CESi alternance

ÉCOLE SUPÉRIEURE DES MÉTIERS

LE CESI :
ENSEIGNEMENT
SUPERIEUR ET
FORMATION
PROFESSIONNELLE

CESi alternance

ÉCOLE SUPÉRIEURE DES MÉTIERS

Web Hacking
I. Intro

LE CESI : ENSEIGNEMENT SUPERIEUR ET FORMATION PROFESSIONNELLE

CESi alternance

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**".

But... for unlighted people,

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

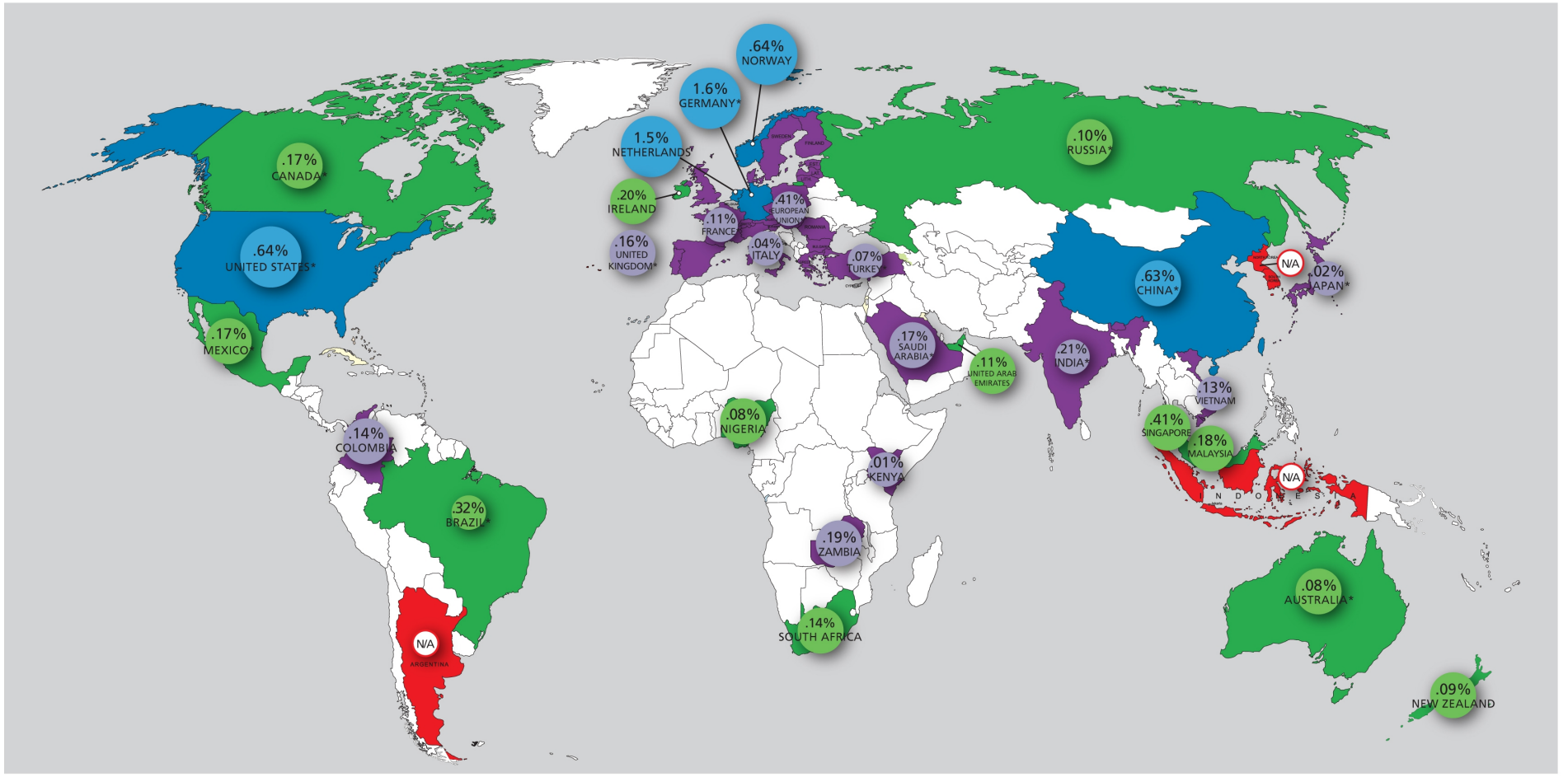
Hacking is a chance

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Hacking is a cancer

McAfee
An Intel Company

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



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

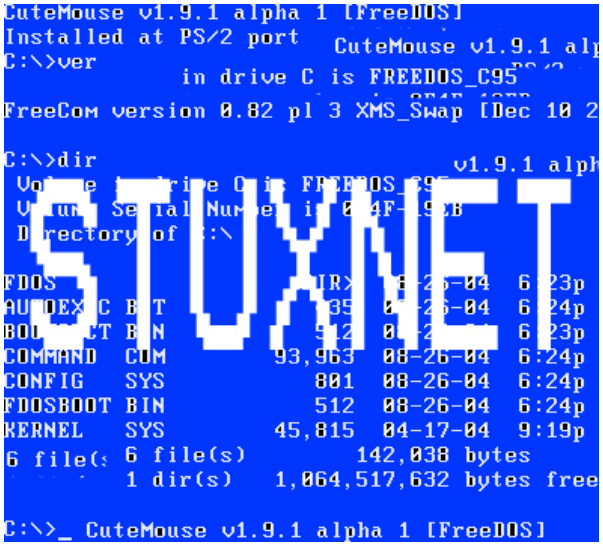
- % High Confidence Level
- % Low Confidence Level
- * G-20 Countries
- % Medium Confidence Level
- N/A - Countries currently not measuring cybercrime loss

$445 BILLION
The annual estimated cost to the global economy from cyber crime

200,000+
Jobs lost in the U.S

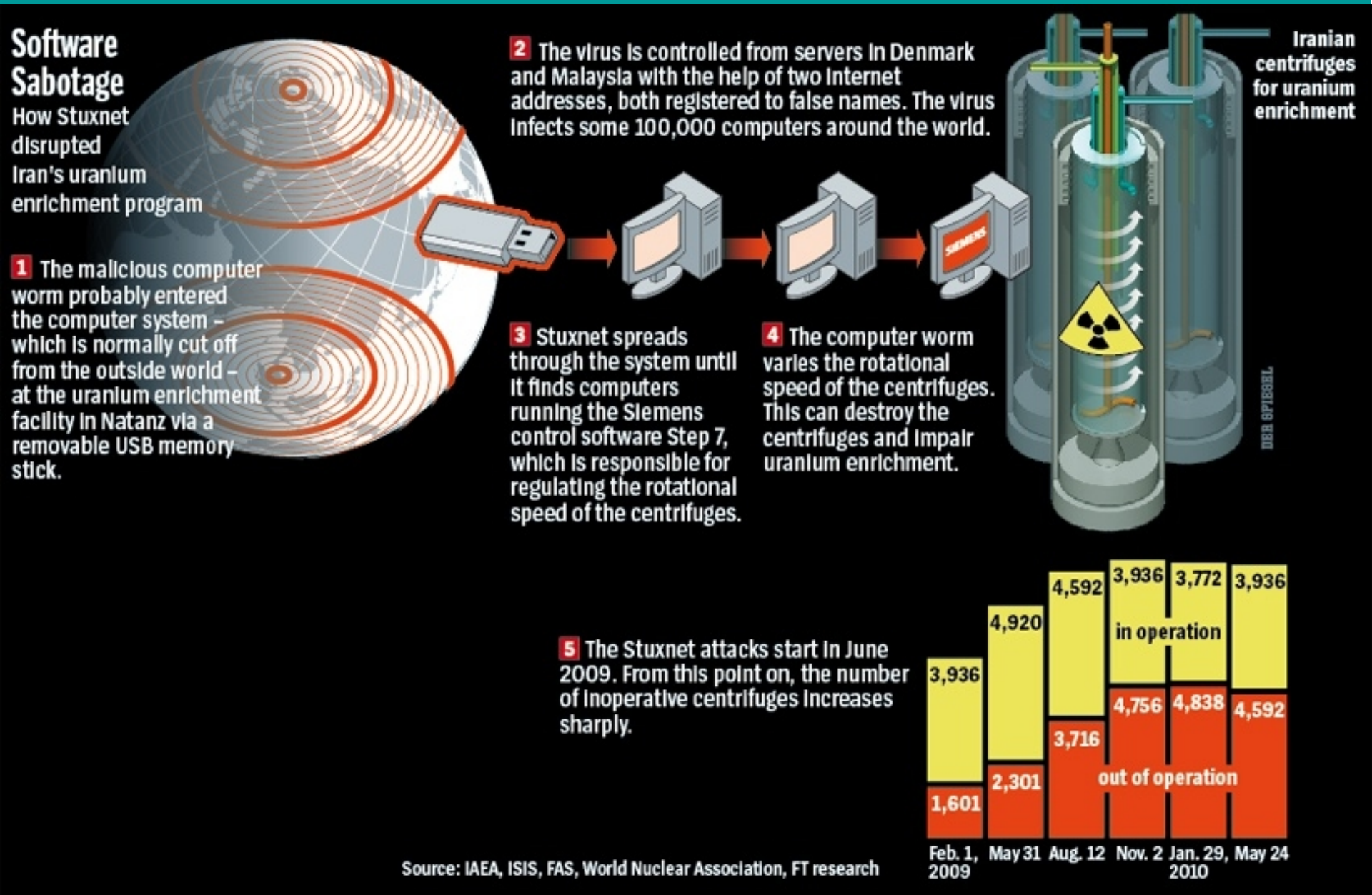
150,000+
Estimated in Europe

Hacking is used by intelligence



CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Hacking is used by intelligence



Hacking is used by intelligence

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Web Hacking II. Threats

That may happen?

