Introduction à la sécurité

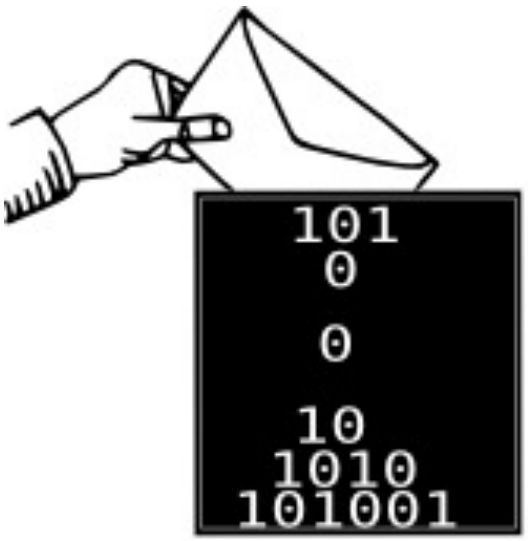
Pascal LAFOURCADE

LIMOS

UNIVERSITÉ Clermont Auvergne

9 Septembre 2020
Aurillac, département STID

L'informatique est omiprésente



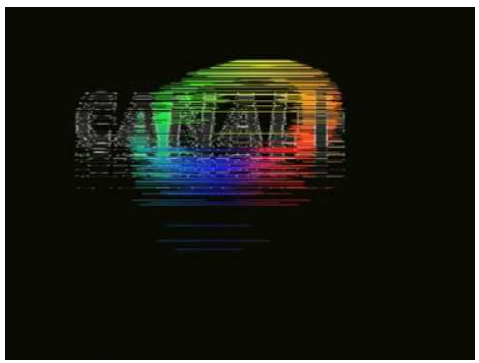
Statistiques en cybersécrurité en 2019

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

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

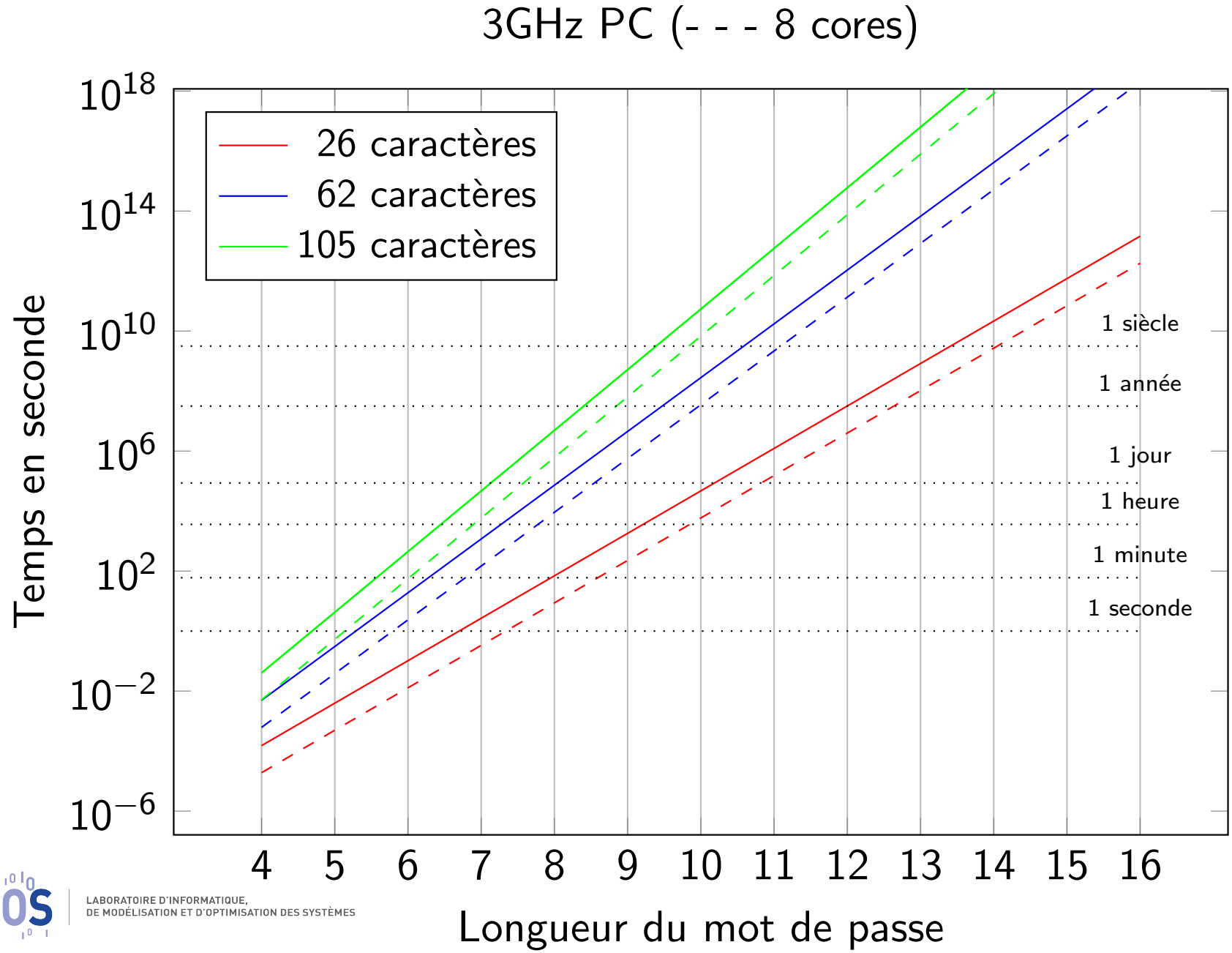
En réalité

Prince Williams

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



LIMOS
LABORATOIRE D'INFORMATIQUE, DE MODÉLISATION ET D'OPTIMISATION DES SYSTÈMES

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 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 d 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' 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.

