Sécurité

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

J. Saraydaryan

CPE - Lyon

Introduction :

Les Enjeux de la Sécurité

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

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

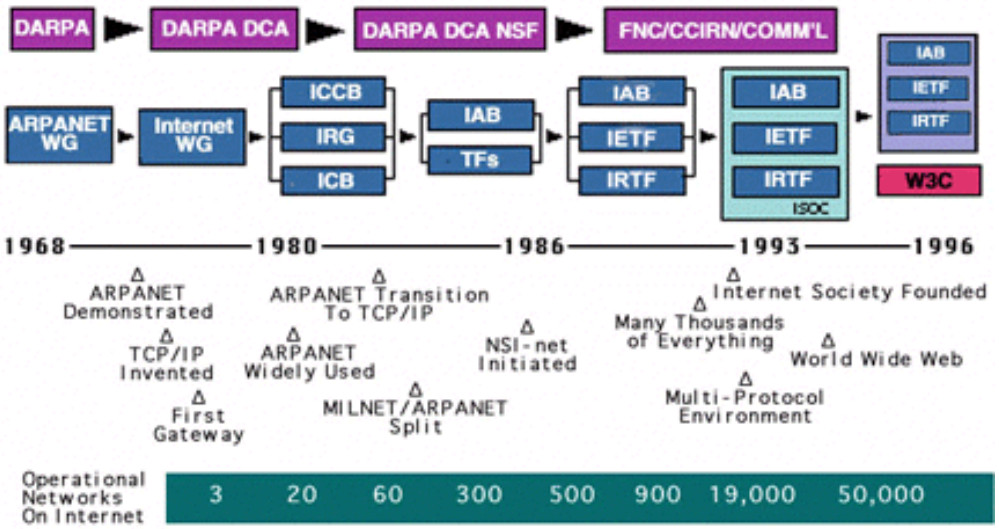
- ARP Spoofing / DNS Spoofing
- TCP Flooding / TCP Session Hijacking
- XSS / Bufferoverflow

Evolution du monde informatique

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

Les enjeux de la sécurité

- **Evolution des réseaux**

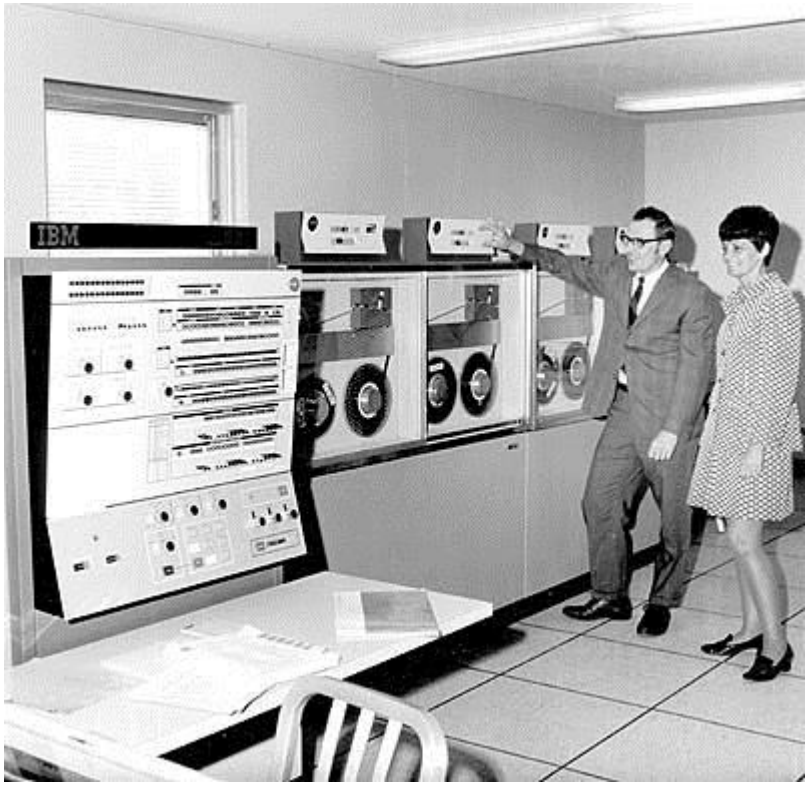


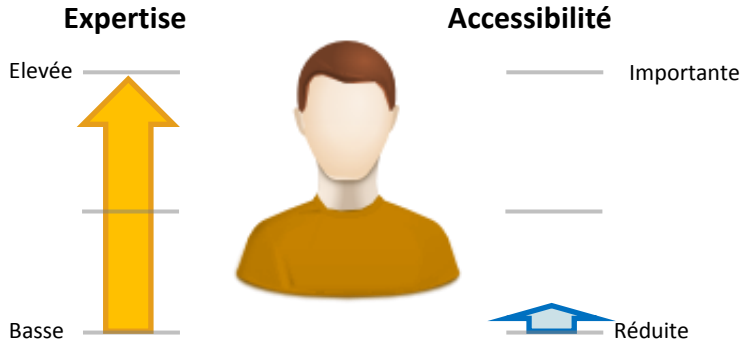
http://www.internetsociety.org/sites/default/files/images/timeline.gif

http://www.evolutionoftheweb.com/

Les enjeux de la sécurité

- **Evolution des réseaux**: Mainframe



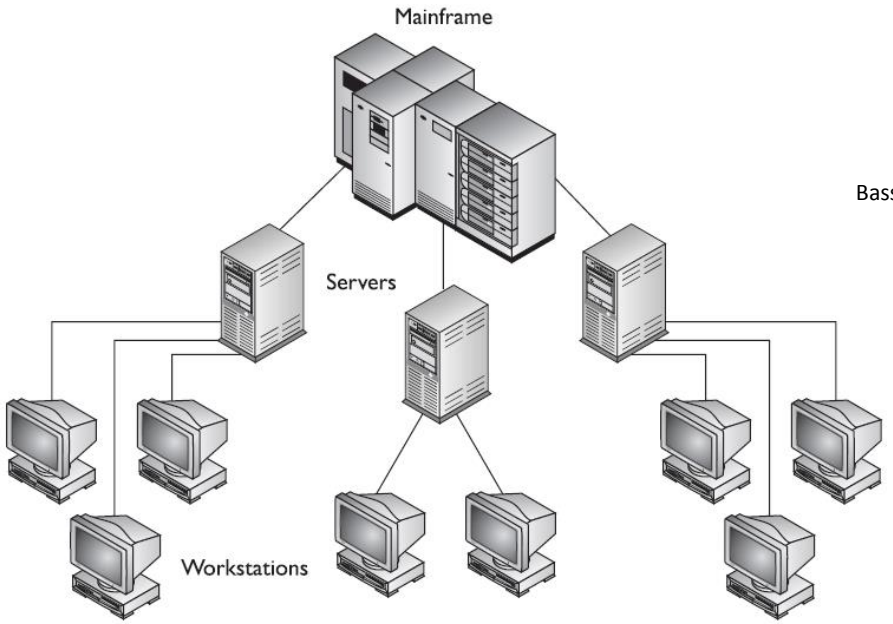


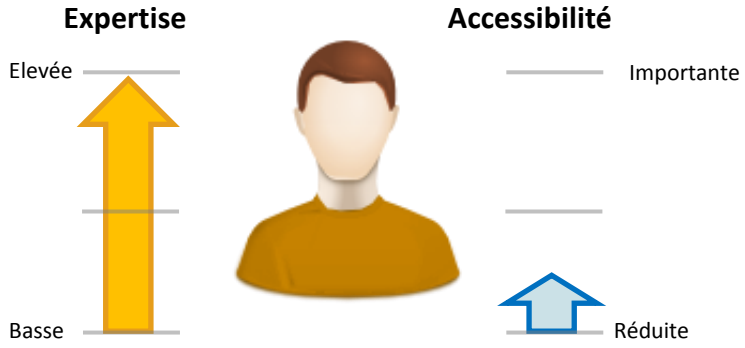
Accès par expert uniquement

Utilisation Scientifique

Les enjeux de la sécurité

- **Evolution des réseaux:** Mainframe

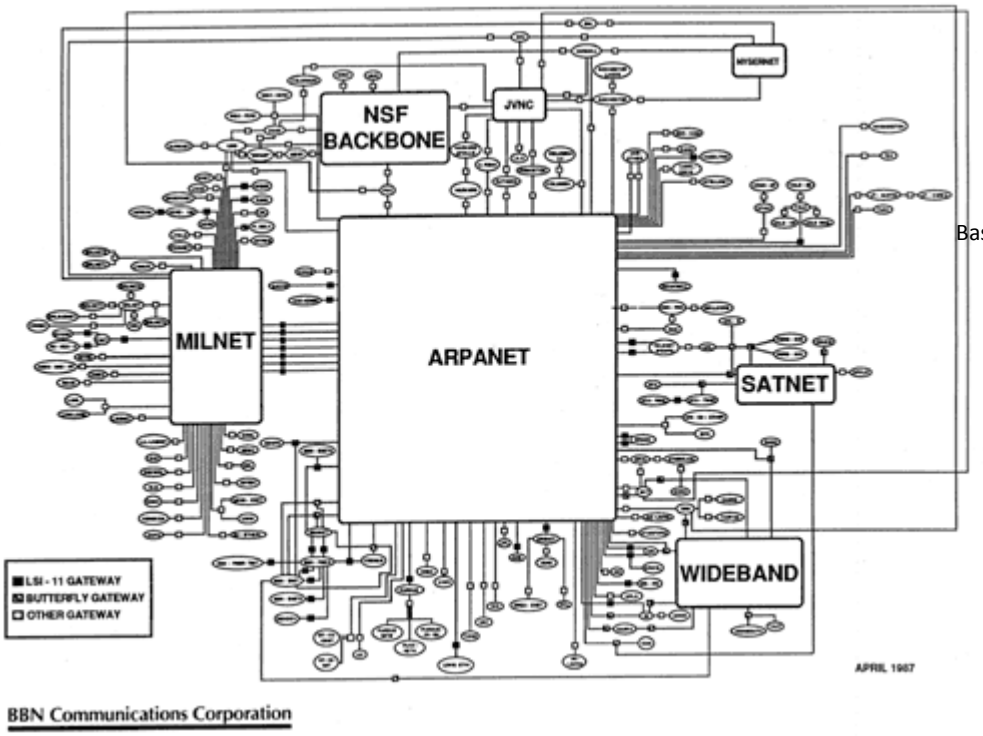


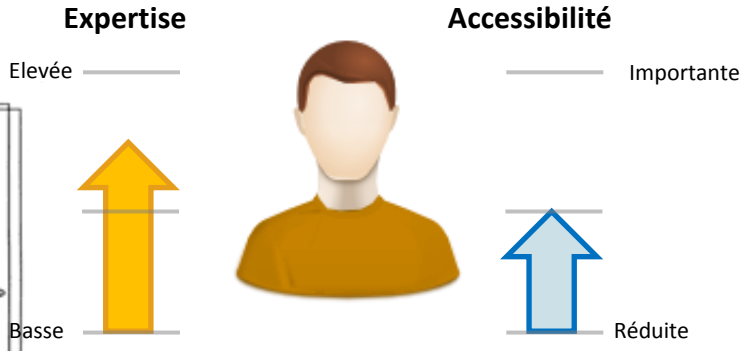


- Accès aux utilisateurs du réseau via des serveurs relais
- Peu de workstation
- Accès physique aux workstations obligatoire

Les enjeux de la sécurité

- **Evolution des réseaux:** ARPNET (1983)

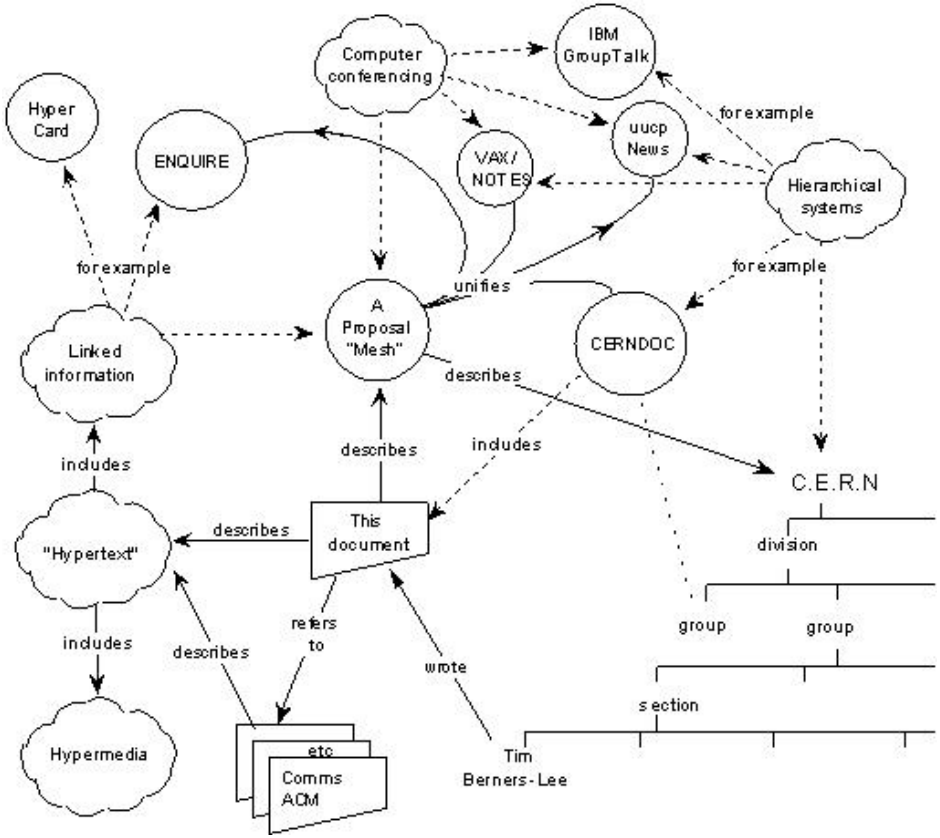


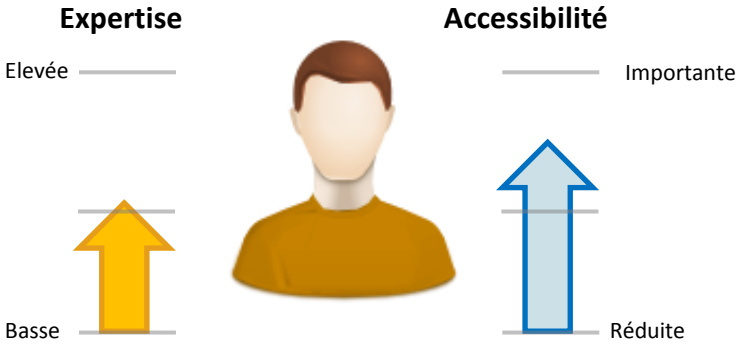


- Accès aux utilisateurs du réseau membre ARPANET
- Workstation plus étendues

Les enjeux de la sécurité

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

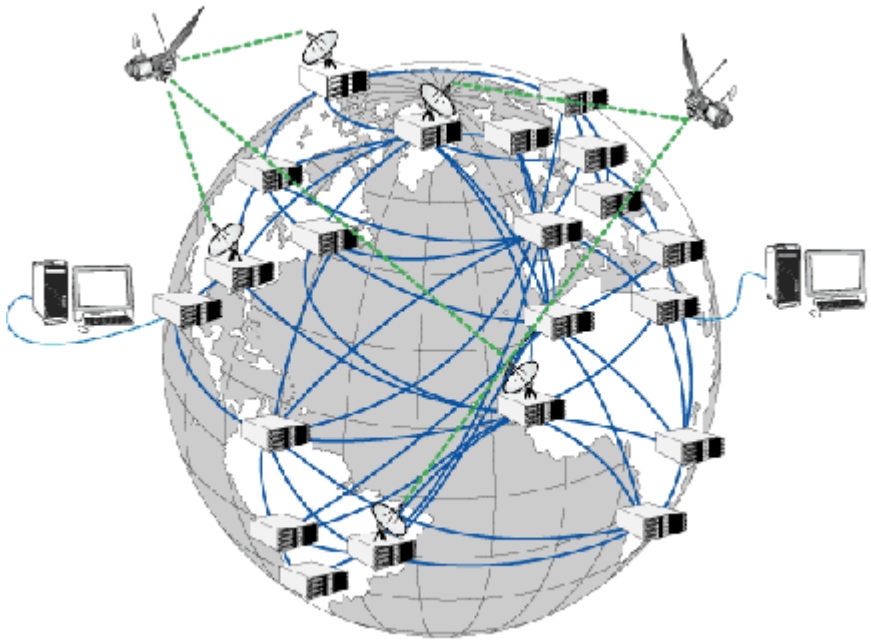


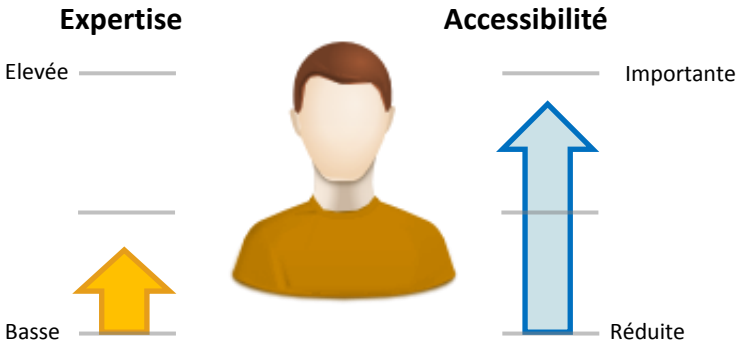


- Proposition d'ouvertue du réseau ARPANET
- DNS, PC, EMail

Les enjeux de la sécurité

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

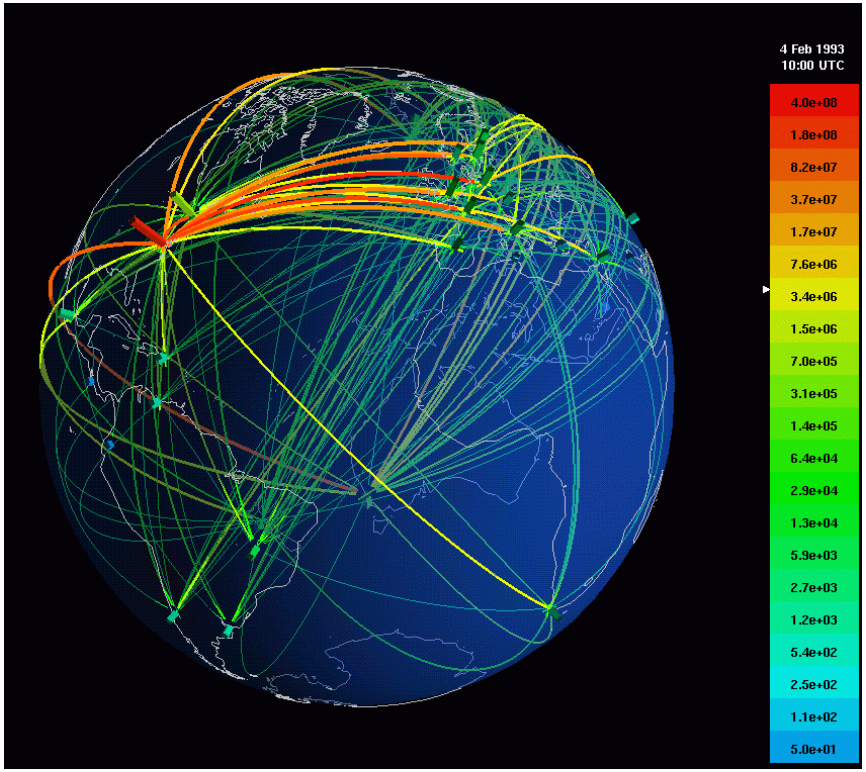


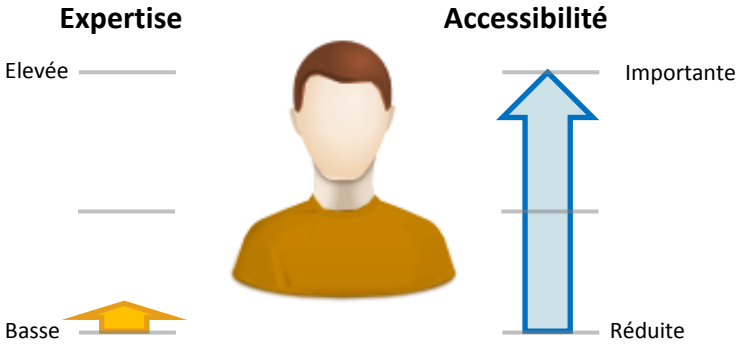


- Accès à tous les utilisateurs possédant un provider
- HTTP/HTML, navigateur web

