



CESI alternance

ÉCOLE SUPÉRIEURE DES MÉTIERS

LE CESI :
ENSEIGNEMENT
SUPERIEUR ET
FORMATION
PROFESSIONNELLE



CESI
alternance

ÉCOLE SUPÉRIEURE DES MÉTIERS

Web Hacking

I. Intro



Document confidentiel - ne pas diffuser

LE CESI :
ENSEIGNEMENT
SUPERIEUR ET
FORMATION
PROFESSIONNELLE



ÉCOLE SUPÉRIEURE DES MÉTIERS

The **hacker** culture is a subculture of individuals who enjoy the intellectual challenge of creatively overcoming and circumventing limitations of systems to achieve novel and clever outcomes. The act of engaging in activities in a spirit of playfulness and exploration is termed "**hacking**".



Document confidentiel - ne pas diffuser

LE CESI :
ENSEIGNEMENT
SUPERIEUR ET
FORMATION
PROFESSIONNELLE

But... for unlighted people,



Hacking is a chance

<+> HACKING HEALTH CAMP

*Create the future
of healthcare*

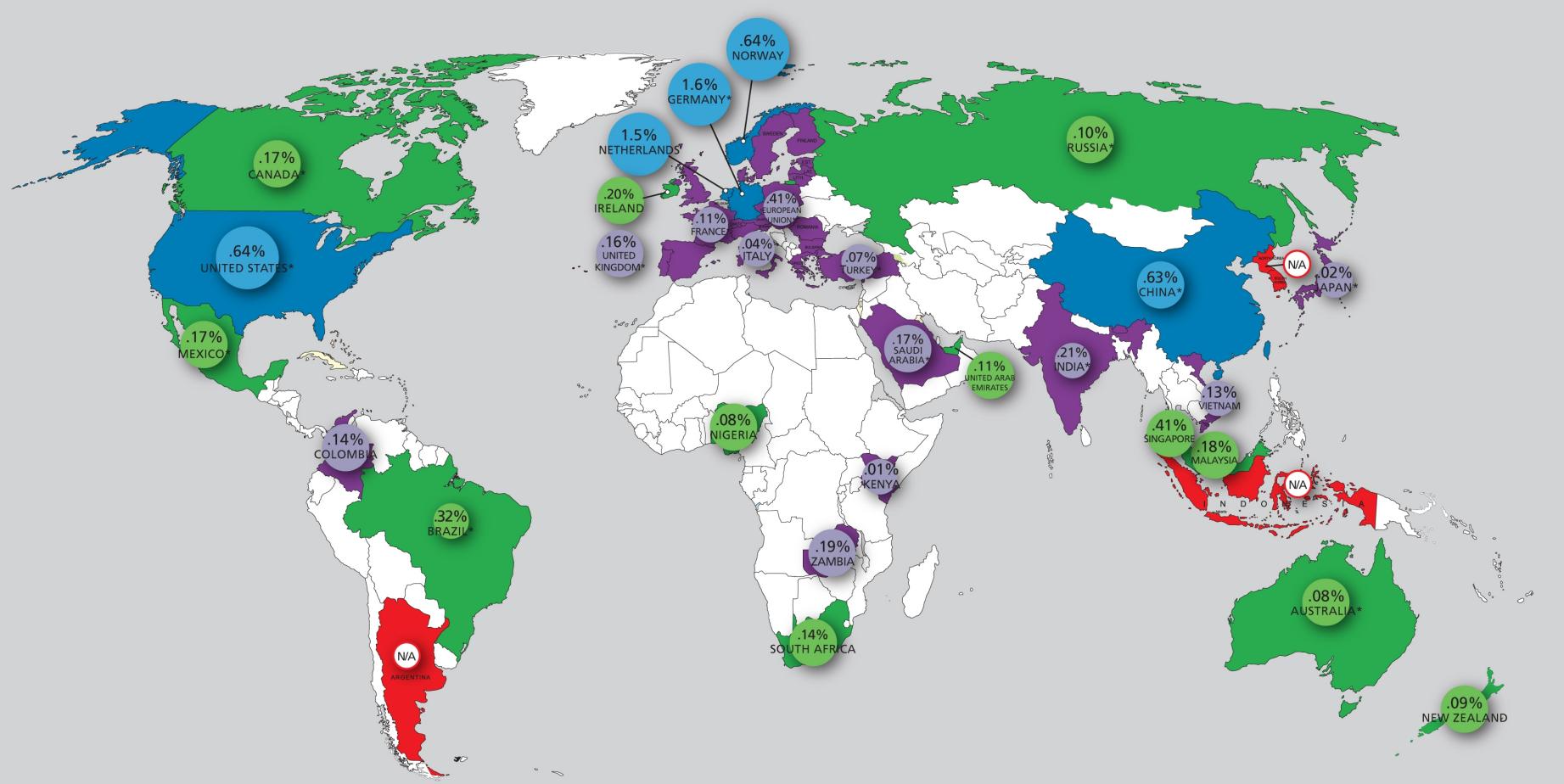
< Conferences / Workshops / Hackathon >



Hacking is a cancer



CYBERCRIME LOSS AS A PERCENT OF GDP (GROSS DOMESTIC PRODUCT)



Confidence Ranking: Countries Current Tracking of Cybercrime within Their Borders.

% High Confidence Level

% Medium Confidence Level

% Low Confidence Level

* G-20 Countries

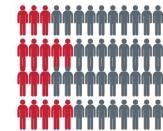
N/A - Countries currently not measuring cybercrime loss

\$445 BILLION

The annual estimated cost to the global economy from cyber crime



200,000+
Jobs lost in the U.S.



150,000+

Estimated in Europe

Hacking is used by intelligence

```
CuteMouse v1.9.1 alpha 1 [FreeDOS]
Installed at PS/2 port  CuteMouse v1.9.1 alpha 1
C:>ver
      in drive C is FREEDOS_C95
FreeCom version 0.82 p1 3 XMS_Swap [Dec 10 2002]

C:>dir
Volume in drive C is FREEDOS_C95
Volume Serial Number is 004F-9A8B
Directory of C:\N
FDDOS          08-26-04   6:23p
AUDEX.CBT       85    08-26-04   6:24p
BOLET.BIN        512   08-26-04   6:23p
COMMAND.COM     93,963  08-26-04   6:24p
CONFIG.SYS       801   08-26-04   6:24p
FDOSBOOT.BIN     512   08-26-04   6:24p
KERNEL.SYS      45,815  04-17-04  9:19p
6 file(s)   142,038 bytes
1 dir(s)  1,064,517,632 bytes free

C:>_ CuteMouse v1.9.1 alpha 1 [FreeDOS]
```

STUXNET

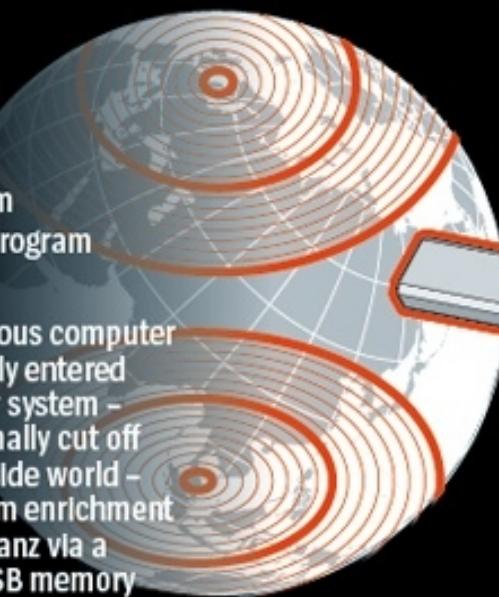


Hacking is used by intelligence

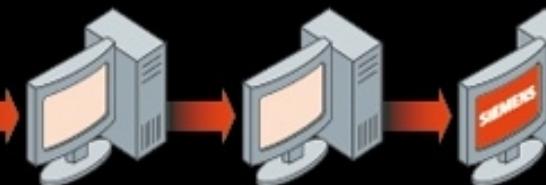
Software Sabotage

How Stuxnet disrupted Iran's uranium enrichment program

1 The malicious computer worm probably entered the computer system – which is normally cut off from the outside world – at the uranium enrichment facility in Natanz via a removable USB memory stick.

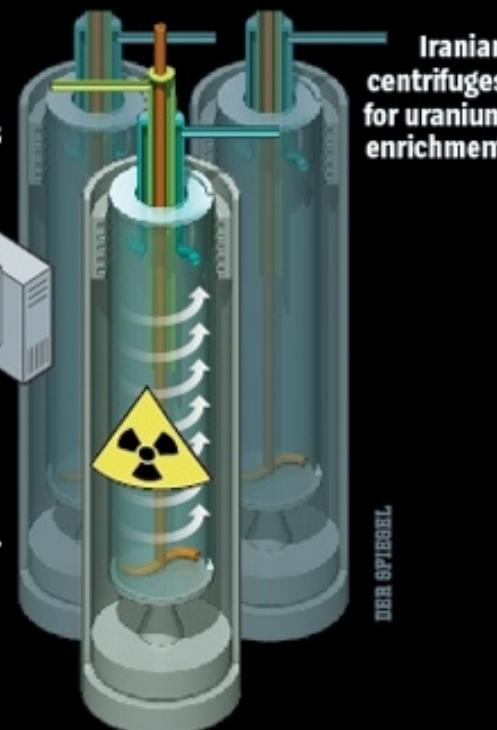


2 The virus is controlled from servers in Denmark and Malaysia with the help of two Internet addresses, both registered to false names. The virus infects some 100,000 computers around the world.



3 Stuxnet spreads through the system until it finds computers running the Siemens control software Step 7, which is responsible for regulating the rotational speed of the centrifuges.

4 The computer worm varies the rotational speed of the centrifuges. This can destroy the centrifuges and impair uranium enrichment.