OR

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Business needs Trust!

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Business needs Trust!

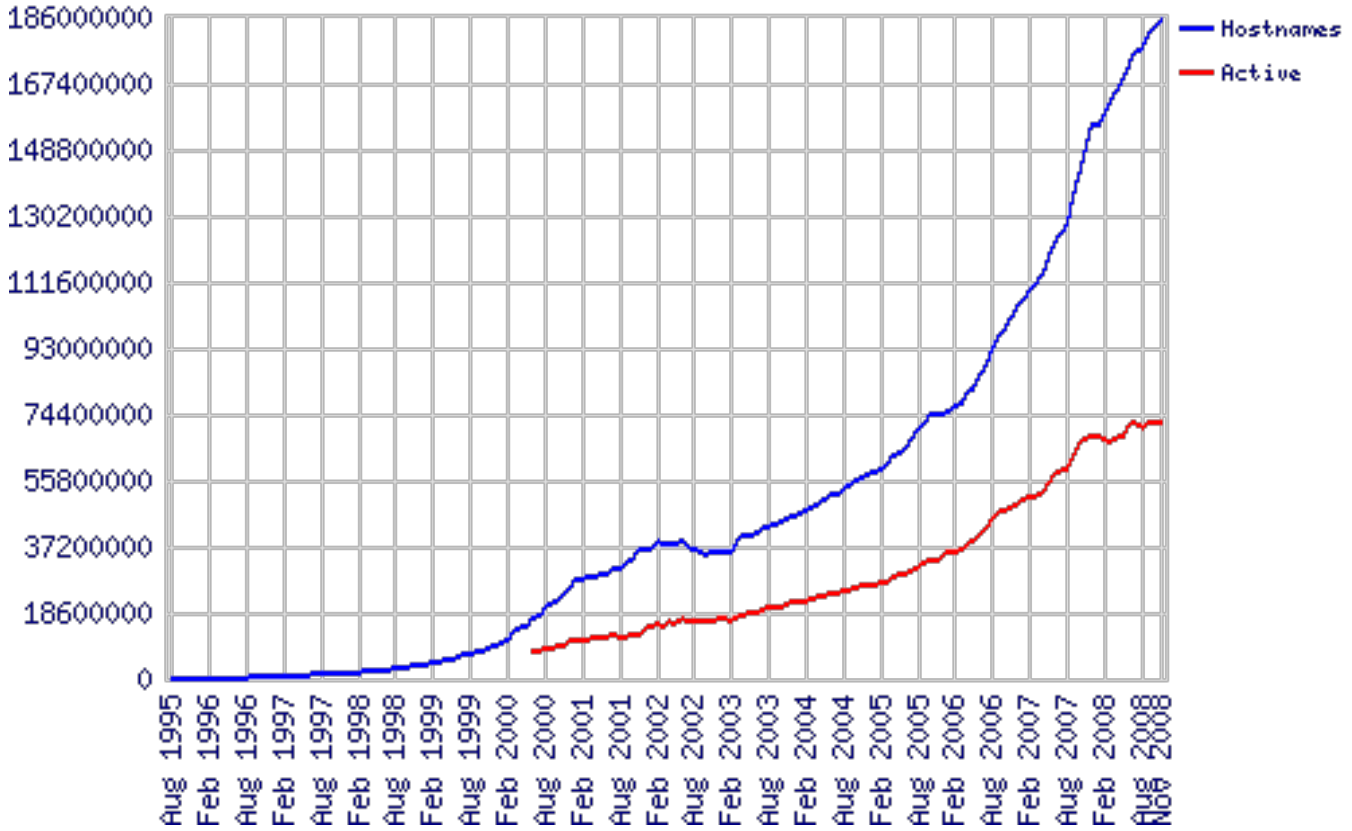
CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