Les enjeux de la sécurité

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

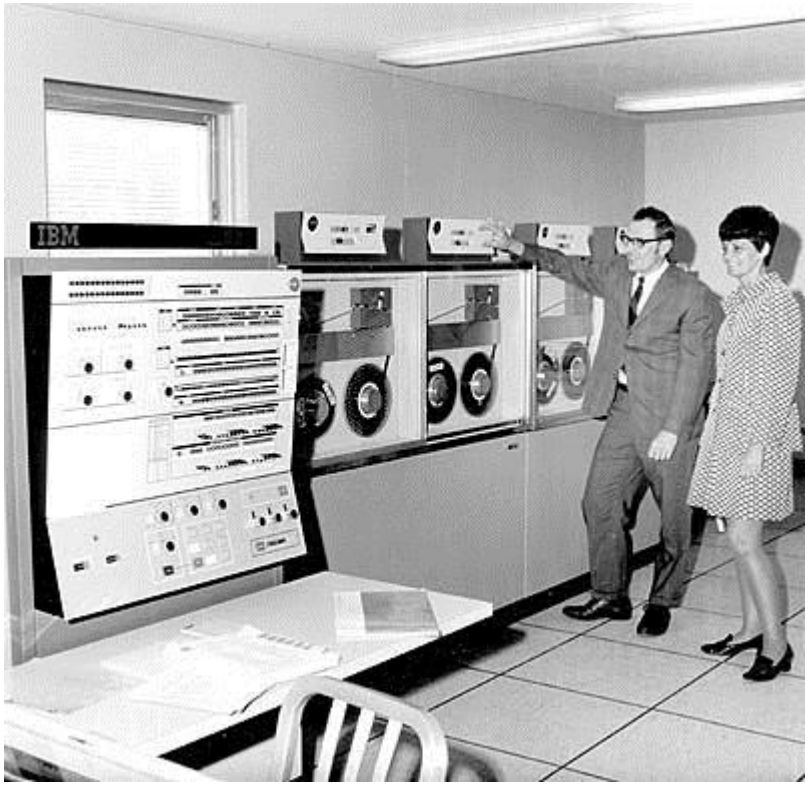


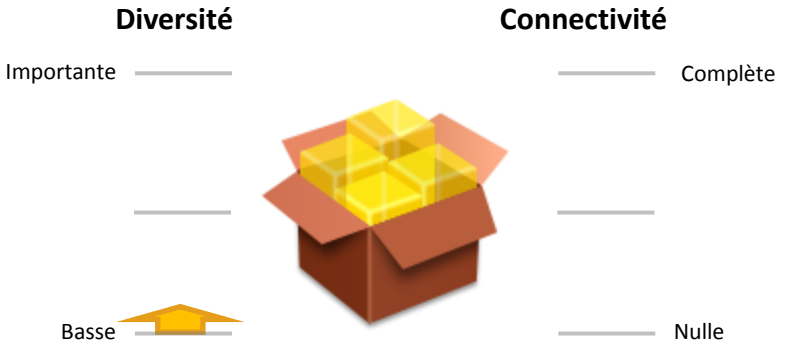


- Multiplication des points d'accès, 3G, objets communicants.
- Simplification des interfaces, vers un tout connecté

Les enjeux de la sécurité

- **Evolution des réseaux**: Mainframe

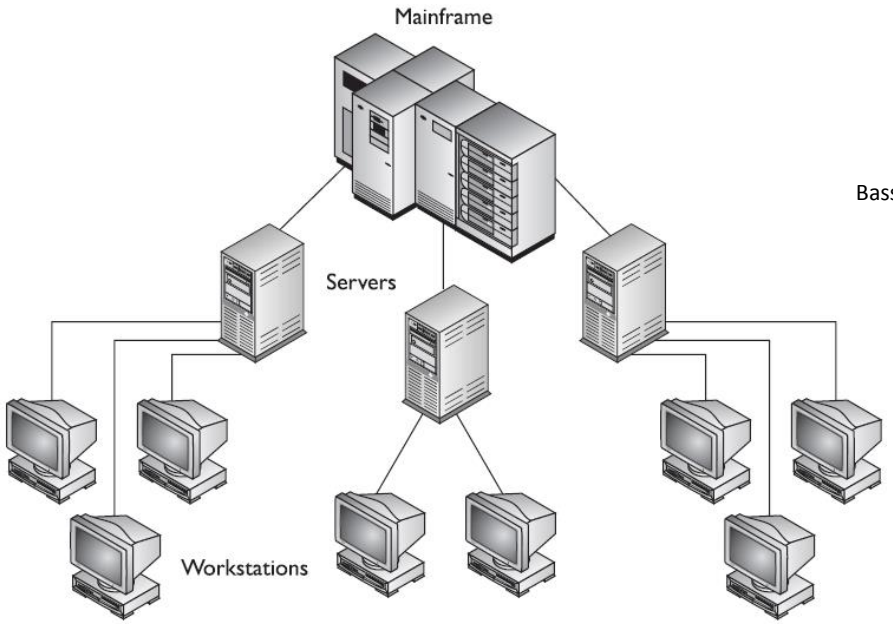


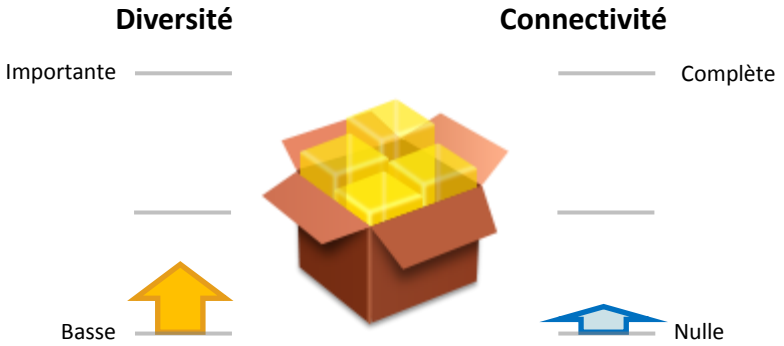


- Programme Scientifique Unique,
- Aucune connexion extérieur

Les enjeux de la sécurité

- **Evolution des réseaux**: Mainframe

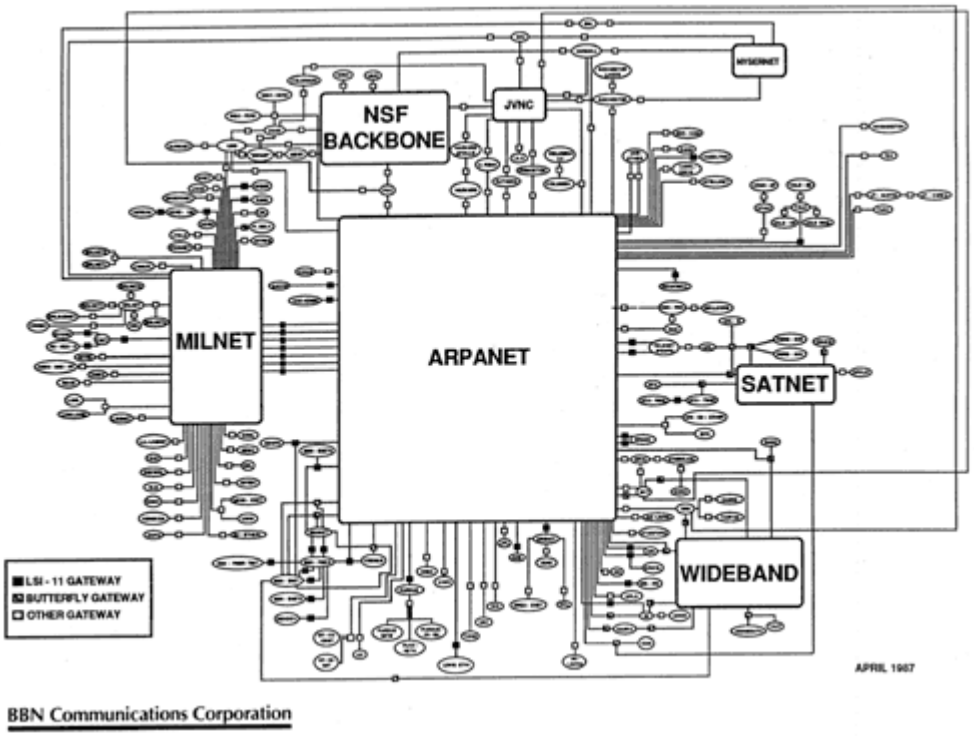


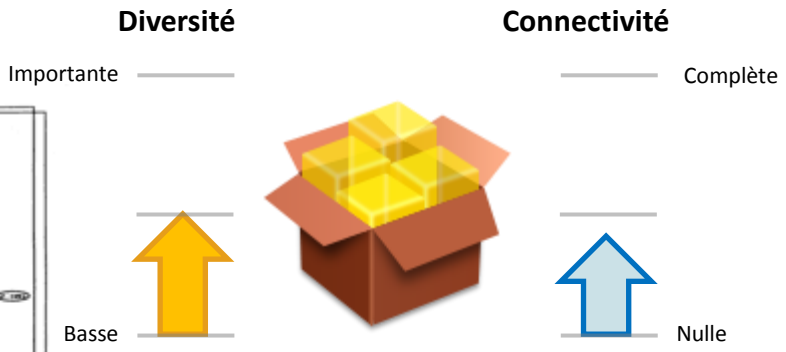


- Applications métiers dédiées
- Pas ou très peu de communication inter-applications
- Communication entre Mainframe-server-workstation

Les enjeux de la sécurité

- **Evolution des réseaux**: ARPNET (1983)

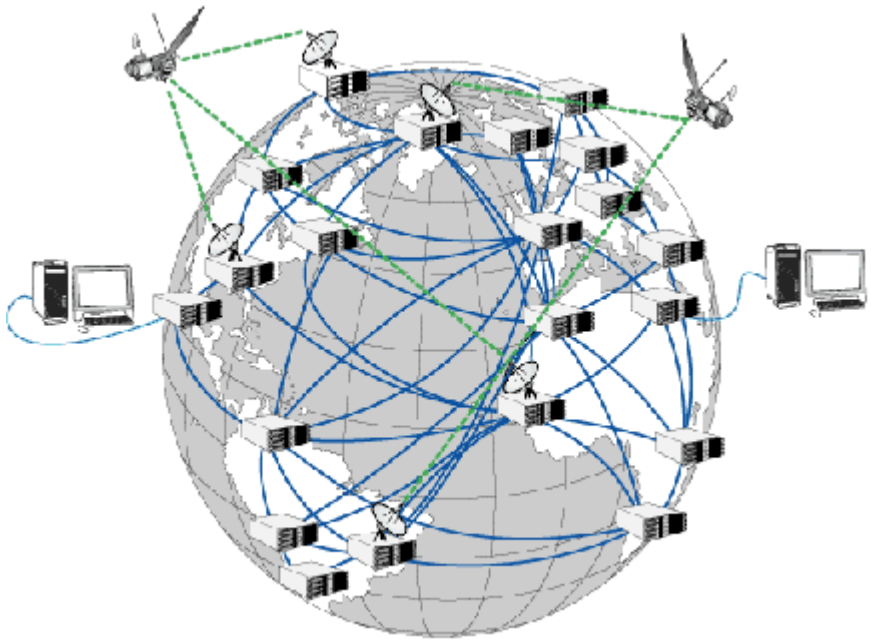


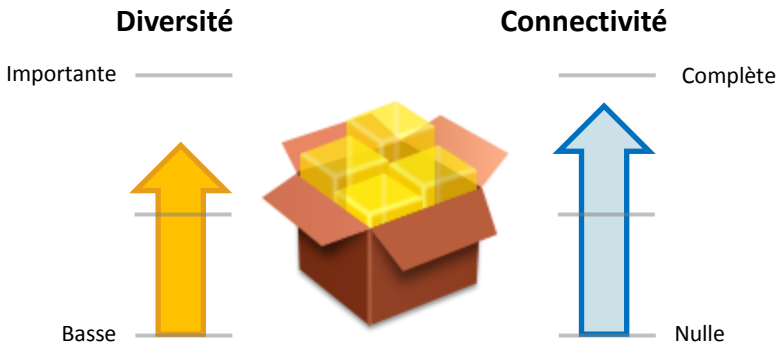


- Elargissement des applications (BBS Bulletin Board System, email client, Usenet)
- Début du TCP/IP, communication inter-applications en pleine croissance

Les enjeux de la sécurité

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

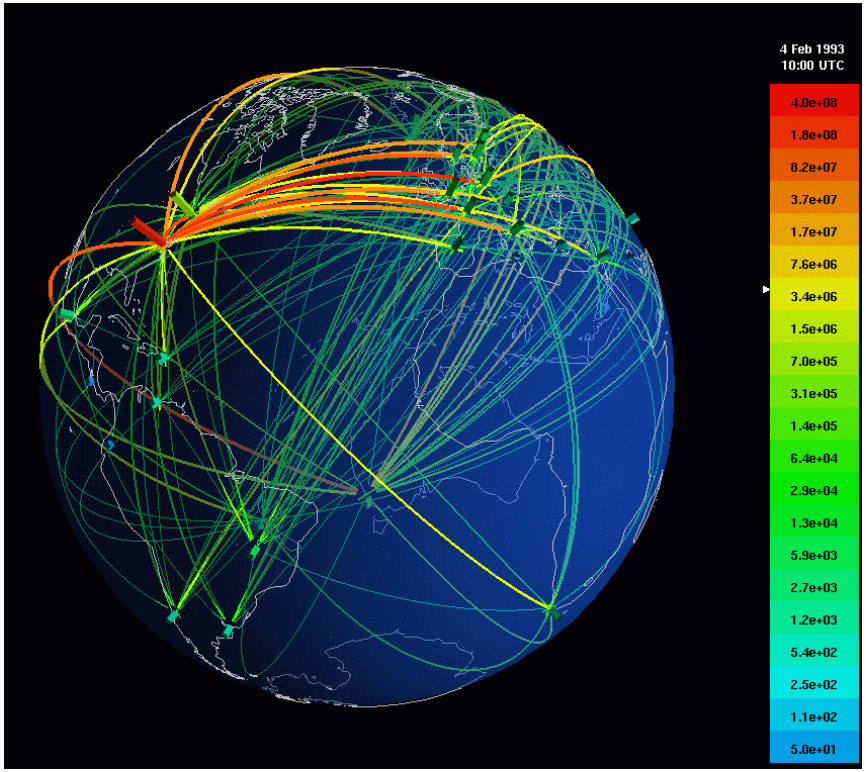


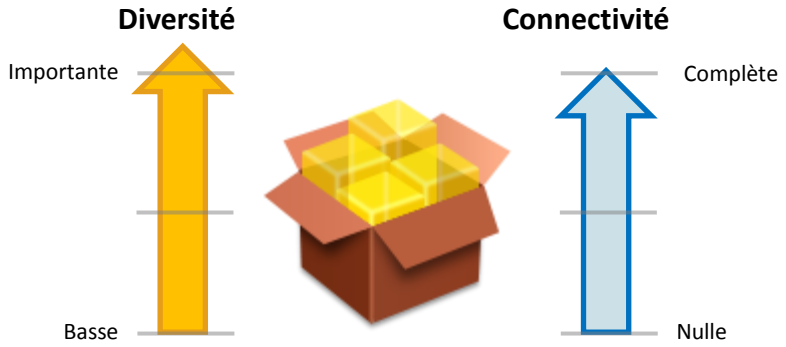


- Multiplication des applications, commerciales, éducatives
- Communications inter-applications élevées grace à l'arrivée de protocoles HTTP/HTML, IRC, SSL

Les enjeux de la sécurité

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

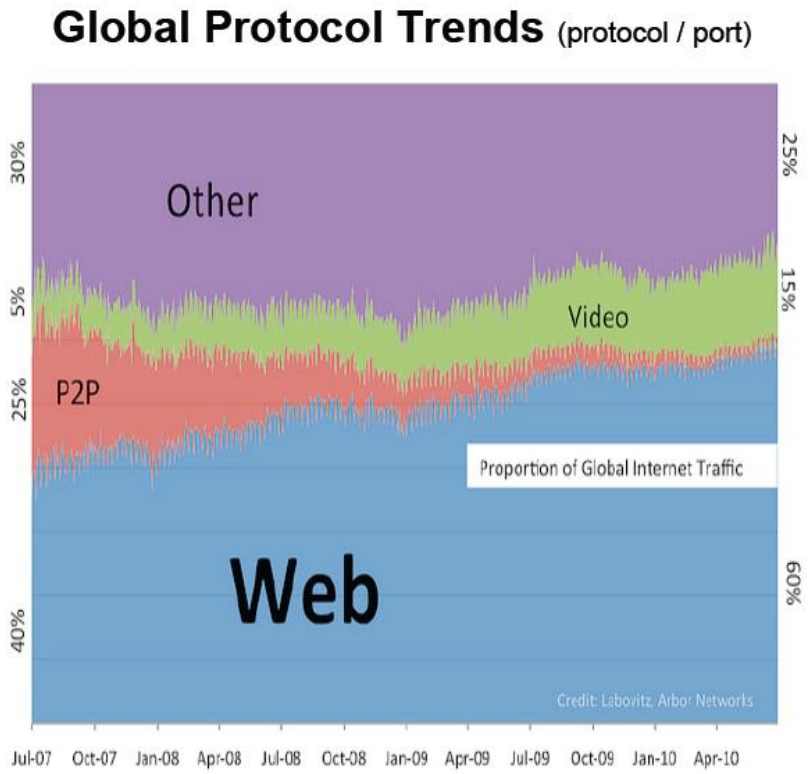


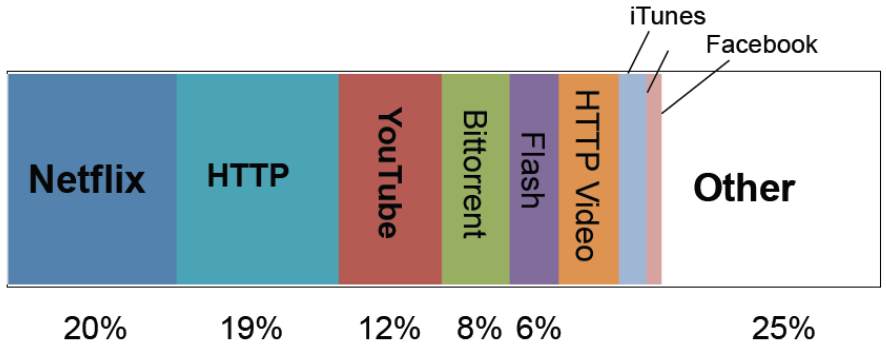


- Développement d'applications mobiles, cloud computing, Applications entièrement en ligne
- Tout connecté, l'activité et la vie d'une application nécessite presque toujours une connexion.

Les enjeux de la sécurité

- **Evolution des activités et logiciels**



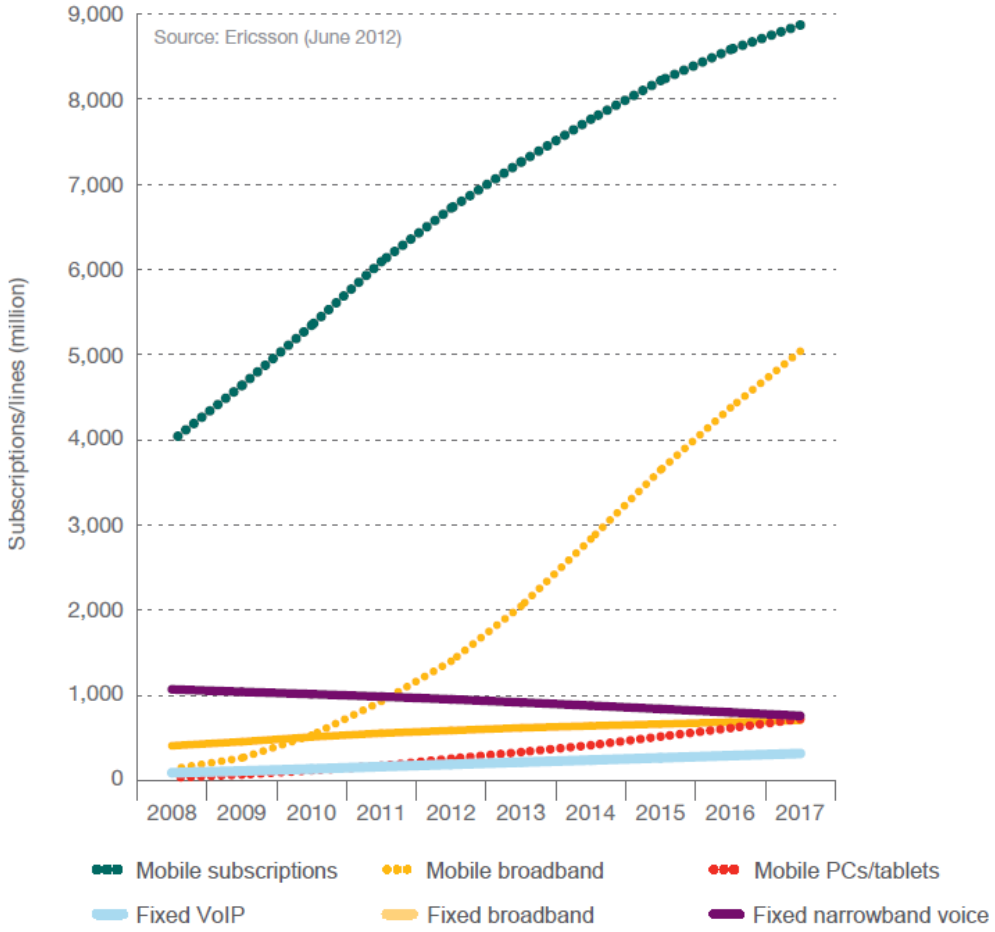


Internet Traffic Evolution 2007 – 2011 Craig Labovitz *April 6, 2011*

Les enjeux de la sécurité

- **Evolution des activités et logiciels**

Figure 4: Fixed and mobile subscriptions 2008-2017

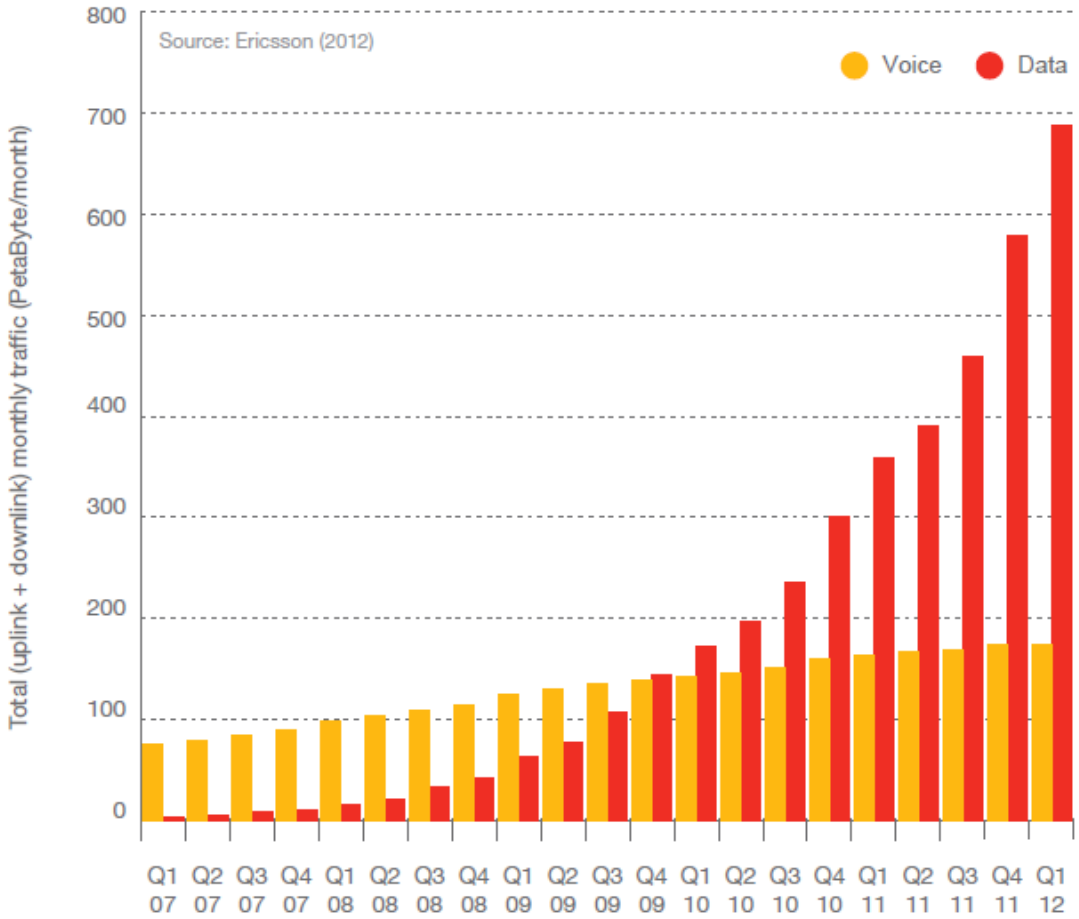


TRAFFIC AND Market report June 2012 ON THE PULSE OF THE NETWORKED SOCIETY, Ericsson