Iranian centrifuges for uranium enrichment

DER SPIEGEL

5 The Stuxnet attacks start in June 2009. From this point on, the number of inoperative centrifuges increases sharply.



Hacking is used by intelligence

Operation “Red October”

Victims of advanced cyber-espionage network



Web Hacking II. Threats



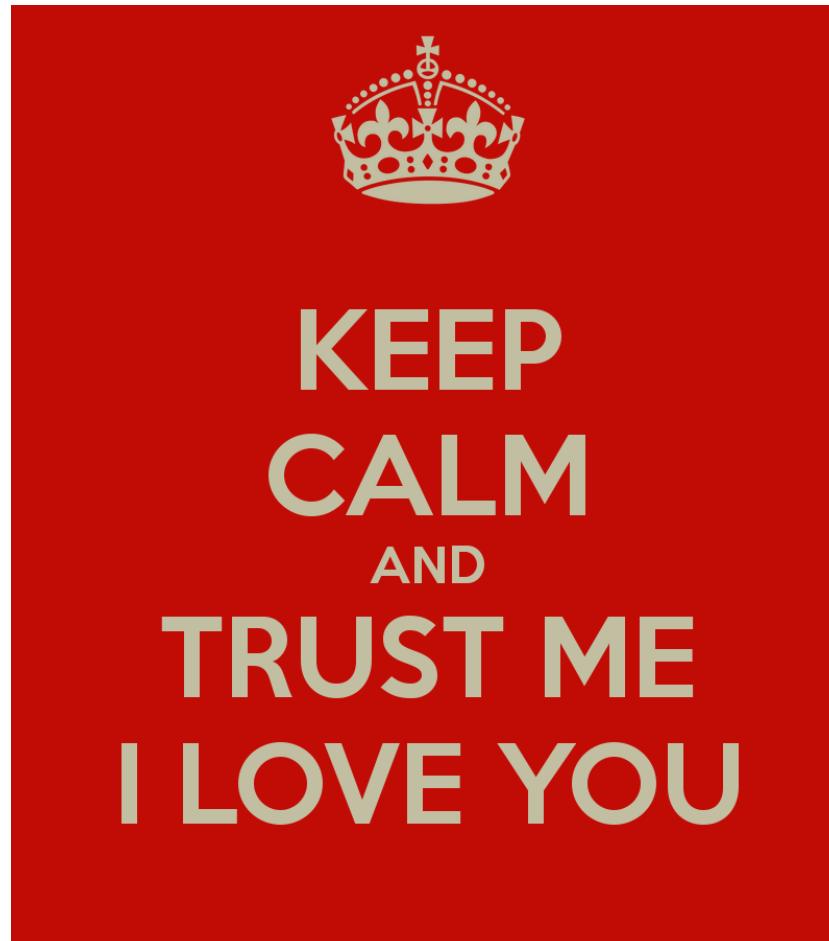
That may happen?



OR



Business needs Trust!



Business needs Trust!