The end of the fortress metaphor

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

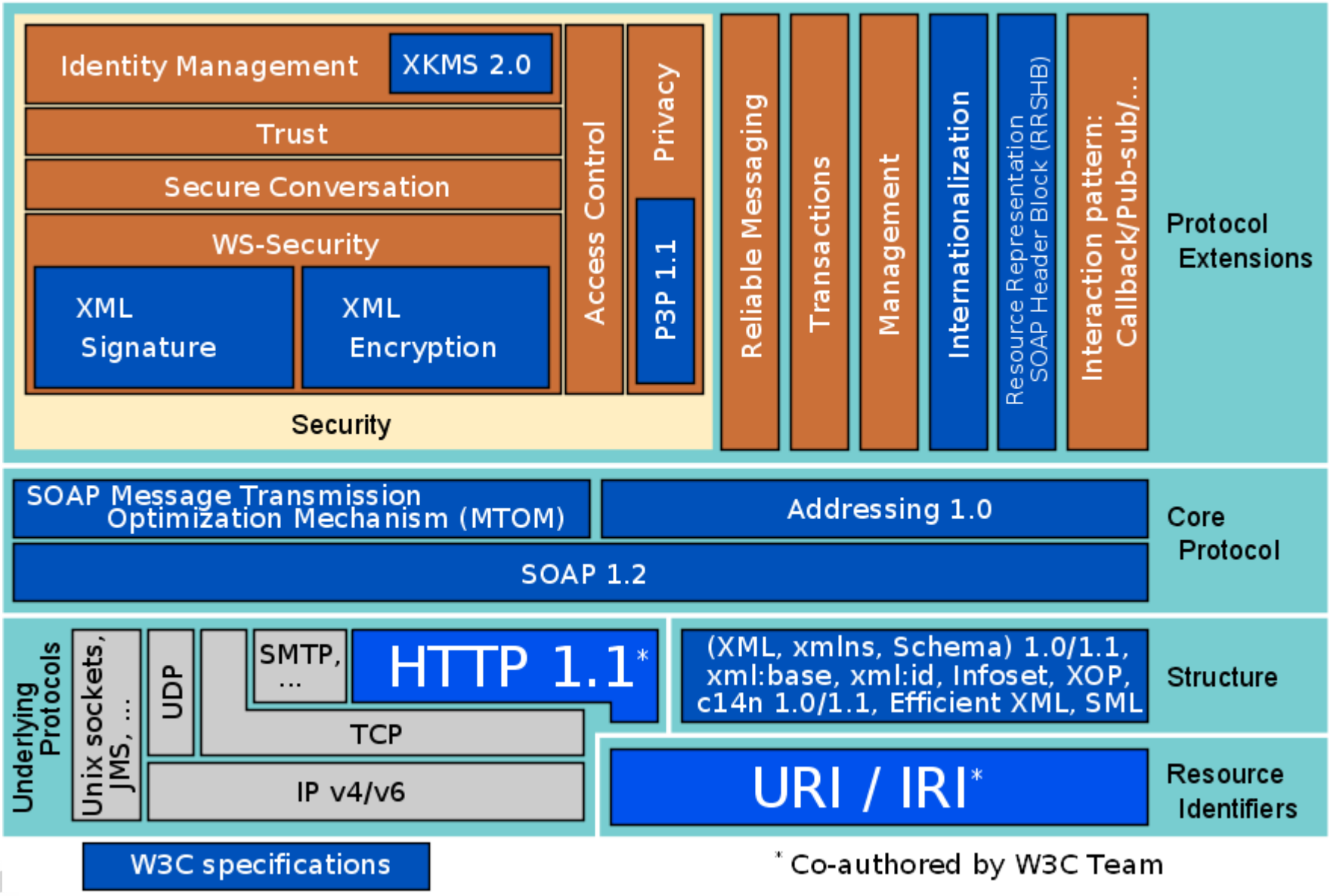
The end of the fortress metaphor

The end of the fortress metaphor

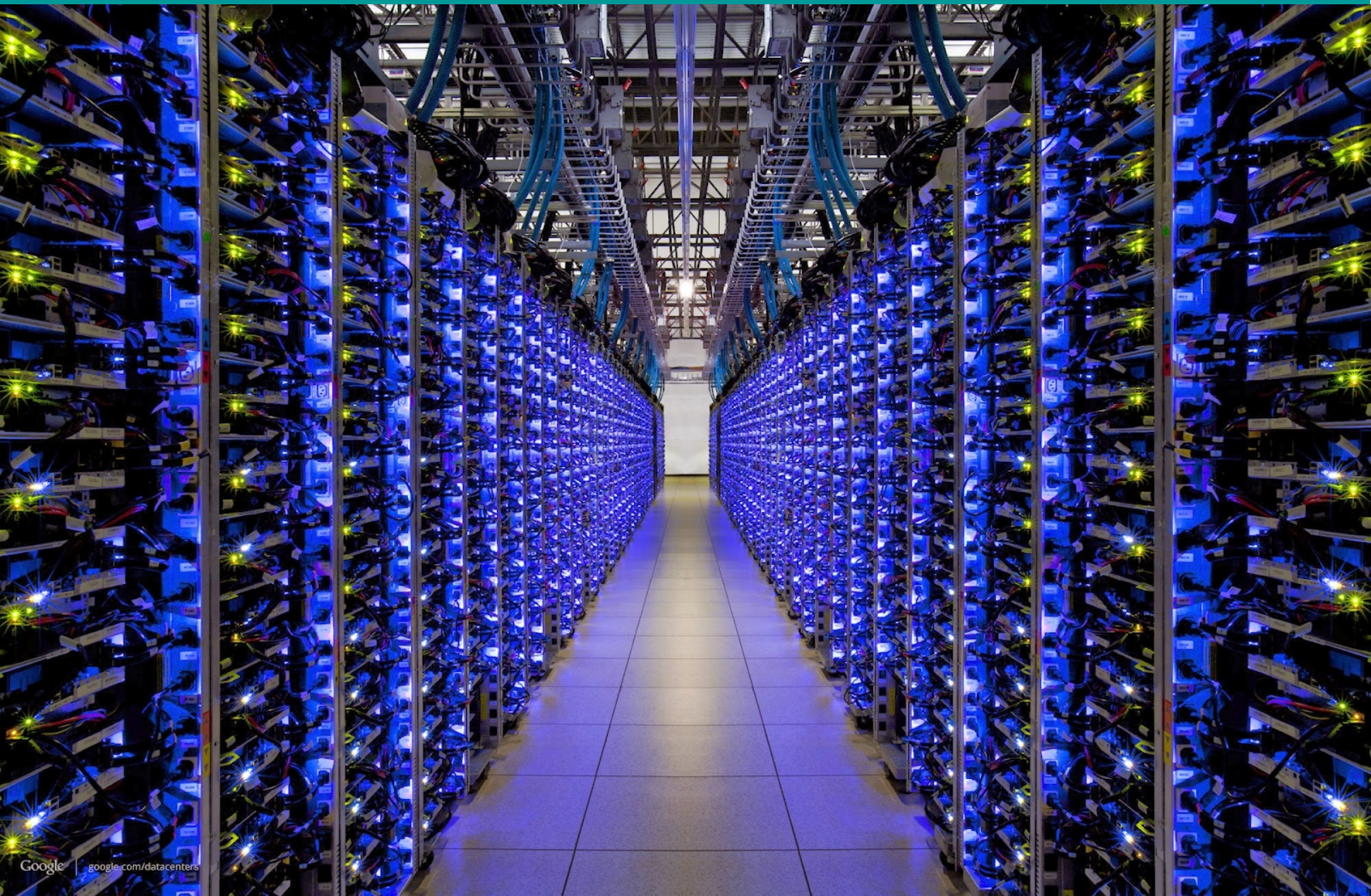


CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

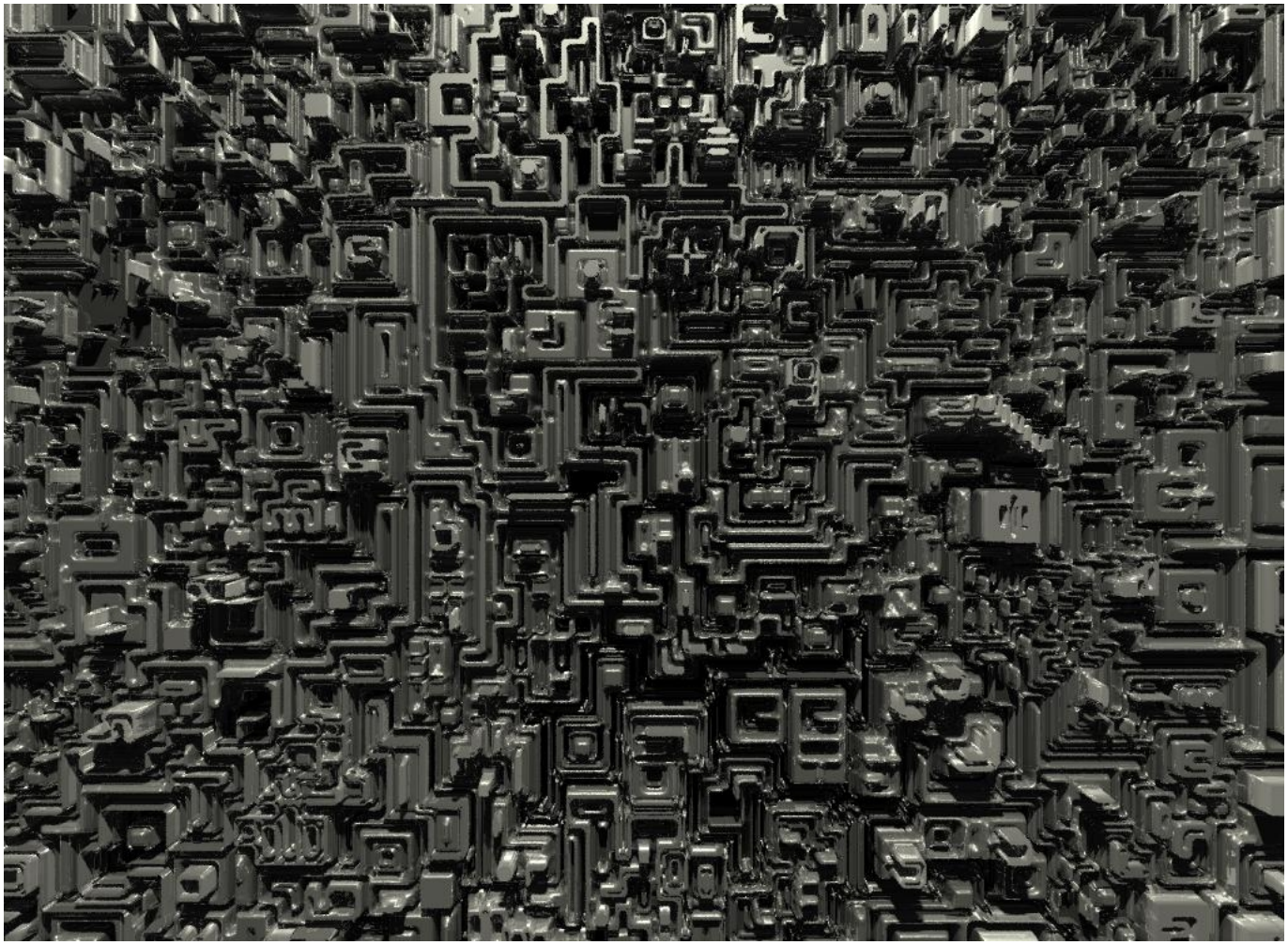
The end of the fortress metaphor



The end of the fortress metaphor

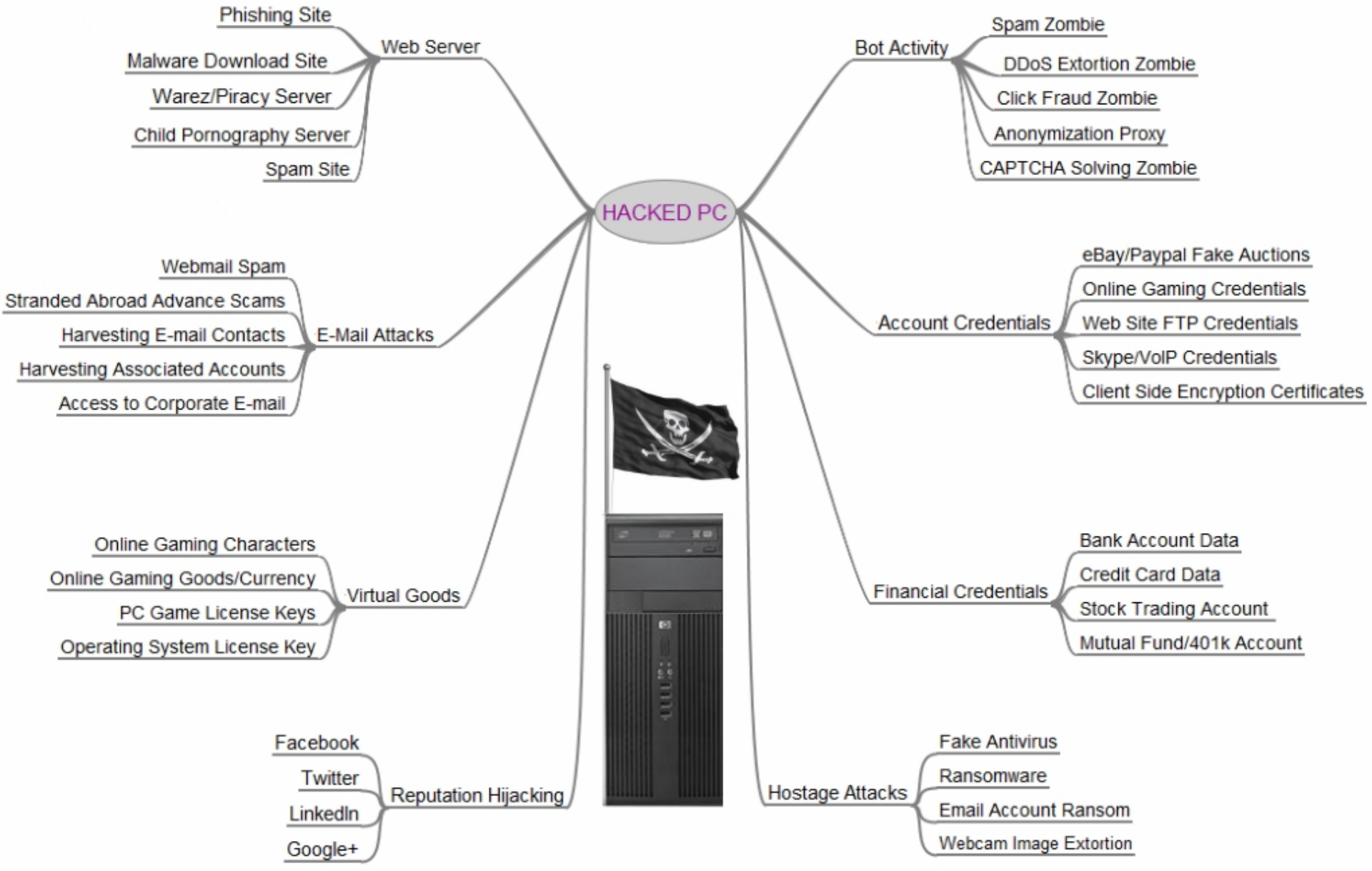


The end of the fortress metaphor



CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

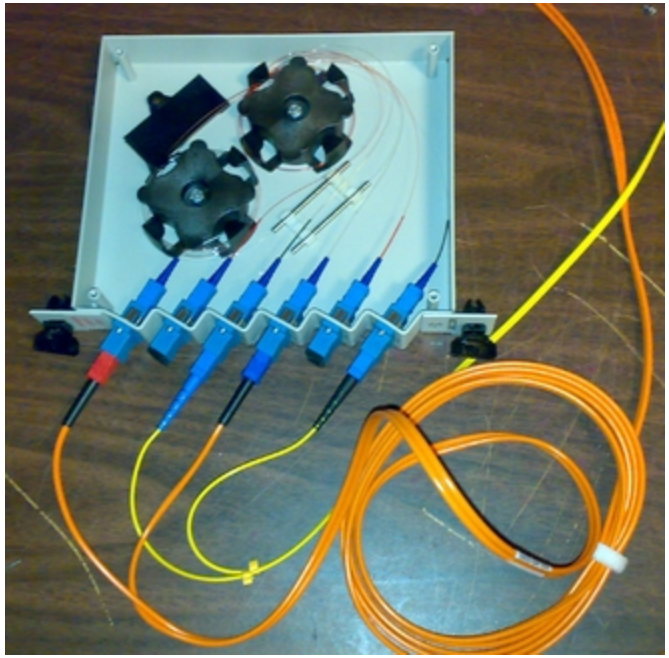
On the client



On the network

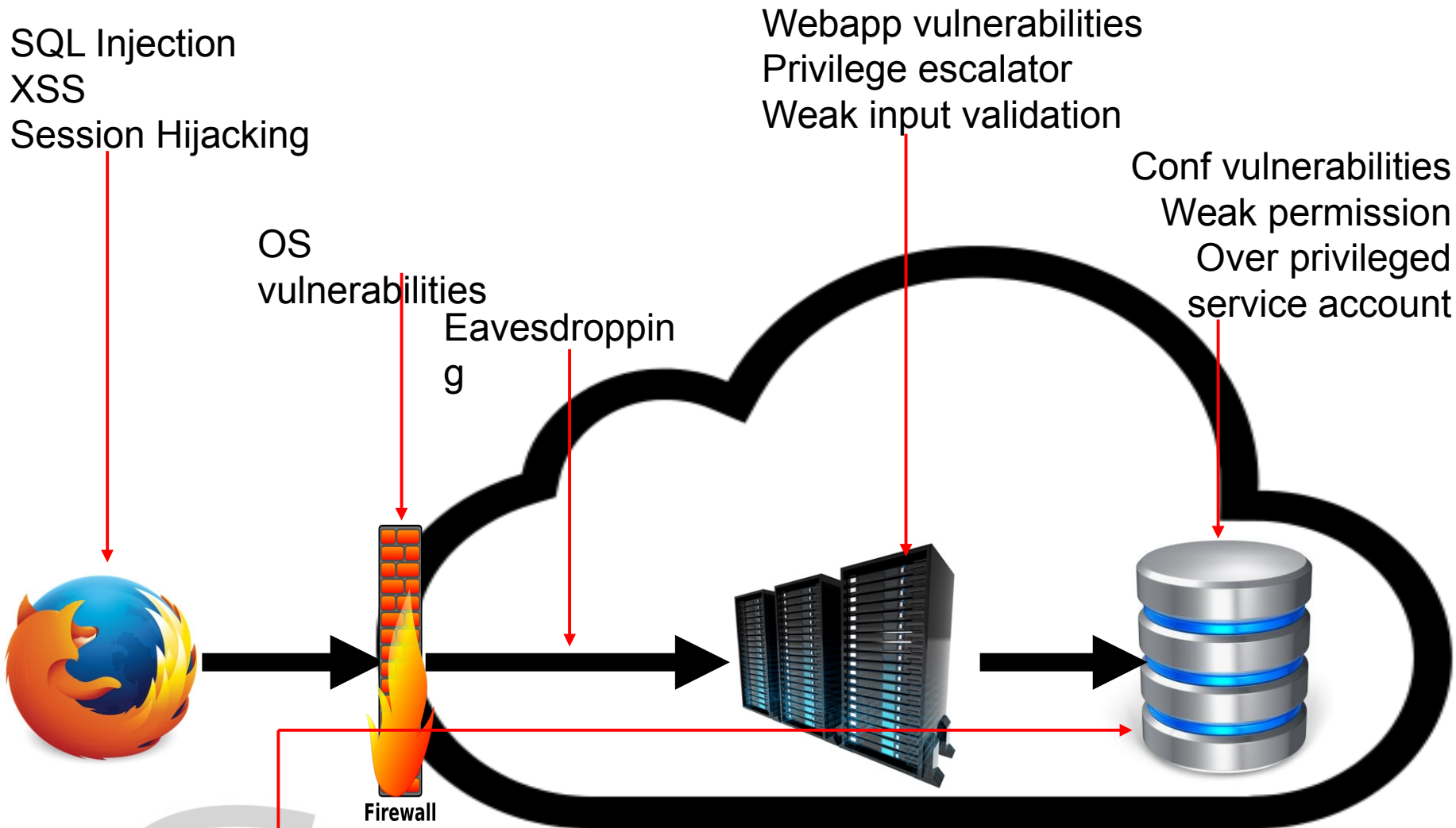
Passive attacks: Wireless or Fiber eavesdropper

Active attacks: - evil Wifi router
- DNS poisonning



CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

On the server

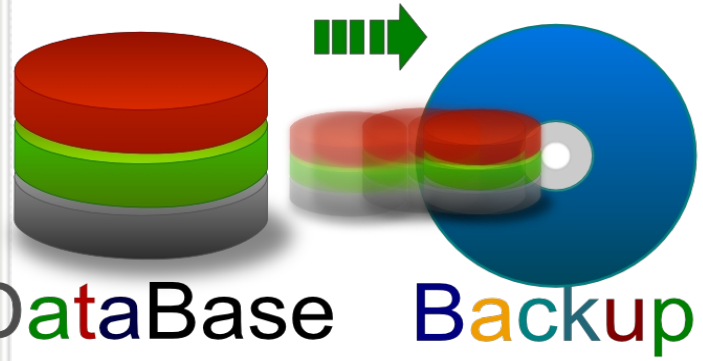


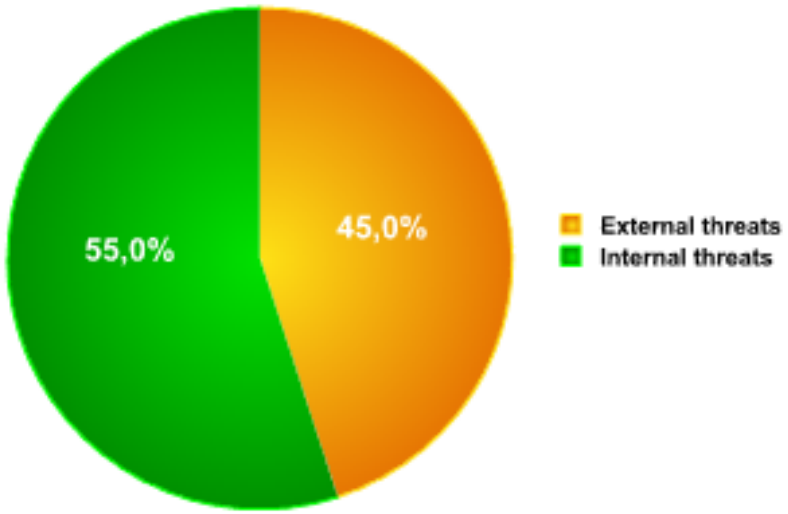
CESI alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

