

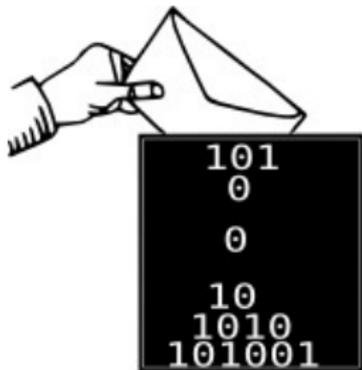
# Introduction à la sécurité

Pascal LAFOURCADE



9 Septembre 2020  
Aurillac, département STID

# L'informatique est omniprésente



# Statistiques en cybersécurité en 2019



1. 92% malwares sont propagés par email
2. Ransomwares coûteront \$11.5 milliards en 2019
3. Phishing par email est responsable de 91% de cyberattaques
4. Coût global du cybercrime 2 millions de milliards \$ en 2019
5. 7 entreprises sur 10 ne sont pas prêtes face aux cyber attaques
6. 43% des cyberattaques visent les petites entreprises
7. 90% des violations de données sont dues à une erreur humaine.

Source : <https://thebestvpn.com/cyber-security-statistics-2019>

# Plan

Introduction

La sécurité et vous ?

Cybercriminalité

Intelligence Économique

IoT

Définir la sécurité

Sécurité des données

RGPD

Conclusion

# 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



# En réalité



# En réalité

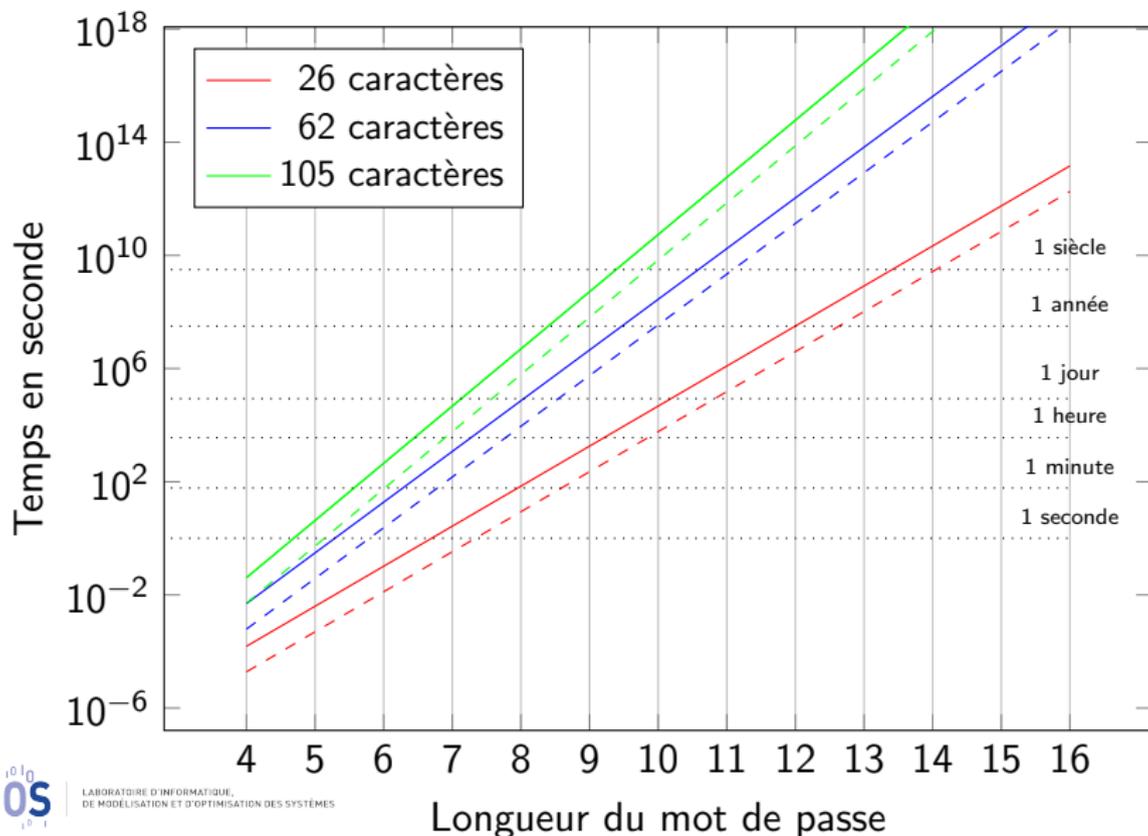


# TOP 25 Passwords

#	2011	2012	2013	2014	2015	2016	2017	2018
1	password	password	123456	123456	123456	123456	123456	123456
2	123456	123456	password	password	password	password	password	password
3	12345678	12345678	12345678	12345	12345678	12345	12345678	123456789
4	qwerty	abc123	qwerty	12345678	qwerty	12345678	qwerty	12345678
5	abc123	qwerty	abc123	qwerty	12345	football	12345	12345
6	monkey	monkey	123456789	123456789	123456789	qwerty	123456789	111111
7	1234567	letmein	111111	1234	football	1234567890	letmein	1234567
8	letmein	dragon	1234567	baseball	1234	1234567	1234567	sunshine
9	trustno1	111111	iloveyou	dragon	1234567	princess	football	qwerty
10	dragon	baseball	adobe123	football	baseball	1234	iloveyou	iloveyou
11	baseball	iloveyou	123123	1234567	welcome	login	admin	princess
12	111111	trustno1	admin	monkey	1234567890	welcome	welcome	admin
13	iloveyou	1234567	1234567890	letmein	abc123	solo	monkey	welcome
14	master	sunshine	letmein	abc123	111111	abc123	login	666666
15	sunshine	master	photoshop	111111	1qaz2wsx	admin	abc123	abc123
16	ashley	123123	1234	mustang	dragon	121212	starwars	football
17	bailey	welcome	monkey	access	master	flower	123123	123123
18	passw0rd	shadow	shadow	shadow	monkey	passw0rd	dragon	monkey
19	shadow	ashley	sunshine	master	letmein	dragon	passw0rd	654321
20	123123	football	12345	michael	login	sunshine	master	!@#% ^ &*
21	654321	jesus	password1	superman	princess	master	hello	charlie
22	superman	michael	princess	696969	qwertyuiop	hottie	freedom	aa123456
23	qazwsx	ninja	azerty	123123	solo	loveme	whatever	donald
24	michael	mustang	trustno1	batman	passw0rd	zaq1zaq1	qazwsx	password1
25	Football	password1	000000	trustno1	starwars	password1	trustno1	qwerty123

# Passwords Brute Force

3GHz PC ( - - - 8 cores)



# Quelques chiffres

number of Characters	Numbers only	Upper or lower case letters	upper or lower case letters mixed	numbers, upper and lower case letters	numbers, upper and lower case letters, symbols
3	Instantly	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	3 secs	10 secs
6	Instantly	Instantly	8 secs	3 mins	13 mins
7	Instantly	Instantly	5 mins	3 hours	17 hours
8	Instantly	13 mins	3 hours	10 days	57 days
9	4 secs	6 hours	4 days	1 year	12 years
