le meilleur et pour le pire...).
- ☞ possibilité de faire des connexions «totalement» anonymes et (très) difficilement traçable (mais vulnérabilité de certains protocoles si l'on contrôle suffisamment de noeuds).

## L'écosystème du cybercriminel (suite)

- Les réseaux les plus connus ; TOR, FreeNet, GNUnet, I2P,
- Doivent être combinés avec un fournisseur de VPN non tracable (e.g., IPVanish),
- Nécessité d'anonymiser le poste de travail pour une protection maximale (e.g., utiliser des LiveUSB avec modifications d'adresses matérielles).
- Le bitcoin est, de fait, la monnaie d'échange (usuellement utilisé via un « tiers de confiance »).

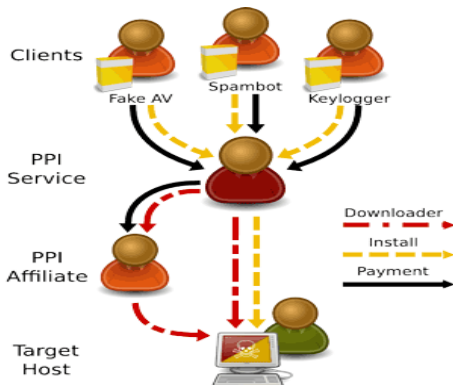
☞ Mais danger si on arrive à contrôler suffisamment de nœuds de distributions, possibilité de faire sauter l'anonymat (d'où la nécessité de VPN anonymisé).

## L'écosystème du cybercriminel (suite)

De fait, cela a créé une économie parallèle (avec son propre réseau de distribution) où l'on peut acheter en ligne des vulnérabilités logicielles, ou réseau, des données volées (pour fraude, usurpation d'identité), des outils «clef-en-main». En particulier,

- Achat en ligne de kit de phishing, facile à installer sur un serveur, afin de collecter des données et de les revendre via le «boncoin» du cybercriminel ou des forums spécialisés,
- Achat de vulnérabilités, d'exploits, de ransomware, etc (de quelques dollars à des milliers de dollars),
- Location de machines zombies pour attaques réseaux (DDOS), mise en place de botnets,
- Service de cassage de mots-de-passe sur une base de données,
- Achat ou vente de données volées (compte bancaire, messageries, identités, photos/vidéos, PI).

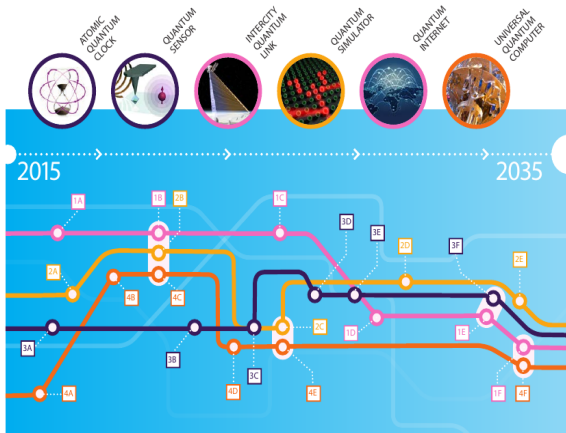
## L'écosystème du cybercriminel (suite)



(C) Juan Caballero, IMDEA Software Institute, Madrid, 2012.

Un exemple de fonctionnement de services cybercriminels de type PPI (Pay-Per-Install).

# The Post-Quantum Era ?



(C) 2016 «Quantum Manifesto»

☞ Both cryptographic primitives RSA and ECC are vulnerable to a (universal) quantum computer...

## Concrete examples

**SSL/TLS/WTLS, AACs, GSM/UMTS,  
WiFi, OpenPGP, SSH**

# TLS/SSL/WTLS

Transport Layer Security (TLS), formerly known as Secure Socket Layer (SSL) is a secure protocol for the web, initially developed by Netscape in 1994. It has been renamed Transport Layer Security (TLS) by IETF (Internet Engineering Task Force) in 2001. The name SSL is nevertheless still very popular. The versions 2 and 3 of the SSL protocol are commonly used by numerous servers.

👉 The goal is to achieve a fully secured channel between a web site and a navigator.

**Technical remark :** TLS differs from SSL mainly for symmetric keys generation, even if it is compatible with SSLv2/SSLv3. WTLS is the WAP version of TLS.

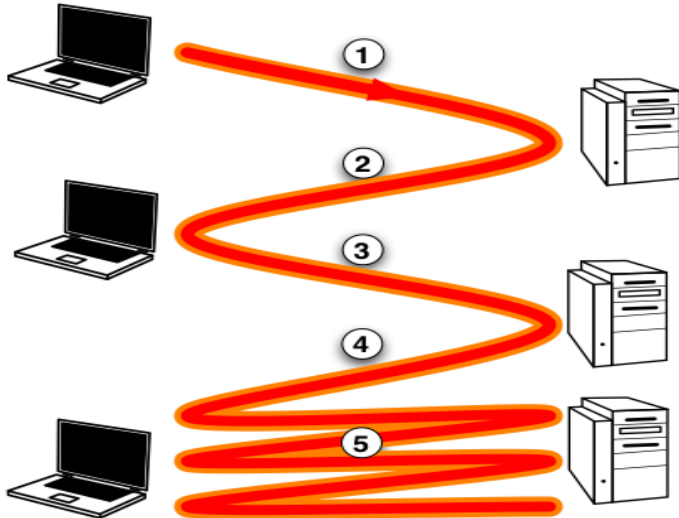
The SSL protocol works in a **client-server** mode and fulfils the essential goals of security :

- ❑ **server authentication** ;
- ❑ **confidentiality** of the data ;
- ❑ **integrity** of the data ;
- ❑ and optionally **authentication of the client**.

**From the network technical viewpoint** : SSL is between the applications layer (as HTTP, FTP, SMTP, etc) and the transport layer such as TCP. Its common use remains with the HTTP layer (either for web shopping or banking access).



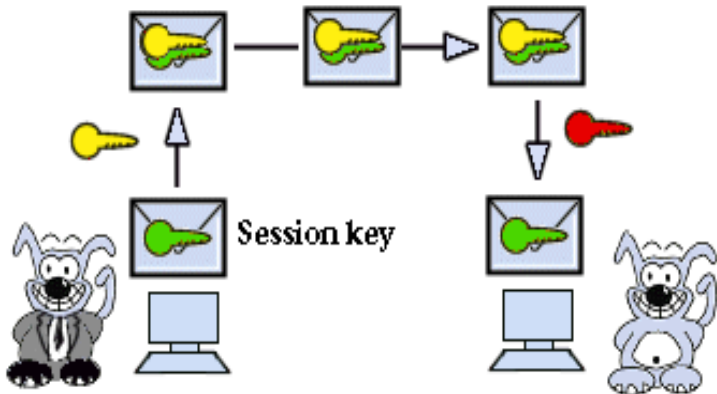
The principle of the exchange is described in the picture below :



The details of the different steps is as follows :

- ① The web navigator sends a request for secure channel to the web server.
- ② The web server sends **its certificate** (i.e., an ID delivered by a trusted authority) and **its public key**.
- ③ The web navigator **checks the certificate**. If the certificate is validated (i.e., authentication of the web site is successful) then the web navigator sends **a secret key (for use with a symmetric cipher) “randomly” generated** which will be **encrypted with the public key of the web server**.
- ④ The web server decrypts the secret key using its private key.
- ⑤ The navigator and the web server establish a secure channel encrypted with the secret key (called **session key**)

Let summarise it !



The couple private/public key is illustrated by the couple **red key**/**yellow key**.

The session key (**green key**) shows the use of the symmetric cipher.

👉 While several choices are available for the encryption/decryption parameters, it is common to find RSA1024 with public exponent 65537 ( $= 2^{16} + 1$ ) for the asymmetric part, AES128, RC4 (128 bits) and AES256 for the symmetric part, and SHA-1 as hash function. Notice that in OpenSSL 0.9.8 (and above), asymmetric ciphers based on Elliptic Curves are available (we will speak about that in Master 2).

Notice also that the protocol allows the possibility for the server to ask the client for authentication via a certificate.

# AACS



**advanced access content system**

The standard AACS (Advanced Access Content System) is the successor of CSS (used for “protection” of the DVD) and has the goal to be the reference for protection of audio/video contents. This is the method used for the Blue-Ray and the HD–DVD. Developed during the years 2000, it is endorsed by a consortium of big names (such as Intel, Microsoft, Disney, Sony, Warner, IBM,...).

The cryptographic primitives used are :

- ❑ AES128 for the symmetric part ;
- ❑ ECDSA, for the signature based on ECC (Elliptic Curve Cryptography) ;
- ❑ SHA1 as hash function ;
- ❑ and RSA2048 via a TLS/SSL protocol for updating the player (and validate the contents).

👉 *One of the leading company in protection of multimedia content is THOMSON (also owner of the MP3 license).*

A multimedia content protected with AACCS is encrypted with one or several **Title keys** using AES128.

The Title keys are derived from several parameters such as a key associated to a support.

With AACCS, each device (e.g., a Blue-Ray player) has its own key for decryption which could be revoked (in case of illegal use) via an online connexion.

## Example of network connexion with AACS

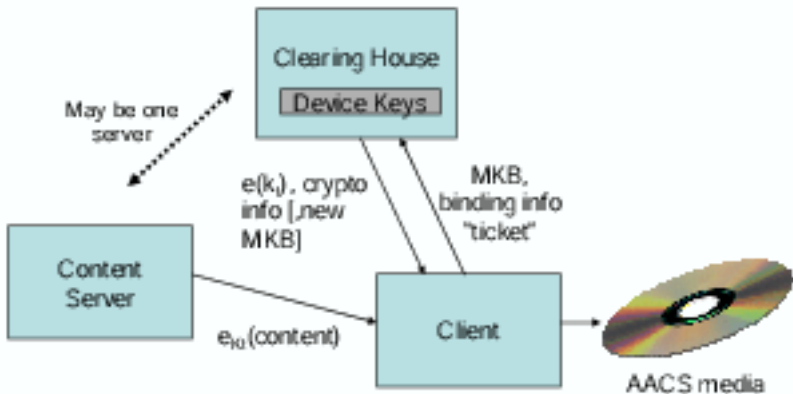


Figure 5-3 – Example System for AACS Network Download



# The Global System for Mobile Communications

communication  
sans fil  
chiffrée



communication  
cablée  
non chiffrée



GSM<sup>®</sup>

Opérateur

## The GSM (continued)

based on the protocol A5 (a symmetric cipher) with a key of

54 bits in USA,

64 bits in Europe.

**The GSM was designed to be breakable...**

...and, as a matter of fact, it is!

GSM USA is breakable in less than 100 000 operations

→ decryption in real time.

GSM Europe is breakable in less than 1000 billions of operations

→ decryption in few minutes.

## UMTS (or 3G)

UMTS (Universal Mobile Telecommunications System) or also called in Europe 3GPP, has a more advanced cipher. The method is based on the algorithm KASUMI with a secret key of 128 bits.

👉 No public key ciphers for the UMTS. It is considered useless and too costly. It is nevertheless technically possible.

## The WiFi (aka IEEE 802.11)



The **WEP (Wired Equivalent Privacy)**, is an algorithm to secure IEEE 802.11 wireless networks. It is based on the protocol RC4.

key length of 40 bits granted in 1992 (after negotiation with the NSA).  
key length of 104 bits granted since 1999 (after prosecution against the US government).

The **WPA (Wi-Fi Protected Access)** use a key of 128 bits and performs dynamic changes of keys as the system is used.

The **WPA2** uses AES 128 bits.

## Some timing attacks for 1 PC

Brute force attack (every keys are tested)

WEP 40 bits	10 minutes
GSM 64 bits	10 years
WEP 104 bits	$10^{14}$ years (The age of the Universe!)
WPA 1/2 128 bits	$10^{22}$ years

Best known attacks

WEP 40/104 bits	10 secondes
WPA2	$10^{22}$ years
GSM Europe	10 minutes
GSM US	milliseconds
Bluetooth	seconds

👉 As a result WEP is now a deprecated algorithm for securing IEEE 802.11 wireless networks.

# OpenPGP



*OpenPGP...*



**History :** The software Pretty Good Privacy (or PGP) is at the beginning a software for securing emails. It was developed by Philip Zimmermann in 1991. Widely used during the 90', its protocol and data formats became a reference and then a standard called "OpenPGP", which is adopted by several tools as PGP, GNU Privacy Guard (GnuPG, also called GPG) the free version of PGP and dozens of others.

It is currently the standard for securing emails.

# Principle of OpenPGP

The start, for the user, is to generate a pair **private key / public key** for the asymmetric part using one of the proposed algorithm (e.g., ElGamal, RSA). We choose also an algorithm for signature and eventually a symmetric algorithm for encryption.

Then, the user gives its public key (put it on a web page for instance), in order to allow others to send encrypted emails to him (there is still the problem to authenticate the public key with its owner).

When we want to send a message, the plaintext is encrypted with a symmetric algorithm using a **session key** which will be encrypted with the public key of the recipient.

The private key of the sender is used for signing the message. The ciphertext is then formatted according to the protocol OpenPGP and then sent on the network (with the usual SMTP protocol).

# SSH

SSH is the abbreviation of Secure Shell, which is both a client/server software and a protocol for secure communication. The protocol is designed for long time connexion between different computers.

**History :** The first version of SSH (SSH-1) was designed by Tatu Ylönen in Finland in 1995. This version had a security hole (used in the movie *Matrix : Reloaded*). In 1996, a revised version of the protocol was proposed and called SSH-2. This is the version in use today. Since 2006, SSH is standardised by the IETF. The free implementation of SSH is called OpenSSH and widely used.

**Principle :** it is a “classical” combination of asymmetric and symmetric methods with session key.



# The “crack” of Trinity (Matrix Reloaded) on SSH-1

```
* Welcome to CityPower Grid Rerouting *
Authorized Users only!
New users MUST notify Sys/Ops.

login:

80/tcp    open      http
81/tcp    open      hosts2-nc
10.2.2.2  [mobile]
11 # nmap -v -sS -O 10.2.2.2
11
13 Starting nmap V. 2.54(11025)
13 Insufficient responses for TCP sequencing (3), OS detection may be less
13 accurate
14 Interesting ports on 10.2.2.2:
14 (The 1539 ports scanned but not shown below are in state: closed)
51 Port      State      Service
51 22/tcp    open      ssh
58
68 No exact OS matches for host
68
74 Nmap run completed -- 1 IP address (1 host up) scanned
50 # sshnuke 10.2.2.2 -rootpw="210N0101"
Connecting to 10.2.2.2:ssh ... successful.
Re Attempting to exploit SSHv1 CRC32 ... successful.
IP Resetting root password to "210N0101".
System open: Access Level <9>
50 # ssh 10.2.2.2 -l root
root@10.2.2.2's password:
RRF-CONTROL> disable grid nodes 21 -- 48
```