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
```





CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Human fails

Technology development

Organization

Psychological weakness

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Business widely impacted

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Web Hacking
III. Countermeasures

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Security audit

?

PENETRATION TESTING

OLD SCHOOL

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Security audit

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Security audit

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

DON'T DELEGATE IT

Security by design

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

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

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Security by design

COVERAGE ALL...
with :

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

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

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

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

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Malware analysis :

- for all untrusted environments

- know your adversary

- don't be weak with known malwares

Security by design

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...

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

You have been hacked

#1 NO LIES #1

#2 OPEN or CLOSE ?

#3 EVALUATE IMPACTS

→ operational

→ reputability

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

React after hacks

#1 lock exploit EVEN with business impact

#2 Communicate clearly

#3 Legal – save hack proofs

But major diseases can occurs

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Initial situation

#1 Main Data Center OOO
(Out Of Order)

#2 Related to a hack

#3 Only aim: destroy you

Expendables

#1 Detect vulnerability vector

#2 Patch emergency site

#3 Don't inject new vulnerabilities

#4 Switch to emergency

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Prepared situation

#1 Scenario written in a DRP

(Disaster Recovery Plan)

#2 Tested in operational conditions

#3 Rebuild it periodically

#4 <u>Often theoretical</u>

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

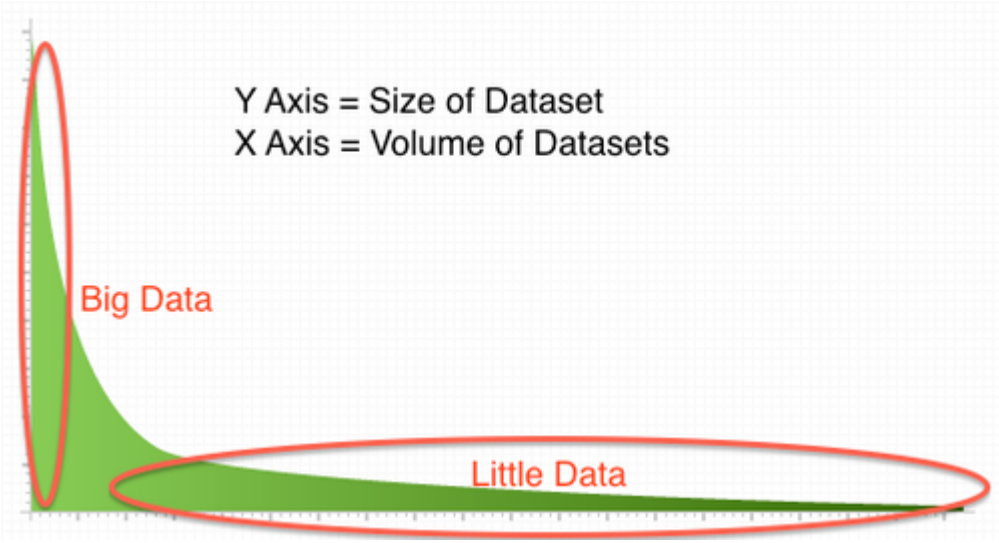
Prepared situation

...May works for institutions

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Prepared situation

They have few data



CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Prepared situation

They have few data

2x 750m2

Scale → Petaoctet

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Prepared situation