10	40 secs	6 days	169 days	106 years	928 years
11	6 mins	169 days	16 years	6k years	71k years
12	1 hour	12 years	600 years	108k years	5m years
13	11 hours	314 years	21k years	25m years	423m years
14	4 days	8k years	778k years	1bn years	5bn years
15	46 days	212k years	28m years	97bn years	2tn years
16	1 year	512m years	1bn years	6tn years	193tn years
17	12 years	143m years	36bn years	374tn years	14qd years
18	126 years	3bn years	1tn years	23qd years	1qt years

Key:

k – Thousand (1,000 or  $10^3$ )

m – Million (1,000,000 or  $10^6$ )

bn – Billion (1,000,000,000 or  $10^9$ )

tn – Trillion (1,000,000,000,000 or  $10^{12}$ )

qd – Quadrillion (1,000,000,000,000,000 or  $10^{15}$ )

qt – Quintillion (1,000,000,000,000,000,000 or  $10^{18}$ )

## Calculer la « force » d'un mot de passe



Type de mot de passe	Taille de clé équivalente	Force	Commentaire
Mot de passe de 8 caractères dans un alphabet de 70 symboles	49	Très faible	Taille usuelle
Mot de passe de 10 caractères dans un alphabet de 90 symboles	65	Faible	
Mot de passe de 12 caractères dans un alphabet de 90 symboles	78	Faible	Taille minimale recommandée par l'ANSSI pour des mots de passe ergonomiques ou utilisés de façon locale.
Mot de passe de 16 caractères dans un alphabet de 36 symboles	82	Moyen	Taille recommandée par l'ANSSI pour des mots de passe plus sûrs.
Mot de passe de 16 caractères dans un alphabet de 90 symboles	104	Fort	
Mot de passe de 20 caractères dans un alphabet de 90 symboles	130	Fort	Force équivalente à la plus petite taille de clé de l'algorithme de chiffrement standard AES (128 bits).

# 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.



## FESTIVAL du FILM SÉCURITÉ

2018

GRAND PRIX DU FESTIVAL

Les 10 commandements de la Cyber-Victime

par Micode

VIDEO

# Fuite de base de données

rockyou

New RockYou Password

Retype Password

I agree to the Terms of Service.

Year of Birth

Sex

Country

Zip/Postal

```
79985232 | -- | - a@fbi.gov-|+u)ciL90fBnIoxG6CatHBw==|-anniversary|--
165089730 | -- | - gon@ic.fbi.gov-| -9nCb38RH1w==|-band|--
108684532 | -- | - burn@ic.fbi.gov-| -EQ7fIp71/Q=-|-numbers|--
63041670 | -- | - v-| -hRwtmq98mkZioxG6CatHBw==|-|--
94038395 | -- | - n@ic.fbi.gov-| -MreVpEovY17ioxG6CatHBw==|-eod date|--
116097938 | -- | - r-| -Tur7Wt2zH5CwIIHfjvchKQ==|-SH?|--
83310434 | -- | - c.fbi.gov-| -NLupdfyYrsM=-|-ATP MIDDLE|--
113389790 | -- | - v-| -iMhæearHXjPioxG6CatHBw==|-w|--
113931981 | -- | - @ic.fbi.gov-| -lTmosXxYnP3ioxG6CatHBw==|-See MSDN|--
114081741 | -- | - lom@ic.fbi.gov-| -ZcDbLlvCad0=-|-fuzzy boy 20|--
106145242 | -- | - @ic.fbi.gov-| -xc2KumNGzYfioxG6CatHBw==|-4s|--
106437837 | -- | - i.gov-| -adIewKvmJEsFqx0HFoFrXg==|-|--
96649467 | -- | - ius@ic.fbi.gov-| -lSjW5KRKNT/ioxG6CatHBw==|-glass of|--
96670195 | -- | - .fbi.gov-| -X4-k4uhy0h/ioxG6CatHBw==|-|--
105095956 | -- | - earthlink.net-| -ZU2tTTFIZq/ioxG6CatHBw==|-socialsecurity#|--
108260815 | -- | - r@genext.net-| -MuKnZ7KtsiHiioxG6CatHBw==|-socialsecurity|--
83508352 | -- | -h @hotmail.com-| -ADEcoaN2oUM=-|-socialsecurityno.|--
83023162 | -- | -k 390@aol.com-| -9HT+kVHQfs4=-|-socialsecurity name|--
96331688 | -- | -b .edu-| -nNiwEcoZTBmXrIXpAZIRHQ==|-ssn#|--
```

# BYOD : Bring Your Own Device

- ▶ Smartphone, tablette, ordinateur personnel
- ▶ Connexion au réseau de l'entreprise,
- ▶ Nouveaux risques (Sécurité, Juridique, RH)



# BYOD : Bring Your Own Device

- ▶ Smartphone, tablette, ordinateur personnel
- ▶ Connexion au réseau de l'entreprise,
- ▶ Nouveaux risques (Sécurité, Juridique, RH)



## Solutions

Cloisonner, contrôler l'accès, chiffrement des flux (VPN, HTTPS),  
procédure en cas de panne/perte, mesures de sécurité élémentaires

**SENSIBILISER**

# BYOD : Bring Your Own Device

- ▶ Smartphone, tablette, ordinateur personnel
- ▶ Connexion au réseau de l'entreprise,
- ▶ Nouveaux risques (Sécurité, Juridique, RH)



## Solutions

Cloisonner, contrôler l'accès, chiffrement des flux (VPN, HTTPS),  
procédure en cas de panne/perte, mesures de sécurité élémentaires

**SENSIBILISER**

CYOD : Choose Your Own Device

FYOD : Fix Your Own Device

DYOD: Download on Your Own Device

# Plan

Introduction

La sécurité et vous ?

Cybercriminalité

Intelligence Économique

IoT

Définir la sécurité

Sécurité des données

RGPD

Conclusion

## 5 Familles de Cybercriminalité

- ▶ Escroquerie
- ▶ Sabotage
- ▶ Ransomwares
- ▶ Espionnage
- ▶ Destabilisation



# Escroquerie : Phishing



Third party Facebook application. This is not Facebook!

**Facebook Verification Page**

Page Name:

Email or Phone:

Password:

By clicking Submit, you agree to our Terms and that you have read our Data Use Policy.

[Forgot your password?](#)

English (US) Македонски Español Português (Brasil) Français (France) Deutsch Italiano العربية 繁體中文 (繁體) 中文 (简体)

Voyant + Papillon

# Escroquerie : Fraude au président



[@PNationale](#) [/ Police Nationale](#)

VIDEO

# Sabotage

## Stuxnet, 2010

### HOW STUXNET WORKED



#### 1. infection

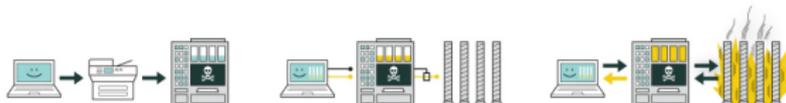
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

#### 2. search

Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

#### 3. update

If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.



#### 4. compromise

The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities—software weaknesses that haven't been identified by security experts.

#### 5. control

In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

#### 6. deceive and destroy

Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

Saudi Aramco 35 000 PC deleted in 2012.

# Ransomwares: Wannacry et al. 12 may 2017

Wana Decrypt0r 2.0

Ooops, your files have been encrypted! English

**What Happened to My Computer?**  
Your important files are encrypted.  
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

**Can I Recover My Files?**  
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.  
You can decrypt some of your files for free. Try now by clicking <Decrypt>.  
But if you want to decrypt all your files, you need to pay.  
You only have 3 days to submit the payment. After that the price will be doubled.  
Also, if you don't pay in 7 days, you won't be able to recover your files forever.  
We will have free events for users who are so poor that they couldn't pay in 6 months.

**How Do I Pay?**  
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.  
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.  
And send the correct amount to the address specified in this window.  
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am  
NOT from Monday to Friday

**Payment will be raised on**  
5/16/2017 00:47:55  
Time Left  
02:23:57:37

**Your files will be lost on**  
5/20/2017 00:47:55  
Time Left  
06:23:57:37

[About bitcoin](#)  
[How to buy bitcoins?](#)  
[Contact Us](#)

**Send \$300 worth of bitcoin to this address:**  
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw Copy

Check Payment Decrypt

<http://stopransomware.fr/>

# Espionnage



- ▶ Little Brother (Individuel)
- ▶ Medium Brother (Entreprise)
- ▶ Big Brother (Gouvernement)

Edward Joseph Snowden, 6th june 2013



# Une technique d'espionnage : MICE

**M**onnaie



**I**déologie



**C**ompromission



**E**go



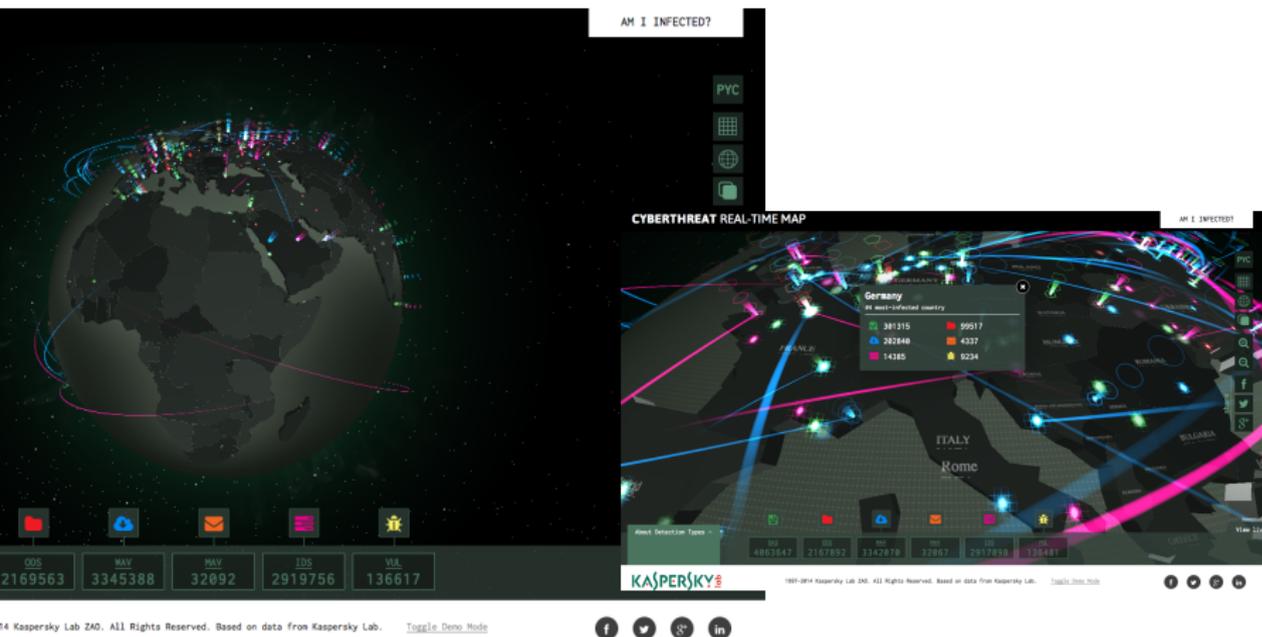
# Destabilisation : Defacement



# Destabilisation: Trojan, Botnets and Zombies



<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 ...

mais faussement anonyme !



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



Rapide, large échelle, semi-automatique ...

mais faussement anonyme !



Internet a été conçu pour fonctionner pas pour être sûr !

# Agences pour la sécurité informatique



# Cyberguerre est une réalité

\$7 milliards pour les opérations cyber en 2017 au USA et plus de \$35 milliards sur 5 ans.

# Cyberguerre est une réalité

\$7 milliards pour les opérations cyber en 2017 au USA et plus de \$35 milliards sur 5 ans.

- ▶ Communication est essentielle : révolutions en Egypte, Tunisie



# Cyberguerre est une réalité

\$7 milliards pour les opérations cyber en 2017 au USA et plus de \$35 milliards sur 5 ans.

- ▶ Communication est essentielle : révolutions en Egypte, Tunisie



- ▶ Identifier les auteurs n'est pas facile



# Cyberguerre est une réalité

\$7 milliards pour les opérations cyber en 2017 au USA et plus de \$35 milliards sur 5 ans.

- ▶ Communication est essentielle : révolutions en Egypte, Tunisie



- ▶ Identifier les auteurs n'est pas facile
- ▶ Stratégies de défense et d'attaques sont différentes



# Cyberguerre est une réalité

\$7 milliards pour les opérations cyber en 2017 au USA et plus de \$35 milliards sur 5 ans.

- ▶ Communication est essentielle : révolutions en Egypte, Tunisie



- ▶ Identifier les auteurs n'est pas facile
- ▶ Stratégies de défense et d'attaques sont différentes



- ▶ Cyberattaques ont des conséquences physiques



# Plan

Introduction

La sécurité et vous ?

Cybercriminalité

**Intelligence Économique**

IoT

Définir la sécurité

Sécurité des données

RGPD

Conclusion

# Intelligence Économique

Maîtrise et protection de l'information stratégique utile pour tout acteur économique



## 3 piliers

- ▶ Maîtrise de l'information, management des connaissances
- ▶ Protection du patrimoine informationnel
- ▶ Stratégie d'influence et lobbying

La compétitivité est la finalité de l'IE

**LIMOS** Intelligence ( = renseignement )

# Maîtriser l'Information

- ▶ Identifier les sources
- ▶ Collecter l'information (veille, reseaux sociaux ...)
- ▶ Exploitation : analyse et aide à la décision
- ▶ Diffusion :



**“Seuls les paranoïaques survivent”**

Andy GROVE, Co-fondateur d'Intel en 1968

## “Seuls les paranoïaques survivent”

Andy GROVE, Co-fondateur d'Intel en 1968

1. Classification de l'information
2. Diagnostic
3. Protection des accès
4. Sensibilisation
5. Surveillance, détection





# Plan

Introduction

La sécurité et vous ?

Cybercriminalité

Intelligence Économique

IoT

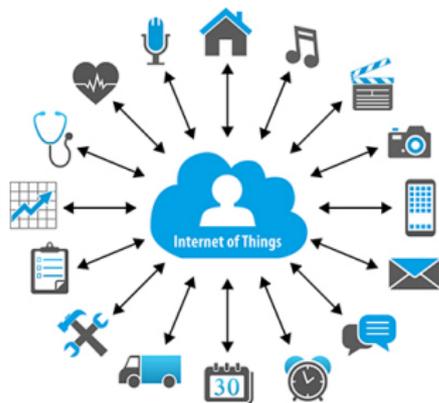
Définir la sécurité

Sécurité des données

RGPD

Conclusion

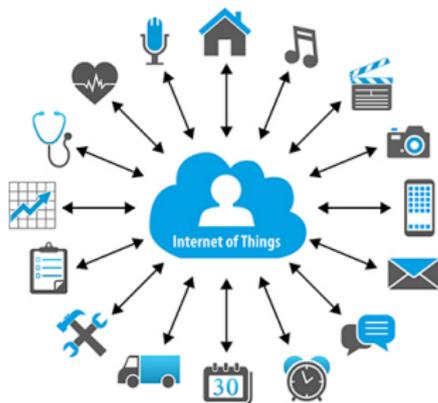
# Raisons du succes de l'IOT



## Technologie

- ▶ Wireless : Wifi, 3G, 4G, 5G, Bluetooth, Sigfox ...
- ▶ Batteries
- ▶ CPU
- ▶ Capteurs
- ▶ Prix

# Raisons du succes de l'IOT



## Technologie

- ▶ Wireless : Wifi, 3G, 4G, 5G, Bluetooth, Sigfox ...
- ▶ Batteries
- ▶ CPU
- ▶ Capteurs
- ▶ Prix

## Usage

- ▶ Surveillance
- ▶ Hyperconnectivité
- ▶ Disponibilité

# Attaques d'IoT depuis 2007 ...



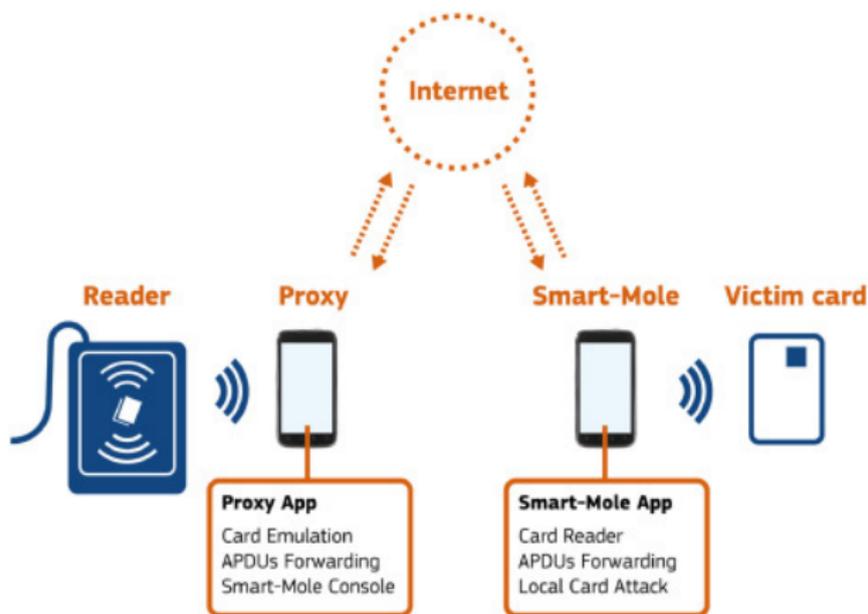
# Attaques d'IoT depuis 2007 ...



# Attaques d'IoT depuis 2007 ...



# Attaque par relais



VIDEO VOITURE + Suisse

# Analyse de Logs

```
C:\Windows\system32\cmd.exe
TCP 192.168.2.104:11062 207.115.110.252:64309 TIME_WAIT
TCP 192.168.2.104:154514 65.52.188.74:443 ESTABLISHED
TCP 192.168.2.104:154585 64.74.103.144:80 ESTABLISHED
TCP 192.168.2.104:154589 74.125.196.100:8228 ESTABLISHED
TCP 192.168.2.104:154636 58.23.164.175:443 ESTABLISHED
TCP 192.168.2.104:154638 54.209.119.12:443 ESTABLISHED
TCP 192.168.2.104:154642 54.184.100.115:443 ESTABLISHED
TCP 192.168.2.104:154643 74.125.21.189:443 ESTABLISHED
TCP 192.168.2.104:154649 52.21.43.125:443 ESTABLISHED
TCP 192.168.2.104:154676 54.209.119.12:443 ESTABLISHED
TCP 192.168.2.104:154728 104.16.32.27:443 ESTABLISHED
TCP 192.168.2.104:154740 54.94.8.82:443 ESTABLISHED
TCP 192.168.2.104:154765 74.125.196.109:443 ESTABLISHED
TCP 192.168.2.104:154776 74.125.196.109:443 ESTABLISHED
TCP 192.168.2.104:155942 104.16.32.27:443 ESTABLISHED
TCP 192.168.2.104:155983 104.16.32.27:443 ESTABLISHED
TCP 192.168.2.104:156480 173.194.219.109:443 ESTABLISHED
TCP 192.168.2.104:156500 216.58.219.101:443 ESTABLISHED
TCP 192.168.2.104:156517 65.65.64.94:443 ESTABLISHED
TCP 192.168.2.104:156518 65.65.64.94:443 ESTABLISHED
TCP 192.168.2.104:157227 157.58.134.171:32033 ESTABLISHED
TCP 192.168.2.104:157425 65.65.64.94:443 ESTABLISHED
TCP 192.168.2.104:157428 65.65.64.100:443 ESTABLISHED
TCP 192.168.2.104:157614 104.16.32.27:443 ESTABLISHED
TCP 192.168.2.104:157630 198.38.124.176:443 ESTABLISHED
TCP 192.168.2.104:157636 198.38.124.181:443 ESTABLISHED
TCP 192.168.2.104:157658 91.190.210.62:12350 ESTABLISHED
TCP 192.168.2.104:157674 216.58.219.65:443 TIME_WAIT
TCP 192.168.2.104:157677 216.58.219.65:443 FIN_WAIT_2
TCP 192.168.2.104:157712 216.58.219.103:443 ESTABLISHED
TCP 192.168.2.104:157725 104.16.32.27:443 ESTABLISHED
TCP 192.168.2.104:157752 58.112.252.181:443 TIME_WAIT
TCP 192.168.2.104:157757 72.246.64.111:80 ESTABLISHED
TCP 192.168.2.104:157761 65.65.64.93:443 TIME_WAIT
TCP 192.168.2.104:157762 65.65.64.93:443 ESTABLISHED
TCP 192.168.2.104:157774 40.117.100.83:443 TIME_WAIT
TCP 192.168.2.104:157775 40.117.100.83:443 TIME_WAIT
TCP 192.168.2.104:157780 65.65.64.100:80 TIME_WAIT
TCP 192.168.2.104:157788 173.216.40.107:31802 TIME_WAIT
TCP 192.168.2.104:157789 79.136.88.109:17126 TIME_WAIT
TCP 192.168.2.104:157793 92.255.89.248:12227 TIME_WAIT
TCP 192.168.2.104:157793 87.240.23.123:3762 TIME_WAIT
TCP 192.168.2.104:157794 104.40.87.245:50003 TIME_WAIT
TCP 192.168.2.104:157796 104.40.87.245:50004 TIME_WAIT
TCP 192.168.2.104:157798 104.40.87.245:50004 TIME_WAIT
TCP 192.168.2.104:157798 83.254.163.212:42773 TIME_WAIT
TCP 192.168.2.104:157799 151.240.200.119:54627 TIME_WAIT
TCP 192.168.2.104:157800 104.40.87.245:50001 TIME_WAIT
TCP 192.168.2.104:157803 159.177.75.123:80 ESTABLISHED
TCP 192.168.2.104:157812 40.117.100.83:443 TIME_WAIT
TCP 192.168.2.104:157813 40.117.100.83:443 TIME_WAIT
TCP 192.168.2.104:157824 216.58.219.165:443 ESTABLISHED
TCP 192.168.2.104:157831 40.117.100.83:443 TIME_WAIT
TCP 192.168.2.104:157832 40.117.100.83:443 TIME_WAIT
TCP 192.168.2.104:157844 54.232.255.200:443 ESTABLISHED
TCP 192.168.2.104:157846 168.63.133.99:443 ESTABLISHED
TCP 192.168.2.104:157847 40.117.100.83:443 ESTABLISHED
```

## Statistiques et IDS (Intruder Detection System)

# Plan

Introduction

La sécurité et vous ?

Cybercriminalité

Intelligence Économique

IoT

Définir la sécurité

Sécurité des données

RGPD

Conclusion

# Propriétés de sécurité traditionnelles

- Confidentialité
- Authentification
- Intégrité
- Disponibilité

# Authentication



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

# Mécanismes d'authentification

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

## Authentification forte

# Autres propriétés de sécurité

- ▶ Non-repudiation
- ▶ Équité
- ▶ Privacy
  - ▶ Anonymat
  - ▶ Pseudonymat

# Plan

Introduction

La sécurité et vous ?

Cybercriminalité

Intelligence Économique

IoT

Définir la sécurité

Sécurité des données

RGPD

Conclusion

# Mesures de sécurité

## Contrôle d'accès

Restreindre l'accès aux données aux utilisateurs autorisés

## Contrôle des flux (Control-flow)

Empêcher que des informations changent d'état  
(autorisé  $\leftrightarrow$  non-autorisé)

▶ explicite :

```
p:=s;
```

▶ implicite :

```
if s=true then p:=true else p:=false;
```

## Chiffrement

Utilisation de la cryptographie pour protéger les données.

# Respect de la vie privée des données (Philippe Golle 2006)

## Données américaines 2000

Date de naissance + Code Postal + Sexe  
= Identification

	ZIP code	Conté
Année	0.2%	0.0%
Année + Mois	4.2%	0.2%
Année + Mois + jour	63.3%	14.8%

# Respect de la vie privée des données (Philippe Golle 2006)

## Données américaines 2000

Date de naissance + Code Postal + Sexe  
= Identification > 63%

# Respect de la vie privée des données (Philippe Golle 2006)

## Données américaines 2000

Date de naissance + Code Postal + Sexe  
= Identification > 63%

	ZIP code	Conté
Année	0.2%	0.0%
Année + Mois	4.2%	0.2%
Année + Mois + jour	63.3%	14.8%

# Deux types de données

- ▶ Données à caractère personnel
- ▶ Données anonymes

## CNIL:

*“Dès lors qu’elles concernent des personnes physiques identifiées directement ou indirectement.”*

## Loi Française:

*“Pour déterminer si une personne est identifiable, il convient de considérer l’ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne.”*

# Comment évaluer la sécurité?

## Trois critères:

- ▶ **Individualisation** : Isoler des données qui identifient un individu.
- ▶ **Liabilité (Corrélation)**: Lier au moins deux données concernant une personne.
- ▶ **Inférence (Deduction)**: Déduire avec une probabilité suffisante la valeur d'un attributs à partir des données.