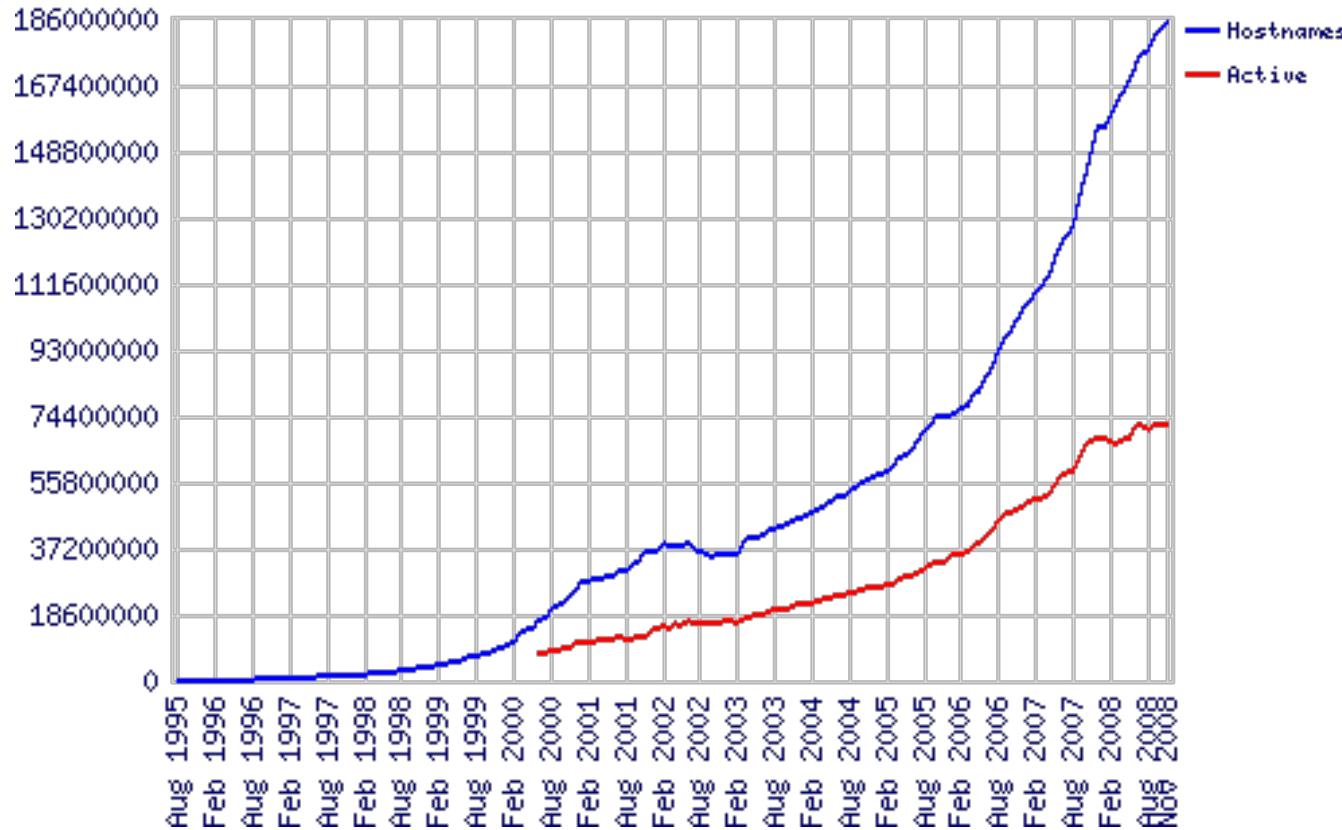
The end of the fortress metaphor



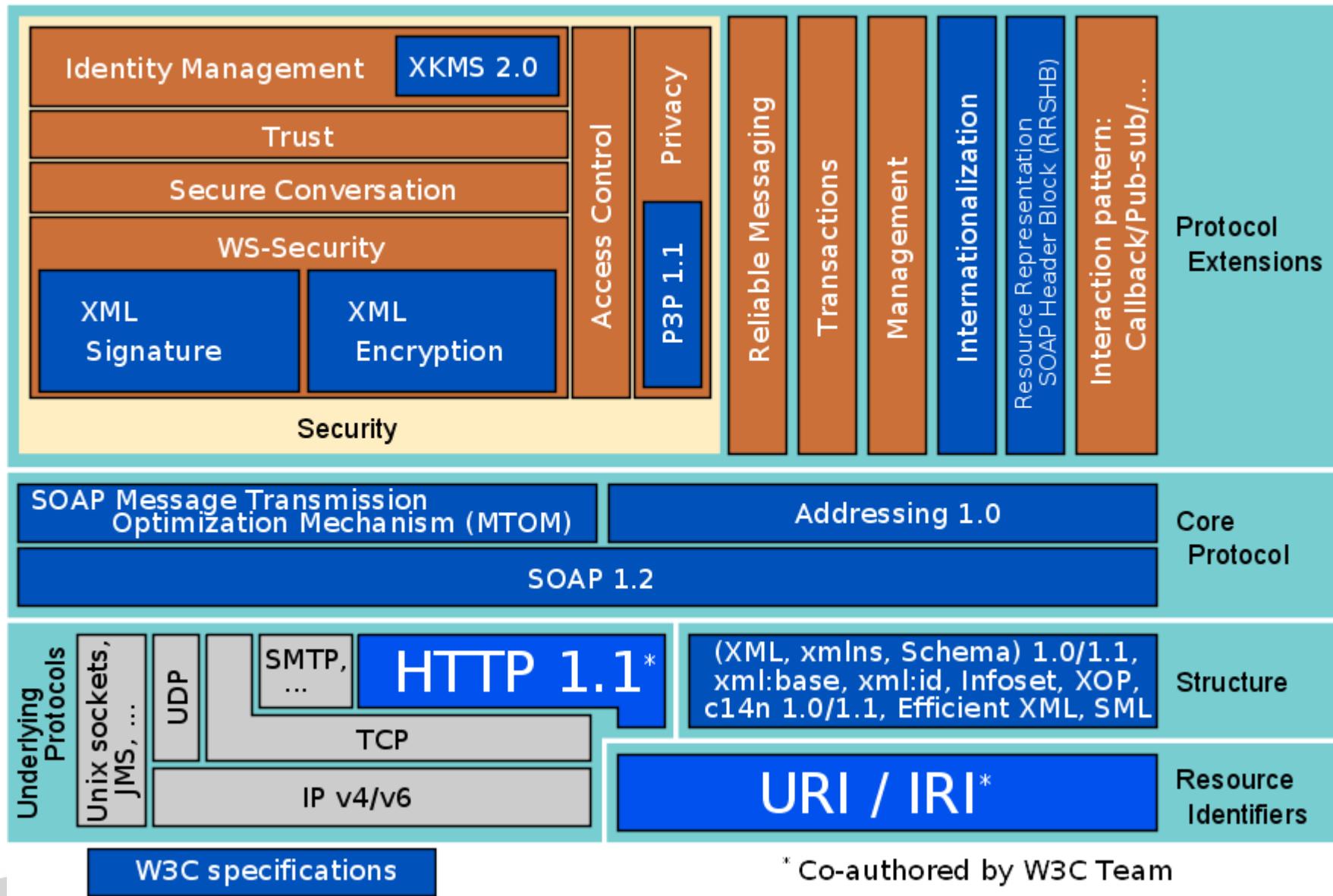
The end of the fortress metaphor



The end of the fortress metaphor



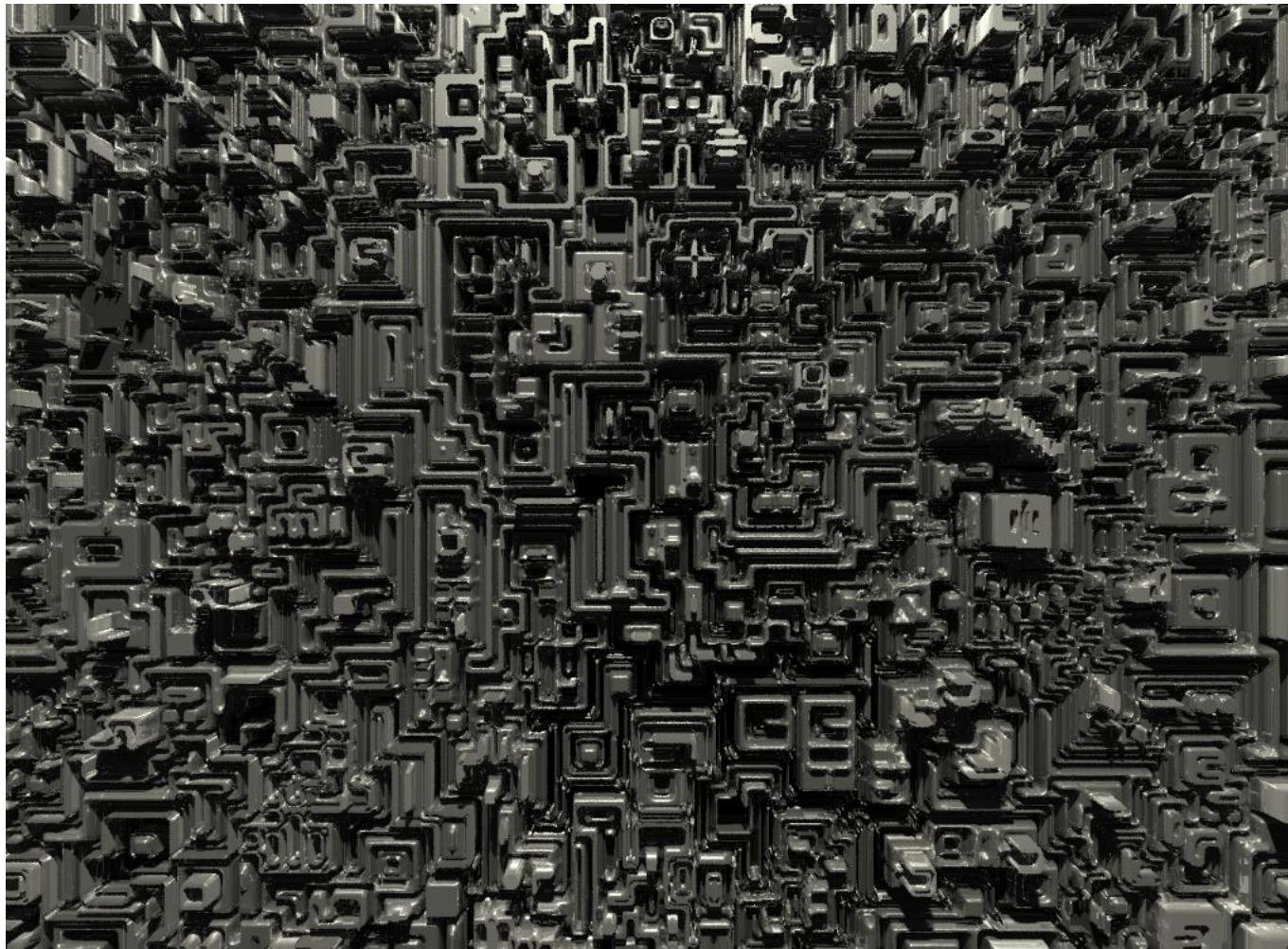
The end of the fortress metaphor



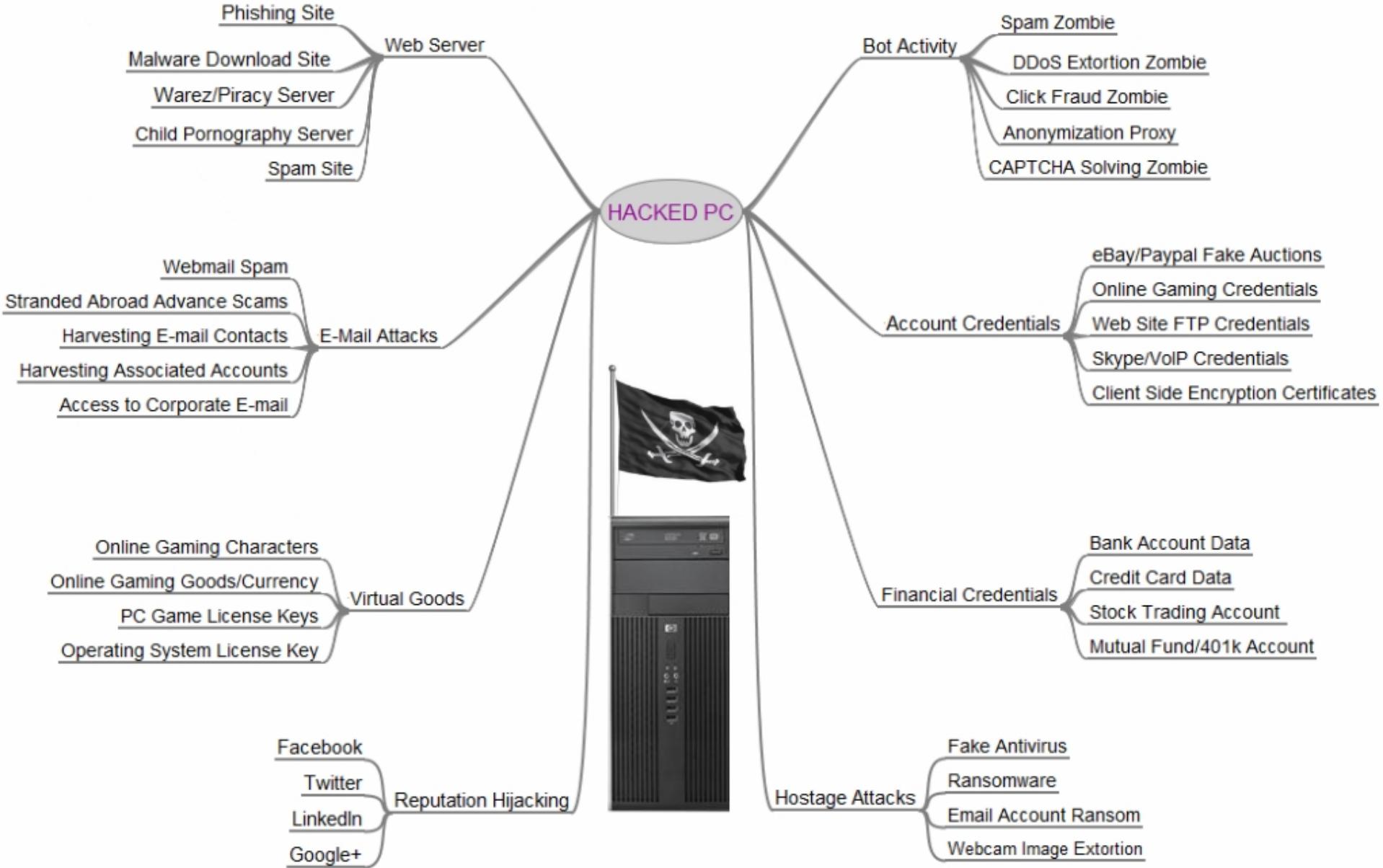
The end of the fortress metaphor



The end of the fortress metaphor



On the client

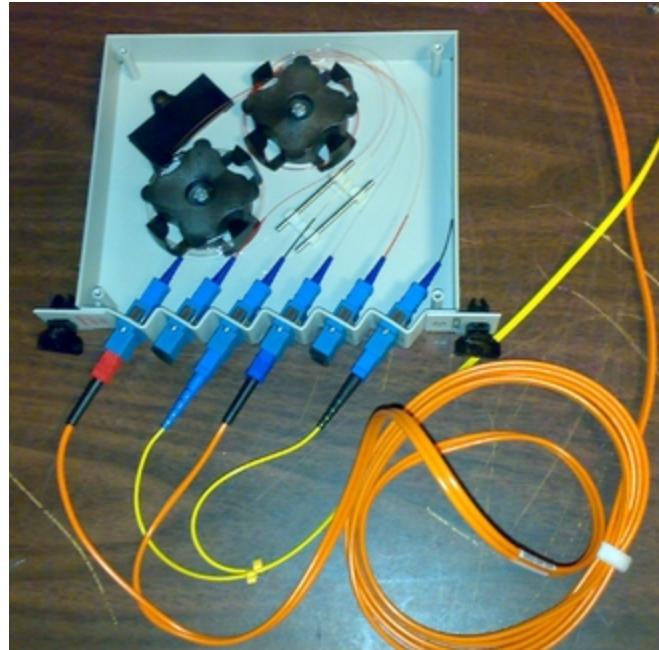


On the network

Passive attacks: Wireless or Fiber eavesdropper

Active attacks:

- evil Wifi router
- DNS poisonning

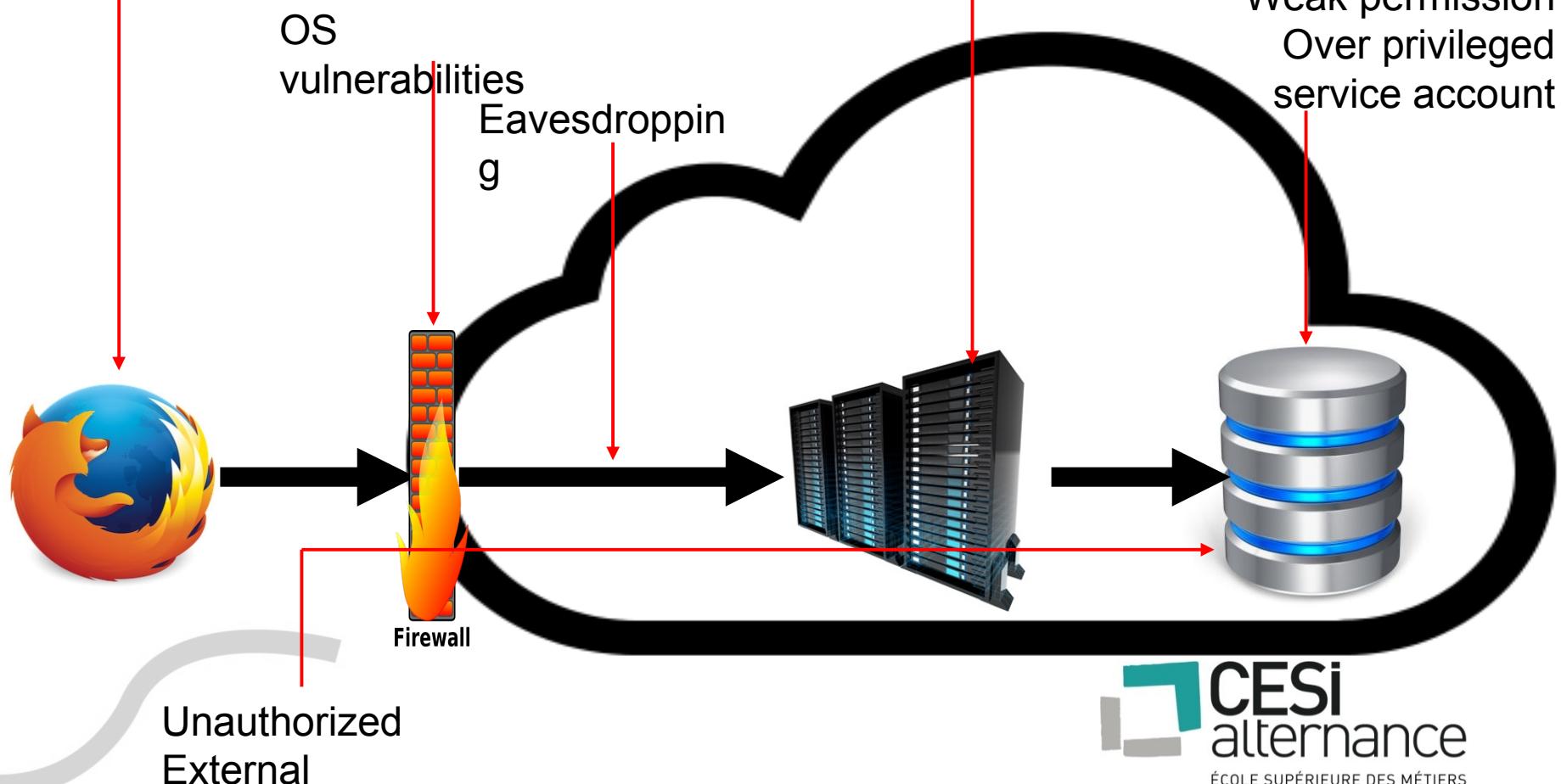


On the server

SQL Injection
XSS
Session Hijacking

Webapp vulnerabilities
Privilege escalator
Weak input validation

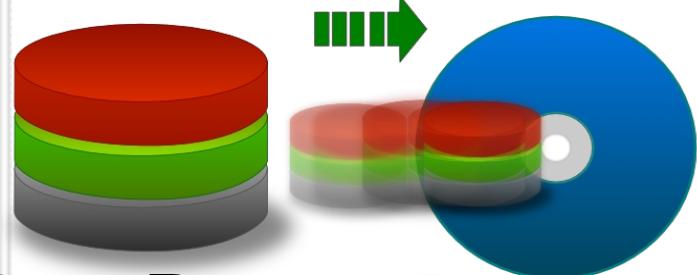
Conf vulnerabilities
Weak permission
Over privileged service account



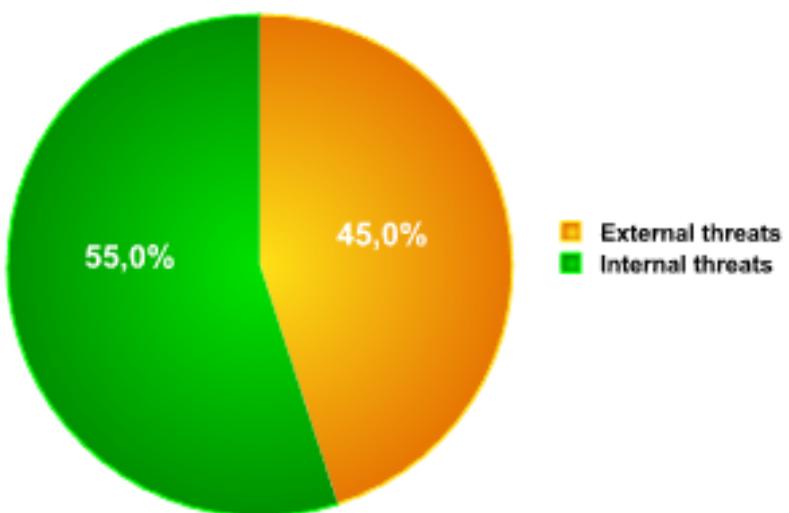
Back Office Threats

View Log File: tot.txt.2008-02-07-16:20:06

```
02-07 16:20:06 +0200 08 tz PROCESSING:00000000: Shepherd thread is started
02-07 16:20:06 +0200 08 tz PROCESSING:00000000: Start scanning queue directory /var
02-07 16:20:07 +0200 08 tz PROCESSING:00000000: Queue directory /var/opt/axigen/que
02-07 16:20:09 +0200 02 tz RPOP:00000001: rpop connection ended, status: 3;Local fo
02-07 16:20:09 +0200 02 tz RPOP:00000002: rpop connection ended, status: 3;Local fo
02-07 16:29:01 +0200 08 tz WEBMAIL:00000003: [192.168.8.179:8000] connection accept
02-07 16:29:01 +0200 08 tz WEBMAIL:00000004: [192.168.8.179:8000] connection accept
02-07 16:29:12 +0200 08 tz WEBMAIL:00000003: Account 'laura.white@mycompany.com' ha
02-07 16:29:16 +0200 08 tz WEBMAIL:00000003: connection closed with [192.168.8.167:
02-07 16:29:16 +0200 08 tz WEBMAIL:00000005: [192.168.8.179:8000] connection accept
02-07 16:29:16 +0200 08 tz WEBMAIL:00000004: connection closed with [192.168.8.167:
02-07 16:29:16 +0200 08 tz WEBMAIL:00000006: [192.168.8.179:8000] connection accept
02-07 16:30:09 +0200 02 tz RPOP:00000007: rpop connection ended, status: 3;Local fo
02-07 16:30:09 +0200 02 tz RPOP:00000008: rpop connection ended, status: 3;Local fo
02-07 16:33:46 +0200 08 tz WEBADMIN:00000009: [192.168.8.179:9000] connection accep
02-07 16:33:51 +0200 08 tz WEBADMIN:00000009: New session 0x2C5EED9B associated wit
02-07 16:33:51 +0200 08 tz WEBADMIN:00000009: Admin user "Admin" /id=0x0000000000000001 - 1
```



DataBase Backup



■ External threats
■ Internal threats



Human fails

Technology development

Organization



Psychological weakness



Business widely impacted



Web Hacking

III. Countermeasures





Security audit



OLD
SCHOOL

Security audit



Security audit

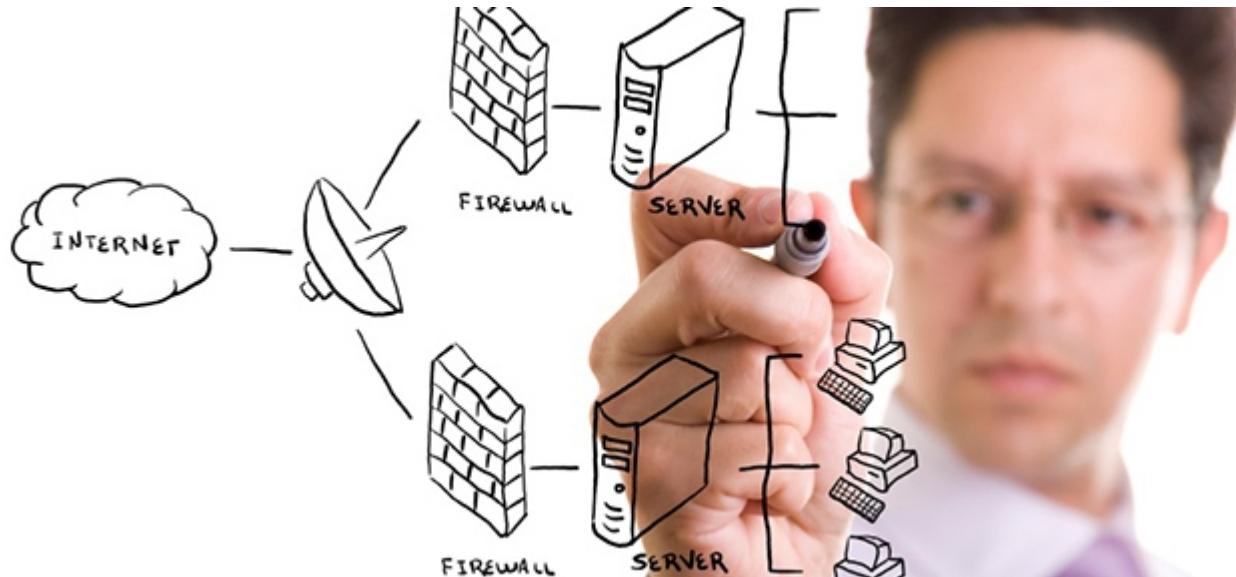


Security audit

DON'T DELEGATE IT



Security by design



Security by design

COVERAGE ALL...

Product design and development

Hardware programming

Application & hardware testing

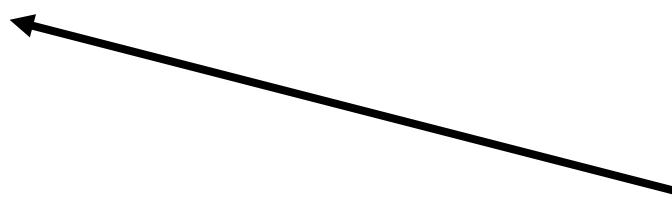
Review code for vulnerabilities

Fix vulnerabilities ASAP

Always aware

Malware analysis, Reverse engineering

Application security review



Security by design



**COVERAGE ALL...
with :**

- developers**
- admin sys**
- threats sentinels**



Review code for vulnerabilities:

- pair review off all entry points
- integrate frameworks security fixes
- white box pen tests



Penetration testing:

- **with trained team (mandatory)**
- **blackbox preferred**
- **apply OWASP guides**



Security by design

Fix vulnerabilities ASAP:

- **deliver small changes continuously**
- **mastering release management**
- **integrate & deploy framework fixes**
- **automated smoke test strategy**



Security by design

Always aware:

- follow OSS release managers
- inspect OSS discussion groups
- look at CVE
- read OWASP references & newsletter



What is a CVE ?

- Common Vulnerabilities & Exposures
- standardized format

<https://cve.mitre.org/>

<https://www.owasp.org>



OWASP Java Project
@OWASP_Java FOLLOW YOU

Malware analysis :

- **for all untrusted environments**
- **know your adversary**
- **don't be weak with known malwares**



Application security review:

- **filter vulnerabilities related to your technical stack**
- **review by vulnerability**
- **maintain compliance matrix**
- **do it deeply for all major release**

Security by design

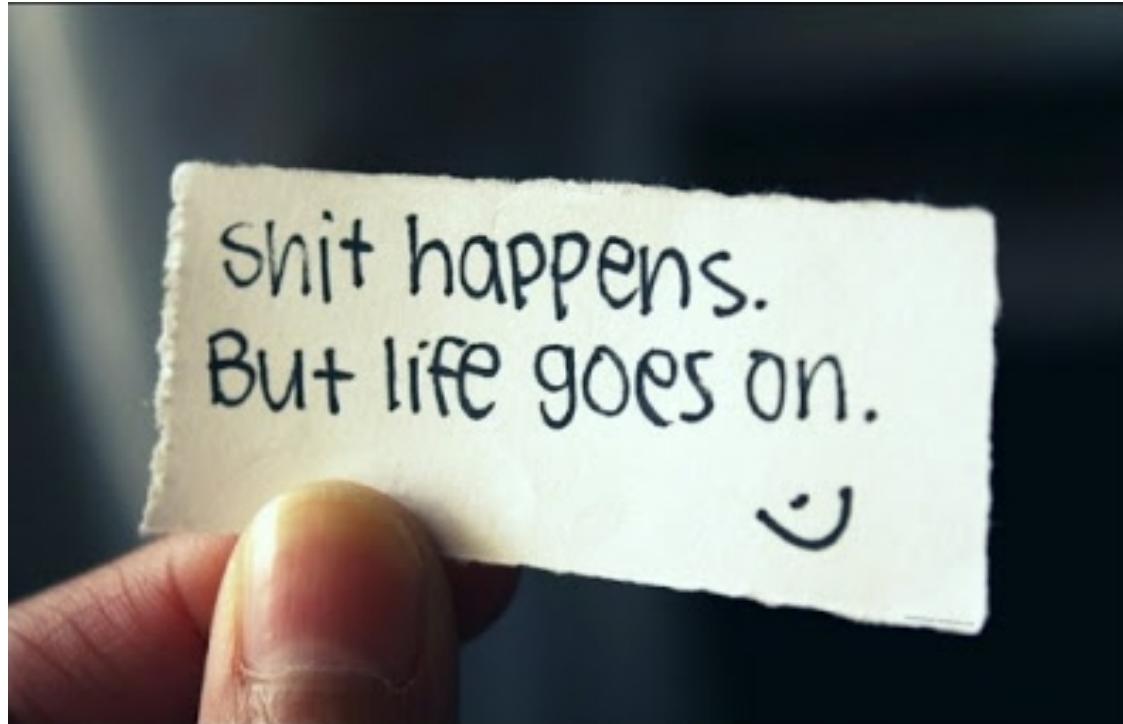


Test developer threats knowledge:

- fix vulnerabilities with untrained developer
- under trained developer supervision
- share the knowledge
(how to Xploit / fix a given vulnerability)
- communicate ONCE the patch in production



Even best developers fails...



You have been hacked

#1 NO LIES #1

#2 OPEN or CLOSE ?

#3 EVALUATE IMPACTS

→ **operational**

→ **reputability**



React after hacks

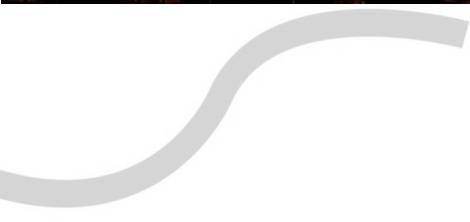
#1 lock exploit EVEN with business impact

#2 Communicate clearly

#3 Legal – save hack proofs



But major diseases can occurs



Initial situation

#1 Main Data Center OOO
(Out Of Order)

#2 Related to a hack

#3 Only aim: destroy you



#1 Detect vulnerability vector

#2 Patch emergency site

#3 Don't inject new vulnerabilities

#4 Switch to emergency

Prepared situation

#1 Scenario written in a DRP

(Disaster Recovery Plan)

#2 Tested in operational conditions

#3 Rebuild it periodically

#4 Often theoretical



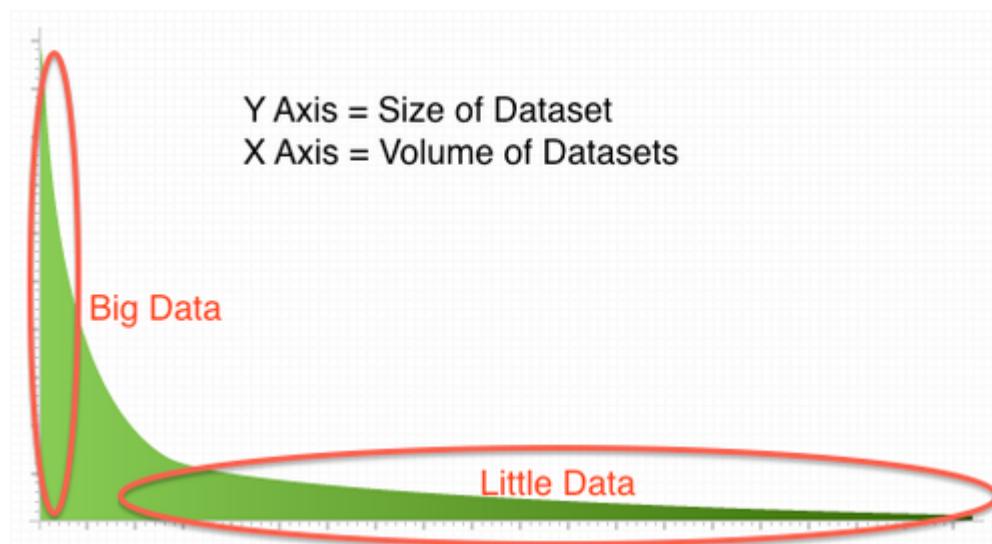
Prepared situation

...May works for institutions



Prepared situation

They have few data



Prepared situation

They have few data

2x 750m²

Scale → Petaoctet

Prepared situation

LIMITS?



Prepared situation

Google

**14 DC x 9000m²
900.000 server... in 2011**

Scale → unknown

Prepared situation

- Replication
- Multi DC
- Multi continents

Is NATIVE



Prepared situation

Other exists



OVH.com

15 DC



7 DC

Global Capacity is huge but limited



4 TB/S

Prepared situation

**Move 9 PB daily
takes time...**

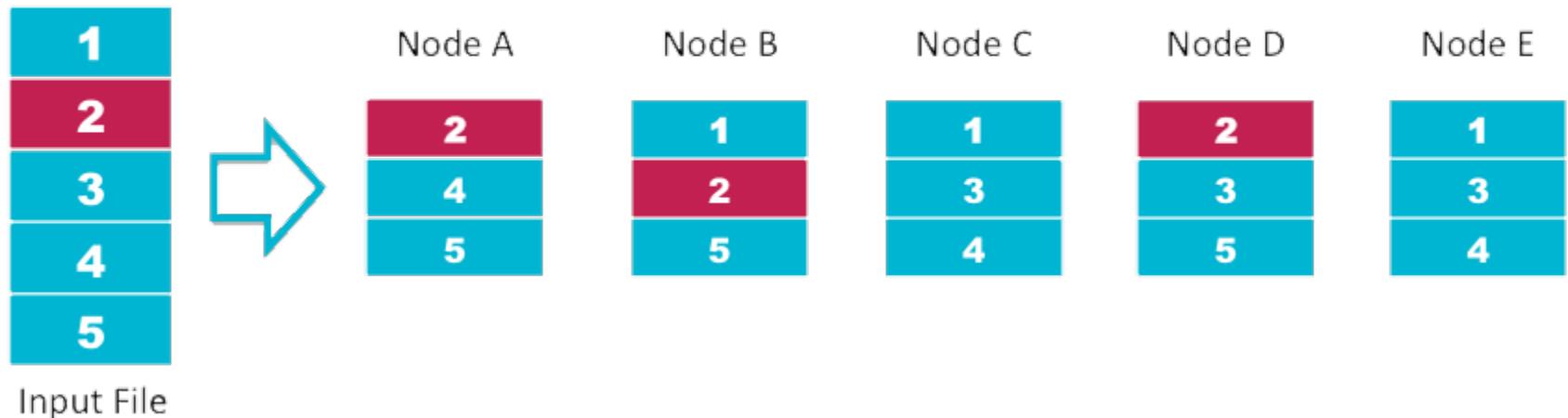
**3 hours with the FULL bandwidth
of the 3rd worldwide IPS**



Prepared situation

Replication

HDFS Data Distribution



Other multiple DC

Be robust even if

- you loose one server
- you loose one rack
 - or in extreme cases
- one DC



Prepared situation

Don't be prepared to the Evil...