LIMITS?

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Prepared situation

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

Scale → unknown

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Prepared situation

→ Replication
→ Multi DC
→ Multi continents

Is NATIVE

Prepared situation

Other exists

15 DC

7 DC

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Prepared situation

Global Capacity is huge but limited

4 TB/S

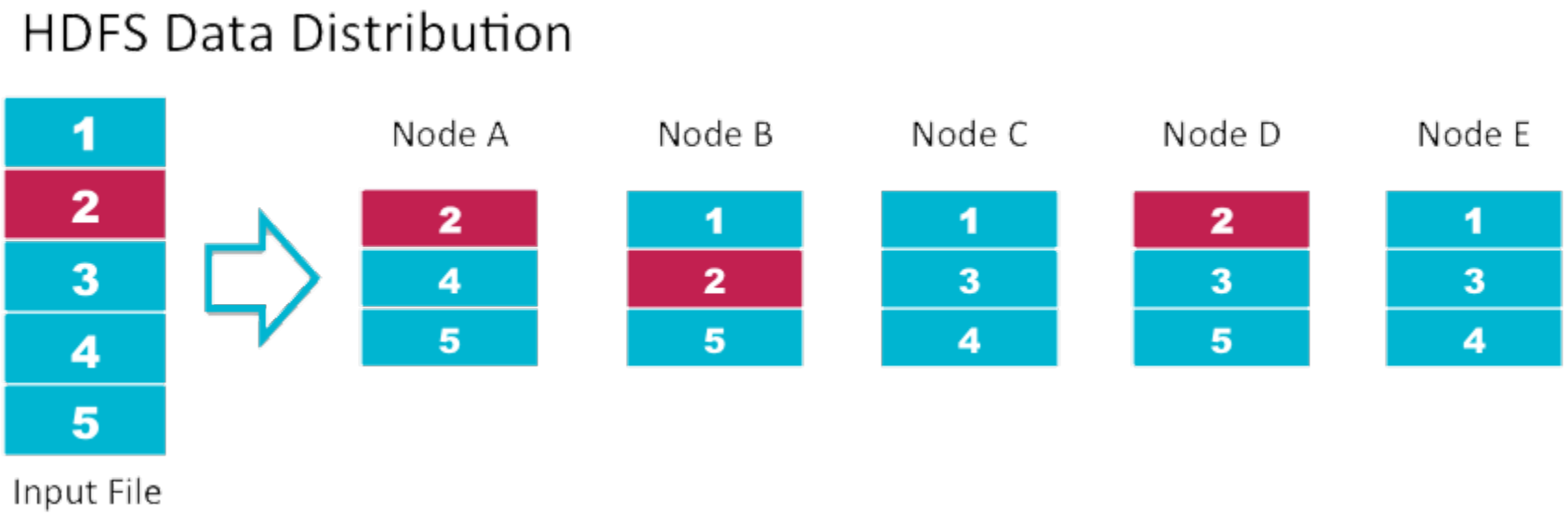
Prepared situation

Move 9 PB daily
takes time...

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

Prepared situation

Replication



Other multiple DC

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

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

NETFLIX

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

CESi alternance

ÉCOLE SUPÉRIEURE DES MÉTIERS

LE CESI :
ENSEIGNEMENT
SUPERIEUR ET
FORMATION
PROFESSIONNELLE

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Web Hacking
I. Intro

LE CESI : ENSEIGNEMENT SUPERIEUR ET FORMATION PROFESSIONNELLE

CESi alternance

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**".

LE CESI : ENSEIGNEMENT SUPERIEUR ET FORMATION PROFESSIONNELLE

But... for unlighted people,

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

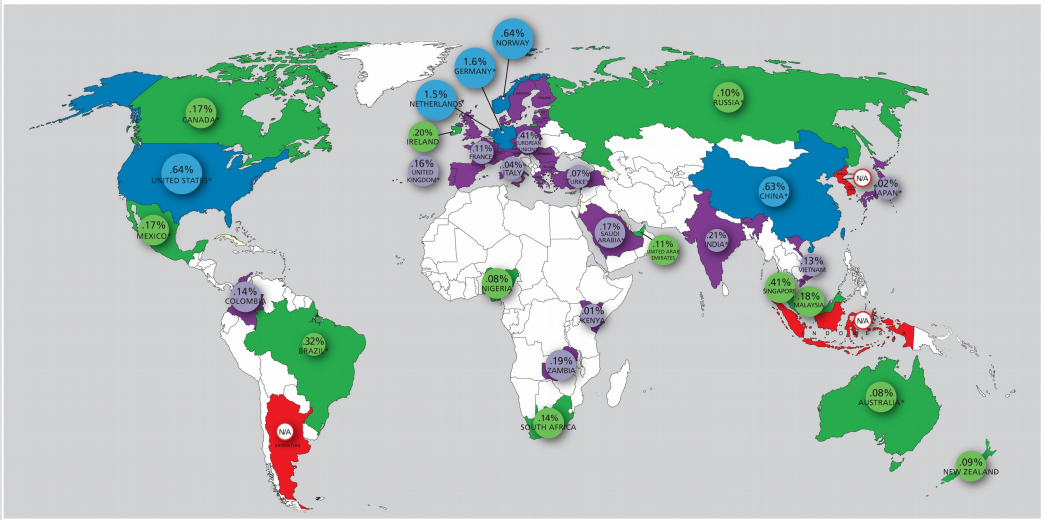
Hacking is a chance

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Hacking is a cancer

McAfee
An Intel Company

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



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

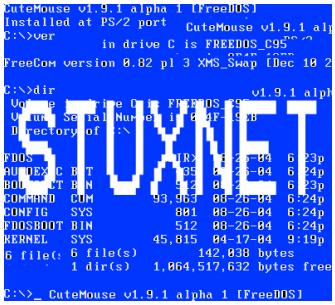
- % High Confidence Level
- % Low Confidence Level
- * G-20 Countries
- % Medium Confidence Level
- N/A - Countries currently not measuring cybercrime loss

$445 BILLION
The annual estimated cost to the global economy from cyber crime

200,000+
Jobs lost in the U.S

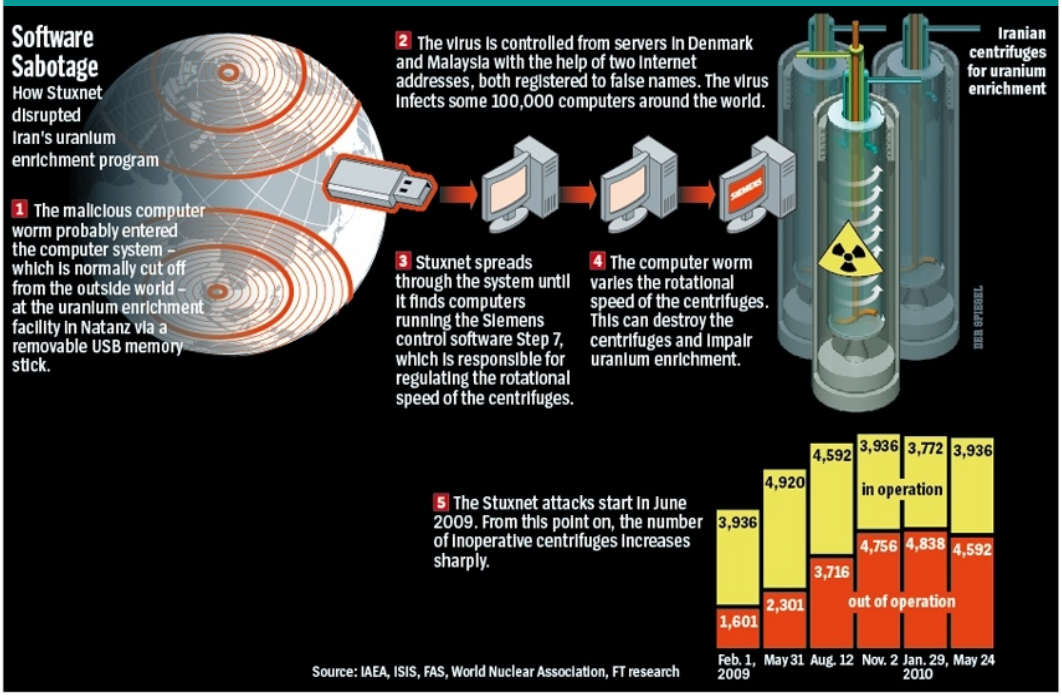
150,000+
Estimated in Europe

Hacking is used by intelligence



CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Hacking is used by intelligence



Hacking is used by intelligence

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Web Hacking
II. Threats

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

That may happen?

OR

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

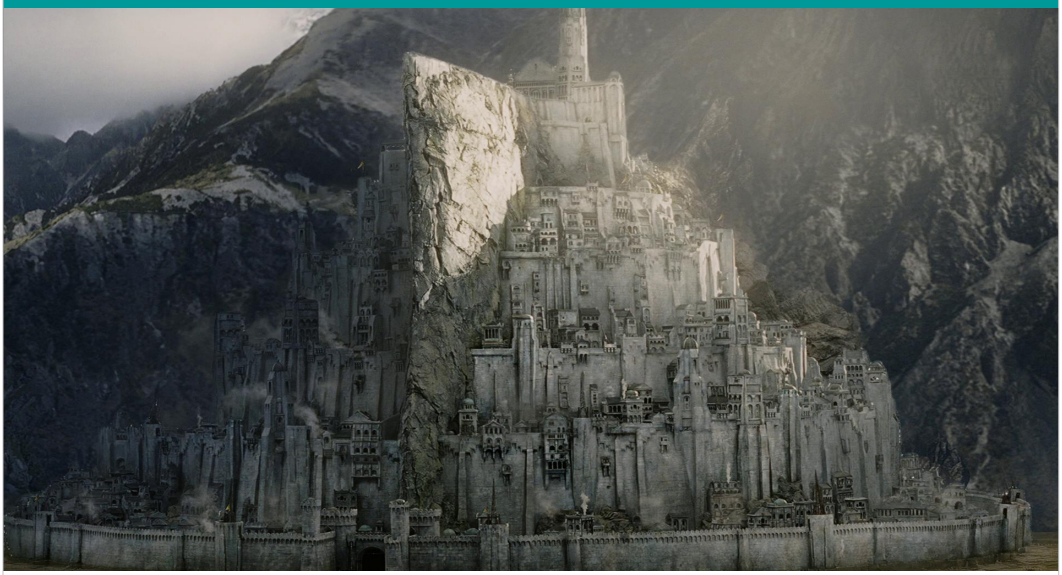
Business needs Trust!

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Business needs Trust!

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

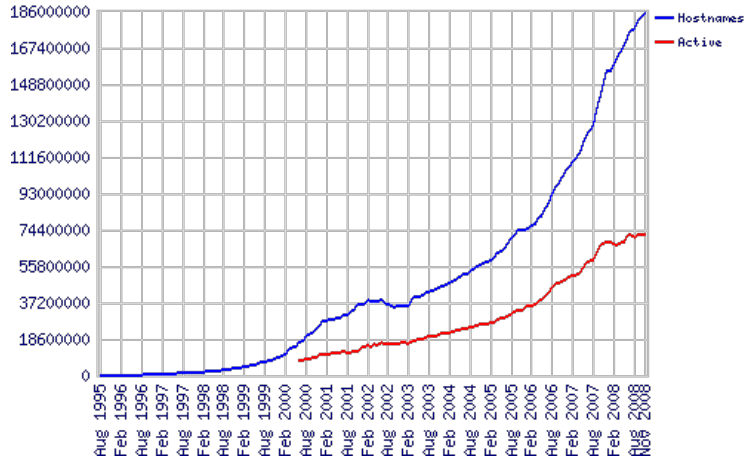
The end of the fortress metaphor



CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