Les enjeux de la sécurité

- **Evolution des activités et logiciels**

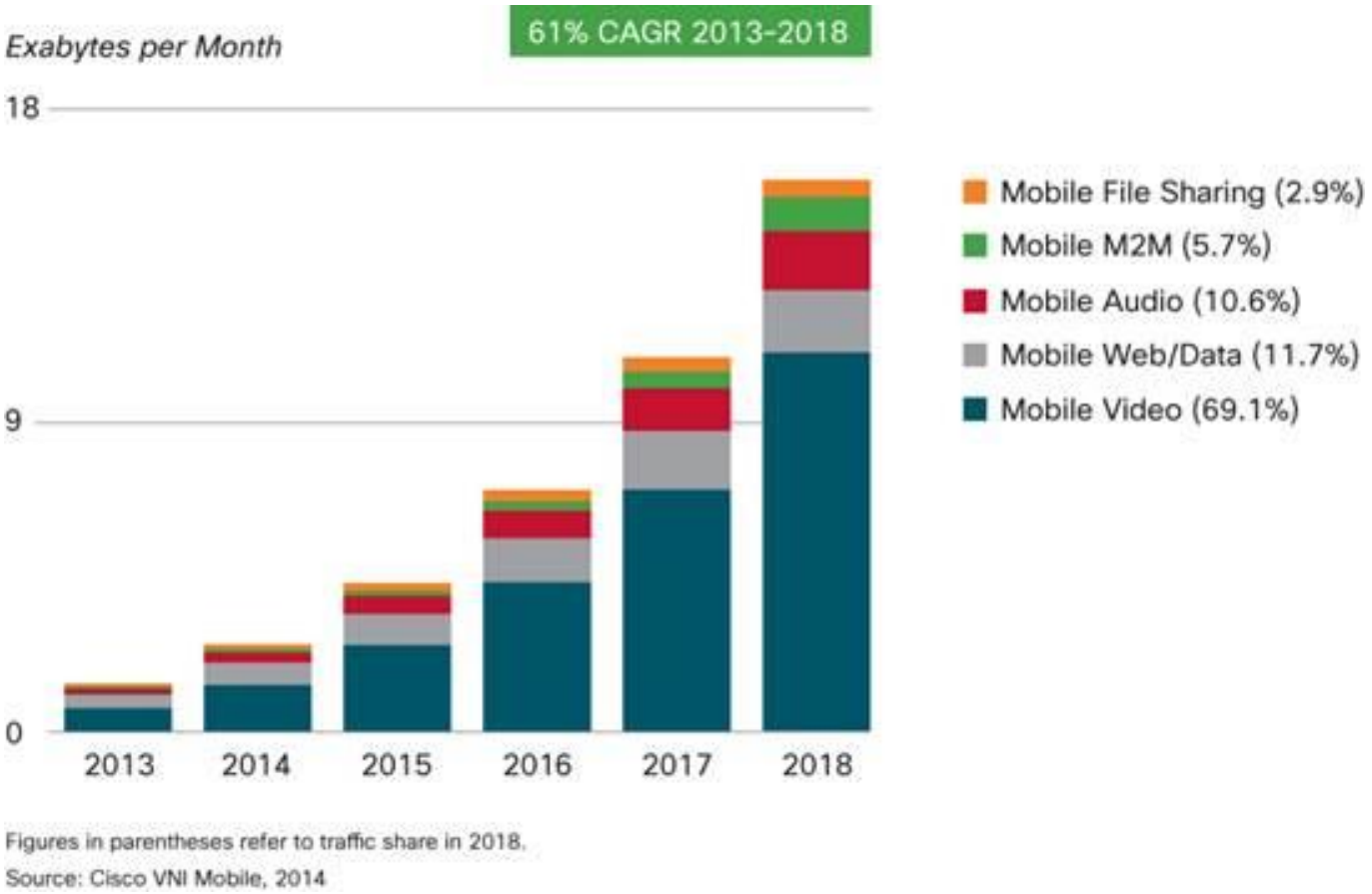
Figure 14: Global total traffic in mobile networks, 2007-2012



TRAFFIC AND Market report June 2012 ON THE PULSE OF THE NETWORKED SOCIETY, Ericsson

Les enjeux de la sécurité

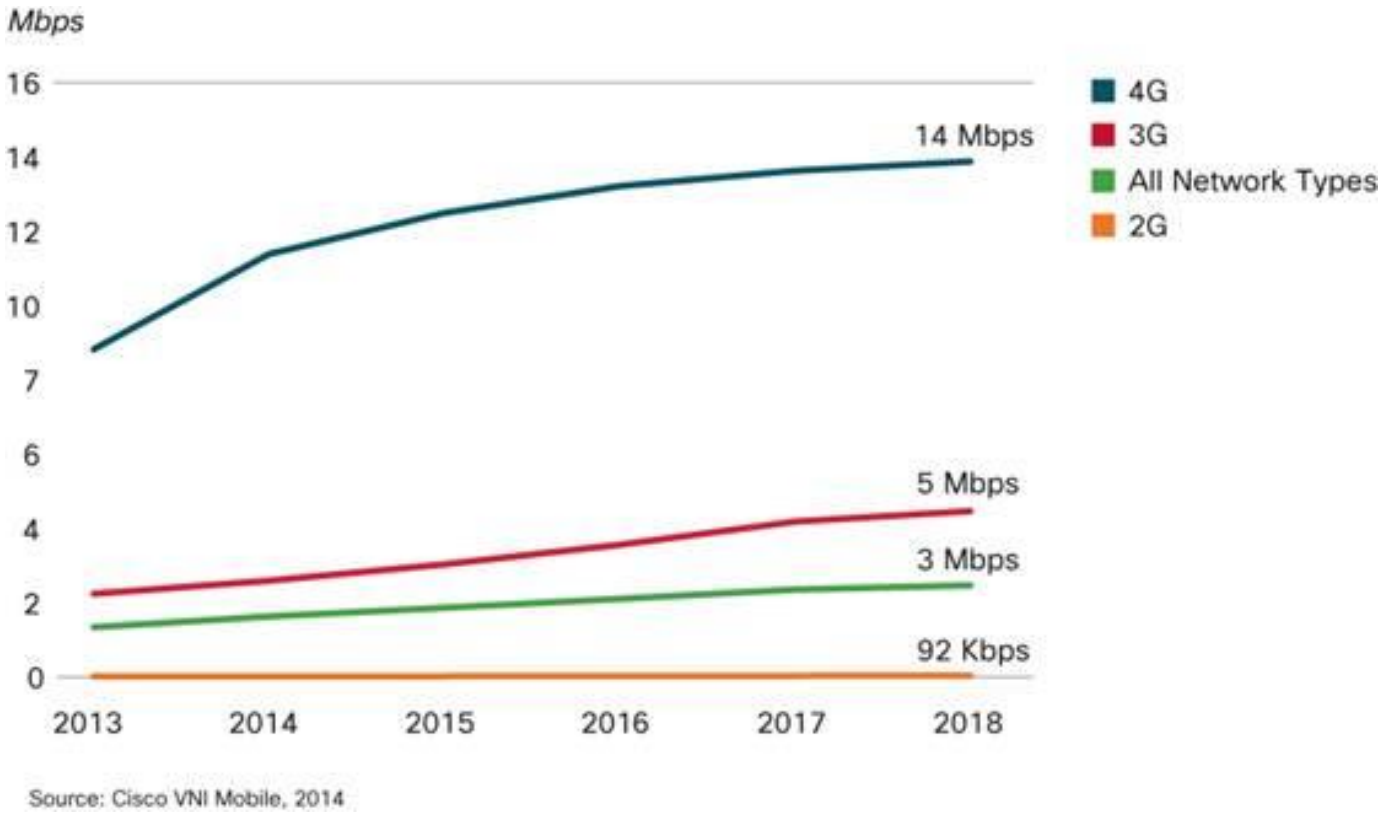
- **Evolution des activités et logiciels**



http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.html

Les enjeux de la sécurité

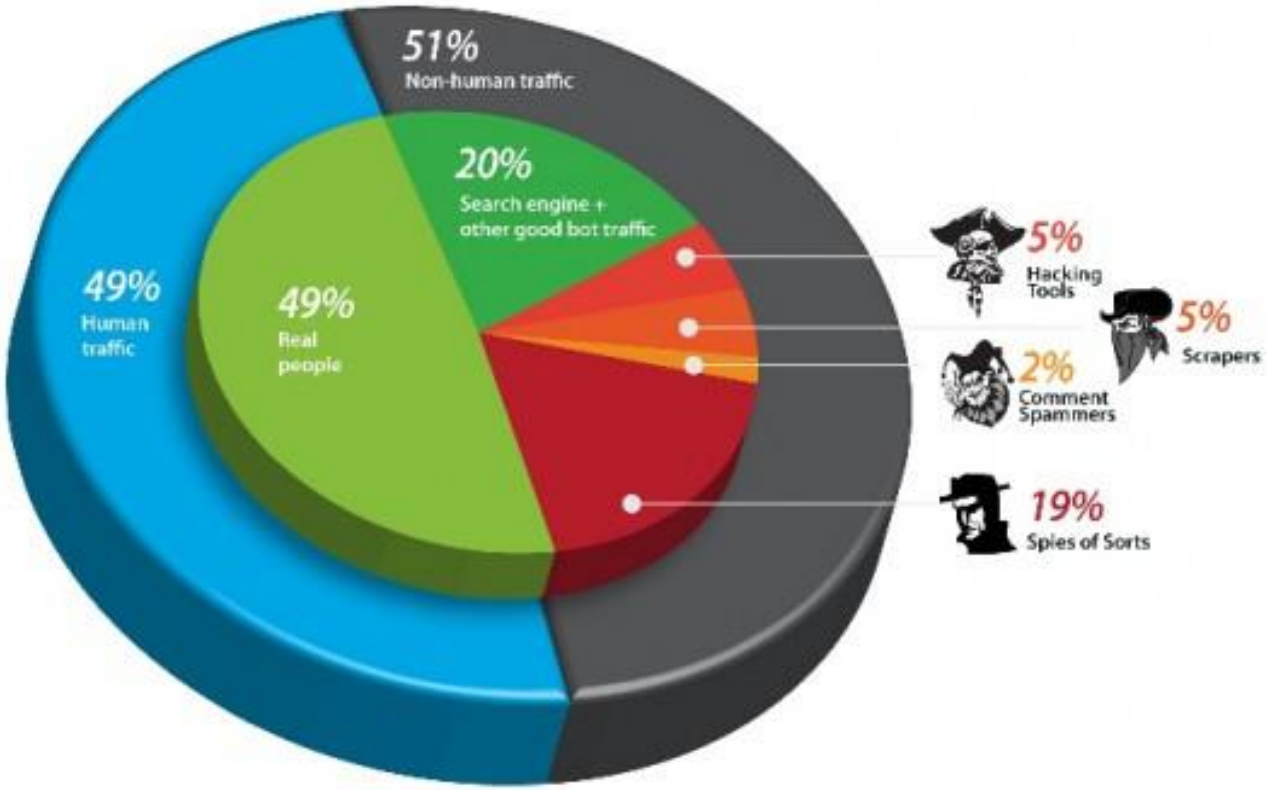
- **Evolution des activités et logiciels**



http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.html

Les enjeux de la sécurité

- **Evolution des activités et logiciels**

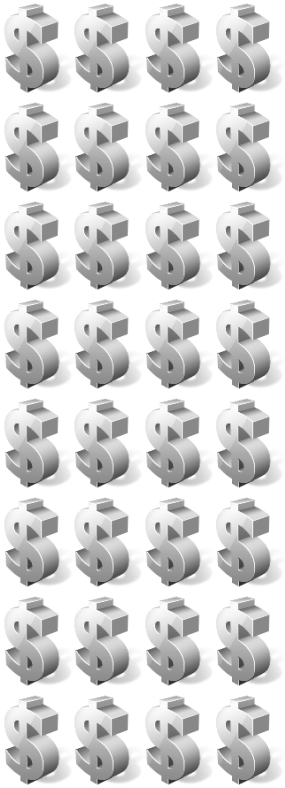


http://www.nextnature.net/2012/03/internet-traffic-is-now-51-non-human/

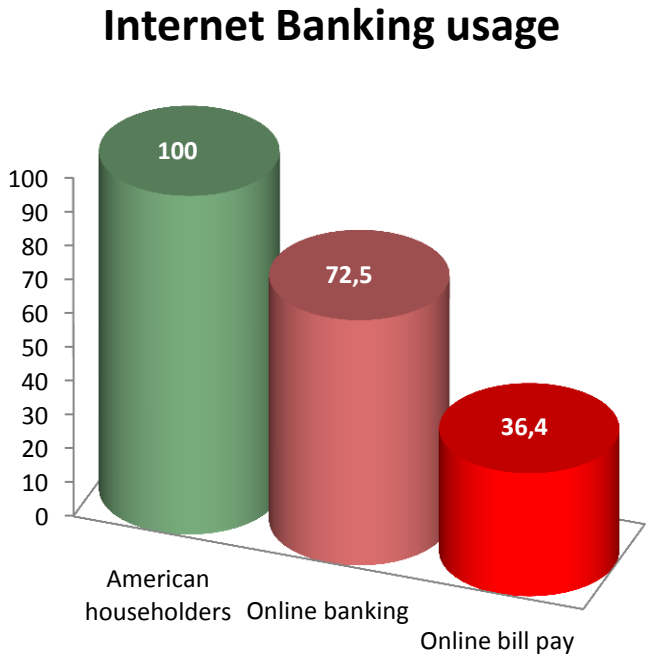
Les enjeux de la sécurité

- **Evolution des activités et logiciels**

2 Milliards D'utilisateurs (2011)



100ene de Milliards de $ chaque année

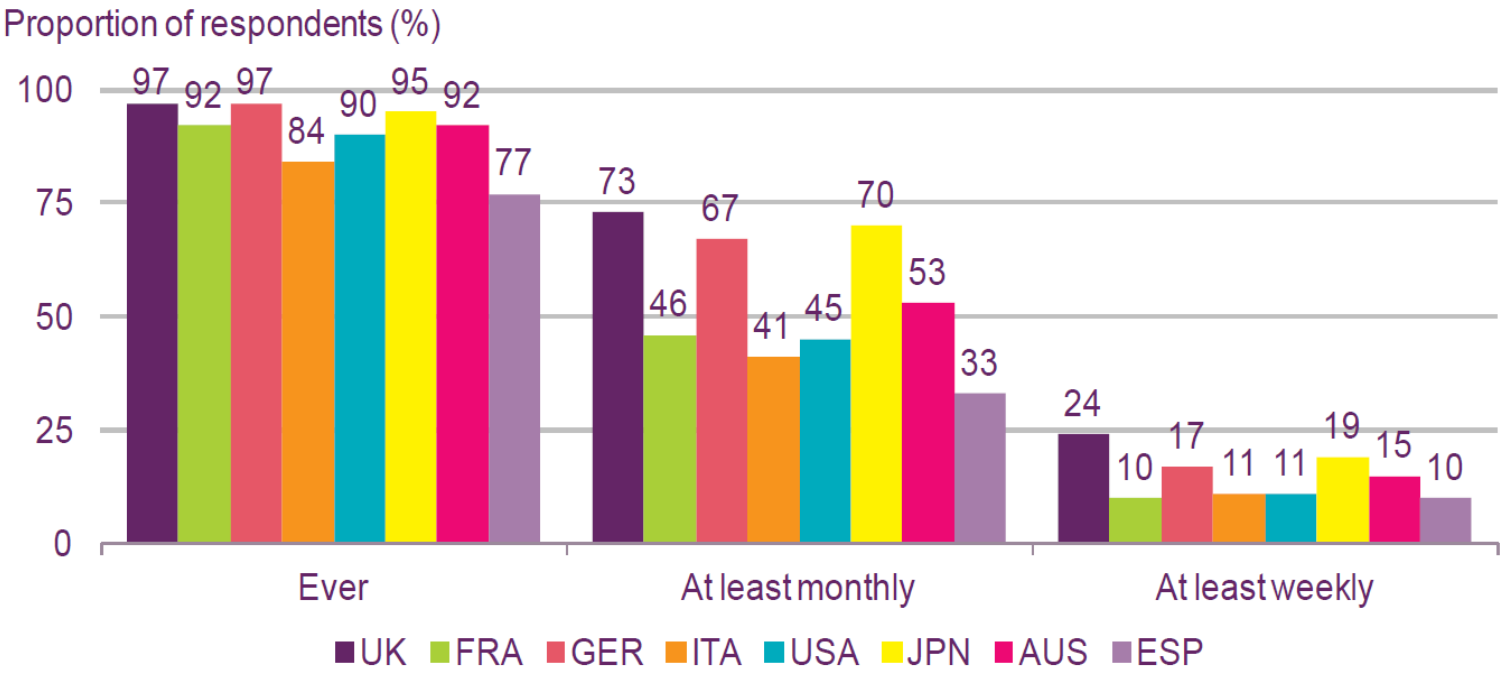


http://www.mybanktracker.com/news/2010/05/27/online-banking-online-bill-pay-growing-in-popularity/

Les enjeux de la sécurité

- **Evolution des activités et logiciels**

Figure 1.21 Frequency of online shopping

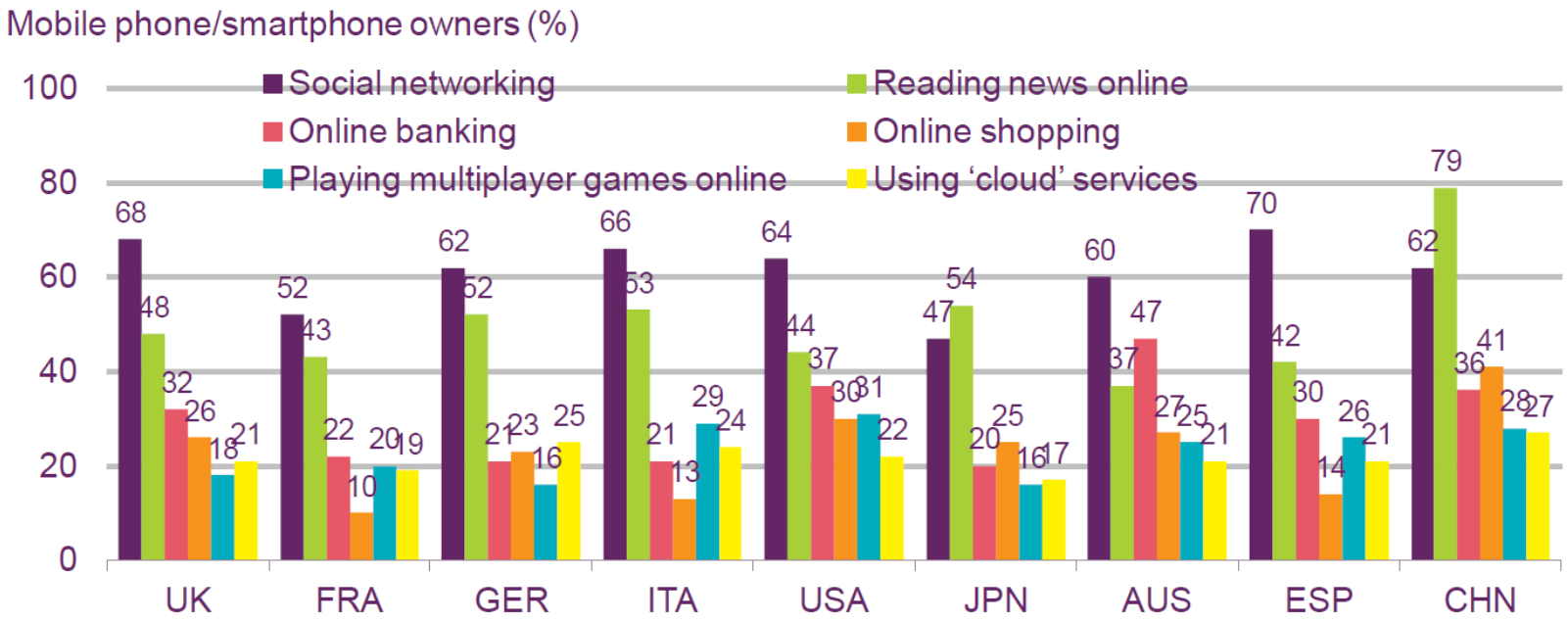


Source: Ofcom research, September 2013
Q01: How often if at all, do you purchase items online for delivery? Base: all respondents (UK=1000, FRA=1007, GER=1010, ITA=1010, USA=1004, JPN=1005, AUS=1007, ESP=1020)

Les enjeux de la sécurité

- **Evolution des activités et logiciels**

Figure 5.13 Mobile-internet activities



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

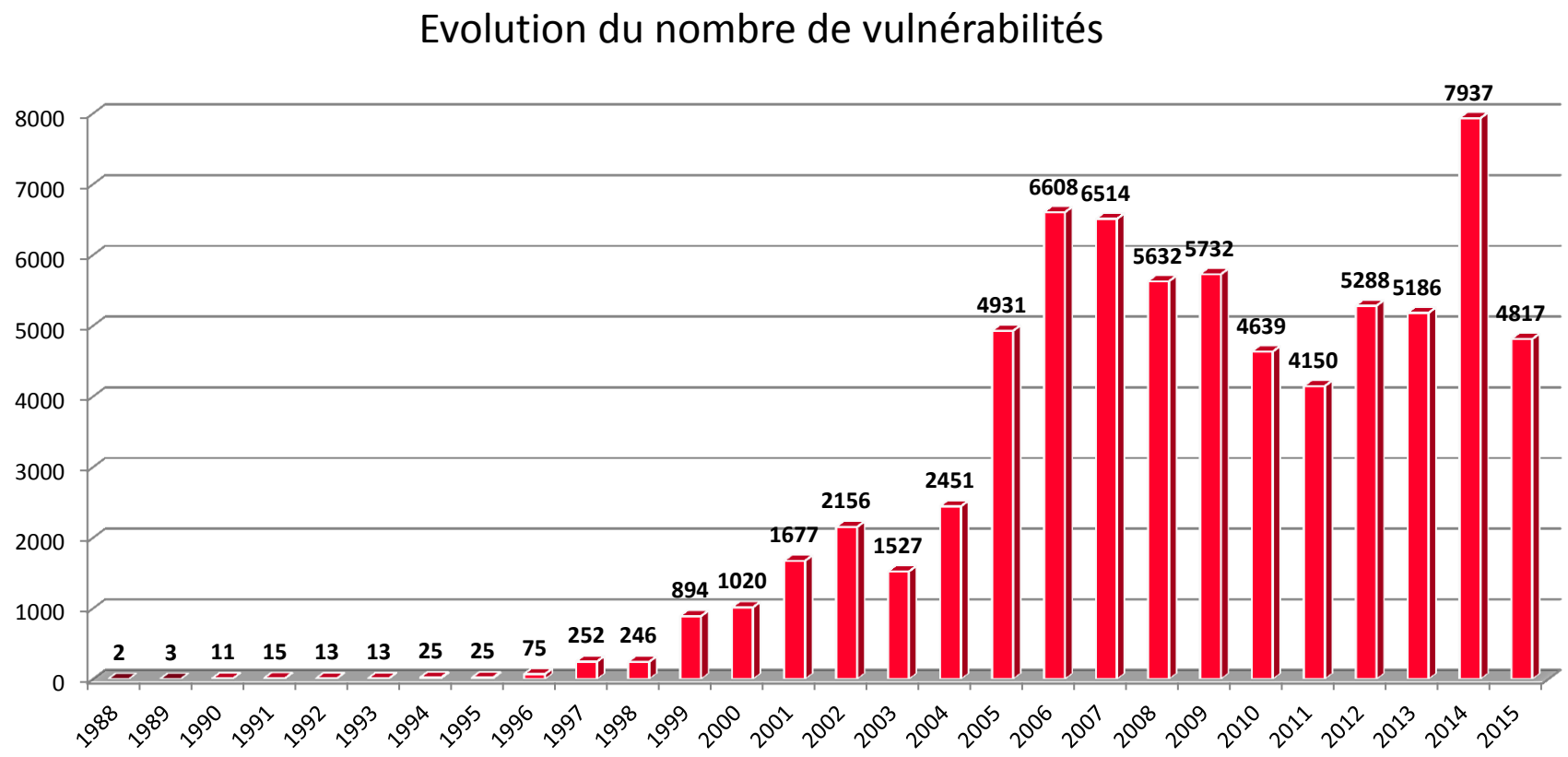
- Evolution des systèmes d'information
- Les Constats de sécurité

Les enjeux de la sécurité

Sommes nous vulnérables ?

Les enjeux de la sécurité

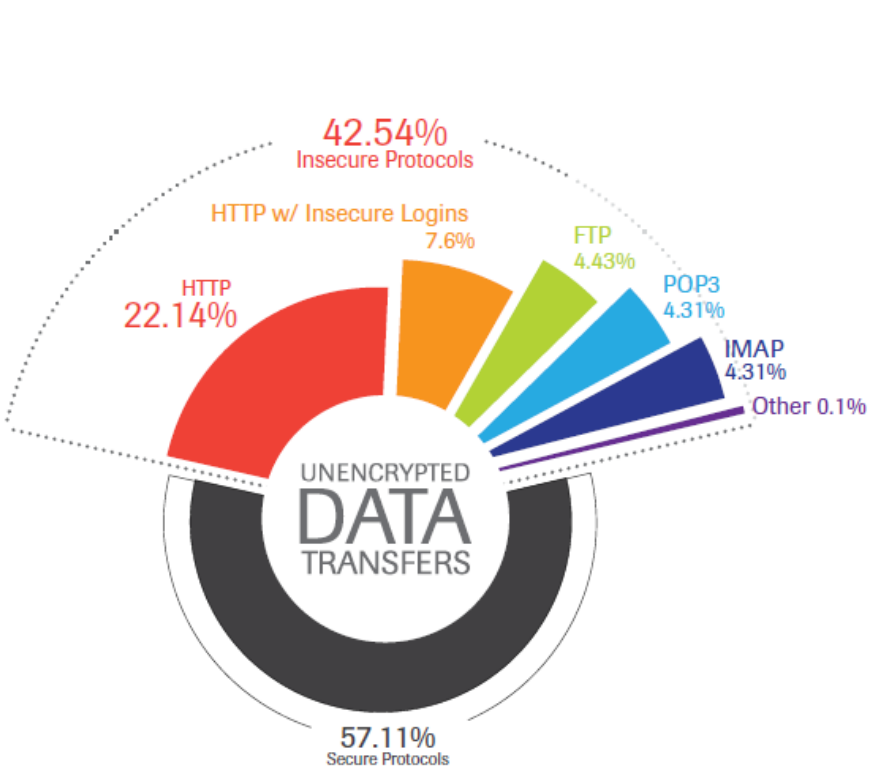
- **Les constats de sécurité: Sommes nous vulnérables ?**

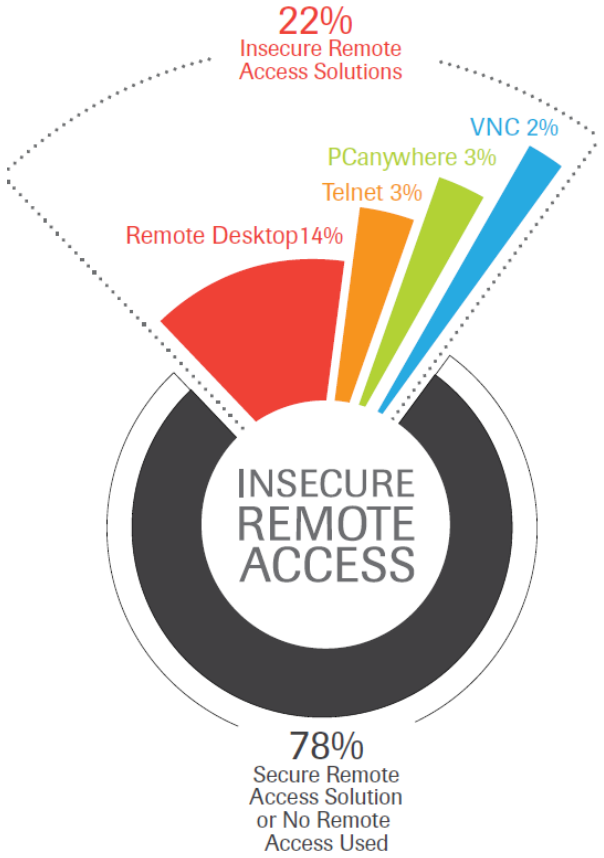


http://web.nvd.nist.gov

Les enjeux de la sécurité

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





TrustWave 2012 Global Security Report

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 enjeux de la sécurité

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

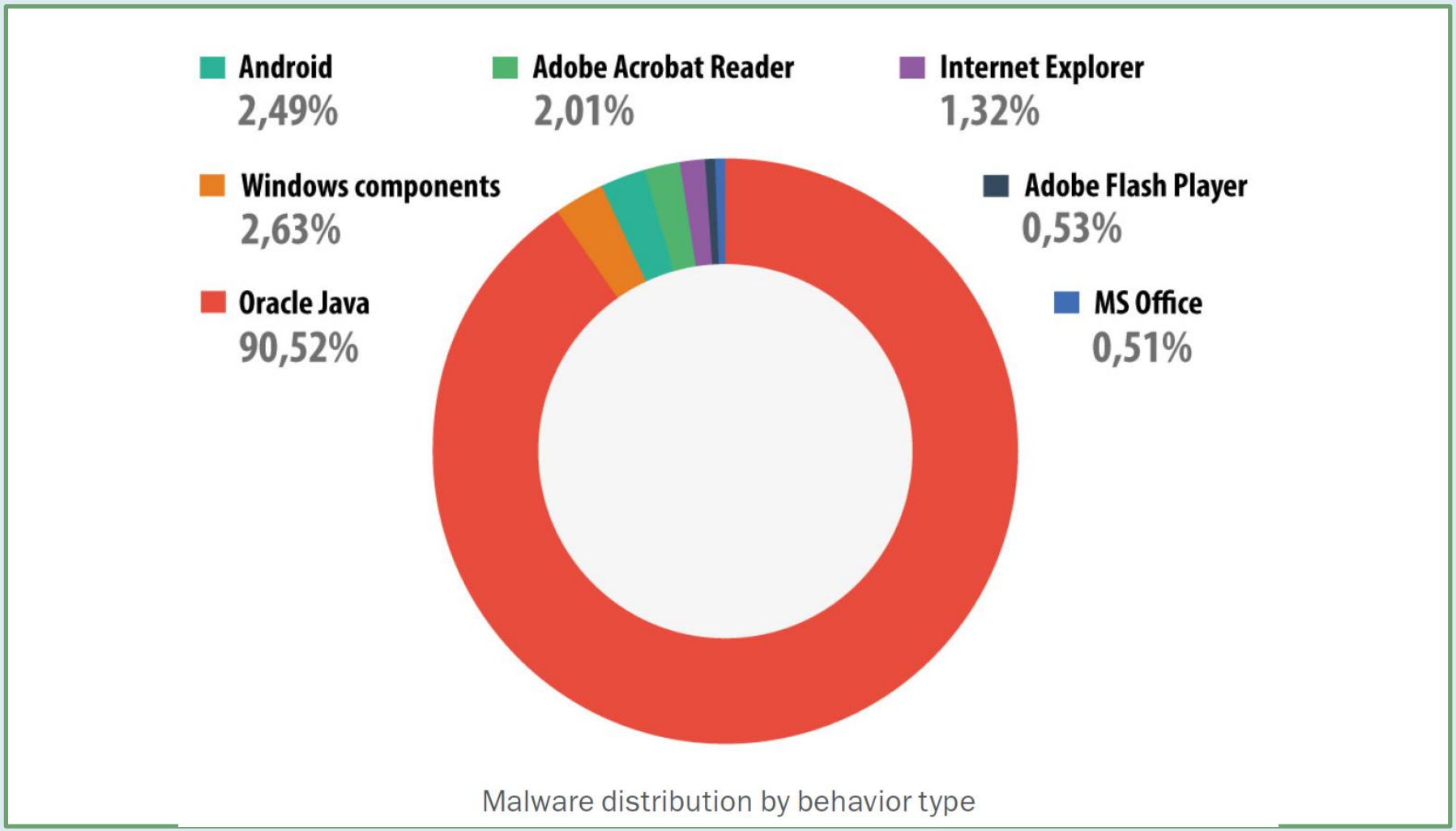
http://www.informationisbeautiful.net/visualizations/million-lines-of-code/

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 enjeux de la sécurité

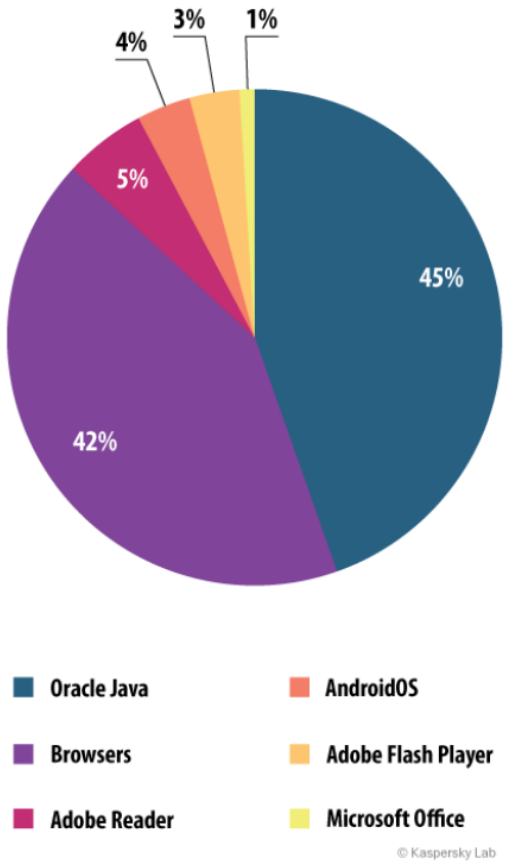
- **Les constats de sécurité: Sommes nous vulnérables ?**



Kaspersky security report 2013: overall statistic

Les enjeux de la sécurité

- **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?**

TrustWave 2013 Global Security Report

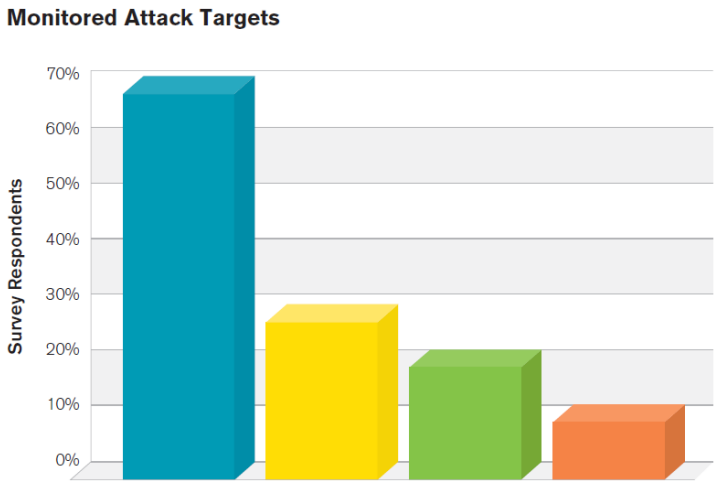


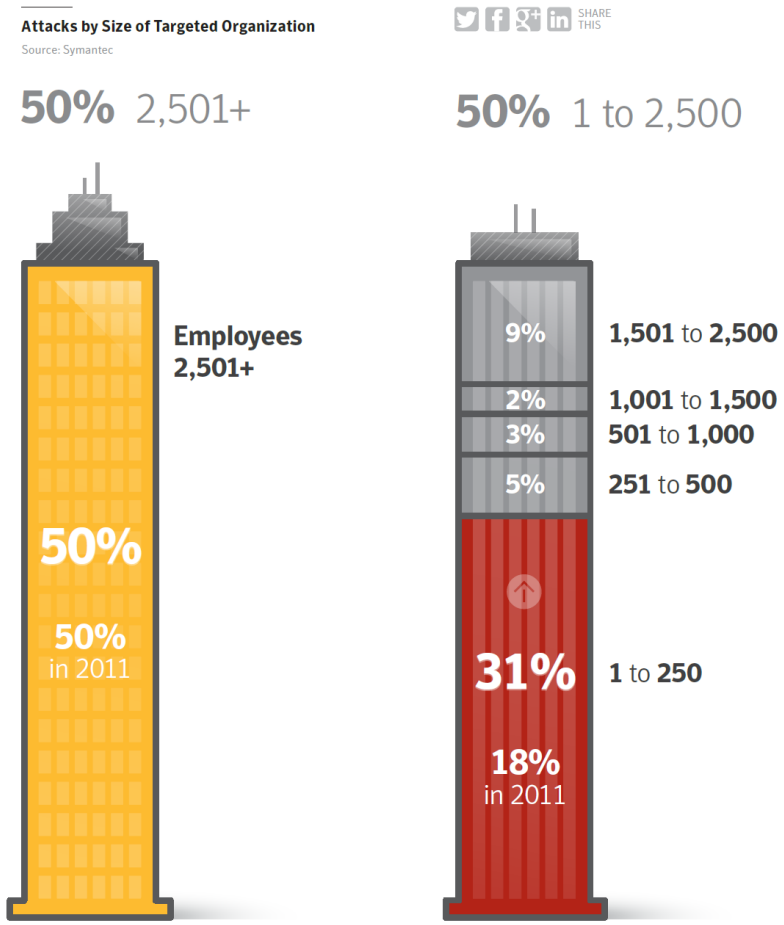
Figure 19 Source: Arbor Networks, Inc.

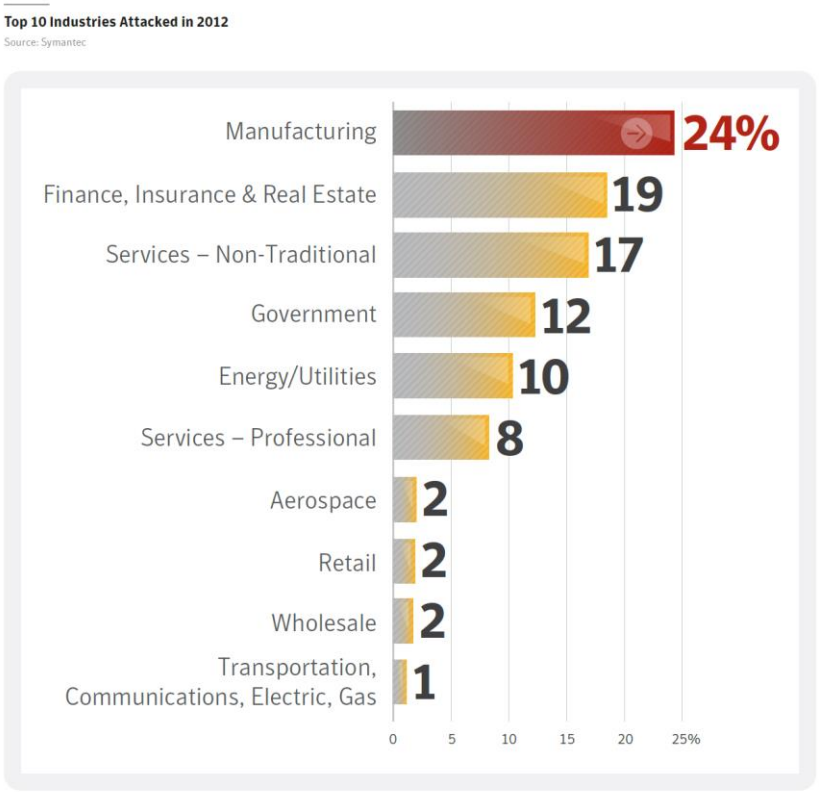
66% Customer
25% Service Infrastructure
17% Network Infrastructure
7% Other

Arbor Network Security Report 2014

Les enjeux de la sécurité

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

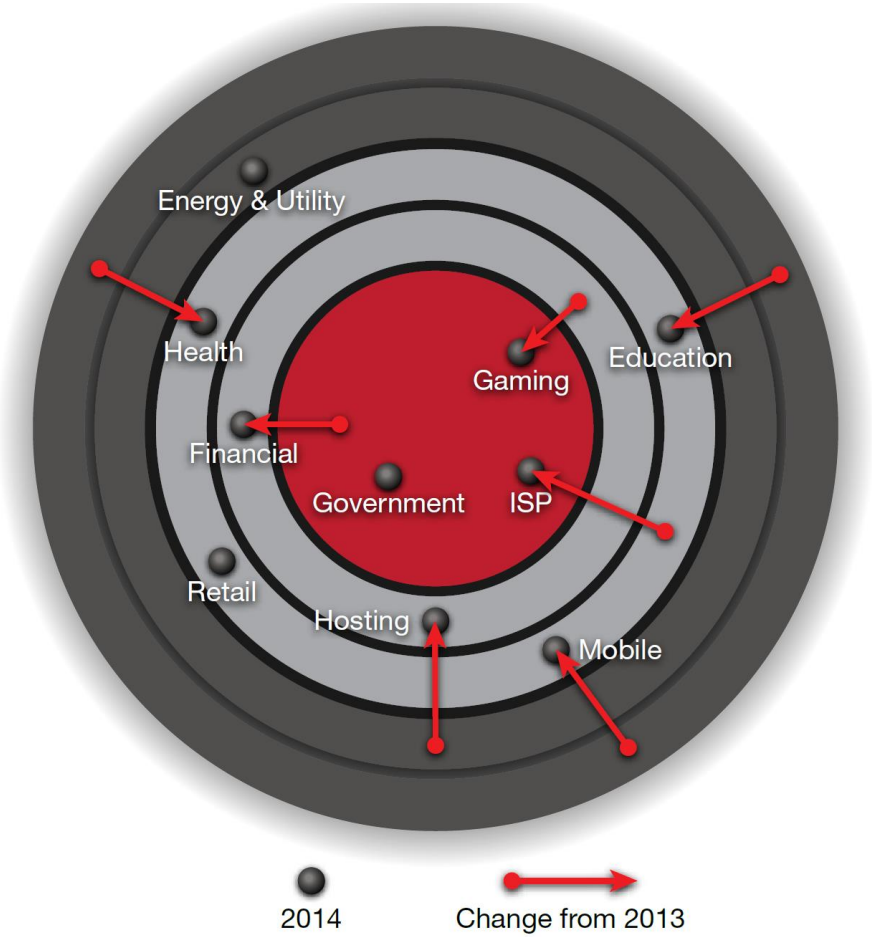




Symantec INTERNET SECURITY THREAT REPORT, 2012 Trends, Volume 18, Published April 2013

Les enjeux de la sécurité

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



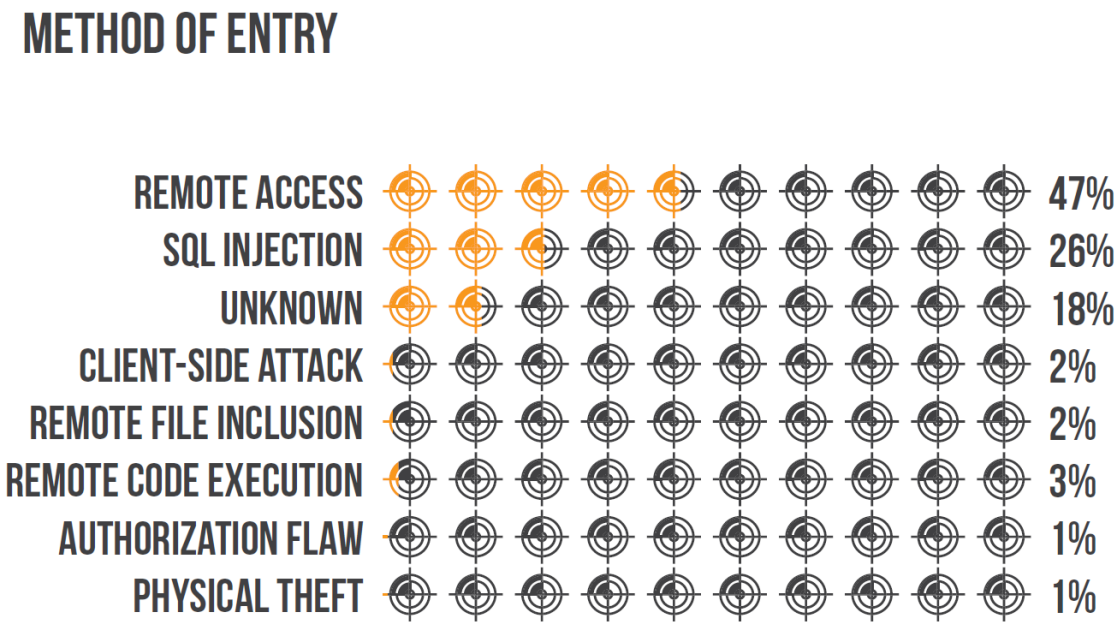
Radware security report 2014-2015

Les enjeux de la sécurité

Comment nous ont-ils attaqué ?

Les enjeux de la sécurité

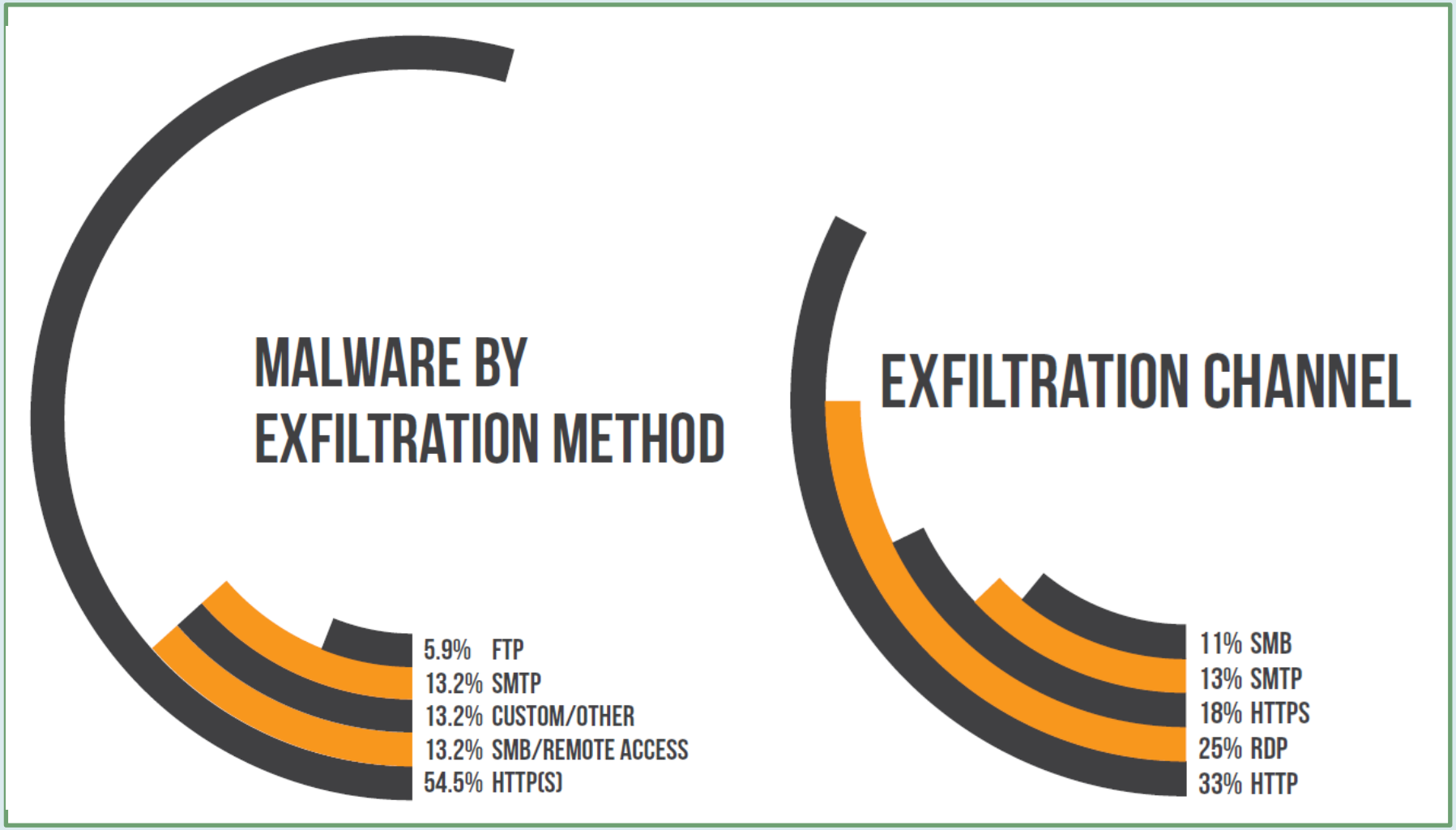
- **Les constats de sécurité: Comment nous ont-ils attaqué?**



TrustWave 2013 Global Security Report

Les enjeux de la sécurité

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



TrustWave 2013 Global Security Report

Les enjeux de la sécurité

Qui nous menace ?

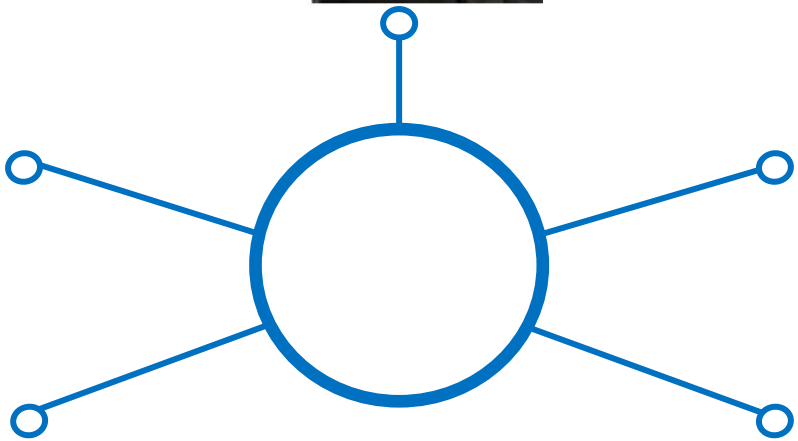
Les enjeux de la sécurité

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

Internal

Coder, old guard hackers

Newbie/Toolkit



Professional criminals, Cyber-terrorists

Cyberpunk

Les enjeux de la sécurité

- **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

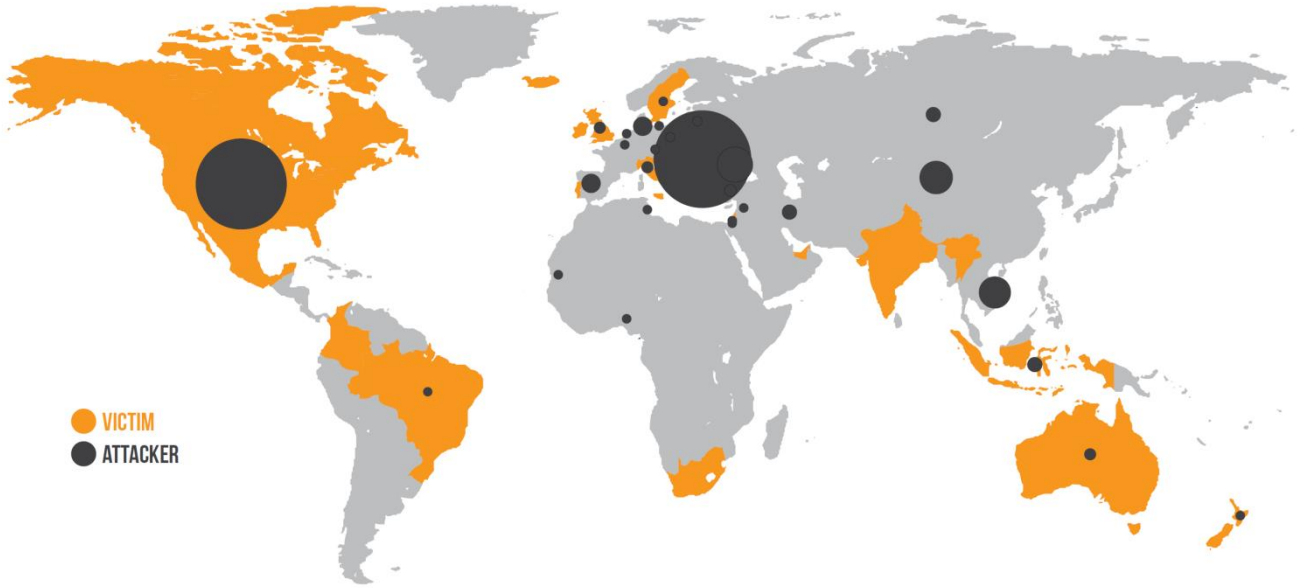
- **Les constats de sécurité: Qui nous menace?**

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 enjeux de la sécurité

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



> 450
DATA BREACHES
19
COUNTRIES

TOP VICTIM LOCATIONS:		TOP ATTACKER LOCATIONS:	
UNITED STATES	73.0%	ROMANIA	33.4%
AUSTRALIA	7.0%	UNITED STATES	29.0%
CANADA	3.0%	UNKNOWN	14.8%
UNITED KINGDOM	2.0%	UKRAINE	4.4%
BRAZIL	1.2%	CHINA	3.9%

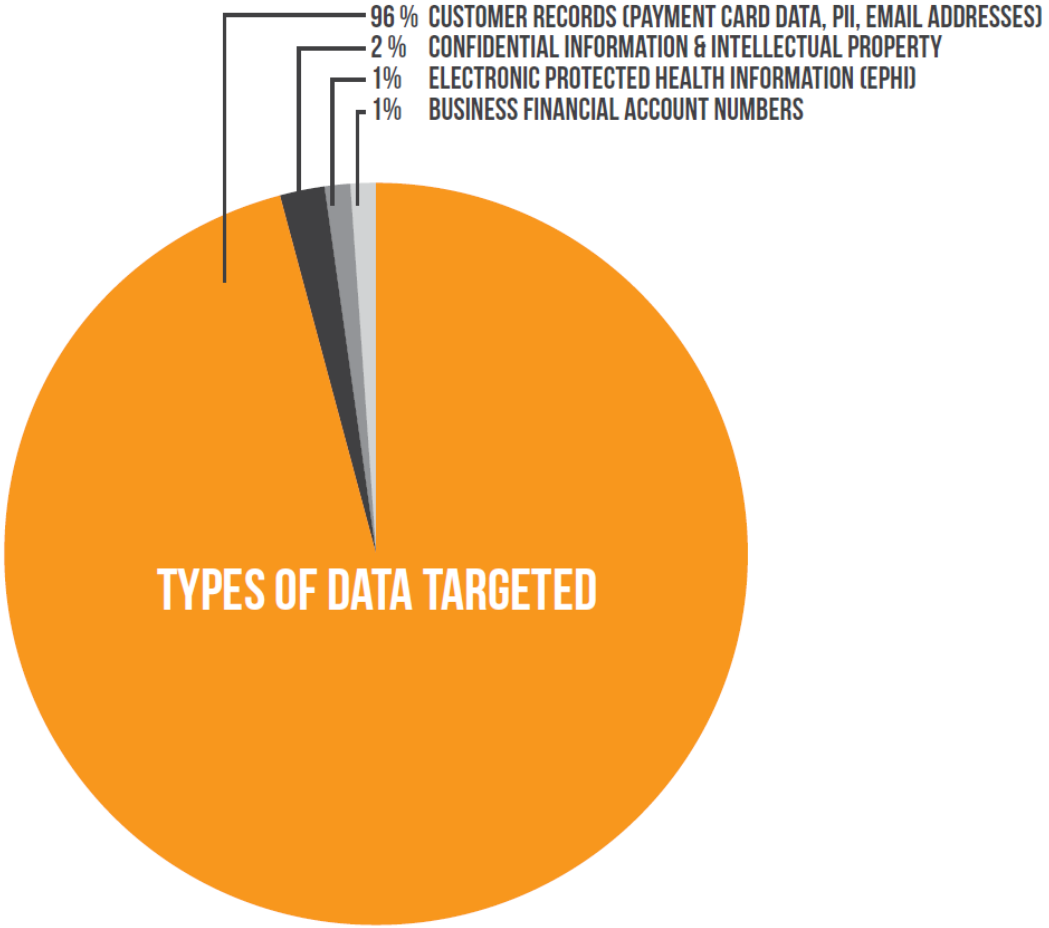
TrustWave 2013 Global Security Report

Les enjeux de la sécurité

Que nous prennent-ils ?

Les enjeux de la sécurité

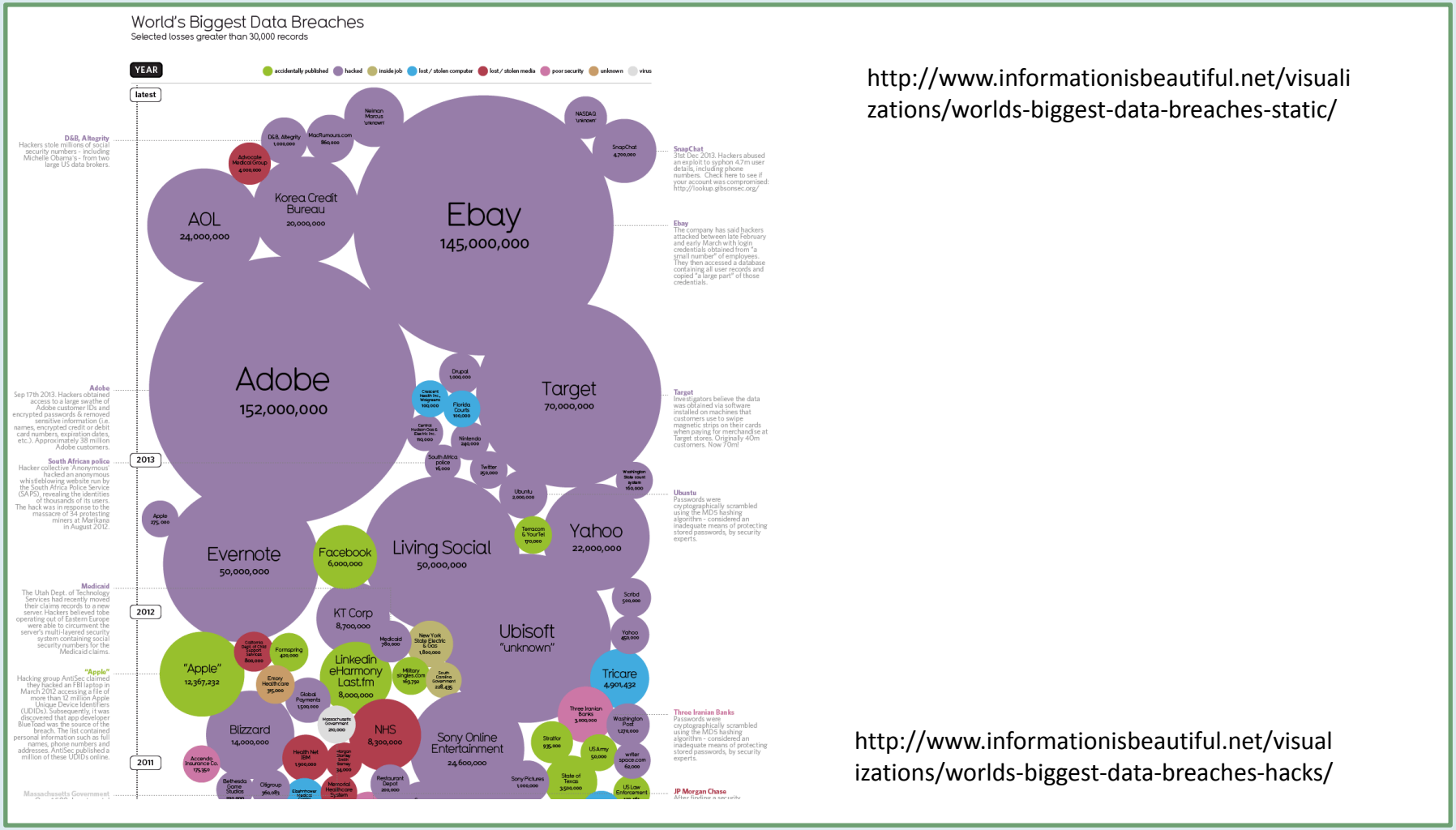
- **Les constats de sécurité: Que nous prennent-ils?**



TrustWave 2013 Global Security Report

Les enjeux de la sécurité

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



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

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

Les enjeux de la sécurité

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

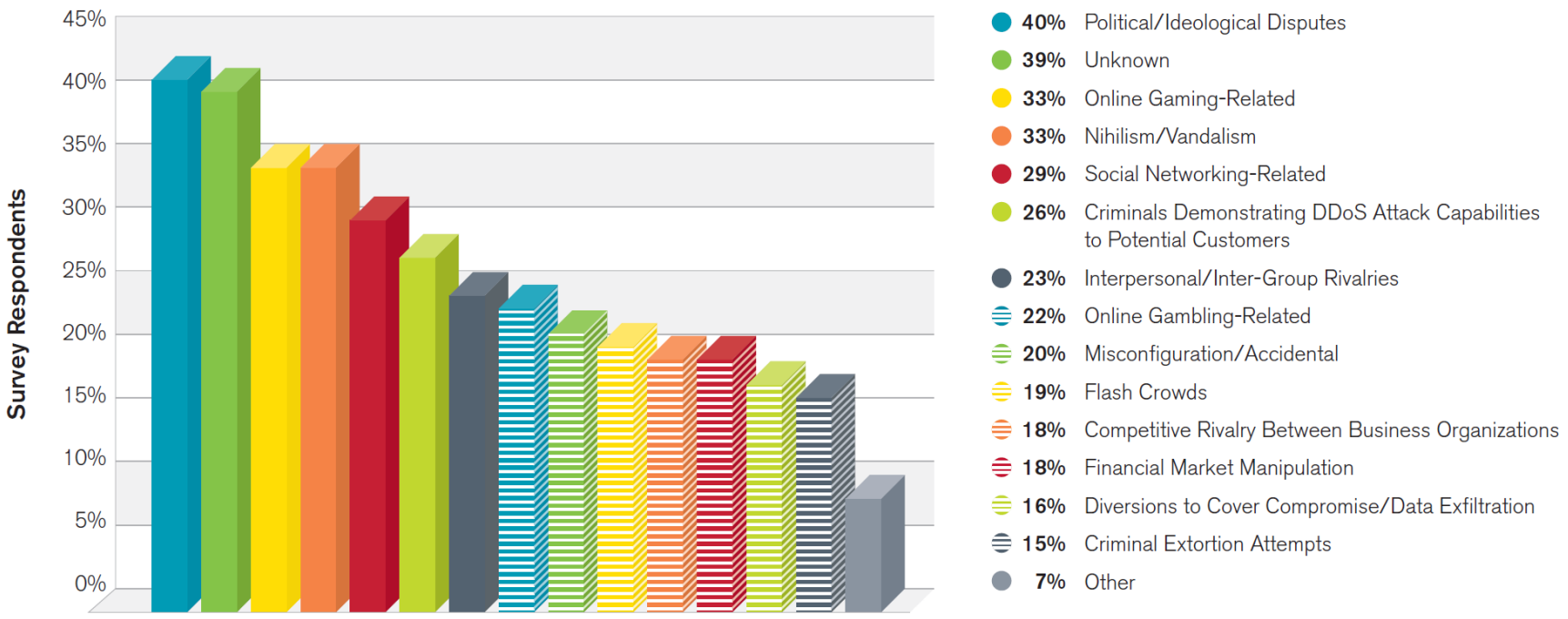


Figure 13 *Source: Arbor Networks, Inc.*

Arbor Network report 2014

Les enjeux de la sécurité

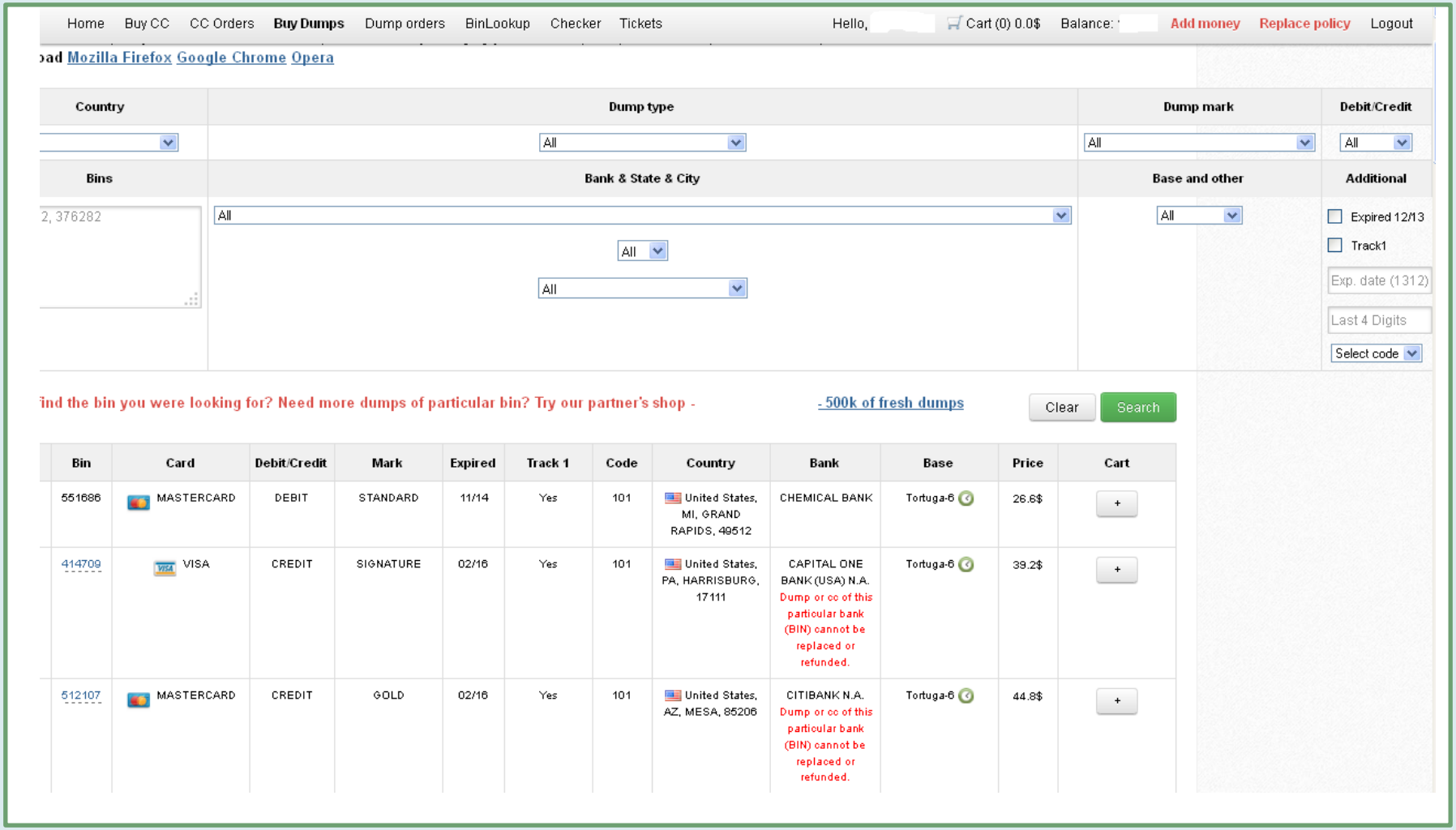
- **Les constats de sécurité: Que nous prennent-ils?**

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 enjeux de la sécurité

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



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

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 enjeux de la sécurité

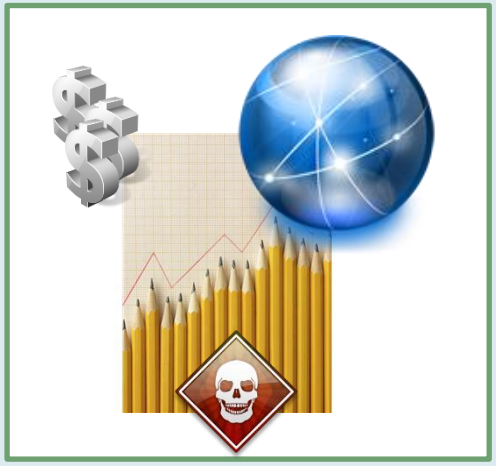
- **Conclusion**

  - ❑ 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



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

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

Les enjeux de la sécurité

- **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

Les enjeux de la sécurité

- **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:

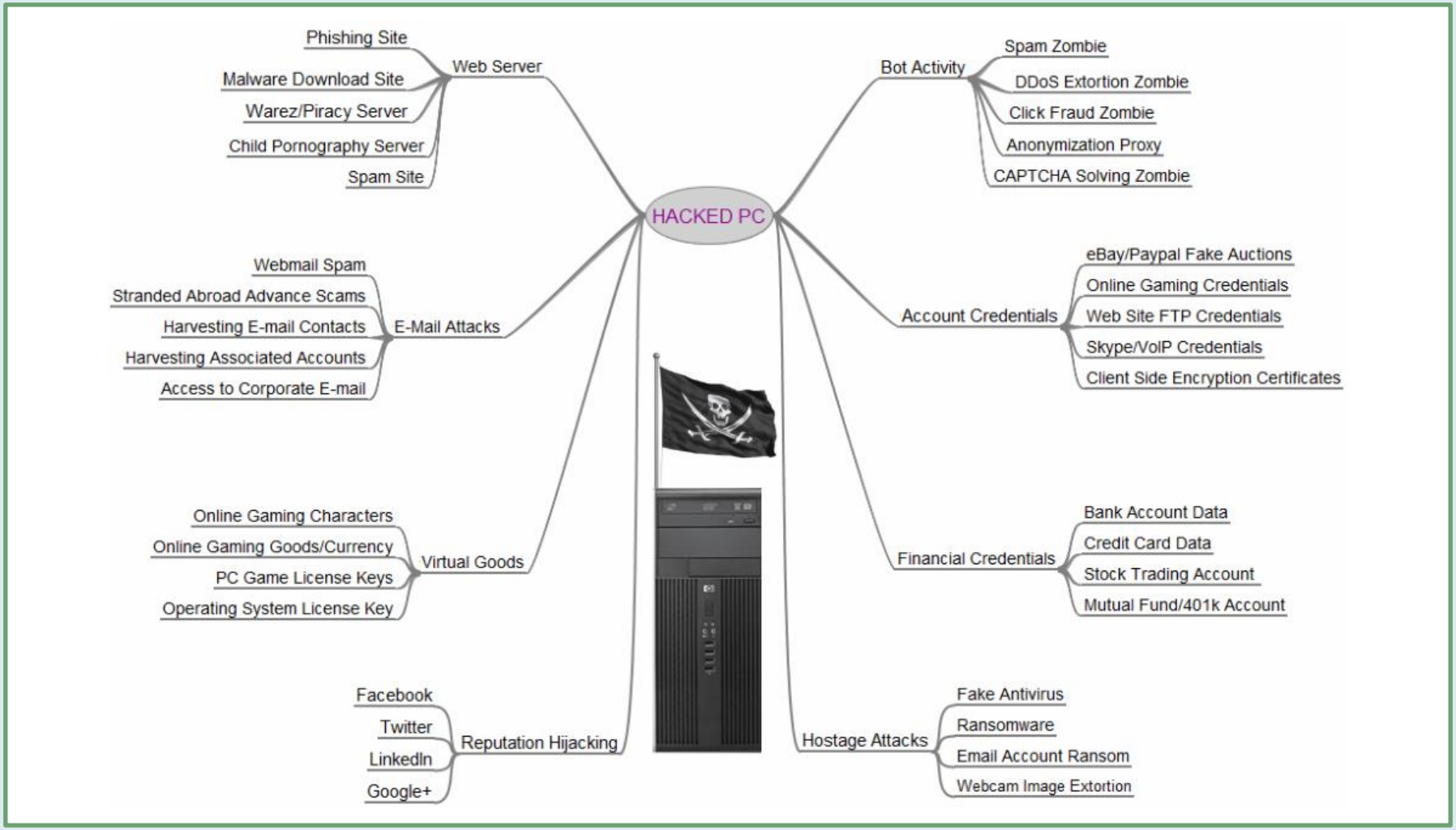
- Arrêt d'activités
- Vol de données sensibles (prototype, portefeuille client)
- Atteinte à la réputation (défacement…)

Nous tous

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

Les enjeux de la sécurité

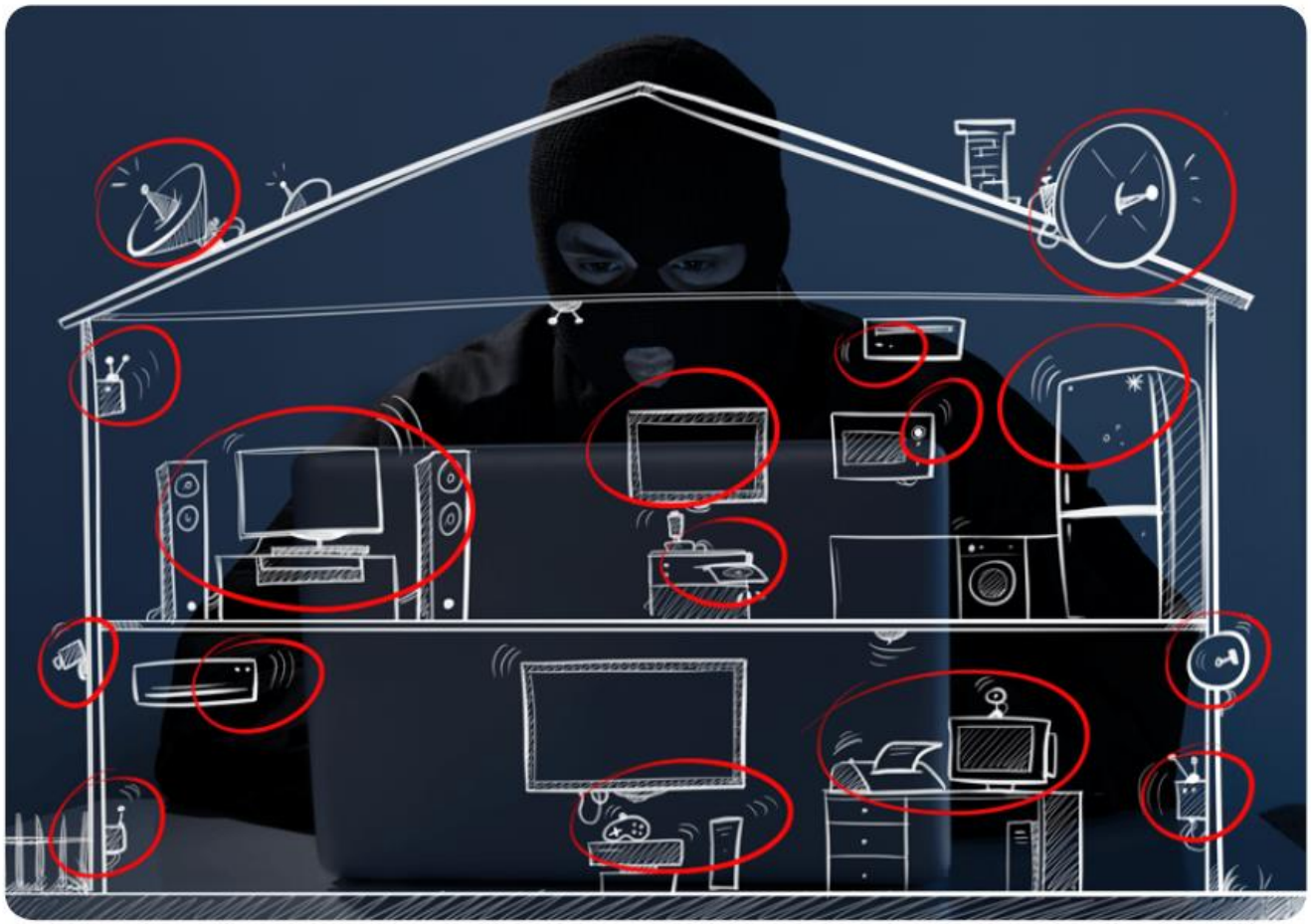
- **Un état d'urgence ?**



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-ton ?**

Viruses

Worms

Buffer overflows

Deny of service attacks

Network attacks

Physical attacks

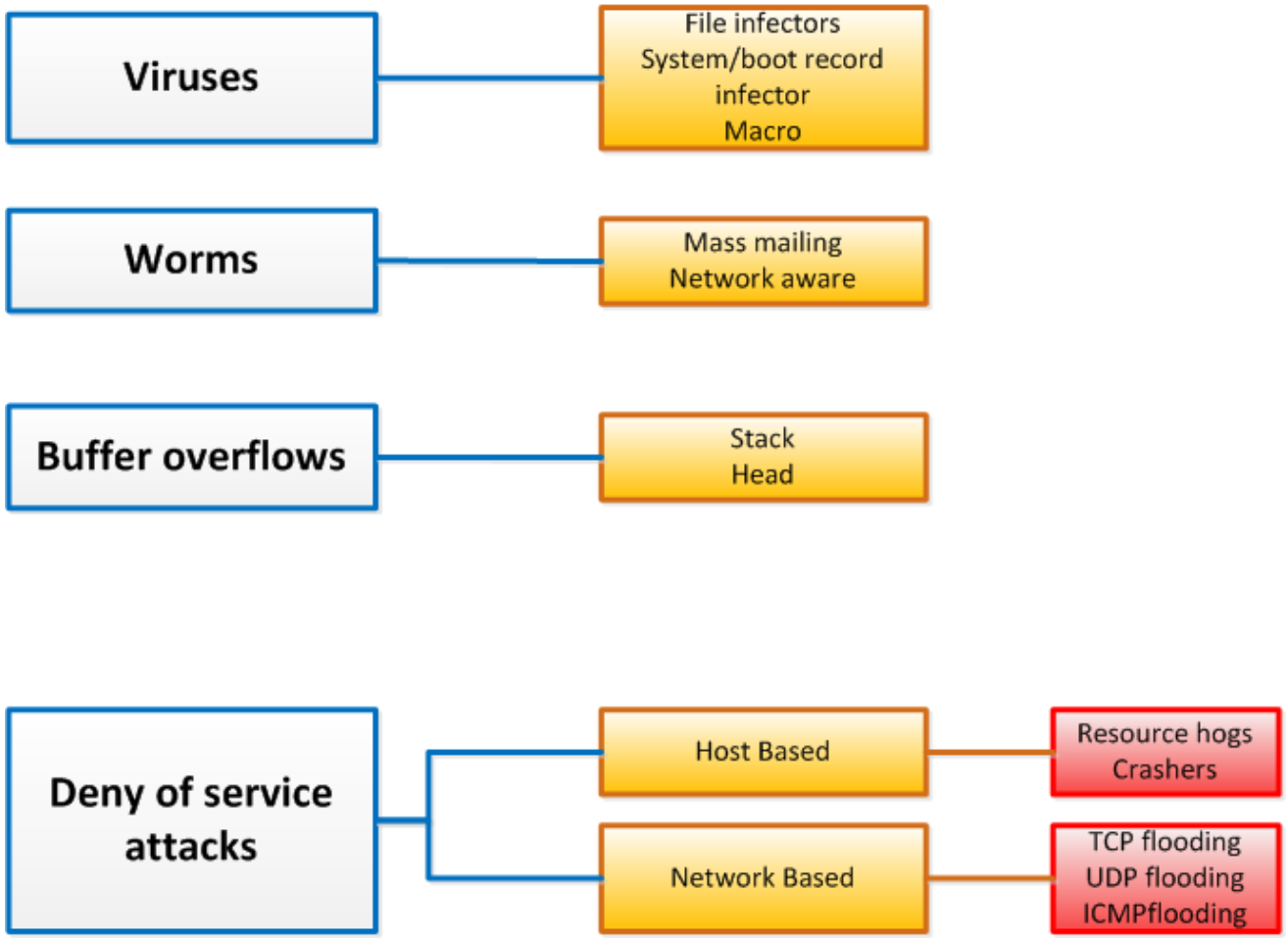
Password attacks

Information Gathering attacks

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

Les enjeux de la sécurité

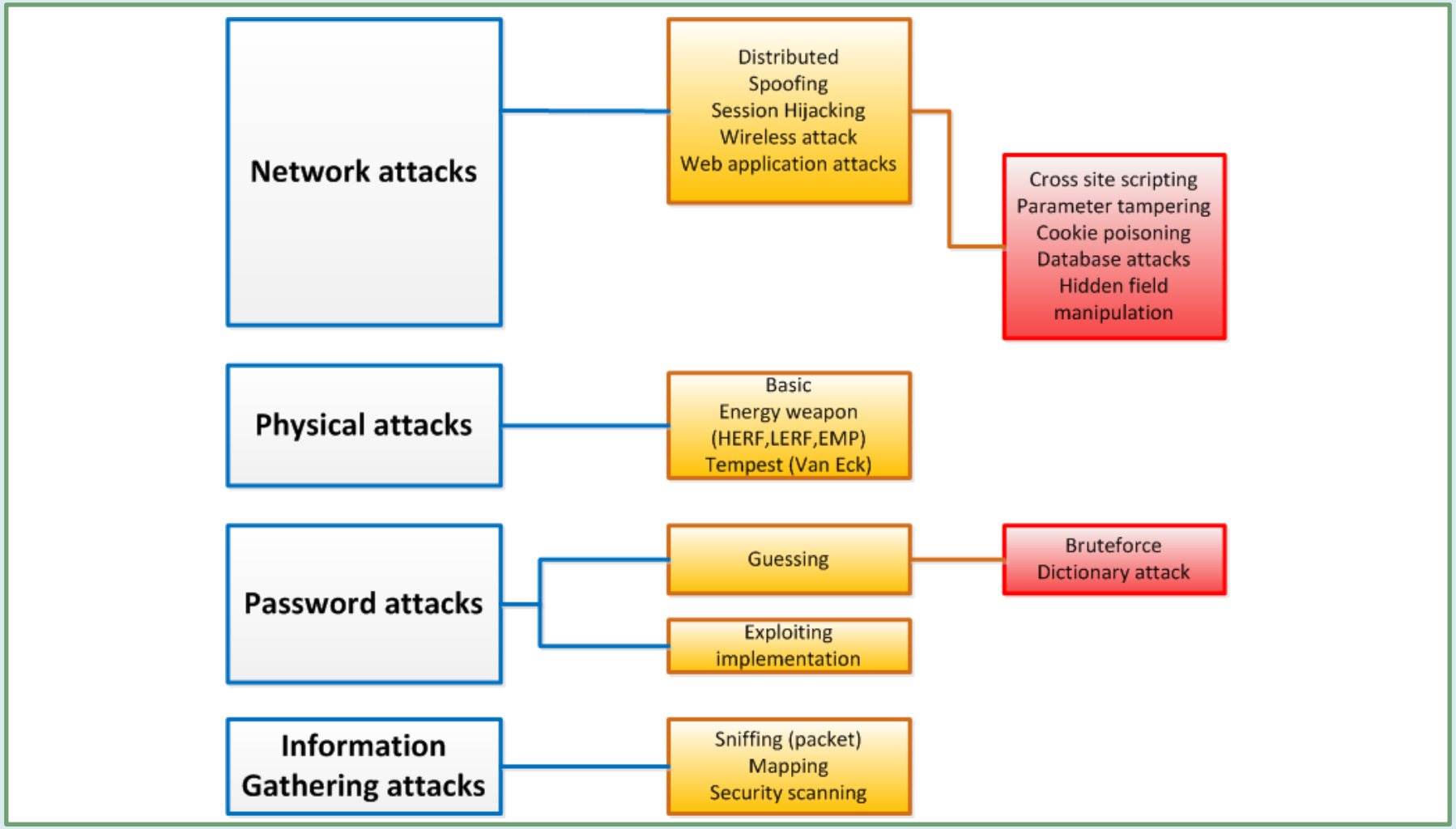
- **Un état d'urgence ? Contre quoi se protège-ton ?**



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-ton ?**

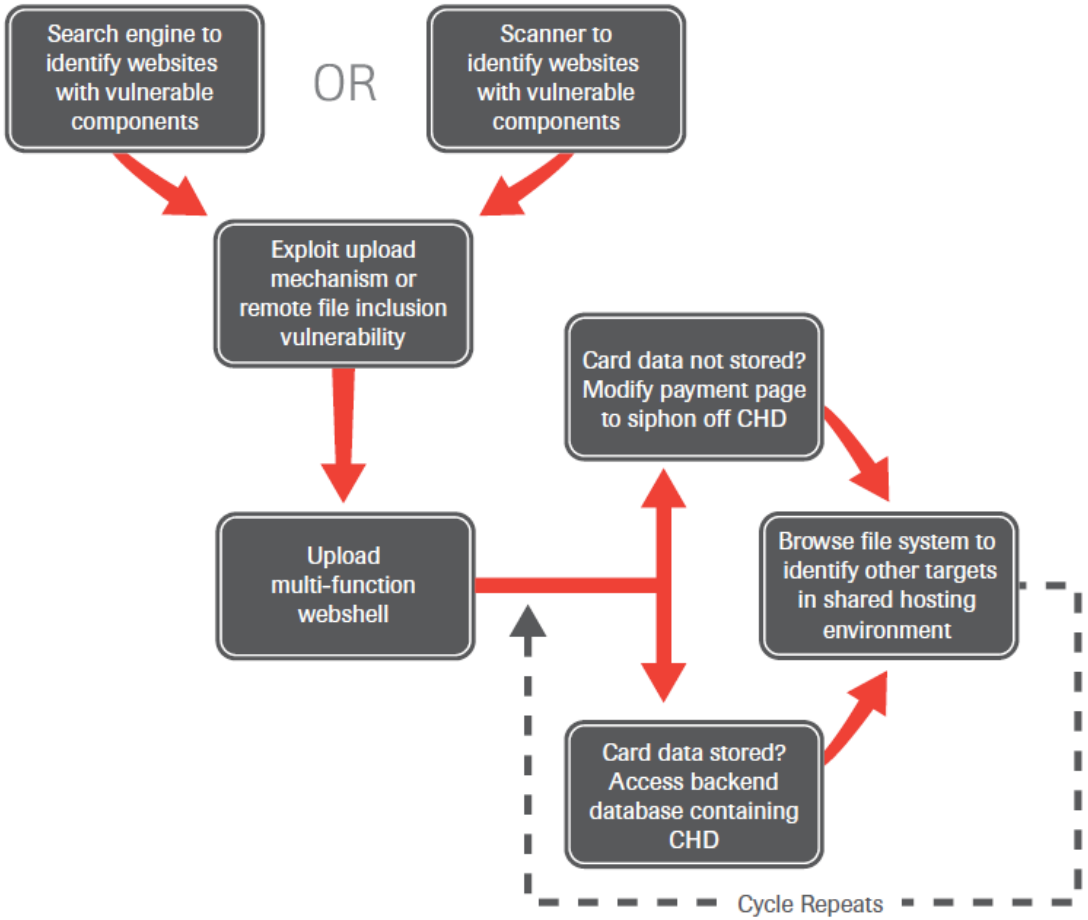


A taxonomy of network and computer attack , Simon Hansman, Ray Hunt,2004

Les enjeux de la sécurité

- **Un état d'urgence ? Contre quoi se protège-ton ?**

Exemple de stratégie d'attaque



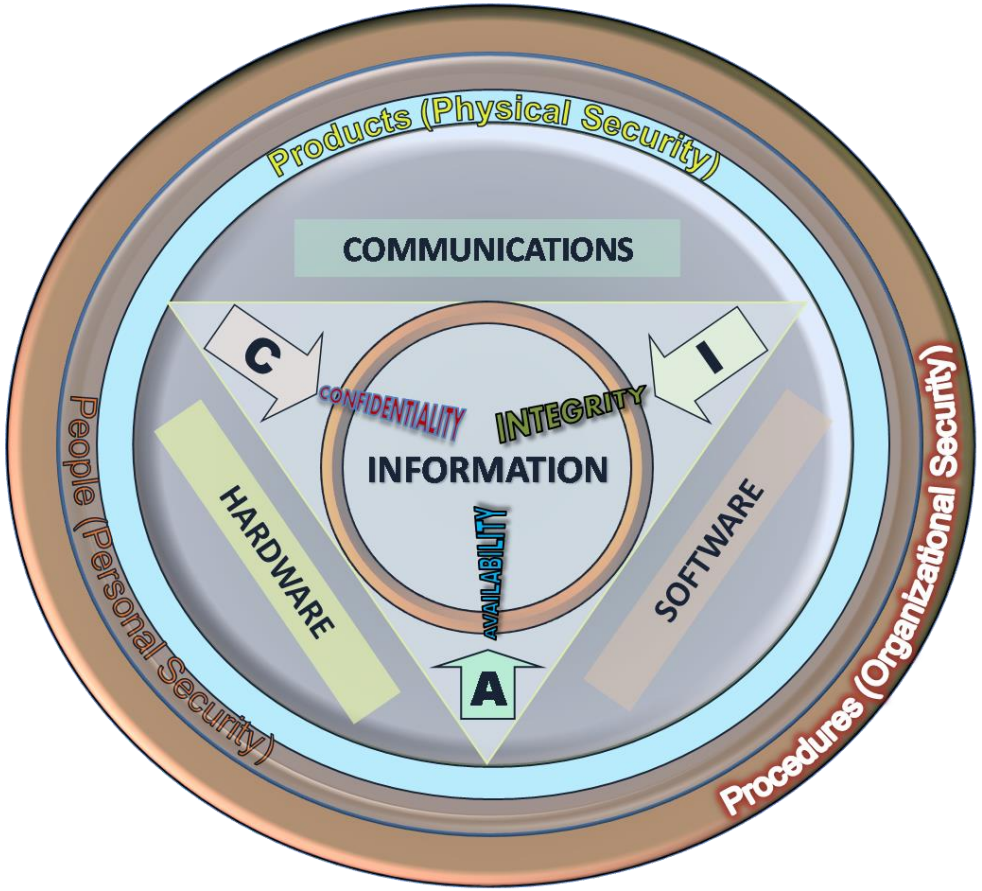
TrustWave 2012 Global Security Report

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

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

Les enjeux de la sécurité

- **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 pas une entité non autorisée. Toute modification d'information entraine 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

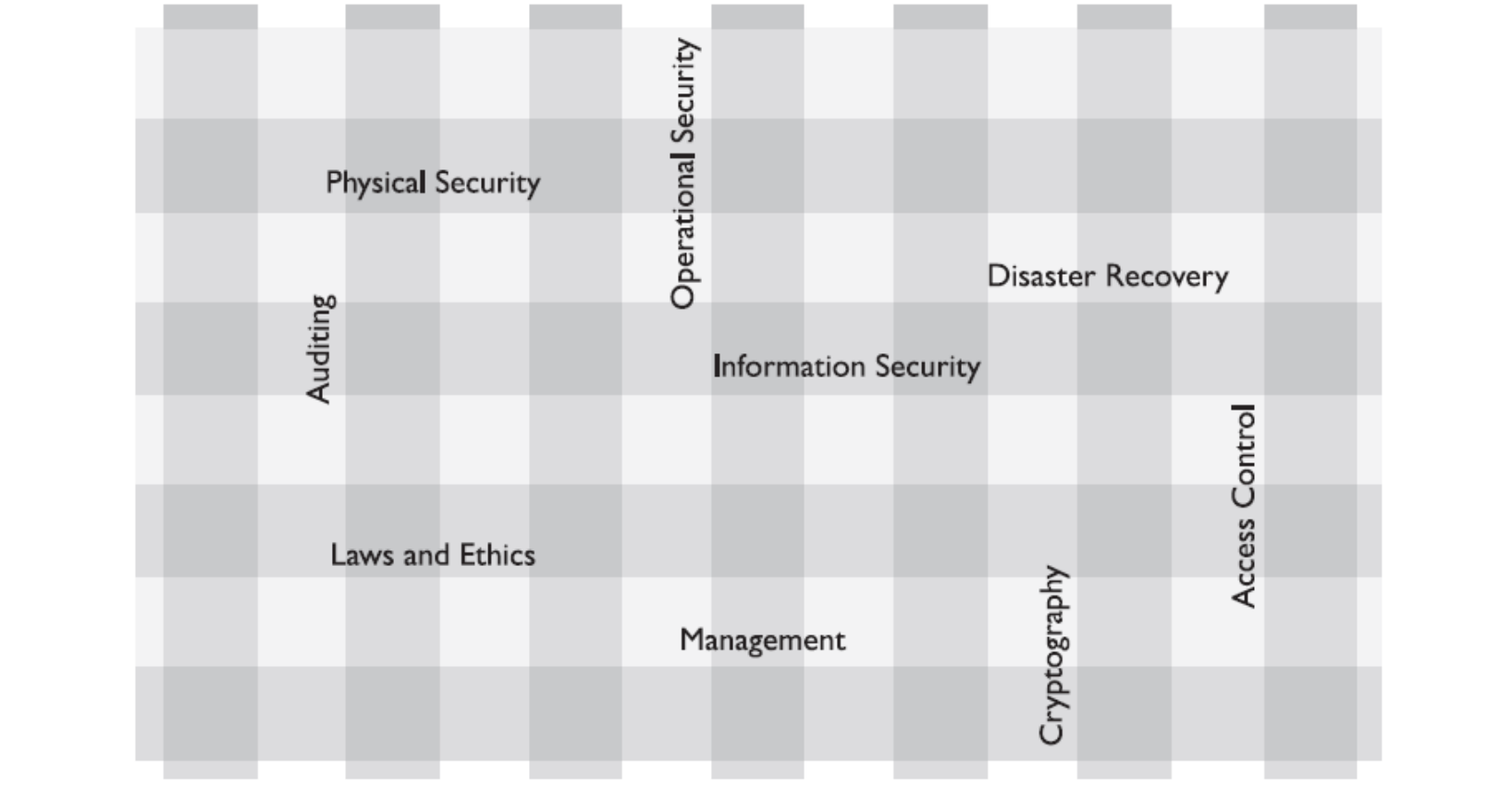
Capacité à traquer et enregistrer les activités du Systèmes d'information et de ses utilisateurs

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**



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.

Les enjeux de la sécurité

- **Comment se protéger ? – Sécurité Définitions**
  - **Exposition**

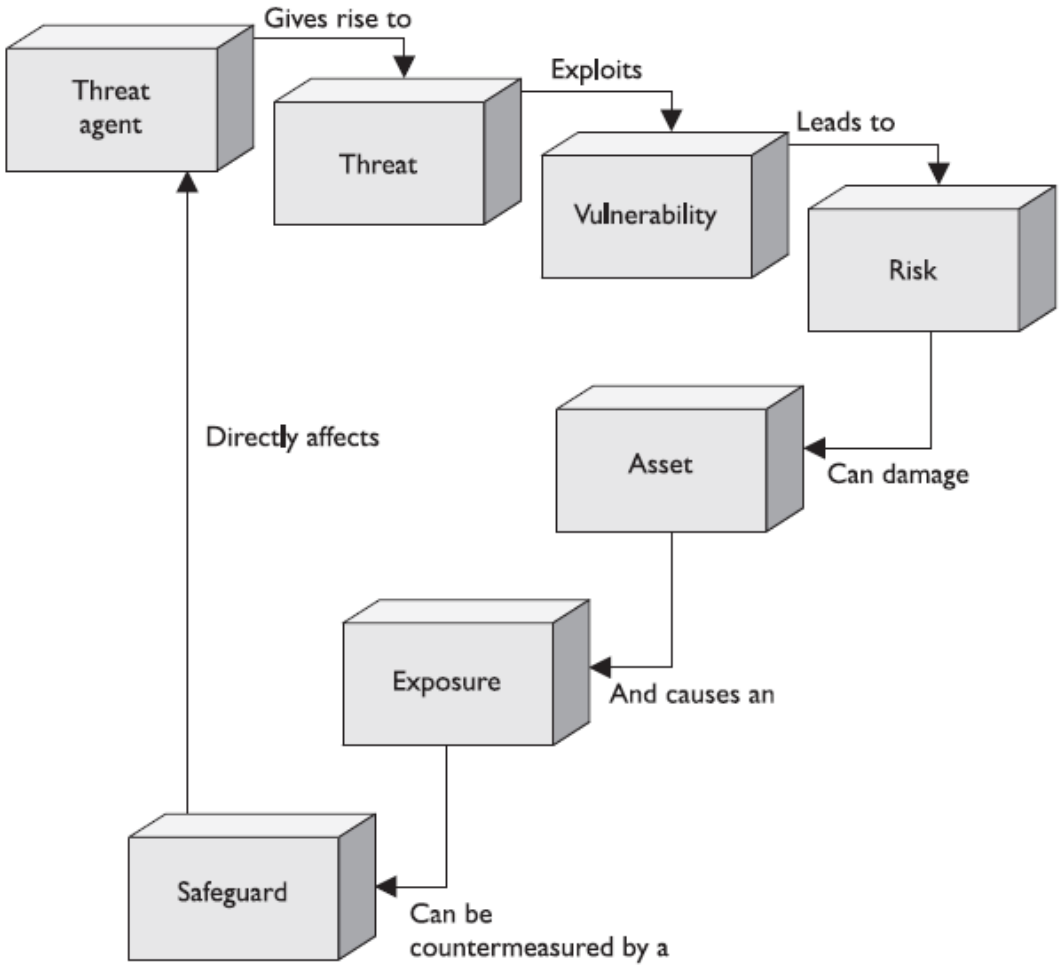
    Ensemble d'éléments du SI exposés à une menace.

  - **Contremesure**

    Elément mis en place permettant de réduire le risque potentiel.

Les enjeux de la sécurité

- **Comment se protéger ? – Sécurité Définitions**



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

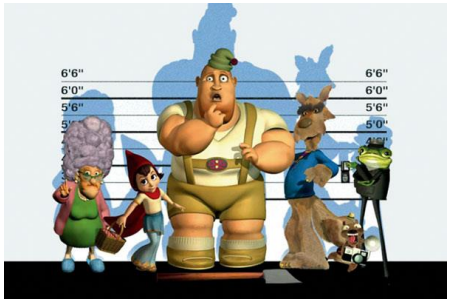
- ARP Spoofing / DNS Spoofing
- TCP Flooding / TCP Session Hijacking
- XSS / Bufferoverflow