Quelques conseils

FESTIVAL du FILM SÉCURITÉ

2018

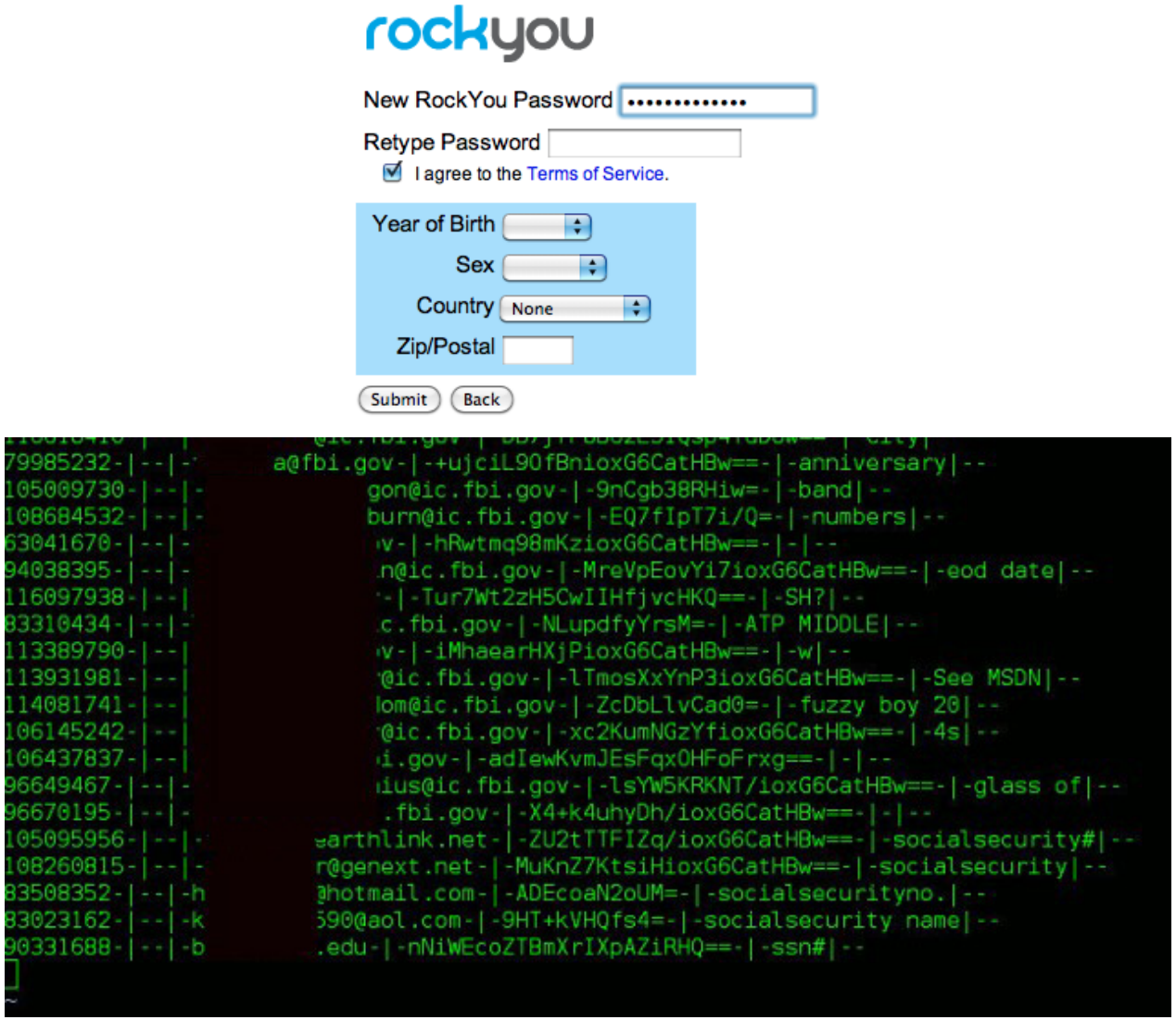
GRAND PRIX DU FESTIVAL

Les 10 commandements de la Cyber-Victime

par Micode

VIDEO

Fuite de base de données



Olivier Heen, Christoph Neumann: On the Privacy Impacts of Publicly Leaked Password Databases. DIMVA 2017

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

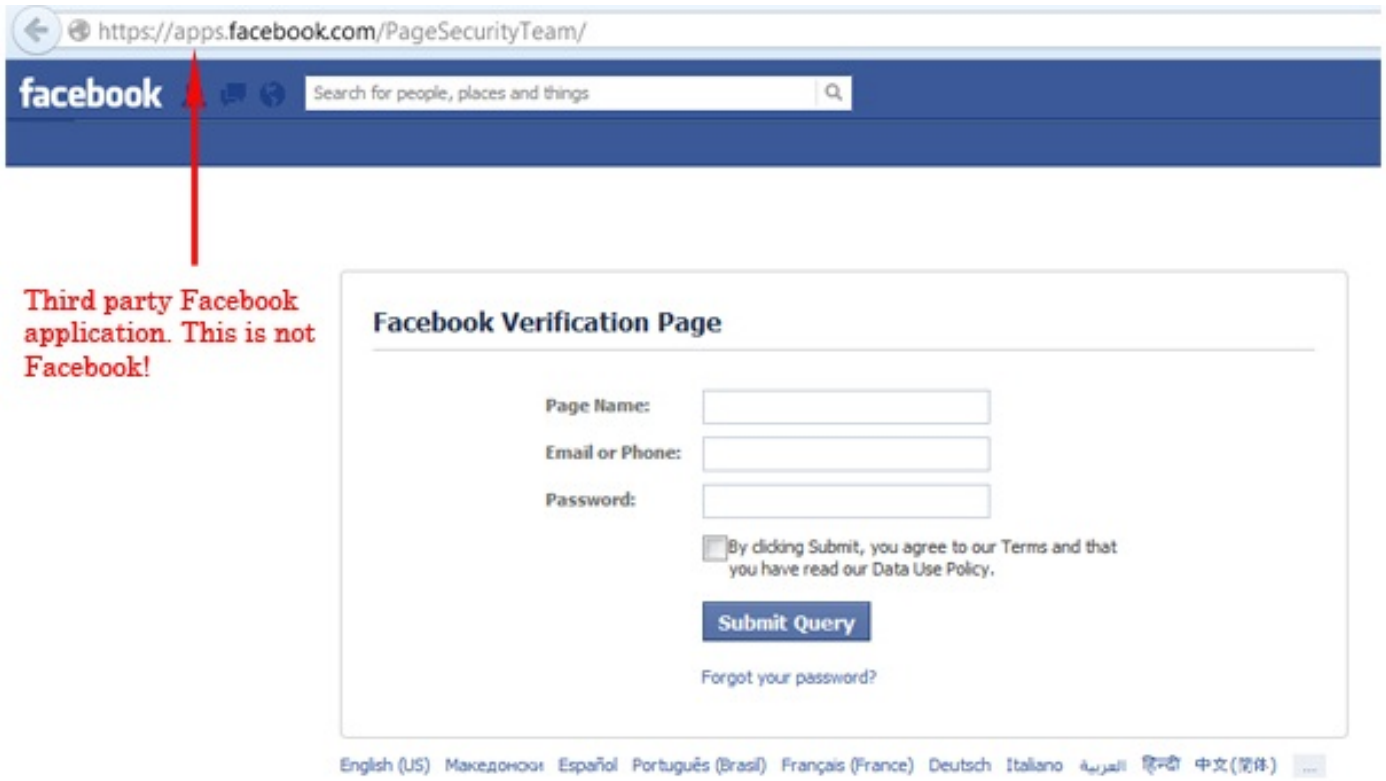
DYOD : Download on Your Own Device

Plan

5 Familles de Cybercriminalité

- Escroquerie
- Sabotage
- Ransomwares
- Espionnage
- Destabilisation

Escroquerie : Phishing



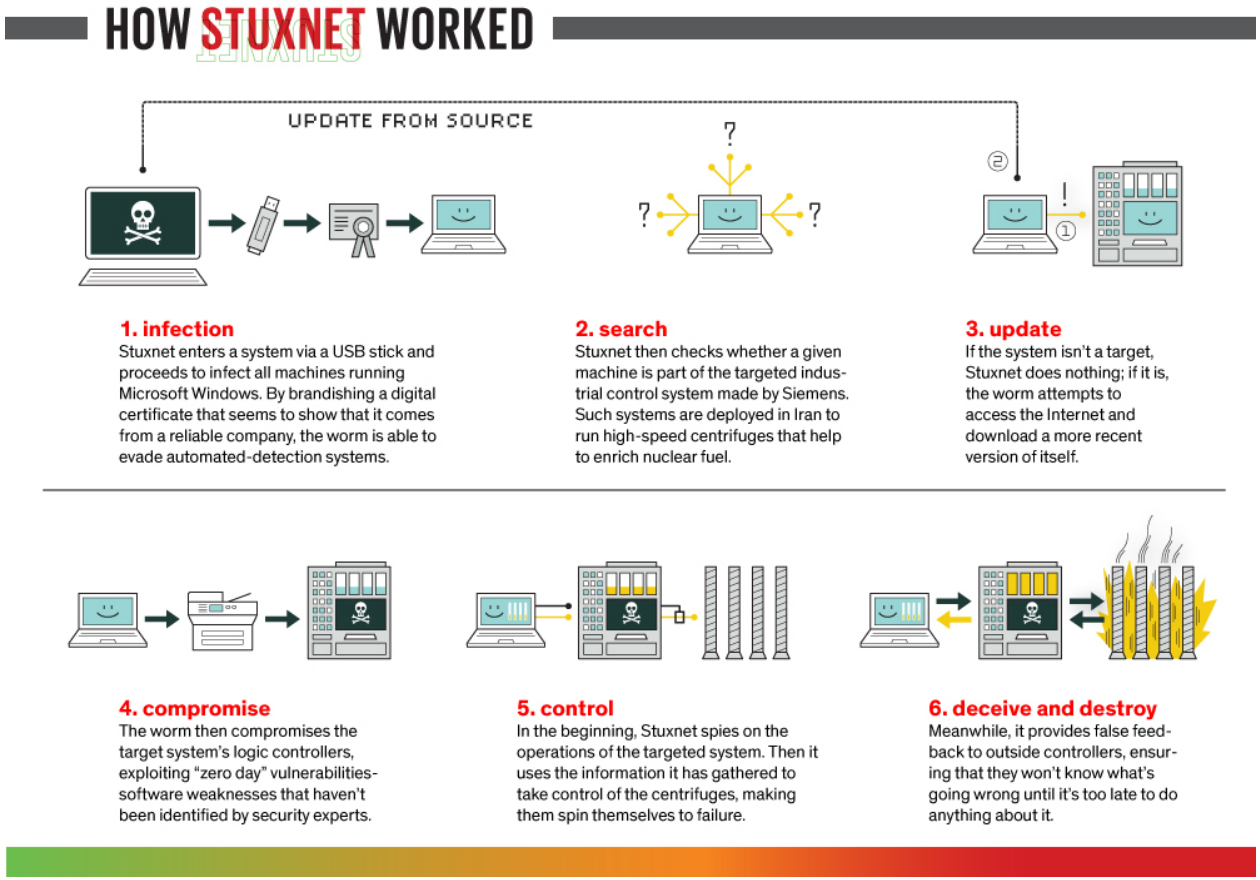
Voyant + Papillon

Escroquerie : Fraude au président

VIDEO

Sabotage

Stuxnet, 2010



Saudi Aramco 35 000 PC deleted in 2012.

Ransomwares: Wannacry et al. 12 may 2017

http://stopransomware.fr/

Espionnage

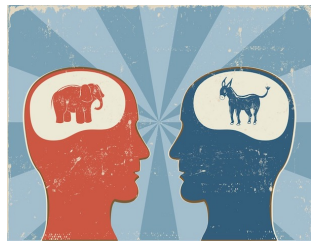
- Little Brother (Individuel)
- Medium Brother (Entreprise)
- Big Brother (Gouvernement)

Edward Joseph Snowden, 6th june 2013

Une technique d'espionnage : MICE

Monnaie

Idéologie



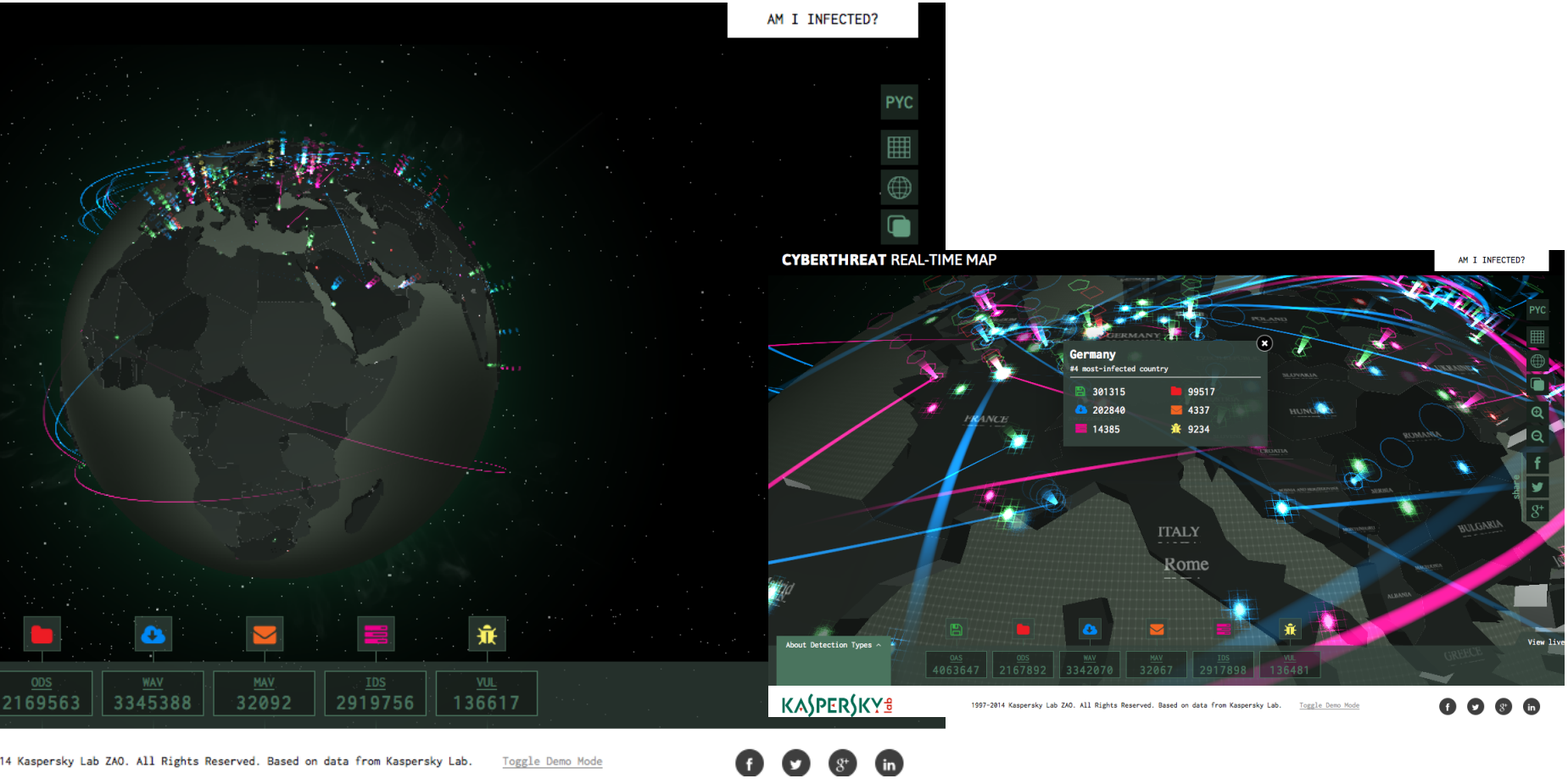
Compromission

Ego

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

- 1919 

- 1952, 

- 1995, 
- 2002, 
- 7 Juillet 2009, 

ANSSI

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

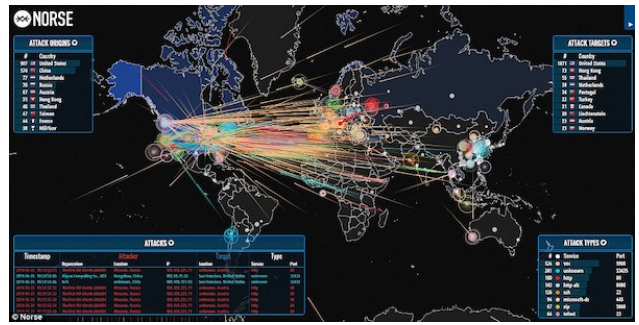
- Identifier les auteurs n'est pas facile

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

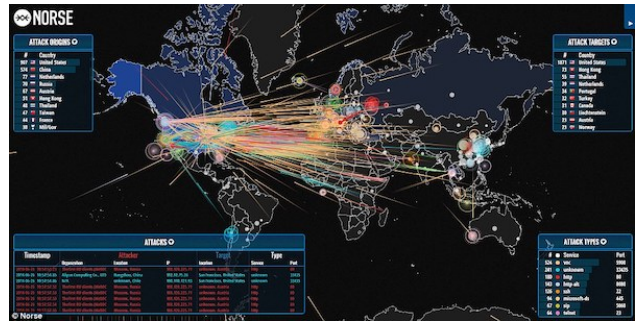


Cyberguerre est une réalité

$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

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

(Intelligence $\neq$ renseignement)

Maîtriser l'Information

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

Protection de l'Information

"**Seuls les paranoïaques survivent**"

Andy GROVE, Co-fondateur d'Intel en 1968

Protection de l'Information

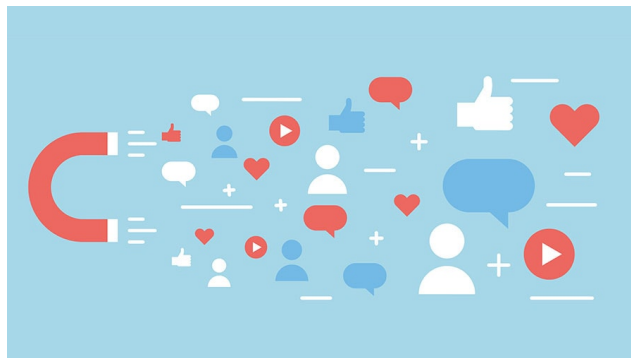
"**Seuls les paranoïaques survivent**"

Andy GROVE, Co-fondateur d'Intel en 1968

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

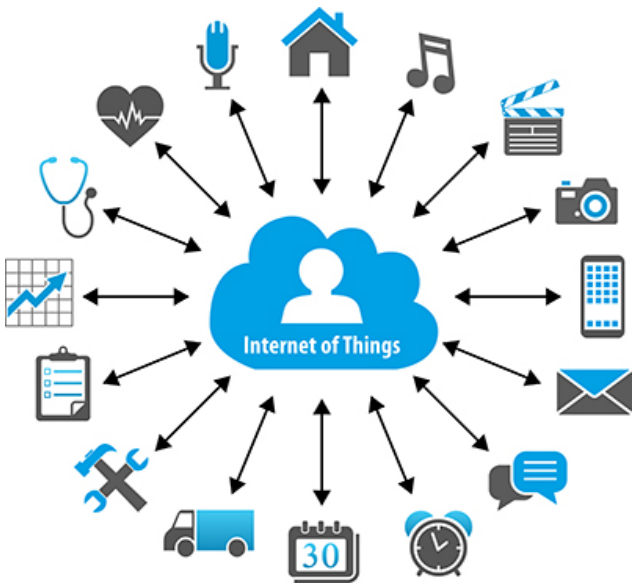
Stratégies d'Influence

- Presse, média
- Blog, réseaux sociaux
- Communication en cas de crise infomration/désinformation



Plan

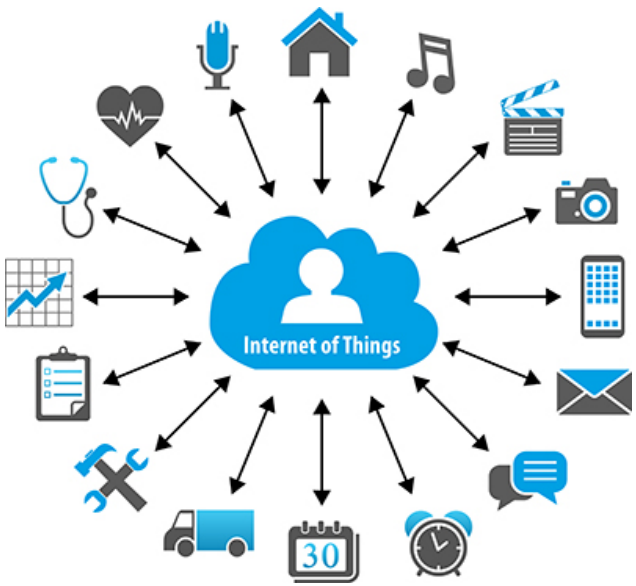
Raisons du succes de l'IOT



Technologie

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

Raisons du succes de l'IOT



Technologie

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

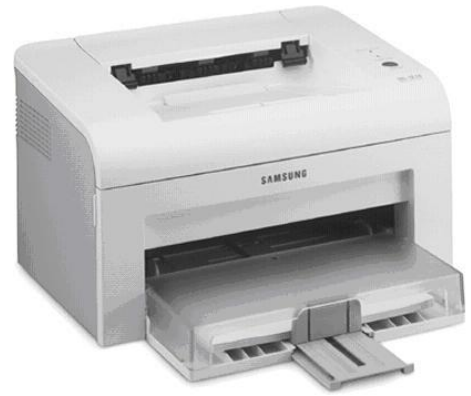
Usage

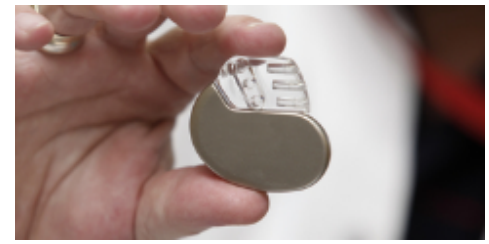
- Surveillance
- Hyperconnectivité
- Disponibilité

Attaques d'IoT depuis 2007 ...

Attaques d'IoT depuis 2007 ...

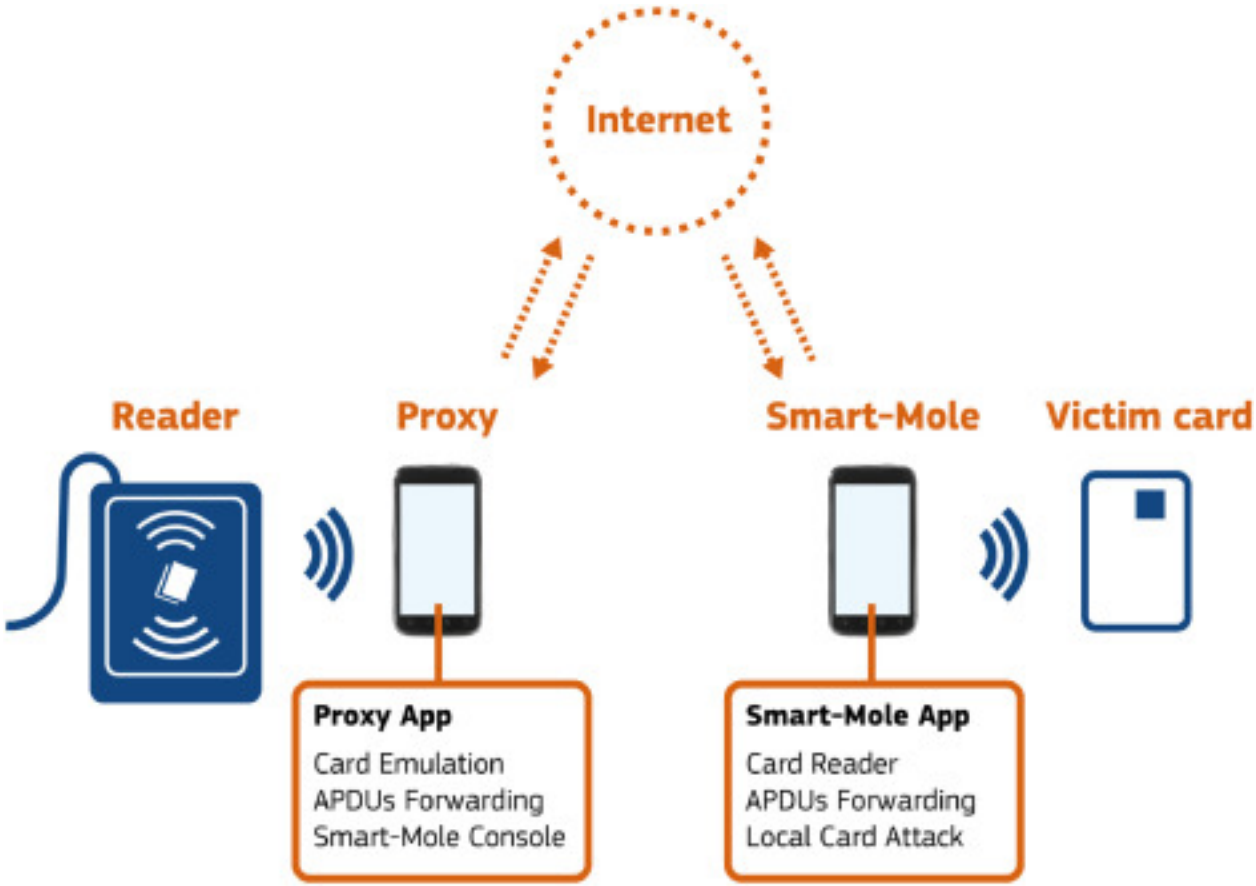
Attaques d'IoT depuis 2007 ...





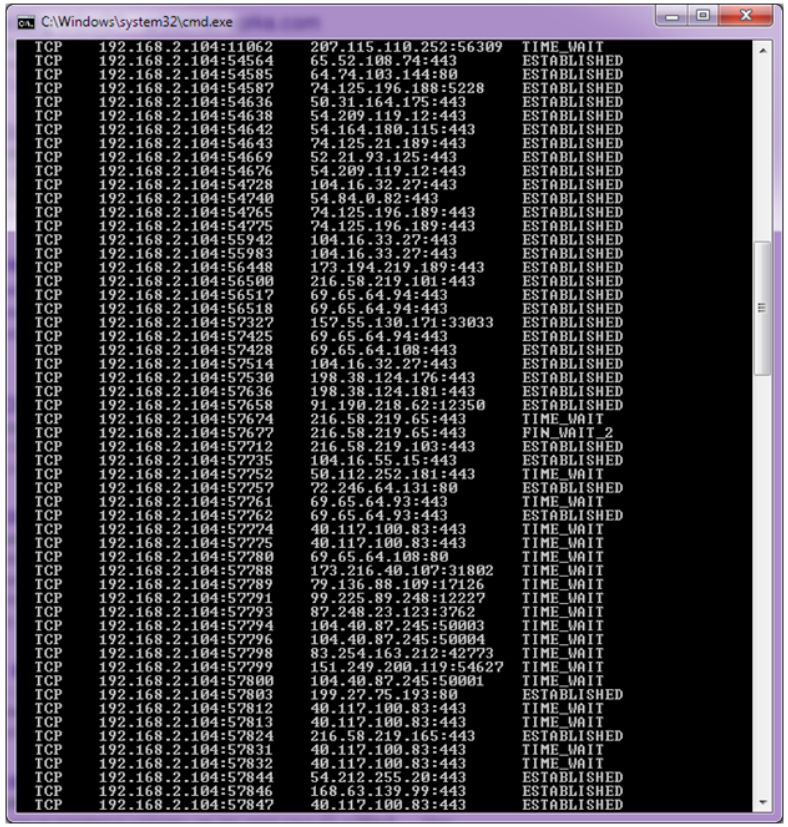
LIMOS
LABORATOIRE DE MODÉLISATION ET D'OPTIMISATION DES SYSTÈMES

Attaque par relais



VIDEO VOITURE + Suisse

Analyse de Logs



Statistiques et IDS (Intruder Detection System)

Plan

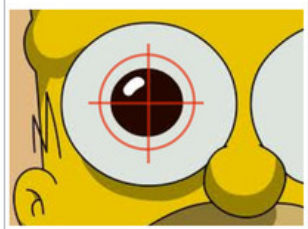
Propriétés de sécurité traditionnelles

- Confidentialité
- Authentification
- Intégrité
- Disponibilité

Authentification

"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

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

$$\text{Date de naissance} + \text{Code Postal} + \text{Sexe}$$
$$= \text{Identification} > 63\%$$

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 suiffisante 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** [1]**:**

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

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

[1] C. Dwork : "Differential Privacy", International Colloquium on Automata, Languages and Programming , 2006.

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

Bilan

Advantages

- 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)

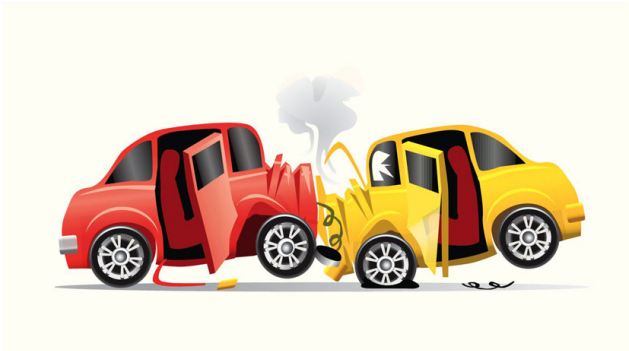
l-diversité

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

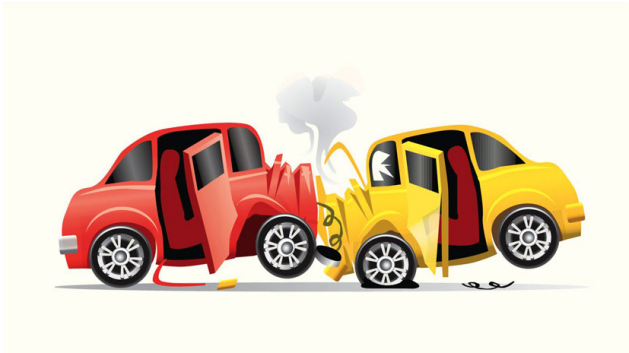
Activité	Age	Pathologie
M2	[22,23]	Cancer
M2	[22,23]	Allergies
M2	[22,23]	VIH
PhD	[24,27]	Cancer
PhD	[24,27]	VIH
PhD	[24,27]	Allergies
L	[20,21]	VIH
L	[20,21]	Allergies
L	[20,21]	Cancer

3-diversité, chaque catégorie a trois valeurs différentes

Plan

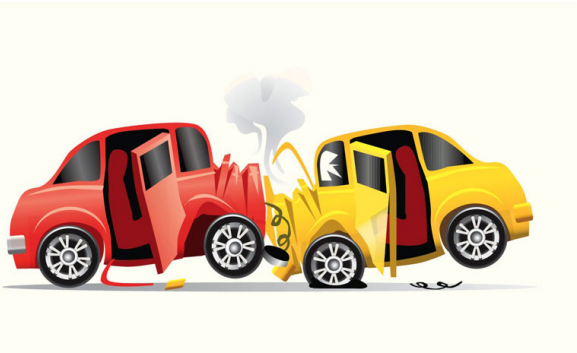



RIP



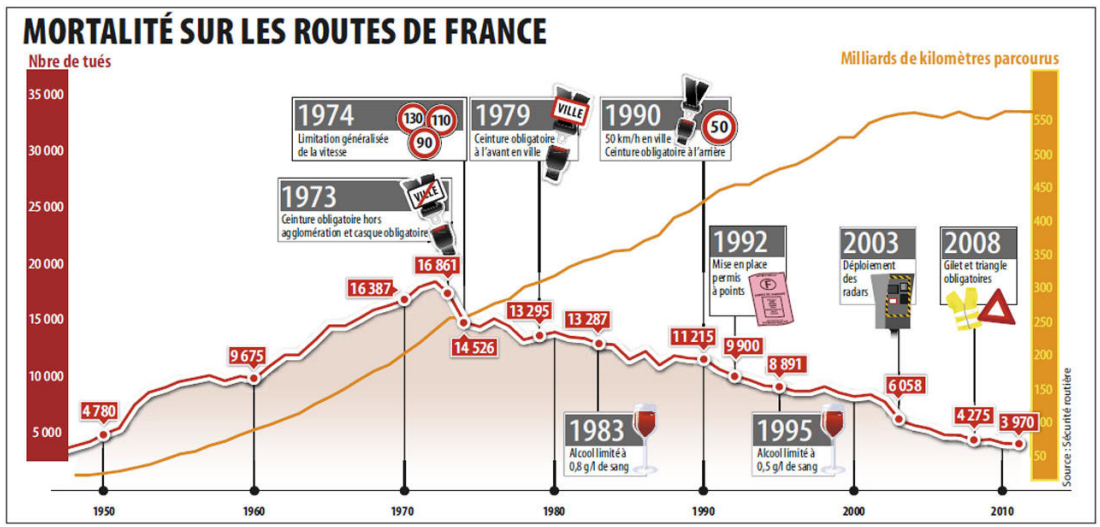

RIP


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

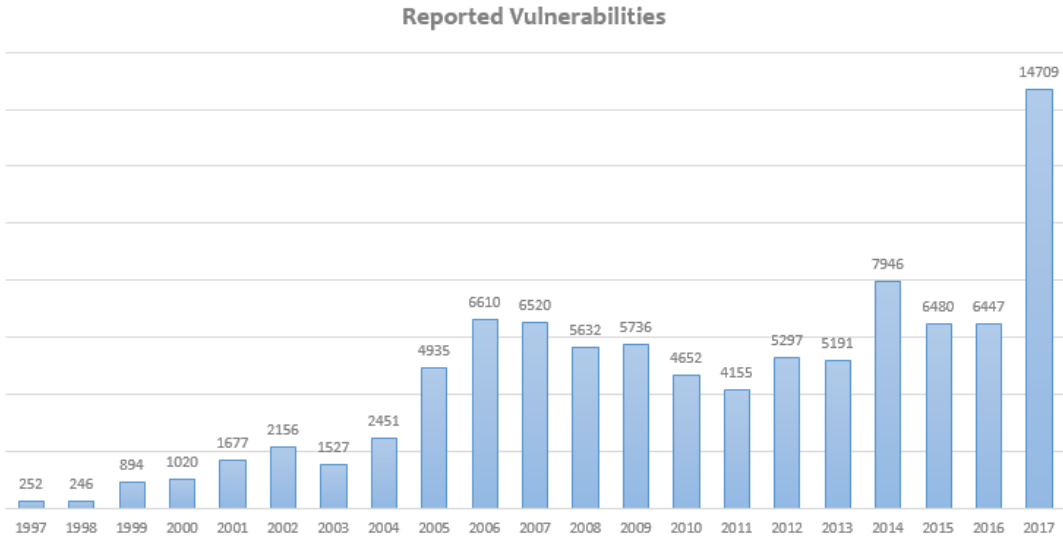


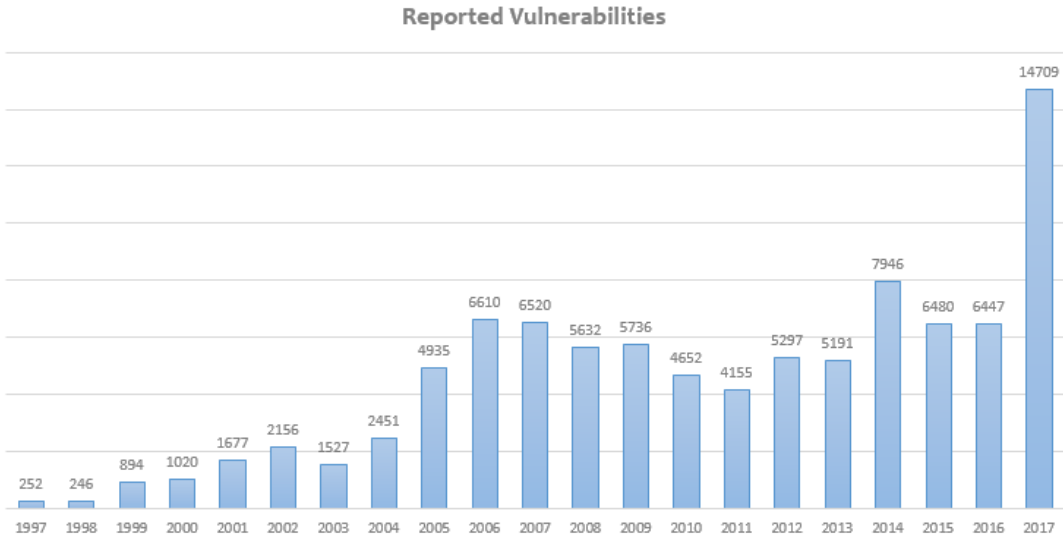

RIP


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
VITESSE
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


Reported Vulnerabilities
252
246
894
1020
1677
2156
1527
2451
4935
6610
6520
5632
5736
4652
4155
5297
5191
7946
6480
6447
14709
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017

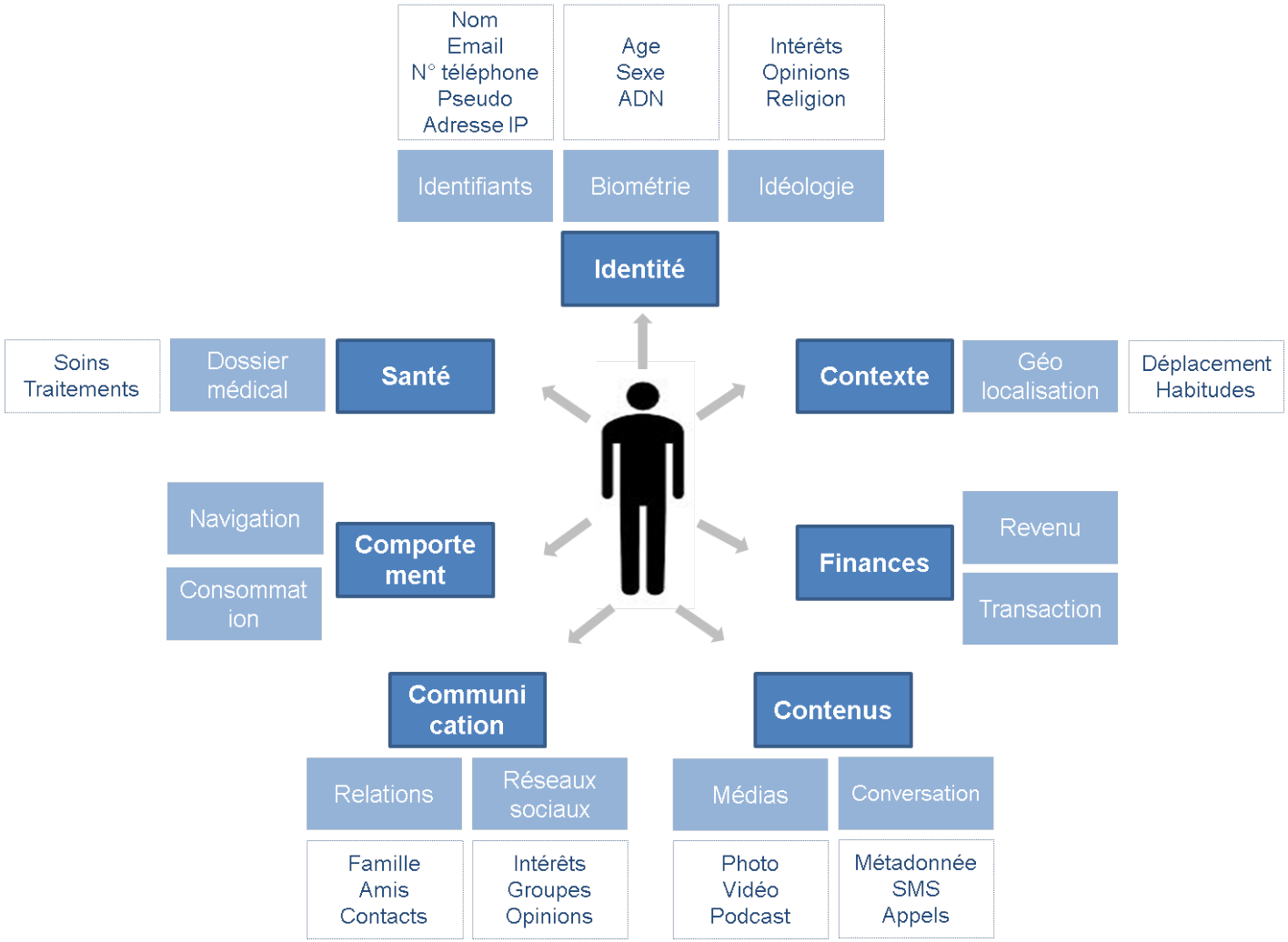


Règlement Général sur la Protection des Données
GDPR : General Data Protection Regulation

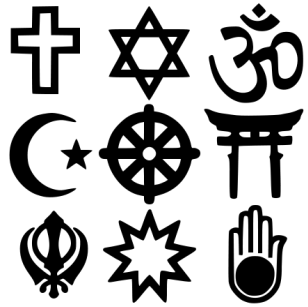
Qui est touché ?

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

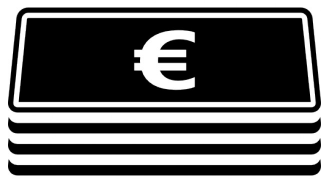
Portabilité

RPGD : en 6 étapes @CNIL

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

Sanctions

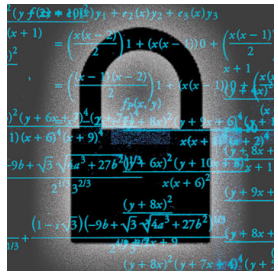
20 millions



ou 4 %

Vérification formelle

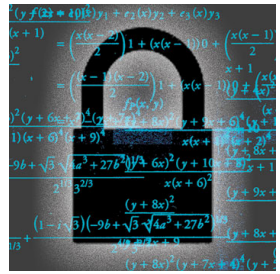
Designer



Attaquant

Vérification formelle

Designer

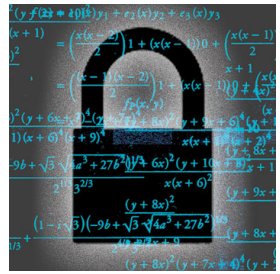


Attaquant

Security Team

Vérification formelle

Designer



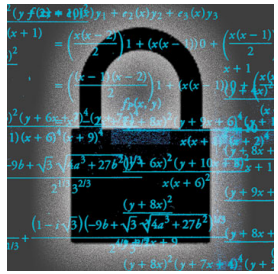
Attaquant

Donner une preuve

Security Team

Vérification formelle

Designer



Attaquant

Donner une preuve

Trouver une attaque

Security Team

Applications

Plan

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

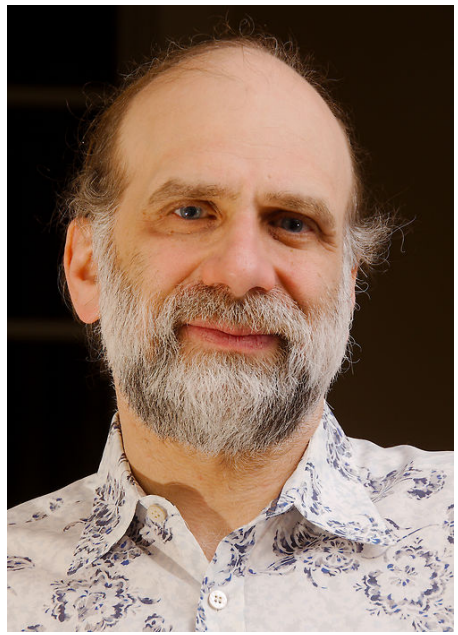
- La sécurité des données est un enjeu crucial.
- Les statistiques à la rescousse pour la sécurité
- Security by design
- RGPD

Des experts recrutés :

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

Bruce Schneier

“Security is a process, not a product.”



Merci pout votre attention

Questions?