# Example

ID	Age	CP	Sexe	Pathologie
Paul Sésame	75	75000	F	Cancer
Pierre Richard	55	78000	F	Cancer
Henri Poincarré	40	71000	M	Grippe

# Techniques aléatoire

En altérant la véracité des données.

- ▶ **Ajout de bruit**
- ▶ **Permutation des données**
- ▶ **Differential Privacy**<sup>1</sup>:

```
Q = select count()  
      where Age = [20,30]  
            and Diagnosis=B+
```

La réponse de Q sur D1 et D2 doit être indistinguishable à un individu près.

# Pseudonymisation

Remplacer un identifiant par un pseudonyme

ID	Age	CP	Sexe	Pathologie
1	75	75000	F	Cancer
2	55	78000	F	Cancer
3	40	71000	M	Grippe

N'assure par l'anonymat

# k-Anonymat

- ▶ Identifier des champs qui peuvent être généralisés
- ▶ Les modifier pour avoir au moins  $k$  lignes différentes avec les mêmes identifiants

# k-Anonymat

- ▶ Identifier des champs qui peuvent être généralisés
- ▶ Les modifier pour avoir au moins  $k$  lignes différentes avec les mêmes identifiants

Activity	Age	Pathology
M2	[22,23]	Cancer
M2	[22,23]	Aveugle
M2	[22,23]	VIH
PhD	[24,27]	Cancer
PhD	[24,27]	Allergies
PhD	[24,27]	Allergies
L	[20,21]	Cancer
L	[20,21]	Cancer
L	[20,21]	Cancer

3-Anonymat : Activité et l'âge sont généralisées

## Avantages

- ▶ Cela réduit la probabilité à  $1/k$
- ▶ Les données ne sont pas altérées

## Inconvénients

- ▶ Fuit de l'information négative : Bob n'est pas dans toutes les autres catégories.
- ▶ Si toutes les personnes ont les mêmes valeurs  $\Rightarrow$  fuite !

3-Anonymat est NP-dur (Dondi et al. 2007)

# I-diversité

Evite que toutes les personnes aient la même valeur une fois généralisées. / valeurs doivent être présentes dans chaque champs.

Activité	Age	Pathologie
M2	[22,23]	Cancer
M2	[22,23]	Allergies
M2	[22,23]	VIH
PhD	[24,27]	Cancer
PhD	[24,27]	VIH
PhD	[24,27]	Allergies
L	[20,21]	VIH
L	[20,21]	Allergies
L	[20,21]	Cancer

3-diversité, chaque catégorie a trois valeurs différentes

# Plan

Introduction

La sécurité et vous ?

Cybercriminalité

Intelligence Économique

IoT

Définir la sécurité

Sécurité des données

**RGPD**

Conclusion





NON PORT DE LA CEINTURE DE SÉCURITÉ

**-4 points**  
sur le permis de conduire

 **135 €**  
Amende forfaitaire

POINTS **12**



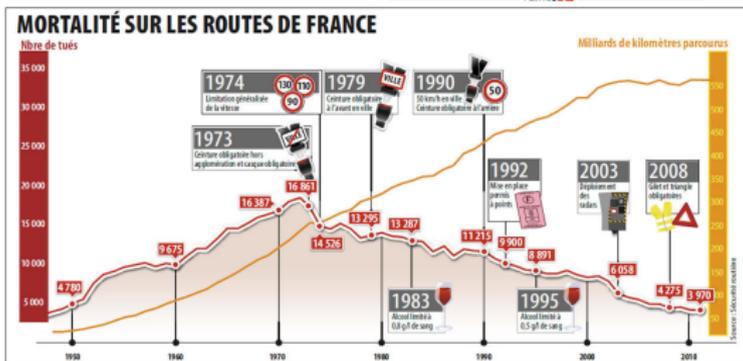
**NON PORT DE LA CEINTURE DE SÉCURITÉ**

**-4 points**  
sur le permis de conduire



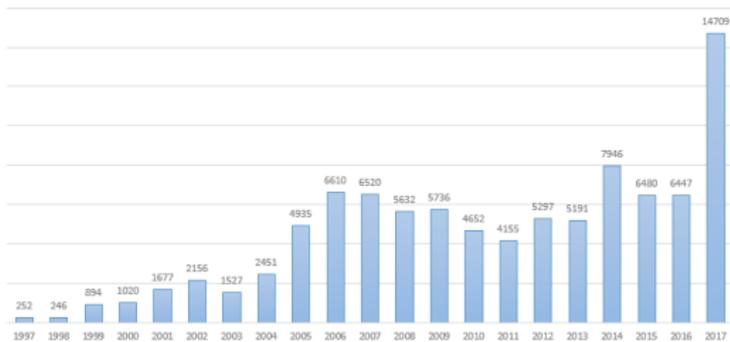
**135 €**  
Amende forfaitaire

POINTS **-12**

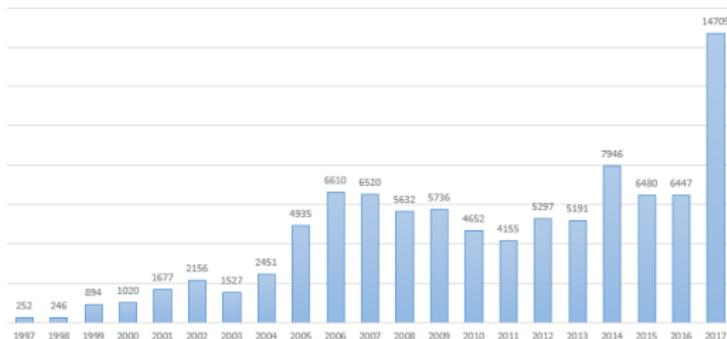


L'orgus

## Reported Vulnerabilities



Reported Vulnerabilities



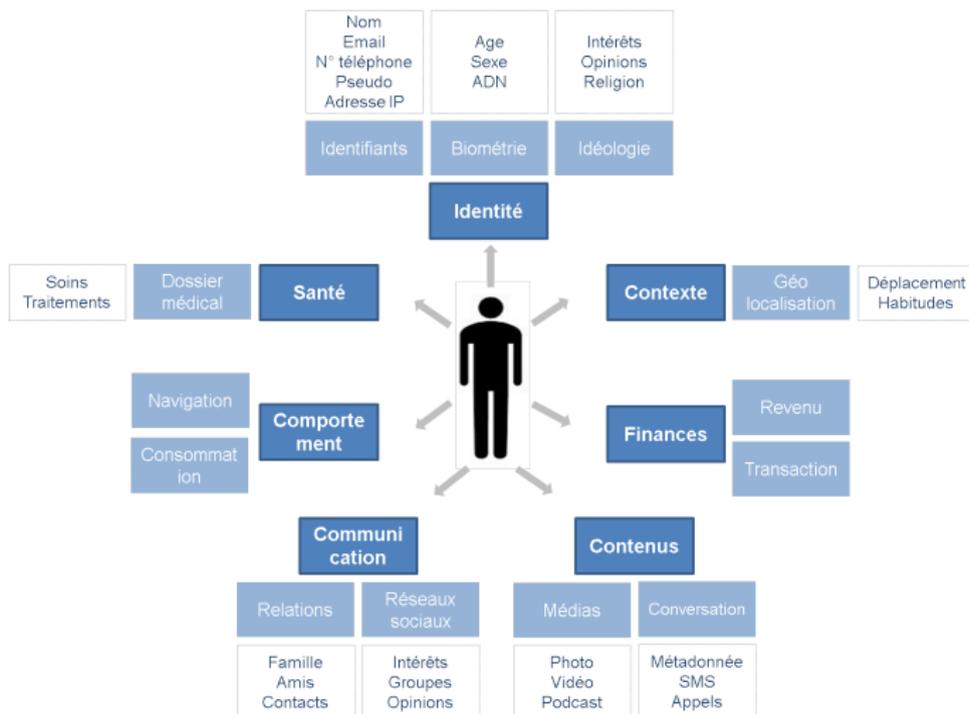
## Règlement Général sur la Protection des Données GDPR : General Data Protection Regulation

# Qui est touché ?



TOUT LE MONDE !

# Qu'est-ce qu'une donnée personnelle ?



# Qu'est-ce qu'une donnée personnelle **sensible**?



Collecte sans consentement préalable écrit, clair et explicite



# Plus de droits pour vos données !



Sanction



Plus de transparence



Droit à l'oubli



Guichet unique



Protection des mineurs



Portabilité

# RPGD : en 6 étapes @CNIL



1. Désigner un pilote
2. Cartographier
3. Prioriser
4. Gérer les risques
5. Organiser
6. Documenter

# Sanctions



20 millions



ou 4 %



# Vérification formelle



Designer



Attaquant

# Vérification formelle



Designer



Attaquant



Security Team

# Vérification formelle



Designer



Attaquant



Donner une preuve



Security Team

# Vérification formelle



Designer



Attaquant



Donner une preuve



Trouver une attaque



Security Team

# Applications



# Plan

Introduction

La sécurité et vous ?

Cybercriminalité

Intelligence Économique

IoT

Définir la sécurité

Sécurité des données

RGPD

Conclusion

# Statistiques et Cyber Sécurité

- ▶ La sécurité des données est un enjeu crucial.
- ▶ Les statistiques à la rescousse pour la sécurité
- ▶ Security by design
- ▶ RGPD

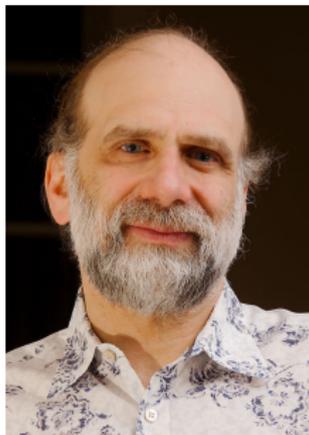
# Statistiques et Cyber Sécurité

- ▶ La sécurité des données est un enjeu crucial.
- ▶ Les statistiques à la rescousse pour la sécurité
- ▶ Security by design
- ▶ RGPD

## Des experts recrutés :

- ▶ Kévin Atighehchi
- ▶ Paul-Marie Grollemund
- ▶ Clément Jacques
- ▶ Maeva Paradis
- ▶ Jean-Yves Bergeron

**“Security is a process, not a product.”**



Merci pour votre attention

Questions?

Les  
**BLOCK  
CHAINS**  
EN 50 QUESTIONS  
Comprendre le fonctionnement et les enjeux  
de cette technologie innovante