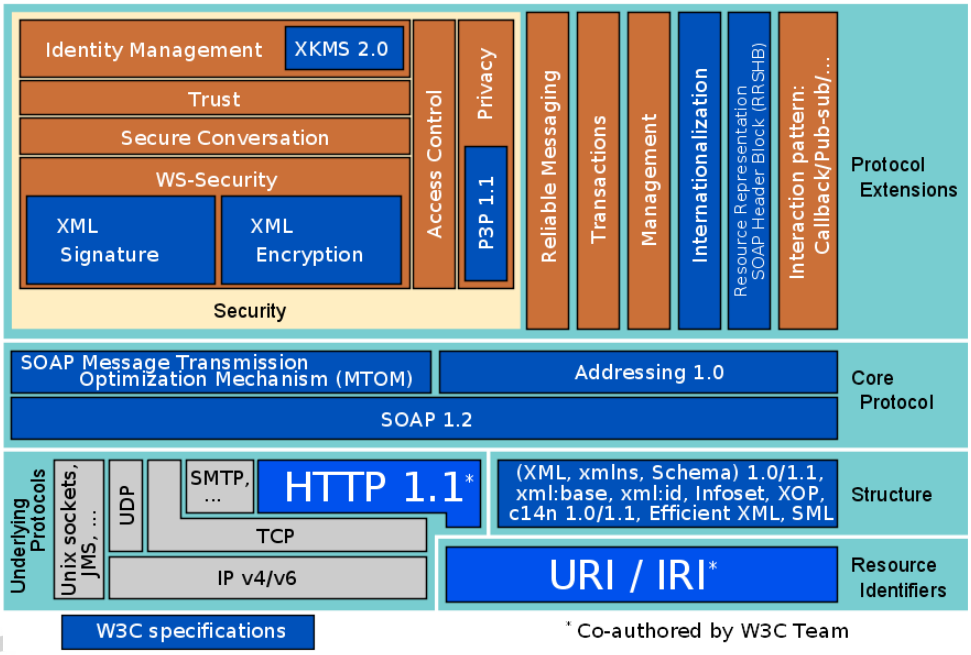
The end of the fortress metaphor

The end of the fortress metaphor

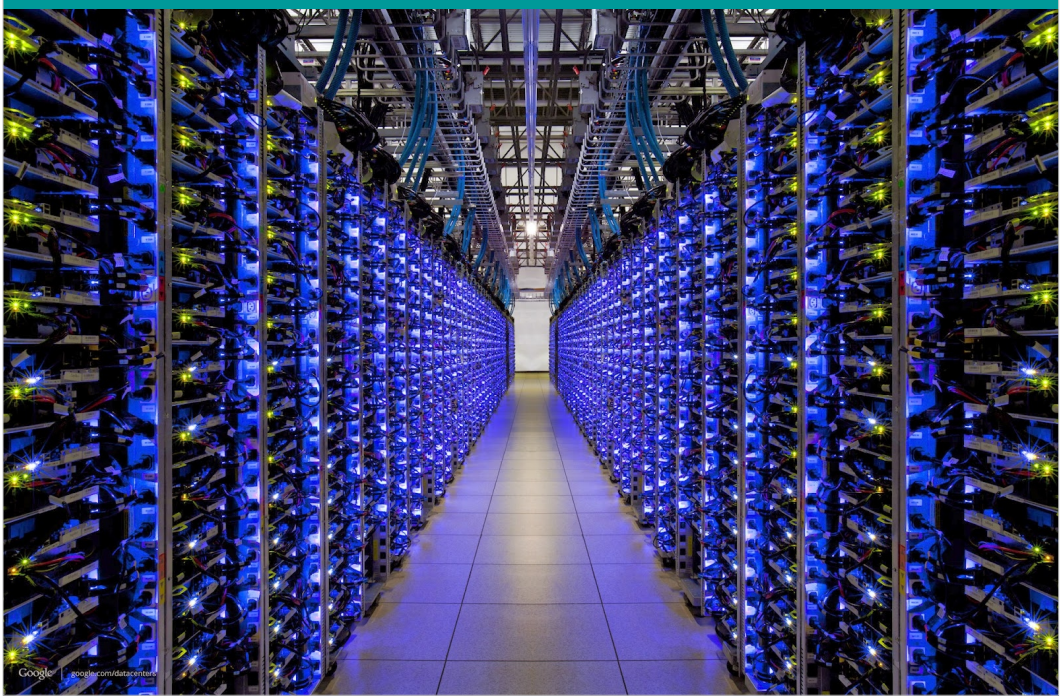


CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

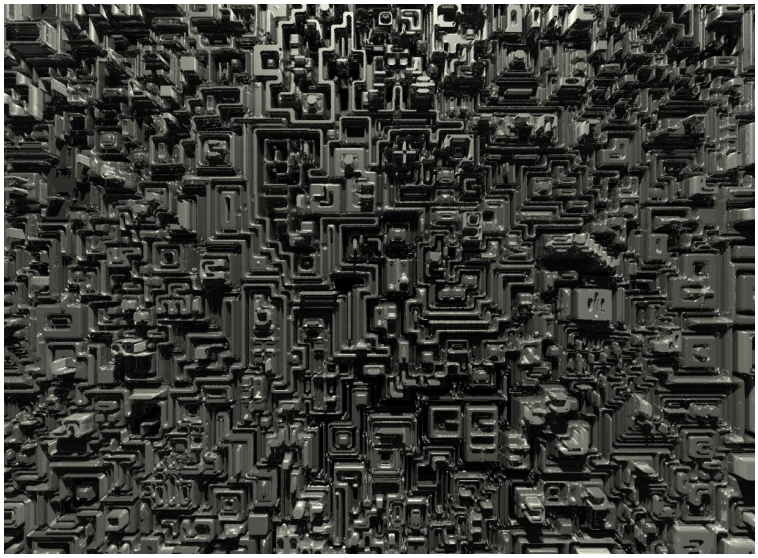
The end of the fortress metaphor



The end of the fortress metaphor

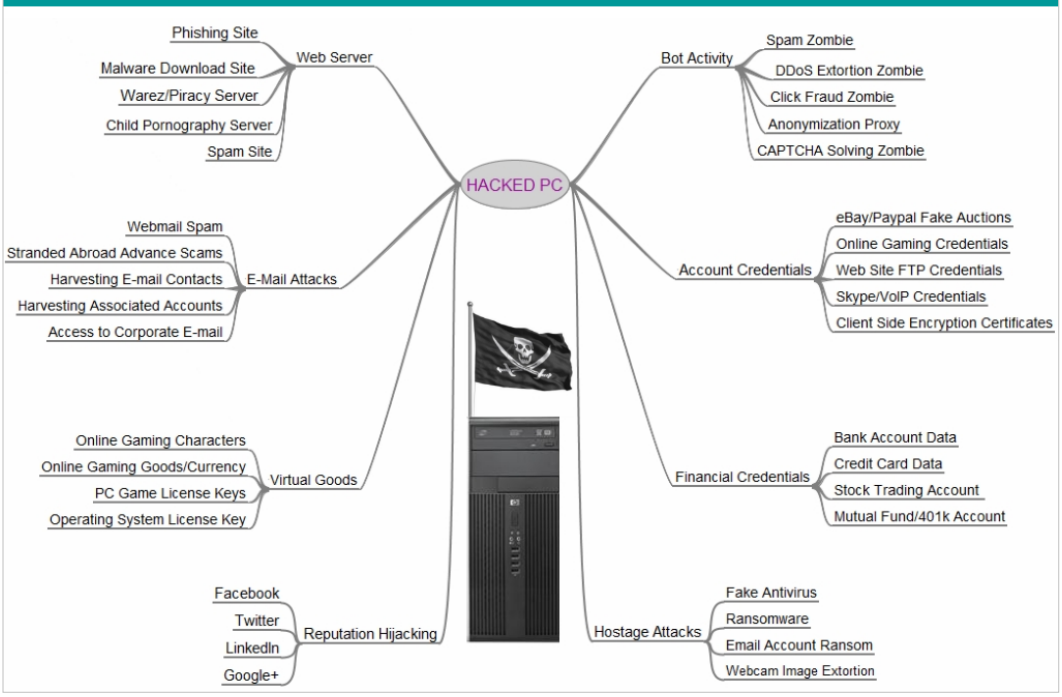


The end of the fortress metaphor



CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

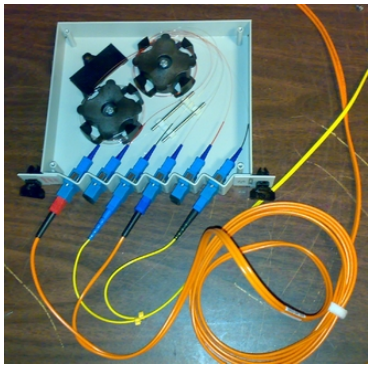
On the client



On the network

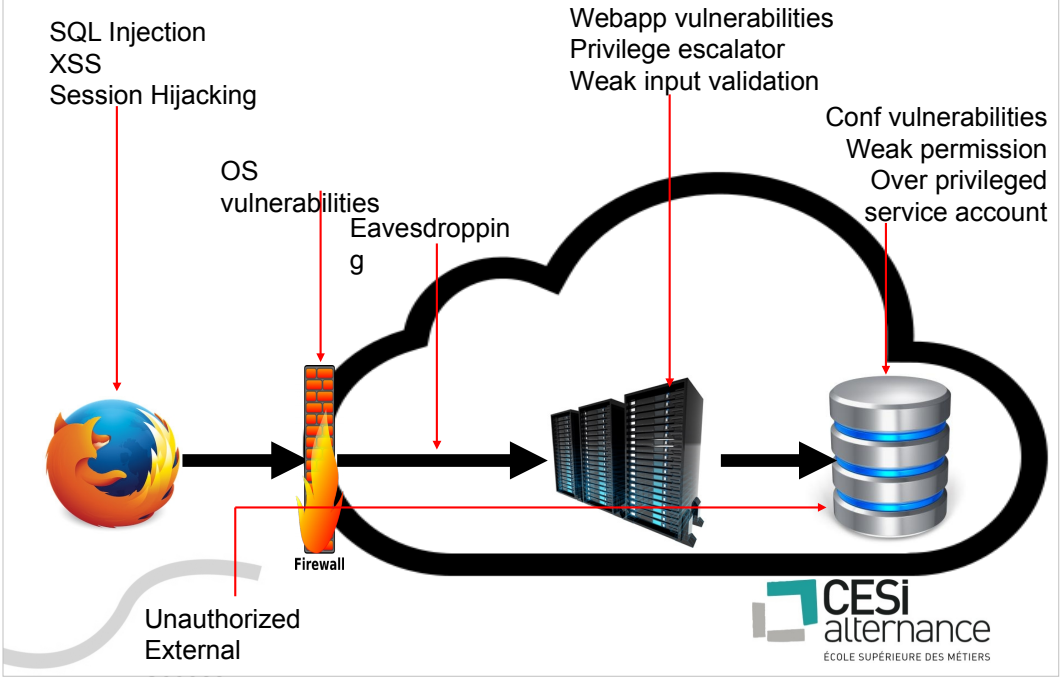
Passive attacks: Wireless or Fiber eavesdropper

Active attacks: - evil Wifi router
- DNS poisonning

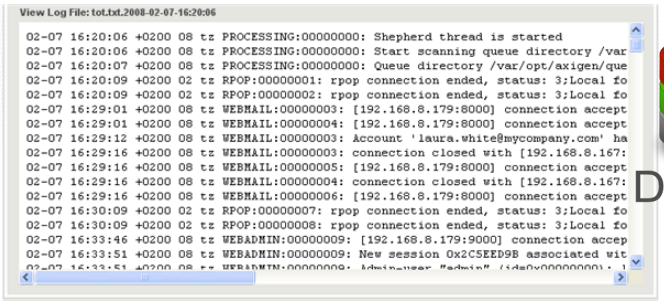


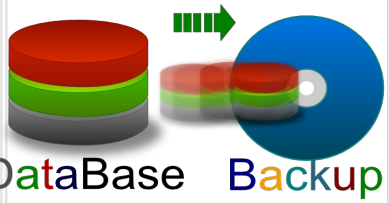
CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

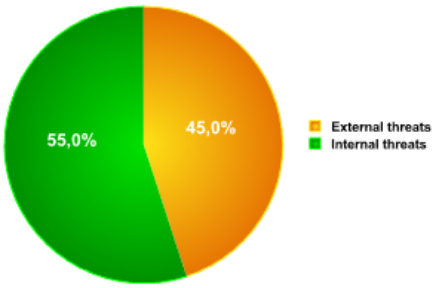
On the server



Back Office Threats







CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Human fails

Technology development

Organization

Psychological weakness

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Business widely impacted

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Web Hacking
III. Countermeasures

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Security audit

?

PENETRATION TESTING

OLD SCHOOL

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Security audit

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

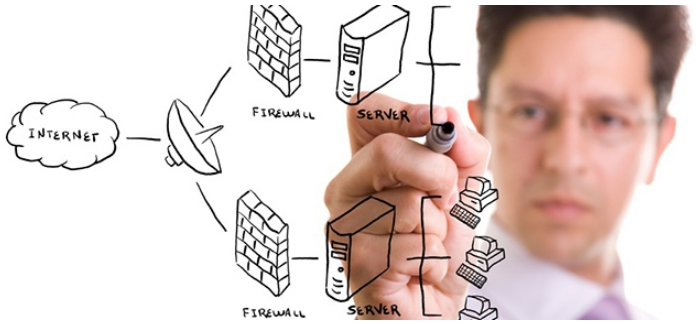
Security audit

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

DON'T DELEGATE IT

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Security by design



CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Security by design

COVERAGE ALL...

Product design and development

Hardware programming

Application & hardware testing

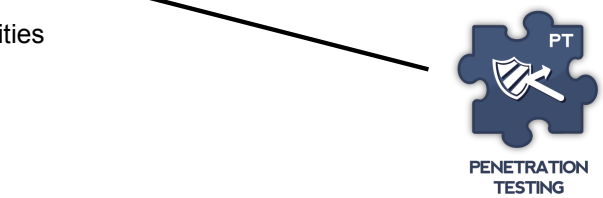
Review code for vulnerabilities

Fix vulnerabilities ASAP

Always aware

Malware analysis, Reverse engineering

Application security review



CESI alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Security by design

COVERAGE ALL...
with :

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

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

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**

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

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

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Malware analysis :

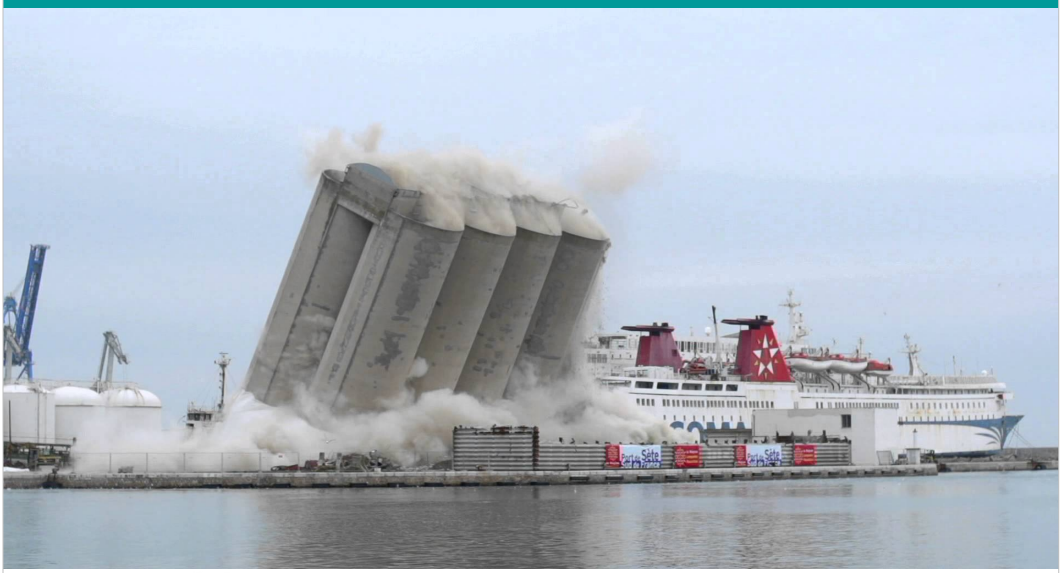
- **for all untrusted environments**
- **know your adversary**
- **don't be weak with known malwares**

Application security review:

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

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

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...

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

You have been hacked

#1 NO LIES #1

#2 OPEN or CLOSE ?

#3 EVALUATE IMPACTS

→ operational

→ reputability

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

React after hacks

#1 lock exploit EVEN with business impact

#2 Communicate clearly

#3 Legal – save hack proofs

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

But major diseases can occurs

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Initial situation

#1 Main Data Center OOO

(Out Of Order)

#2 Related to a hack

#3 Only aim: destroy you

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Expendables

#1 Detect vulnerability vector

#2 Patch emergency site

#3 Don't inject new vulnerabilities

#4 Switch to emergency

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Prepared situation

#1 Scenario written in a DRP

(Disaster Recovery Plan)

#2 Tested in operational conditions

#3 Rebuild it periodically

#4 Often theoretical

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

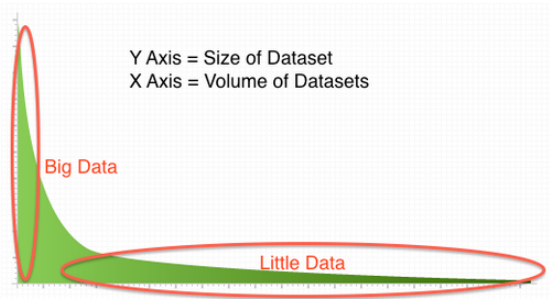
Prepared situation

...May works for institutions

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Prepared situation

They have few data



CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Prepared situation

They have few data

2x 750m2

Scale → Petaoctet

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Prepared situation

LIMITS?

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Prepared situation

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

Scale → unknown

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Prepared situation

→ Replication
→ Multi DC
→ Multi continents

Is NATIVE

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Prepared situation

Other exists

15 DC

7 DC

Prepared situation

Global Capacity is huge but limited

4 TB/S

Prepared situation

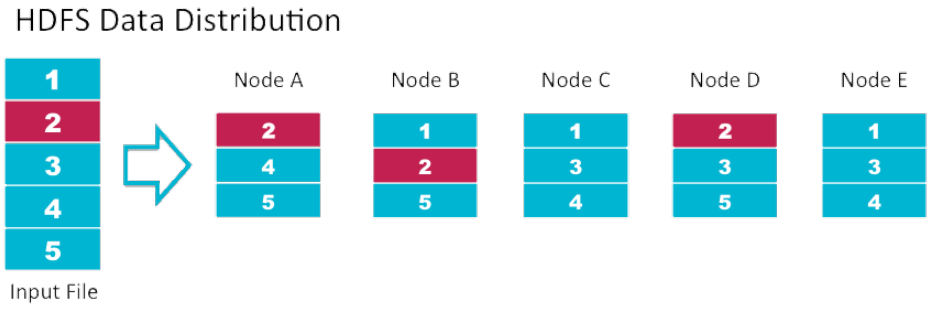
Move 9 PB daily
takes time...

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

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Prepared situation

Replication



Other multiple DC

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Prepared situation

Be robust even if

→ **you loose one server**

→ **you loose one rack**
or in extreme cases
→ **one DC**

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Prepared situation

Don't be prepared to the Evil...

Invite him at your table

NETFLIX

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS