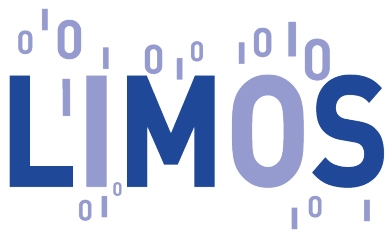
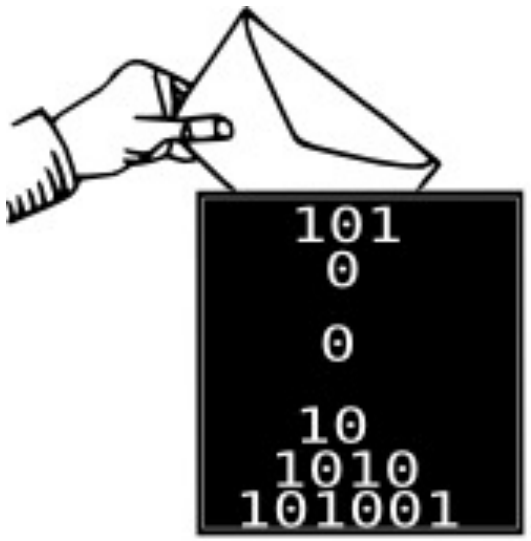
Cybersécurité une réalité

Pascal LAFOURCADE



Novembre 2018

Computers are everywhere!

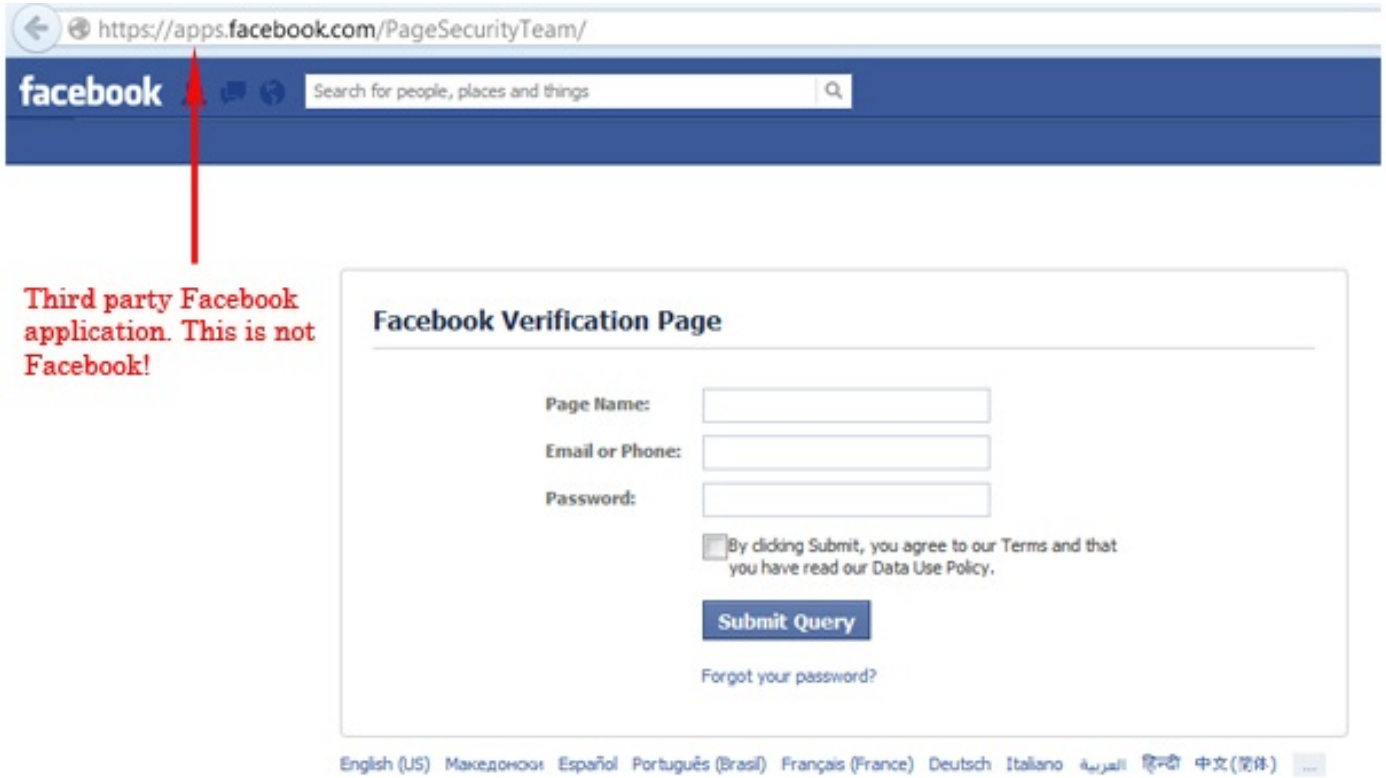


5 Famillies of Cyber Criminality

- Phishing
- Espionnage
- Ransomwares
- Sabotage
- Destabilisation

Phishing


CREDIT CARD
1234 5678 9101 1213
Paul A. Cardholder


https://apps.facebook.com/PageSecurityTeam/
facebook
Search for people, places and things
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.
Submit Query
Forgot your password?
English (US) Македонски Español Português (Brasil) Français (France) Deutsch Italiano العربية हिन्दी 中文(简体)