Invite him at your table





ÉCOLE SUPÉRIEURE DES MÉTIERS



LE CESI :
ENSEIGNEMENT
SUPERIEUR ET
FORMATION
PROFESSIONNELLE



ÉCOLE SUPÉRIEURE DES MÉTIERS

Web Hacking

I. Intro



Document confidentiel - ne pas diffuser

LE CESI :
ENSEIGNEMENT
SUPERIEUR ET
FORMATION
PROFESSIONNELLE



ÉCOLE SUPÉRIEURE DES MÉTIERS

The **hacker** culture is a subculture of individuals who enjoy the intellectual challenge of creatively overcoming and circumventing limitations of systems to achieve novel and clever outcomes. The act of engaging in activities in a spirit of playfulness and exploration is termed "**hacking**".



Document confidentiel - ne pas diffuser

LE CESI :
ENSEIGNEMENT
SUPERIEUR ET
FORMATION
PROFESSIONNELLE

But... for unlighted people,



CESI
alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Hacking is a chance

 HACKING HEALTH **CAMP**

**Create the future
of healthcare**

< Conferences / Workshops / Hackathon >

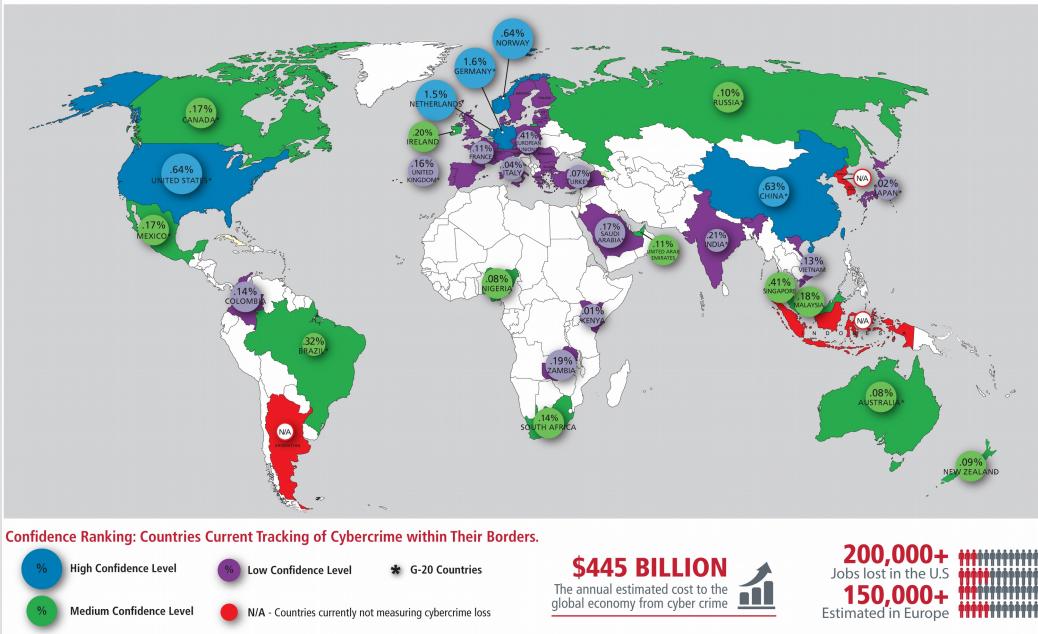


**CESI**
alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Hacking is a cancer



CYBERCRIME LOSS AS A PERCENT OF GDP (GROSS DOMESTIC PRODUCT)



Hacking is used by intelligence

```
CuteMouse v1.9.1 alpha 1 (FreeDOS)
Installed at PS/2 port  CuteMouse v1.9.1 alpha 1
C:\>ver      in drive C is FREEDOS_09500000
FreeDOS version 0.82 pl 3 XMS_Swap [Dec 18 2002]
C:\>dir      v1.9.1 alpha 1
  Volume in drive C has no label
  Volume Serial Number is 0000-0000
  Directory of C:\

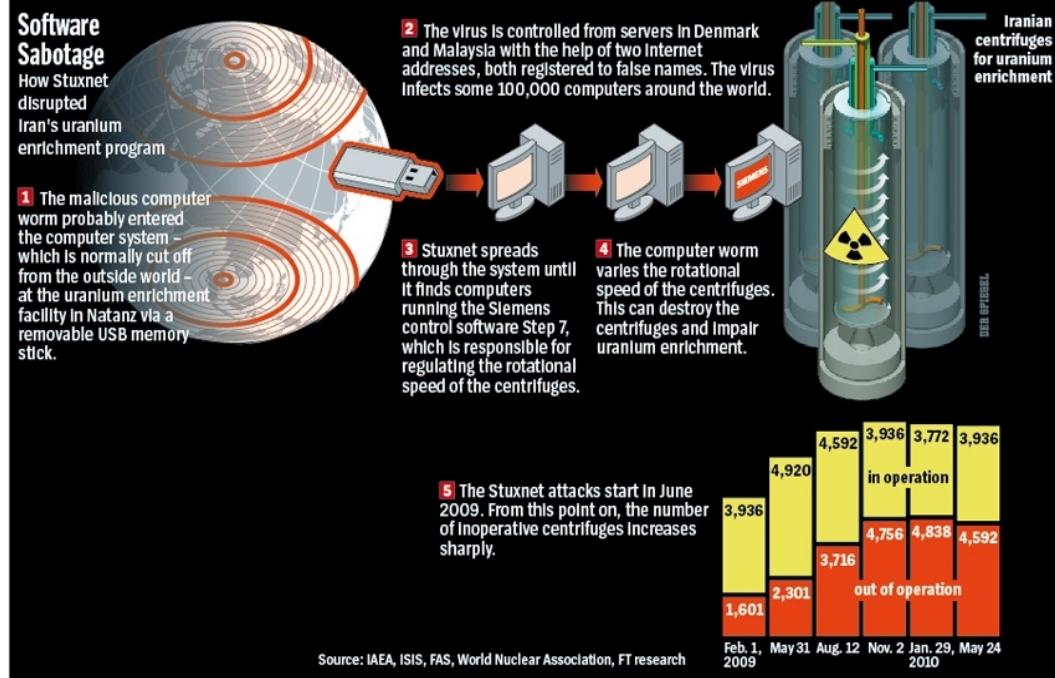
FDOS             1DZ   08-26-04  6:23p
GRUDEX.C   BT    05  08-26-04  6:24p
BOU.LT.BIN    05  08-26-04  6:23p
COMMAND.COM   03,953  08-26-04  6:24p
CONFIG.SYS    881  08-26-04  6:24p
FDOSBOOT.BIN   512  08-26-04  6:24p
KERNEL.SYS    45,815  04-17-04  9:19p
6 file(s)       142,938 bytes
1 dir(s)     1,064,517,632 bytes free

C:\>_ CuteMouse v1.9.1 alpha 1 (FreeDOS)
```

STUXNET



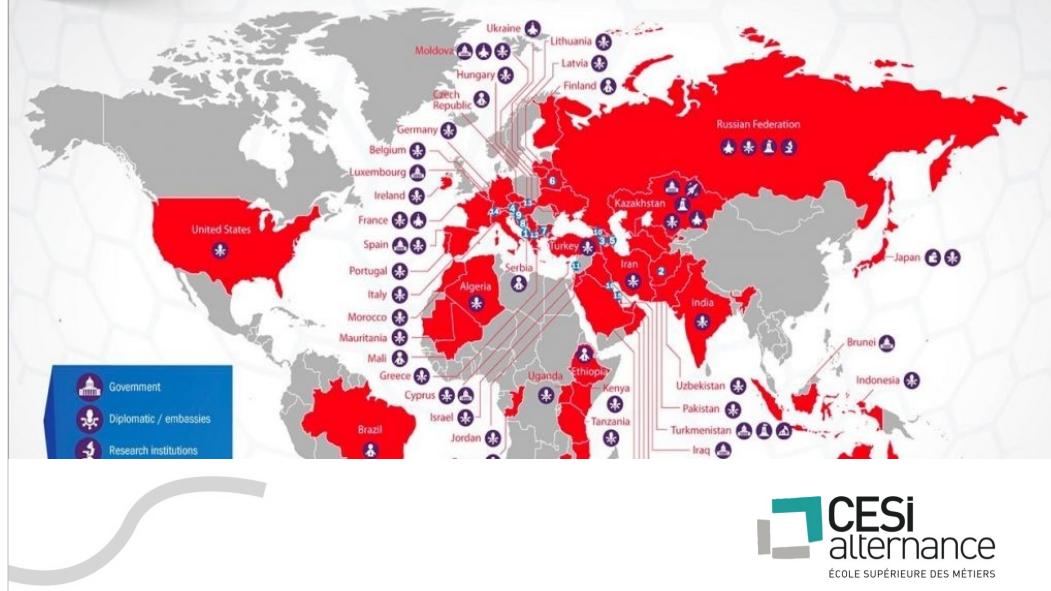
Hacking is used by intelligence



Hacking is used by intelligence

Operation “Red October”

Victims of advanced cyber-espionage network



Web Hacking II. Threats



That may happen?



OR



 CESI
alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Business needs Trust!



Business needs Trust!



The end of the fortress metaphor

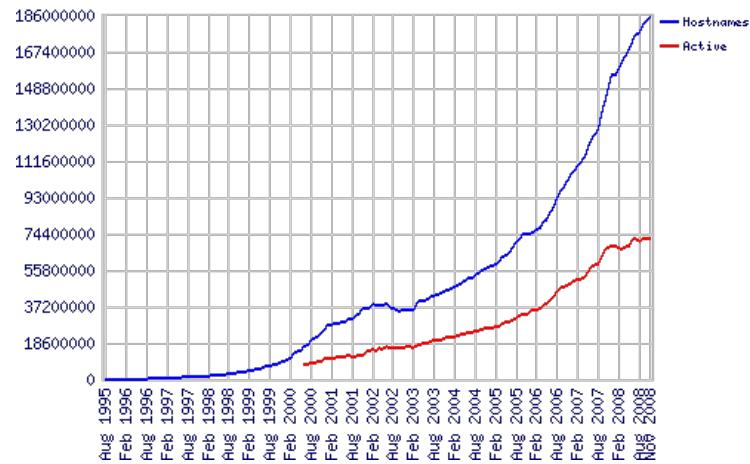


CESi
alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

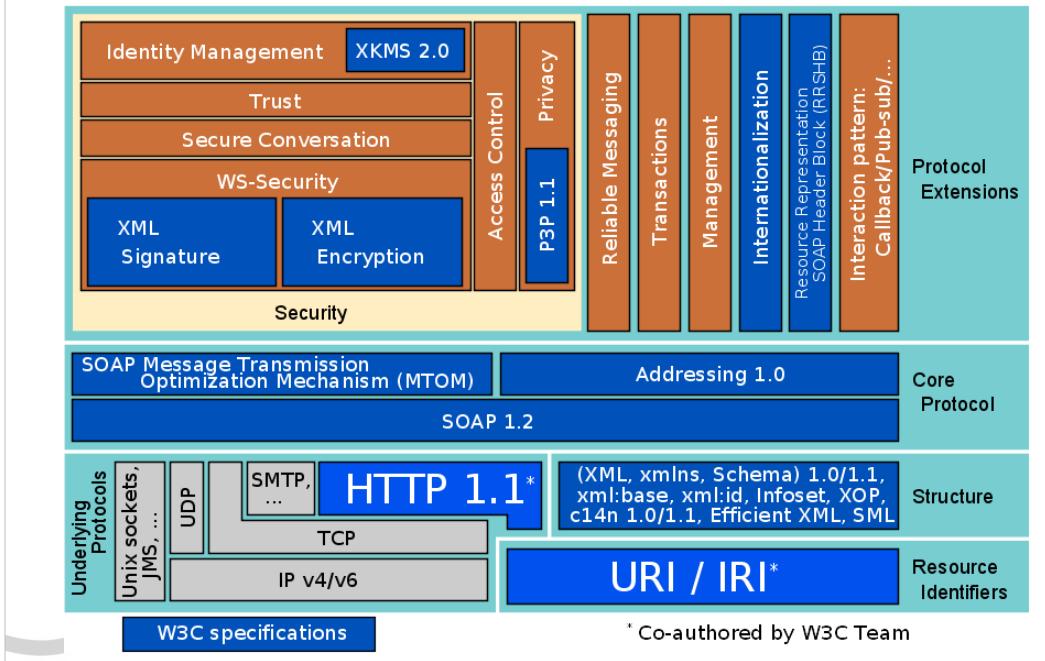
The end of the fortress metaphor



The end of the fortress metaphor



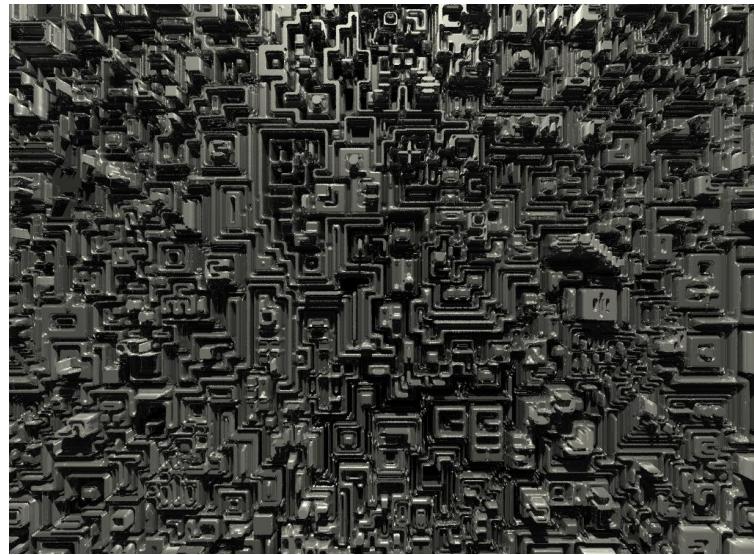
The end of the fortress metaphor



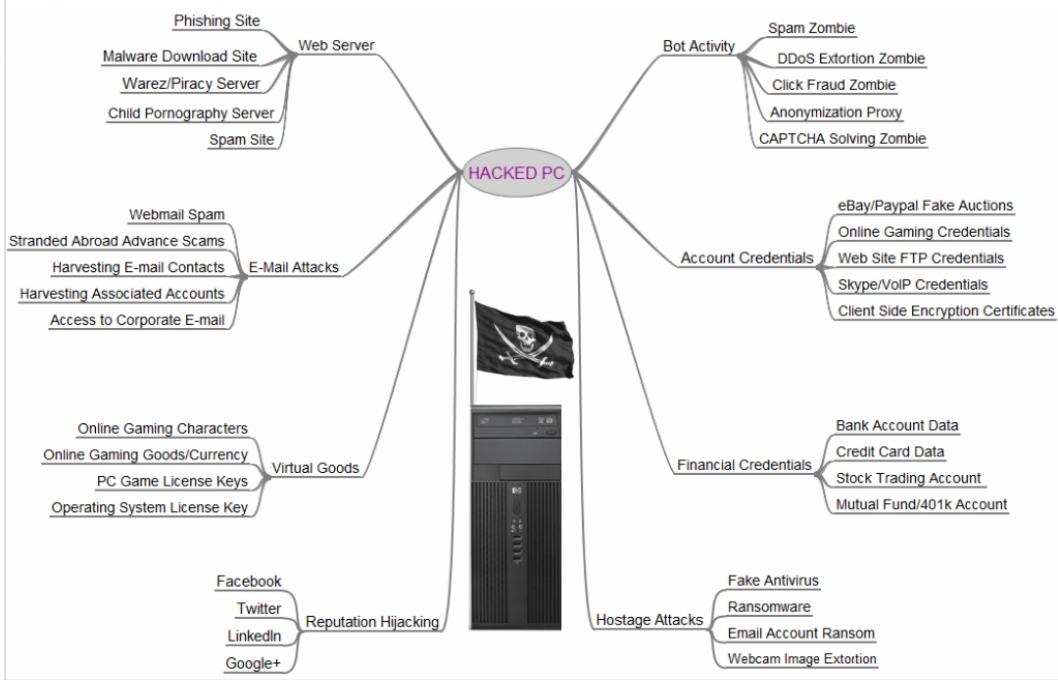
The end of the fortress metaphor



The end of the fortress metaphor



On the client

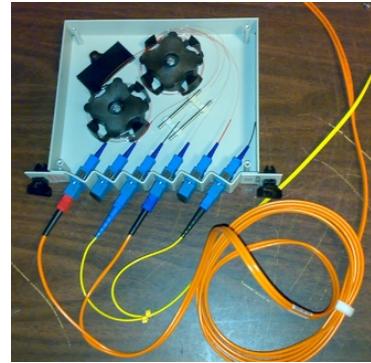


On the network

Passive attacks: Wireless or Fiber eavesdropper

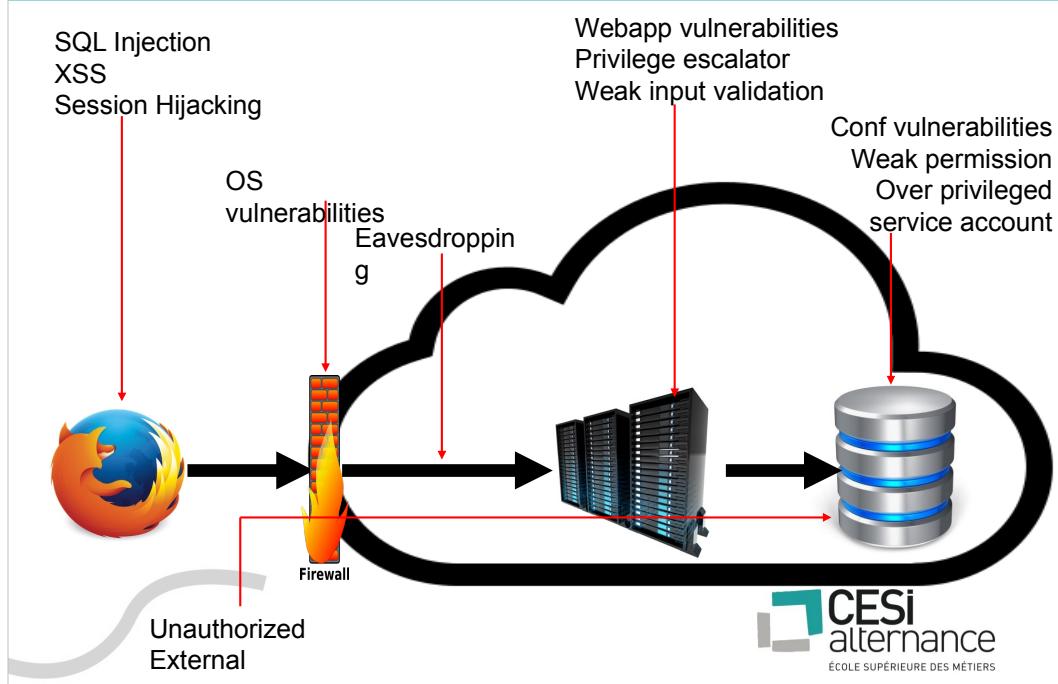
Active attacks:

- evil Wifi router
- DNS poisonning



 CESI
alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

On the server



Back Office Threats

The collage includes:

- A screenshot of a log file titled "View Log File: tot.txt.2008-02-07-162606". The log contains numerous entries related to processing tasks and database connections.
- A red cylinder labeled "DataBase" next to a blue cylinder labeled "Backup". An arrow points from the database cylinder to the backup cylinder.
- A recycling symbol with a hard drive inside, labeled "Recycle".
- A pie chart showing 55.0% in green and 45.0% in orange. A legend indicates orange for "External threats" and green for "Internal threats".
- A circular diagram divided into four quadrants labeled "SALES", "SERVICE", "QUALITY", and "SUPPORT". The word "CRM" is written in the center.
- The CESI alternance logo at the bottom right.