Espionnage

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

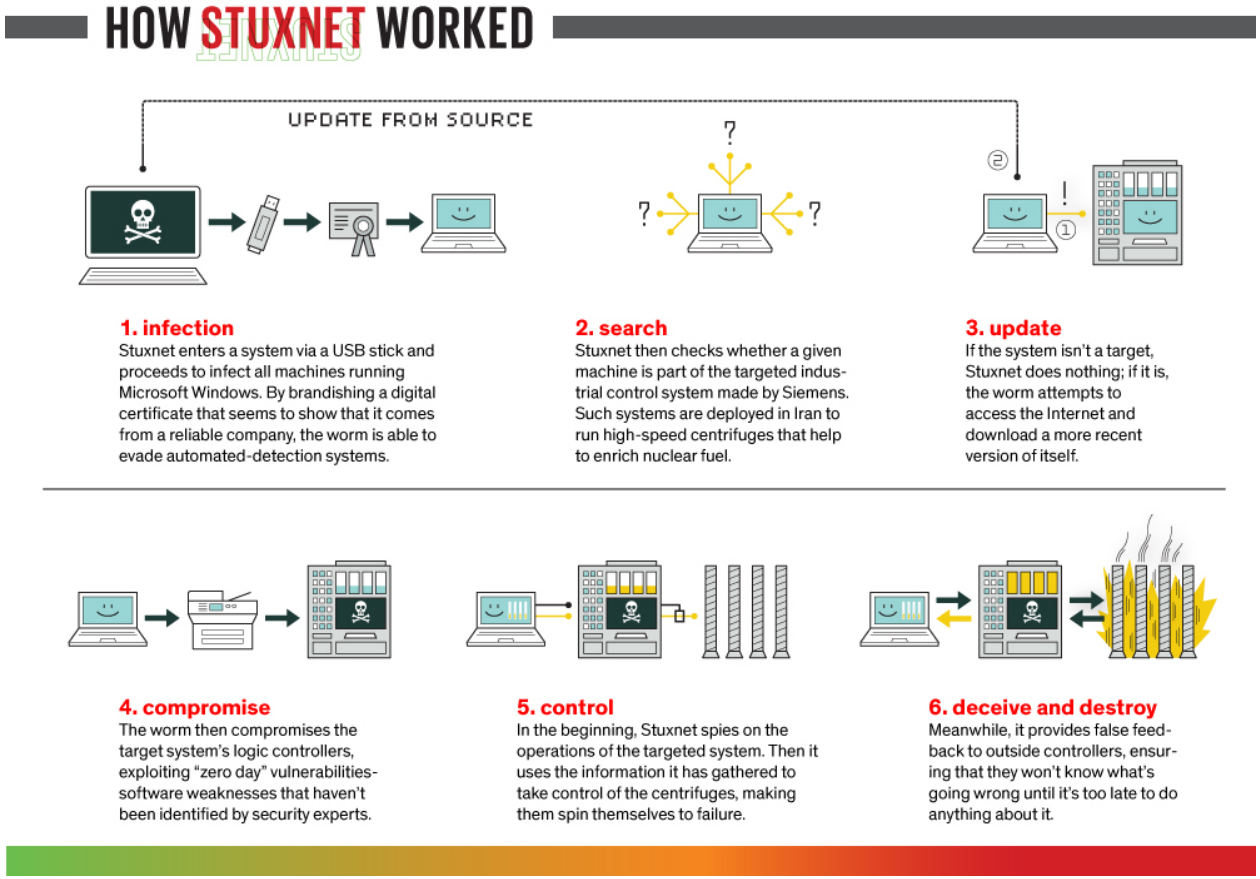
Edward Joseph Snowden, 6th june 2013

Ransomwares: Wannacry et al. 12 may 2017

http://stopransomware.fr/

Sabotage

Stuxnet, 2010

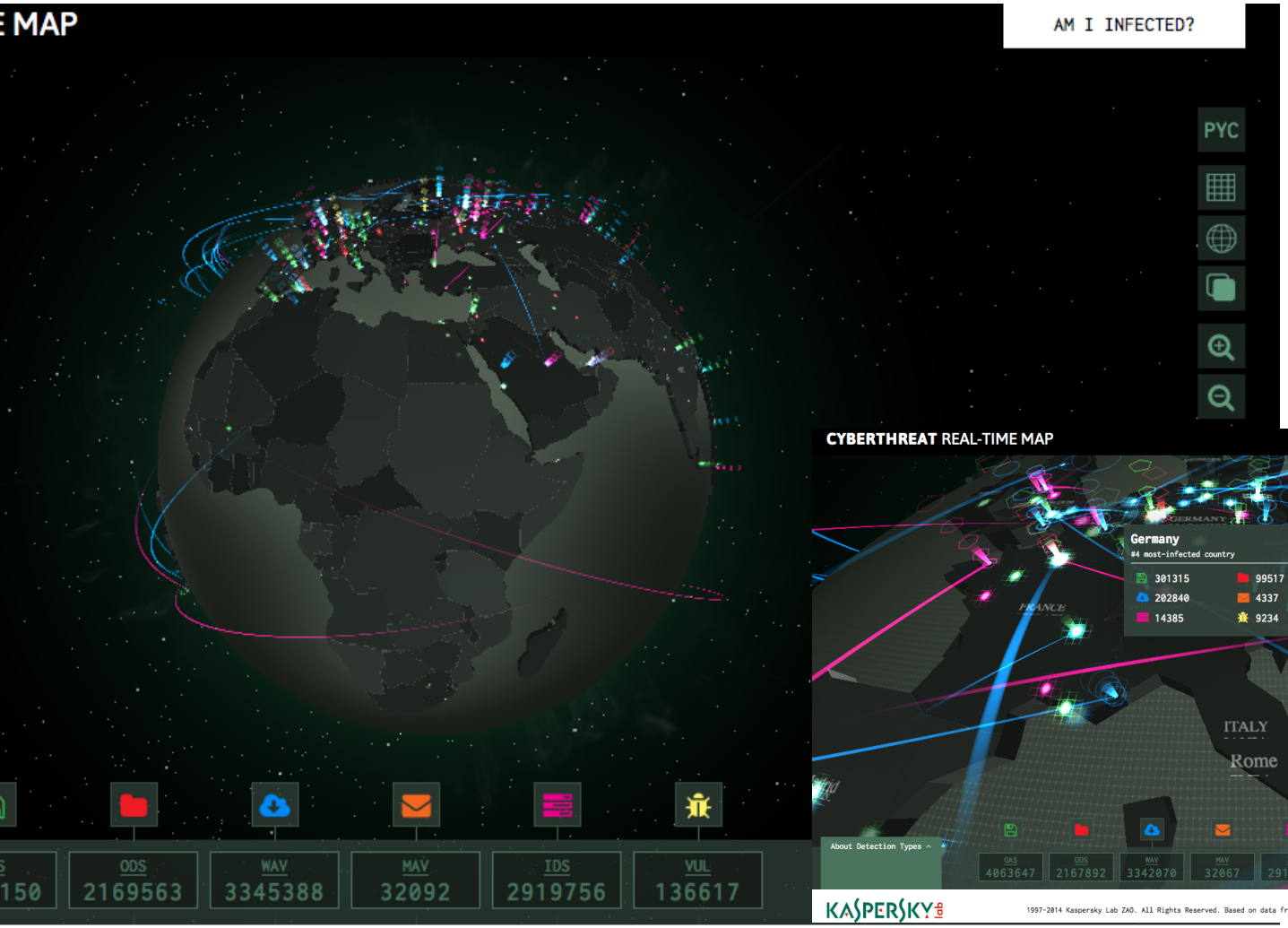


Saudi Aramco 35 000 PC deleted in 2012.

Destabilisation: Defacing

Destabilisation: Trojan, Botnets and Zombies

http://cybermap.kaspersky.com/



http://cybermap.kaspersky.com/

14 September 2017 USA stops to use Kaspersky

29 September 2017 France is doing the same

Why are there more and more attacks?

Why are there more and more attacks?

Why are there more and more attacks?

Why are there more and more attacks?

Fast, large scale, semi-automatic...

Why are there more and more attacks?

Fast, large scale, semi-automatic...

but you wrongly feel anonymous!

Why are there more and more attacks?