Human fails

Technology development

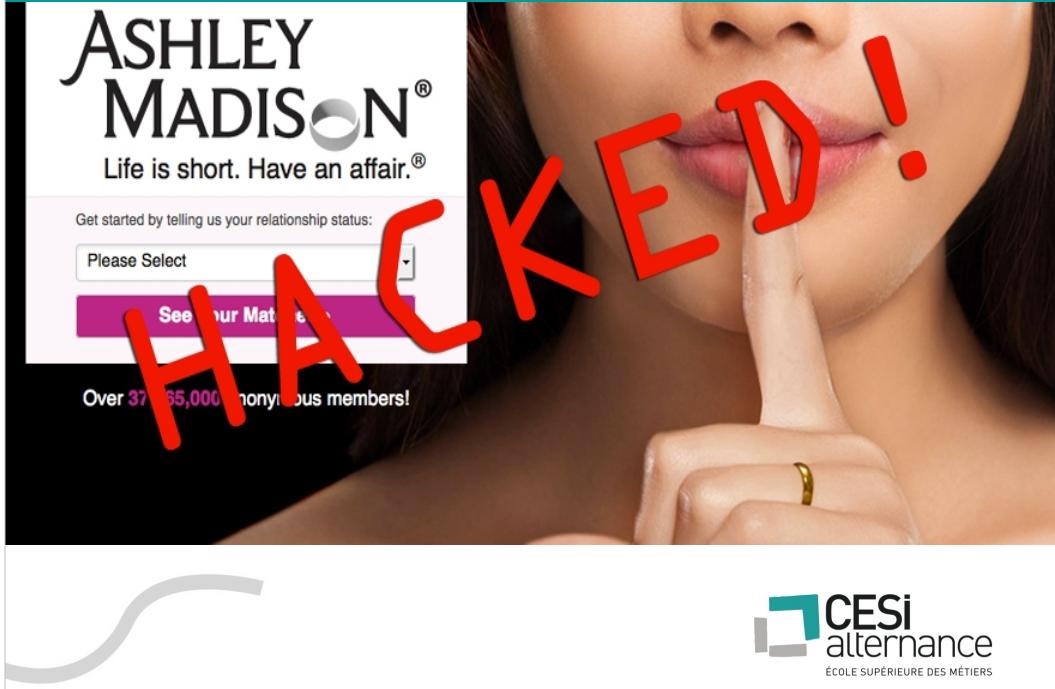
Organization



Psychological weakness



Business widely impacted



CESI
alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Web Hacking

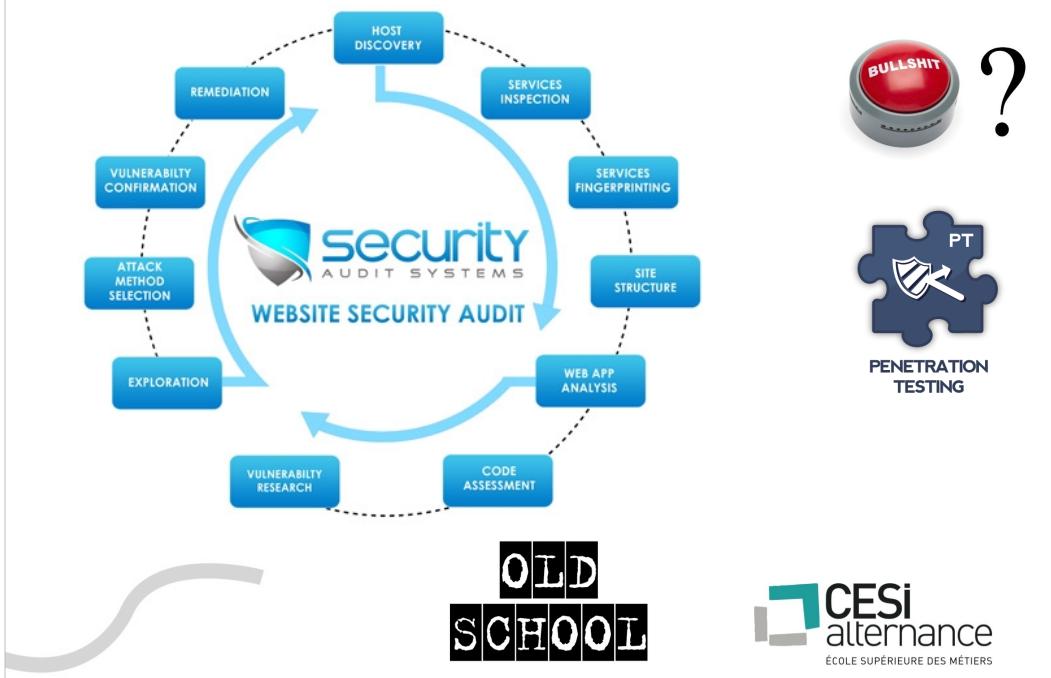
III. Countermeasures





 CESI
alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Security audit



Security audit



 CESI
alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Security audit



Security audit

DON'T DELEGATE IT



Security by design



Security by design

COVERAGE ALL...

Product design and development

Hardware programming

Application & hardware testing

Review code for vulnerabilities

Fix vulnerabilities ASAP

Always aware

Malware analysis, Reverse engineering

Application security review



Security by design



**COVERAGE ALL...
with :**

- developers**
- admin sys**
- threats sentinels**



Security by design

Review code for vulnerabilities:

- pair review off all entry points
- integrate frameworks security fixes
- white box pen tests



Penetration testing:

- **with trained team (mandatory)**
- **blackbox preferred**
- **apply OWASP guides**

Security by design

Fix vulnerabilities ASAP:

- **deliver small changes continuously**
- **mastering release management**
- **integrate & deploy framework fixes**
- **automated smoke test strategy**



Always aware:

- follow OSS release managers
- inspect OSS discussion groups
- look at CVE
- read OWASP references & newsletter



What is a CVE ?

- Common Vulnerabilities & Exposures
- standardized format

<https://cve.mitre.org/>
<https://www.owasp.org>



Malware analysis :

- **for all untrusted environments**
- **know your adversary**
- **don't be weak with known malwares**



Application security review:

- filter vulnerabilities related to your technical stack
- review by vulnerability
- maintain compliance matrix
- do it deeply for all major release

Security by design



CESI
alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Test developer threats knowledge:

- fix vulnerabilities with untrained developer
- under trained developer supervision
- share the knowledge
(how to Xploit / fix a given vulnerability)
- communicate ONCE the patch in production

Even best developers fails...



You have been hacked

#1 NO LIES #1

#2 OPEN or CLOSE ?

#3 EVALUATE IMPACTS

- **operational**
- **reputability**



React after hacks

**#1 lock exploit EVEN with
business impact**

#2 Communicate clearly

#3 Legal – save hack proofs



But major diseases can occurs



Initial situation

#1 Main Data Center OOO
(Out Of Order)

#2 Related to a hack

#3 Only aim: destroy you



#1 Detect vulnerability vector

#2 Patch emergency site

#3 Don't inject new vulnerabilities

#4 Switch to emergency



Prepared situation

#1 Scenario written in a DRP

(Disaster Recovery Plan)

#2 Tested in operational conditions

#3 Rebuild it periodically

#4 Often theoretical



Prepared situation

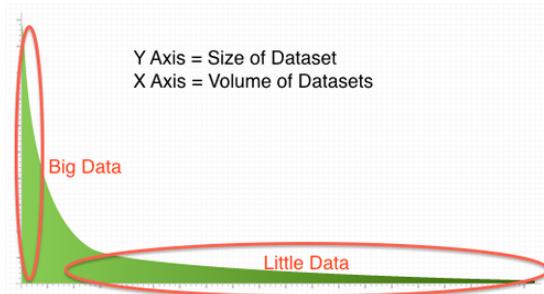
...May works for institutions



 CESI
alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Prepared situation

They have few data



Prepared situation

They have few data

2x 750m²

Scale → Petaoctet



Prepared situation

LIMITS?



 CESI
alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Prepared situation



**14 DC x 9000m²
900.000 server... in 2011**

Scale → unknown



Prepared situation

- Replication
- Multi DC
- Multi continents

Is NATIVE



Prepared situation

Other exists



15 DC



7 DC



Prepared situation

Global Capacity is huge but limited



4 TB/S



Prepared situation

**Move 9 PB daily
takes time...**

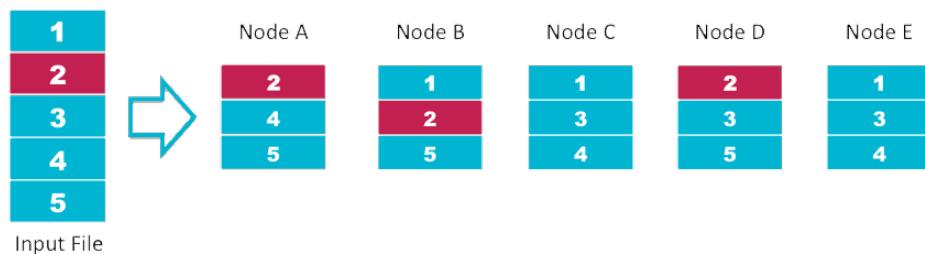
**3 hours with the FULL bandwidth
of the 3rd worldwide IPS**



Prepared situation

Replication

HDFS Data Distribution



Other multiple DC

Prepared situation

Be robust even if

- **you loose one server**
- **you loose one rack**
or in extreme cases
- **one DC**



Prepared situation

Don't be prepared to the Evil...

Invite him at your table



BRACE YOURSELF