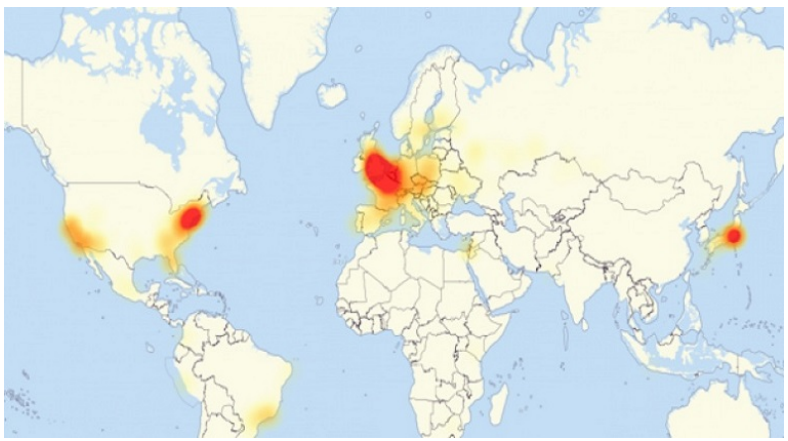
Fast, large scale, semi-automatic...

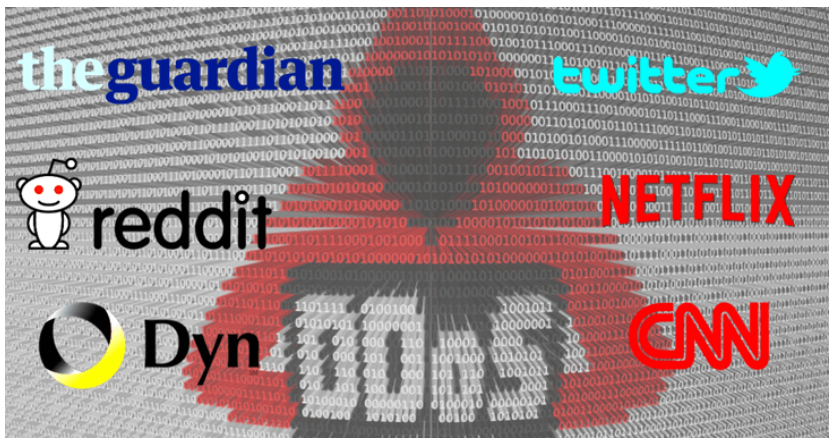
but you wrongly feel anonymous!

Internet was not designed to be secure but just to work!

Cyber Attack against Estonia April 2007

DDos Attack against Dyn DNS 21 October 2016





Advanced Persistent Threat: Govermment attacks

- Titan Rain discovered in 2003: Massive USA data collected during 3 years
- Operation Aurora discovered in 2010: Chinese attack against USA
- November 2014, SONY
- 2011 Bercy, 150 PC infected

Computer Science Security Agencies

- 1919 

- 1952, 

- 1995, 
- 2002, 
- 7 July 2009, 

Backdoors

- NSA's backdoor into `Dual_EC_DRBG` Dual Elliptic Curve Deterministic Random Bit Generator.
- Backdoor identified by academic researchers (Crypto 2007) and revealed by Snowden 2013.

Cyberwar is a reality

$7 billion for USA cyber operations in 2017 over $35 billion over the next 5 years.

Cyberwar is a reality

$7 billion for USA cyber operations in 2017 over $35 billion over the next 5 years.

- Communications are crucial: Egypt, Tunisia revolutions

Cyberwar is a reality

$7 billion for USA cyber operations in 2017 over $35 billion over the next 5 years.

- Communications are crucial: Egypt, Tunisia revolutions

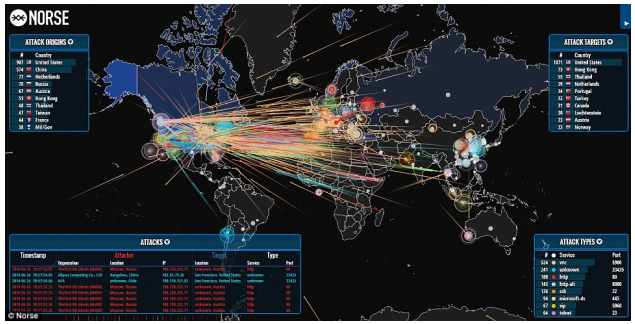
- Tracking authors is not always easy

Cyberwar is a reality

$7 billion for USA cyber operations in 2017 over $35 billion over the next 5 years.

- Communications are crucial: Egypt, Tunisia revolutions

- Tracking authors is not always easy
- Defense and attack strategies are different

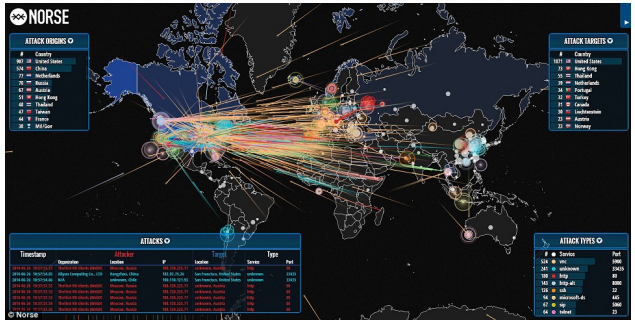


Cyberwar is a reality

$7 billion for USA cyber operations in 2017 over $35 billion over the next 5 years.

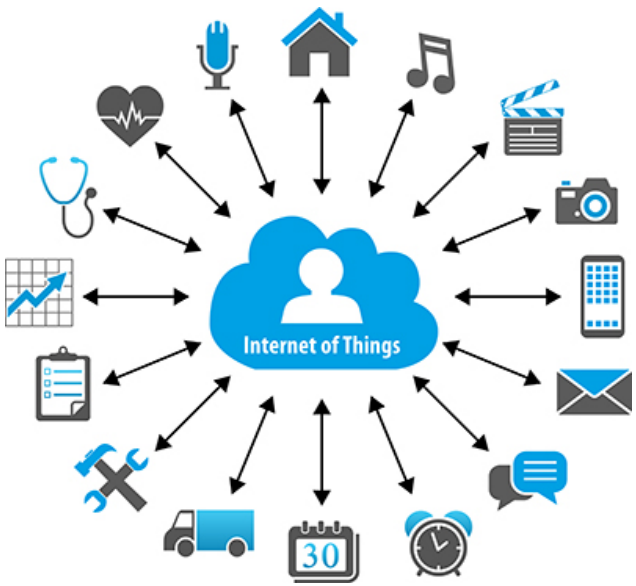
- Communications are crucial: Egypt, Tunisia revolutions

- Tracking authors is not always easy
- Defense and attack strategies are different



- Cyberattacks can have physical consequences

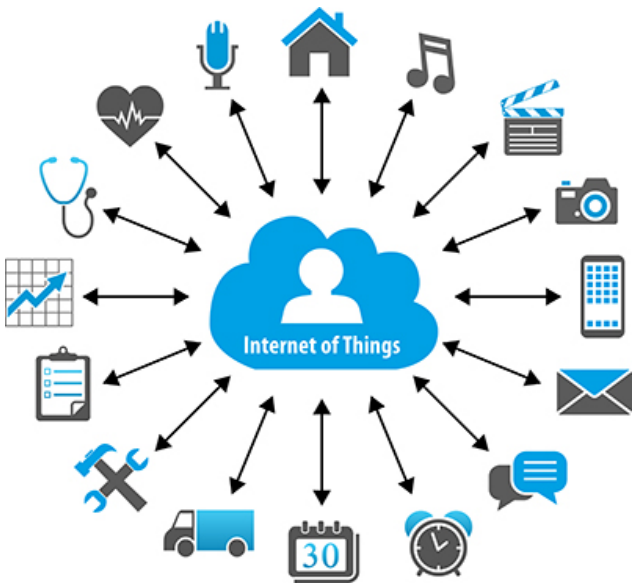
Reasons of the Succes of IOT



Technology

- Wireless Communications:
  Wifi, 3G, 4G, Bluethooth, Sigfox
  ...
- Batteries
- CPU
- Sensors
- Price

Reasons of the Succes of IOT



Technology

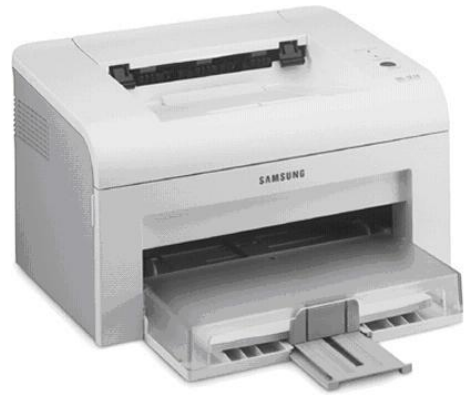
- Wireless Communications:
  Wifi, 3G, 4G, Bluethooth, Sigfox
  ...
- Batteries
- CPU
- Sensors
- Price

Usage

- Monitoring services
- Hyperconnectivity
- Avaibility

Real attacks on IoT from 2007 ...

Real attacks on IoT from 2007 ...



Real attacks on IoT from 2007 ...

LIMOS
LABORATOIRE DE MODÉLISATION ET D'OPTIMISATION DES SYSTÈMES

Is it preserving your privacy?

Is it preserving your privacy?

4096 RSA encryption

Is it preserving your privacy?

4096 RSA encryption

Around 60 possible temperatures: 35 ... 41

Is it preserving your privacy?

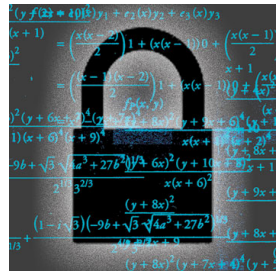
4096 RSA encryption

Around 60 possible temperatures: 35 ... 41

$$\{35\}_{pk}, \{35, 1\}_{pk}, ..., \{41\}_{pk}$$

Formal Verification Approaches

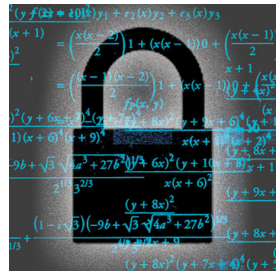
Designer



Attacker

Formal Verification Approaches

Designer

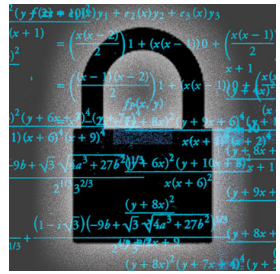


Attacker

Security Team

Formal Verification Approaches

Designer



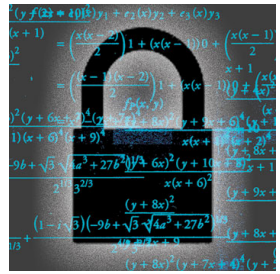
Attacker

Give a proof

Security Team

Formal Verification Approaches

Designer



Attacker

Give a proof

Find a flaw

Security Team

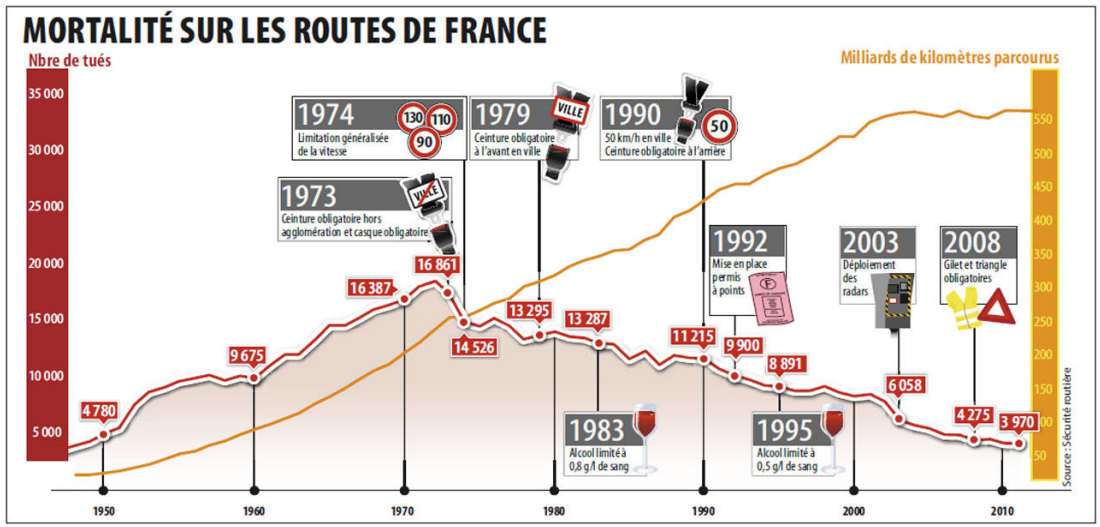

RIP


RIP

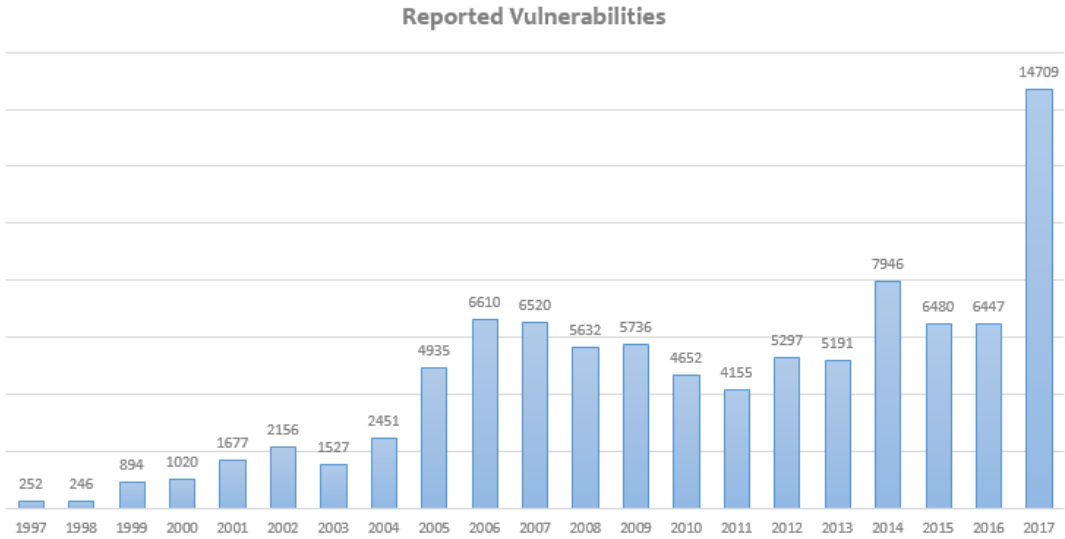

NON PORT DE LA CEINTURE DE SÉCURITÉ
-4 points
sur le permis de conduire
135 €
Amende forfaitaire
POINTS 12

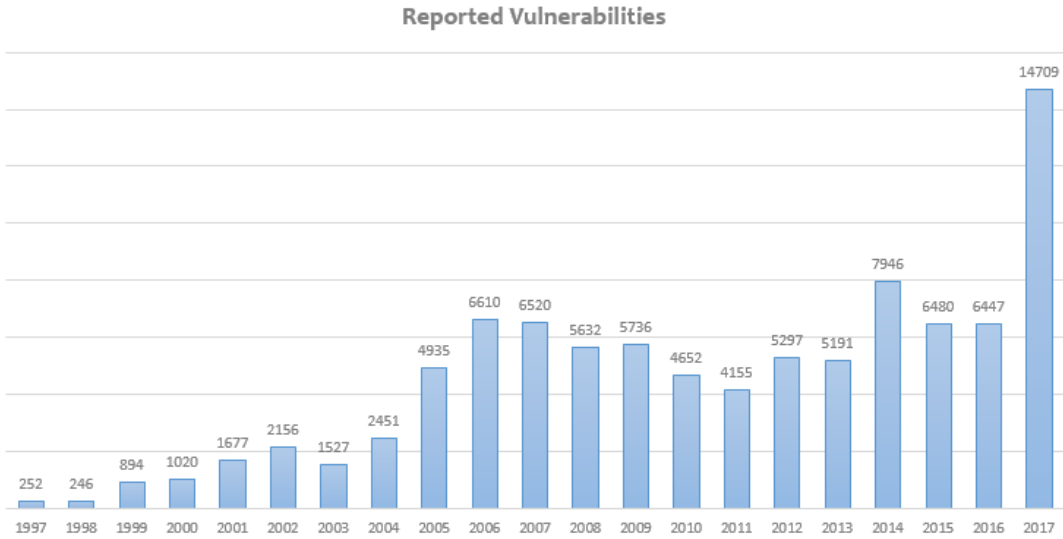

RIP


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
VILLE
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



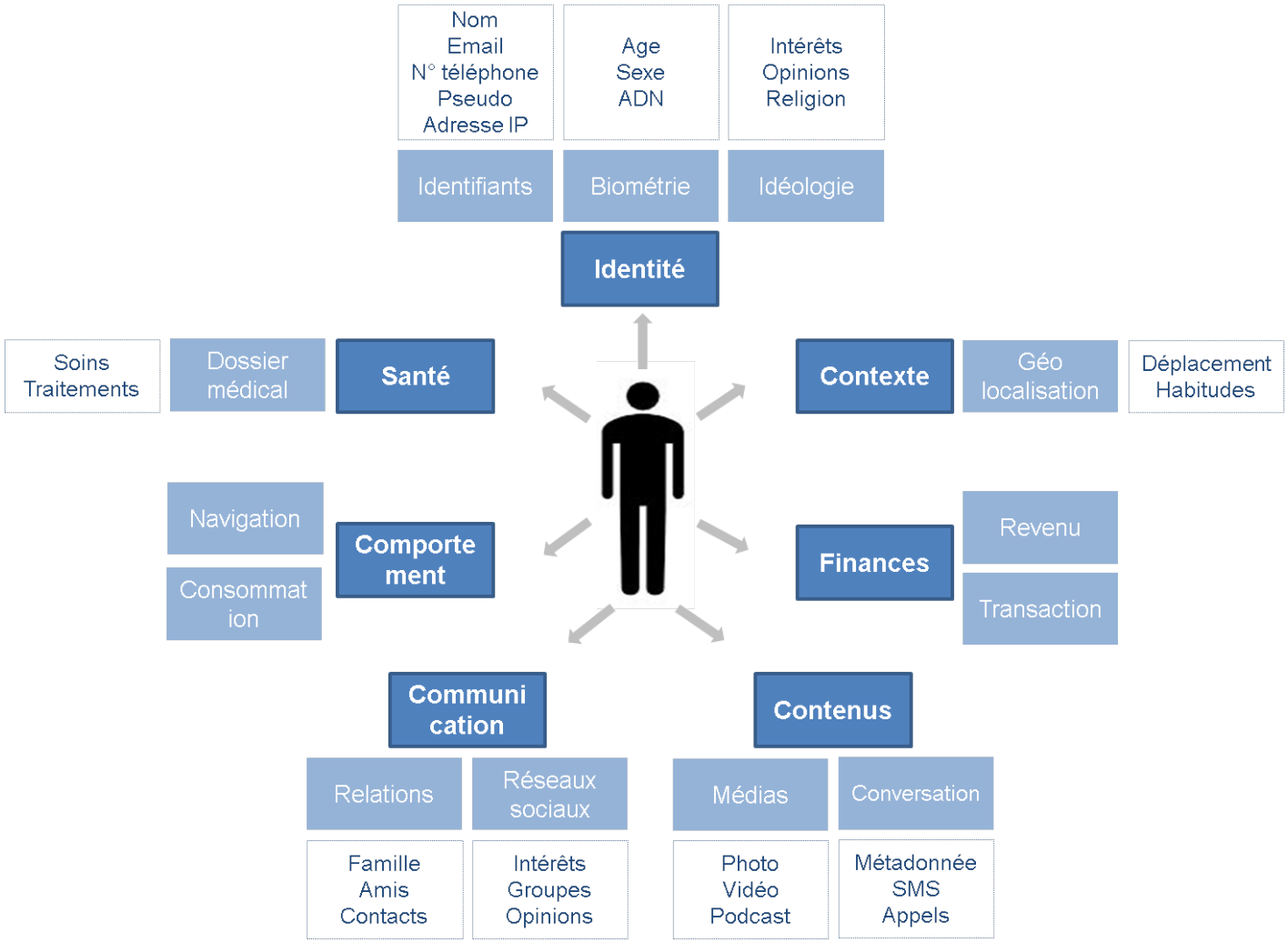
Règlement Général sur la Protection des Données

GDPR : General Data Protection Regulation

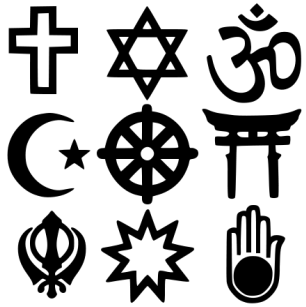
Qui est touché ?

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

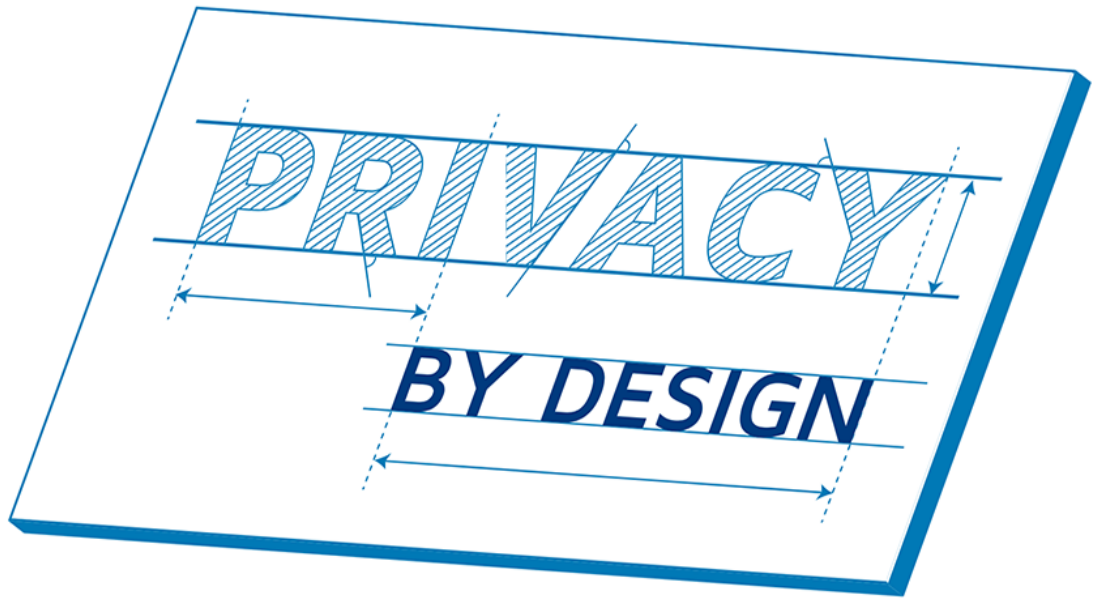
1. Désigner un pilote
2. Cartographier
3. Prioriser
4. Gérer les risques
5. Organiser
6. Documenter

Sanctions

20 millions

ou 4 %

RGPD



Thanks for your attention.

War games, 1983

Questions?