Comprendre les attaques

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

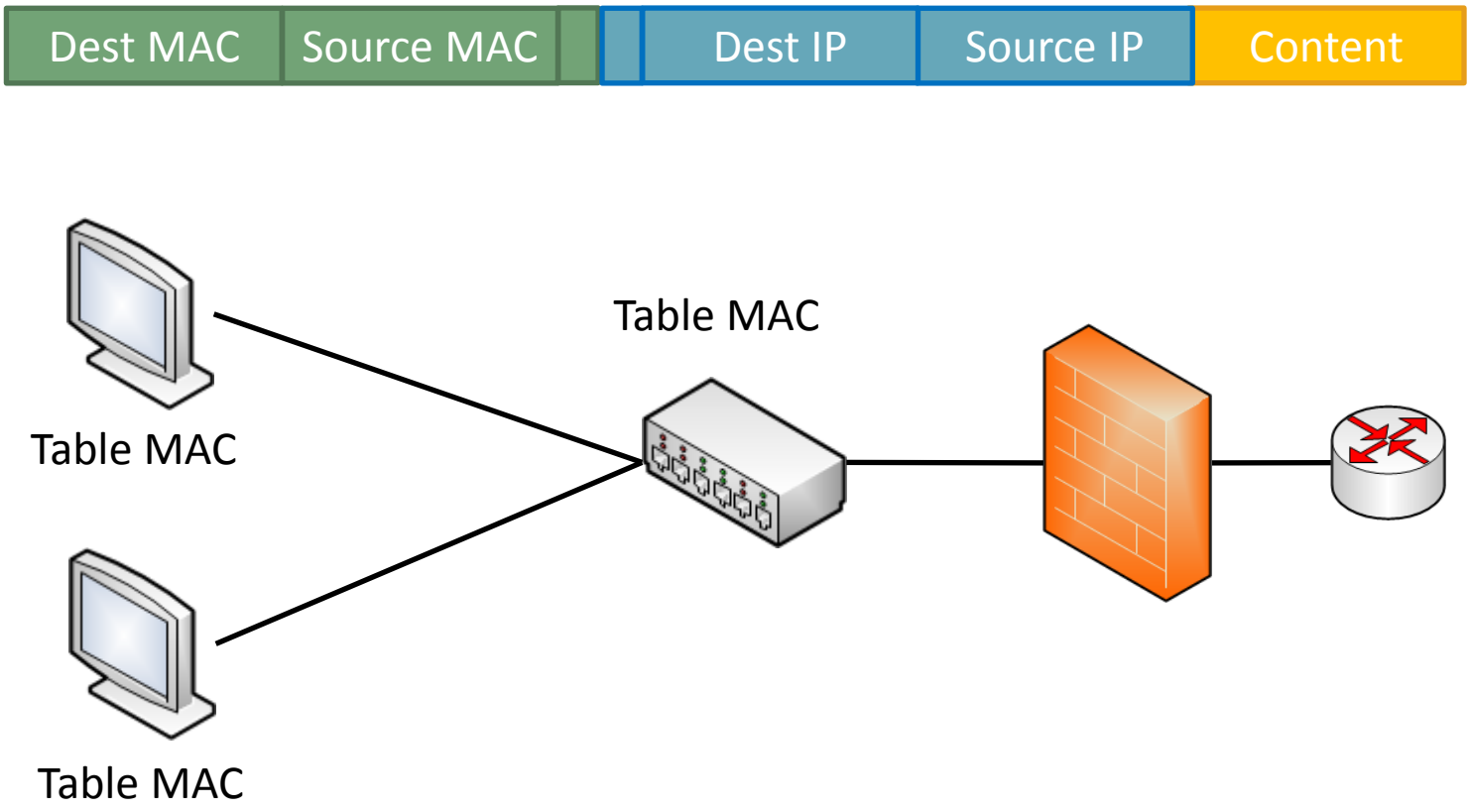
Les enjeux de la sécurité

- **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



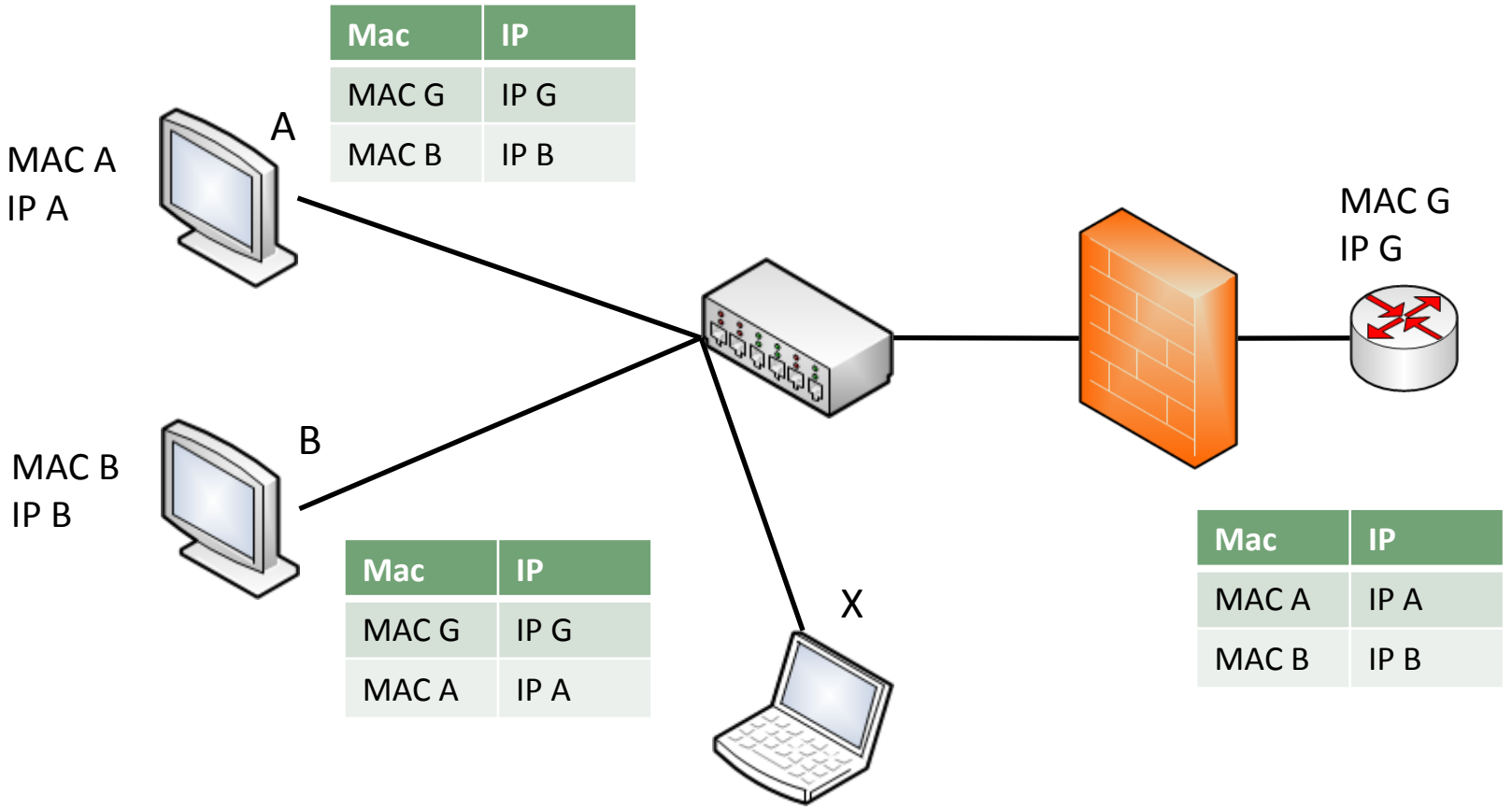
Les enjeux de la sécurité

- **ARP Spoofing**



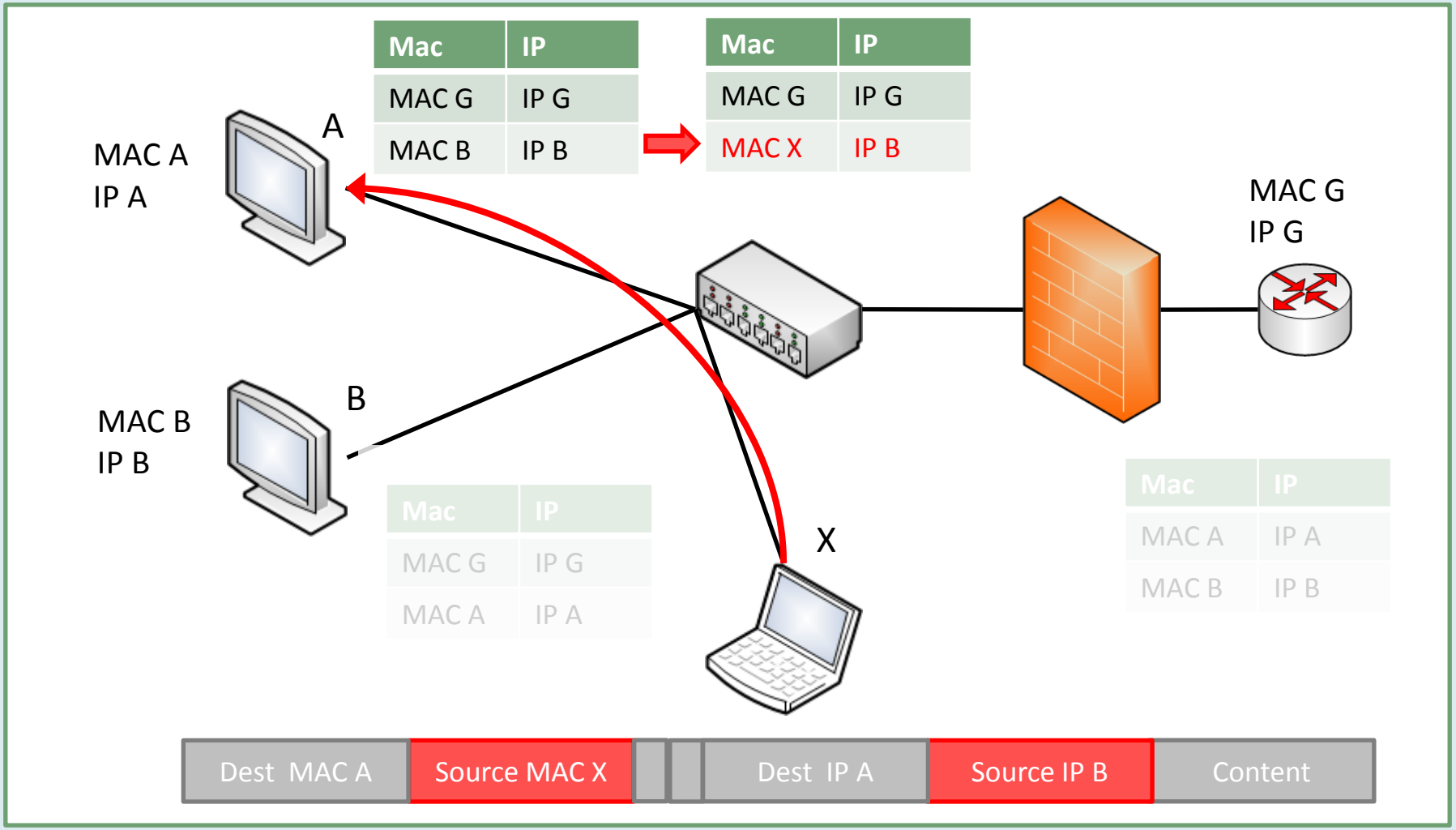
Les enjeux de la sécurité

- **ARP Spoofing**



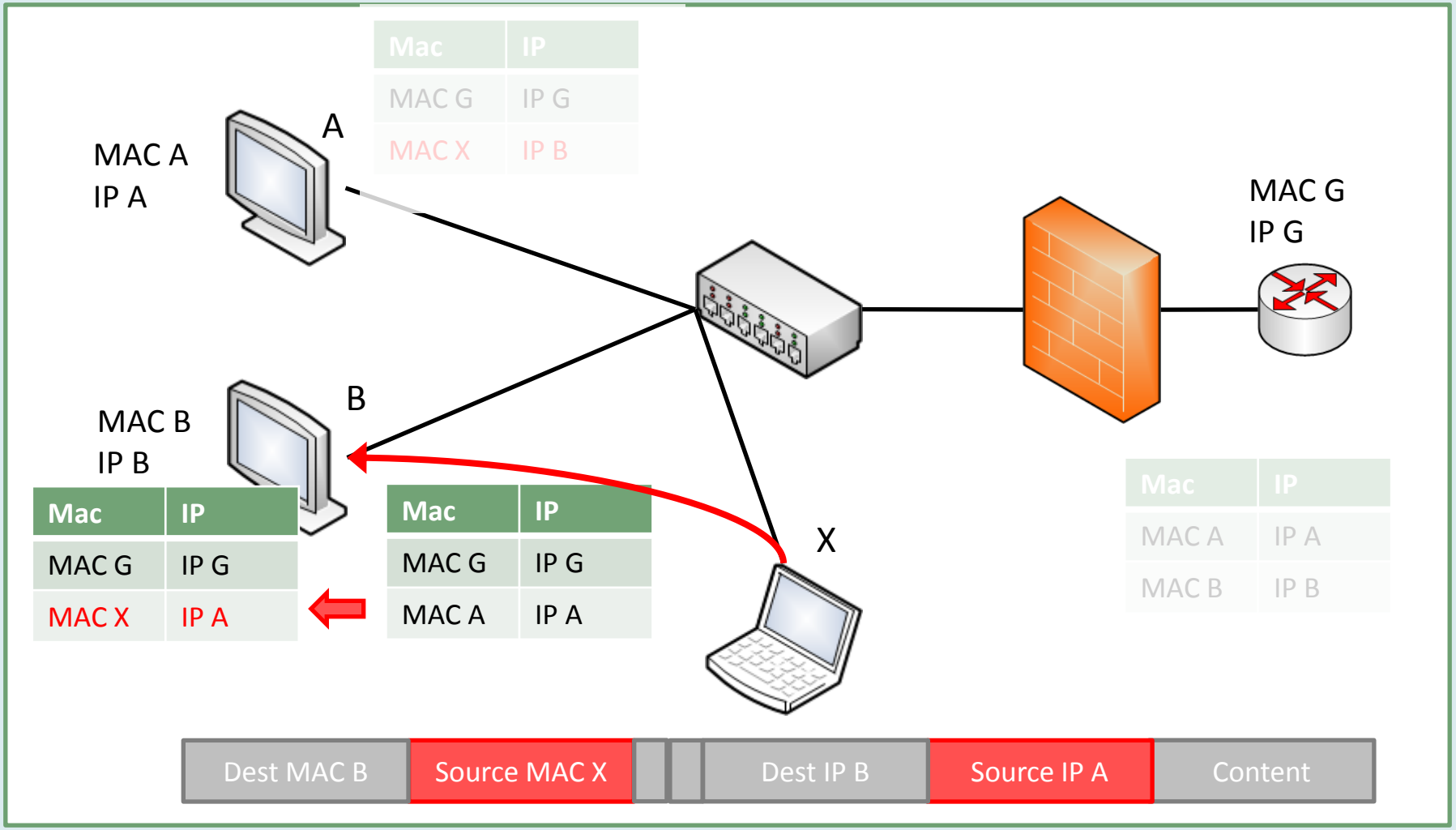
Les enjeux de la sécurité

- **ARP Spoofing**



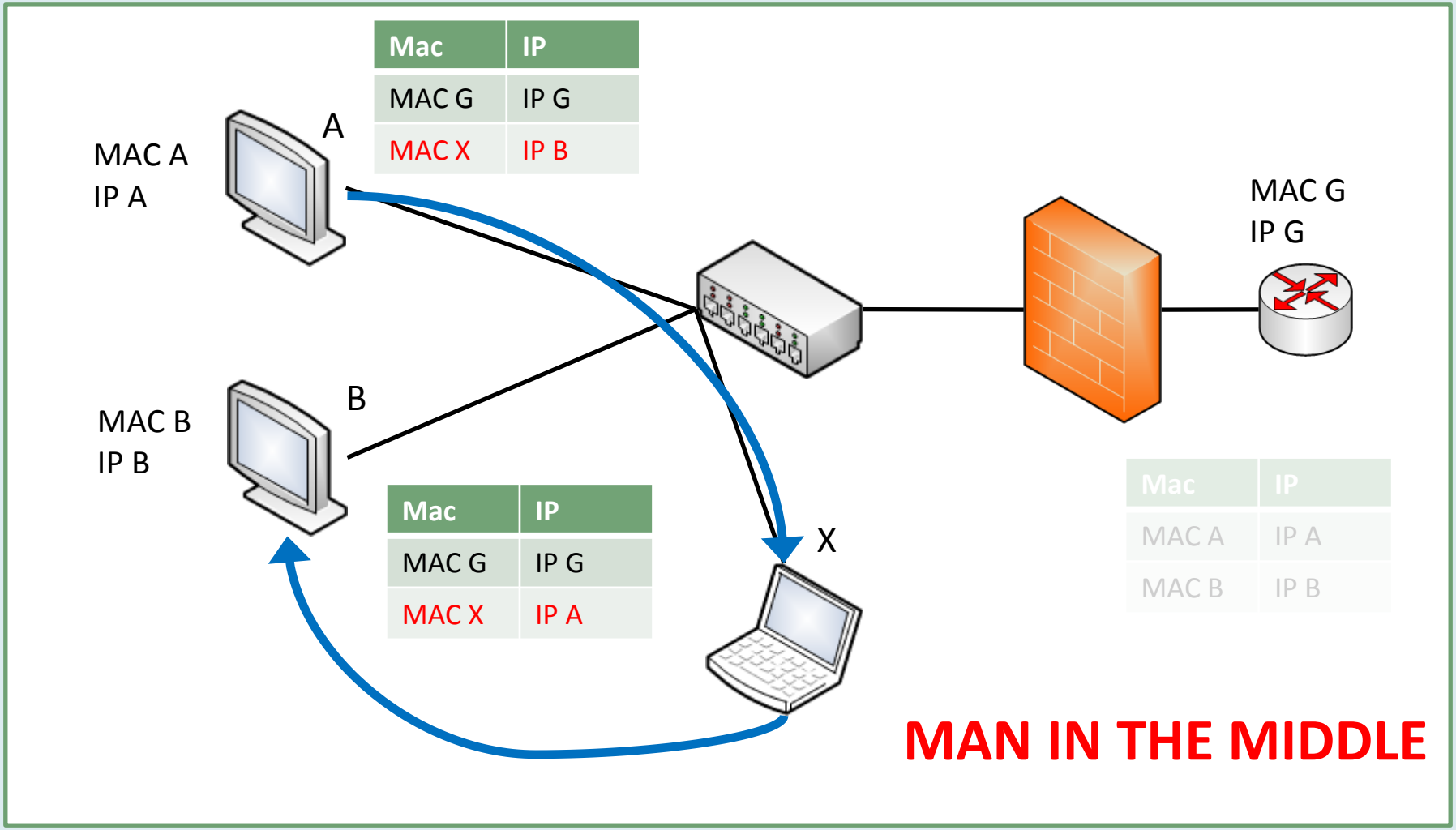
Les enjeux de la sécurité

- **ARP Spoofing**



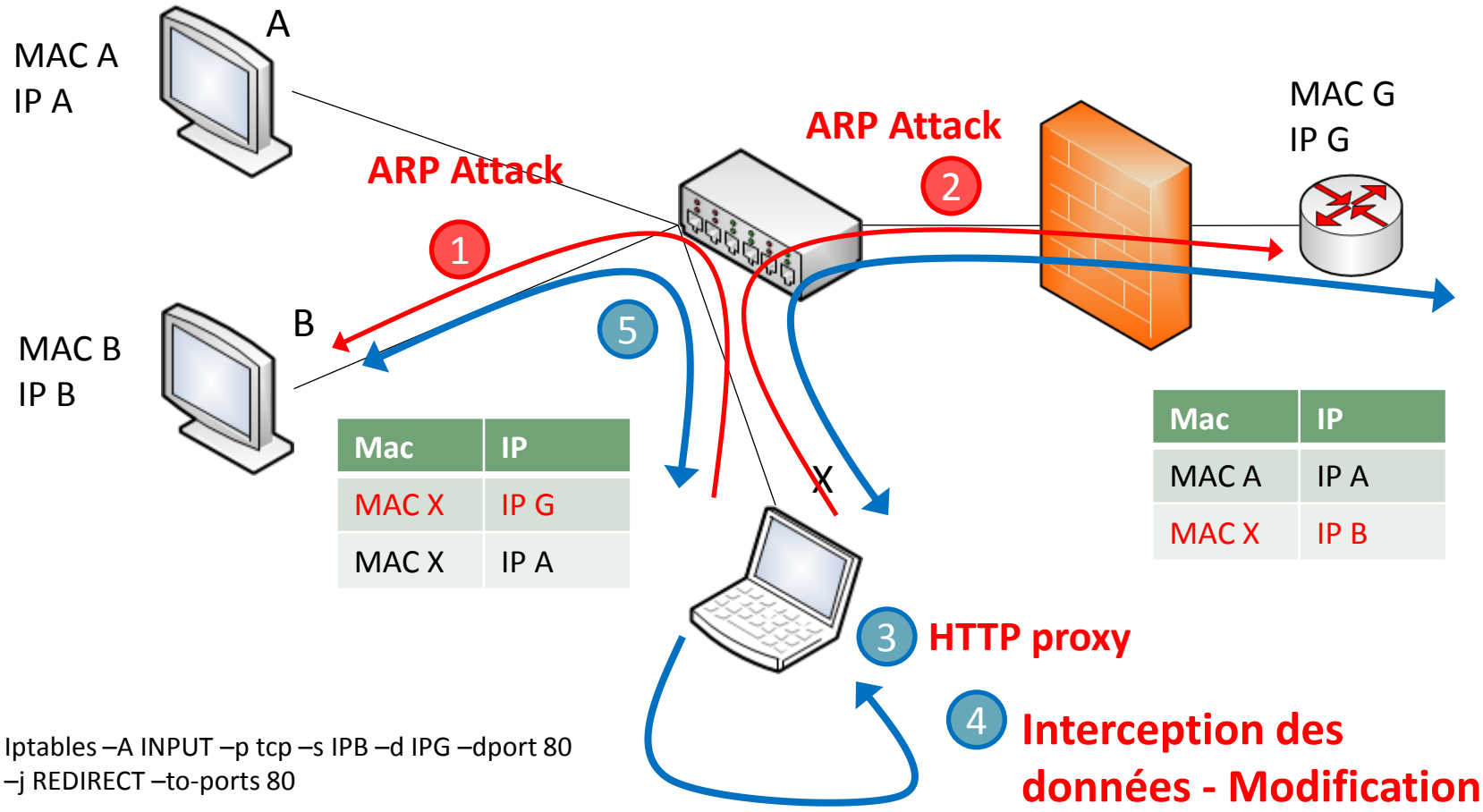
Les enjeux de la sécurité

- **ARP Spoofing**



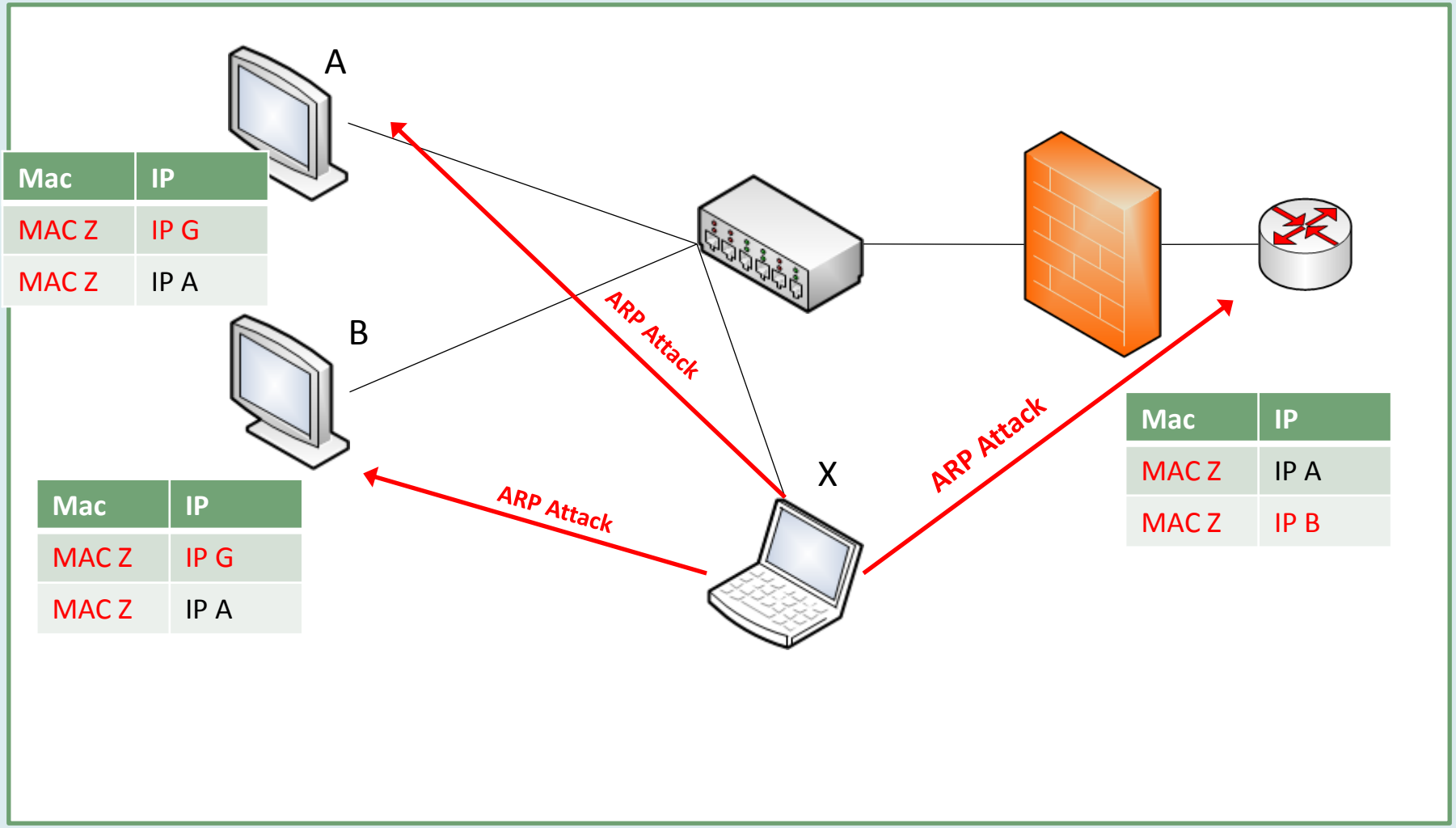
Les enjeux de la sécurité

- **ARP Spoofing**



Les enjeux de la sécurité

- **ARP Spoofing : DOS**

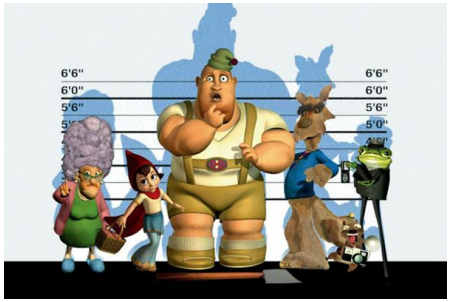


Comprendre les attaques

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

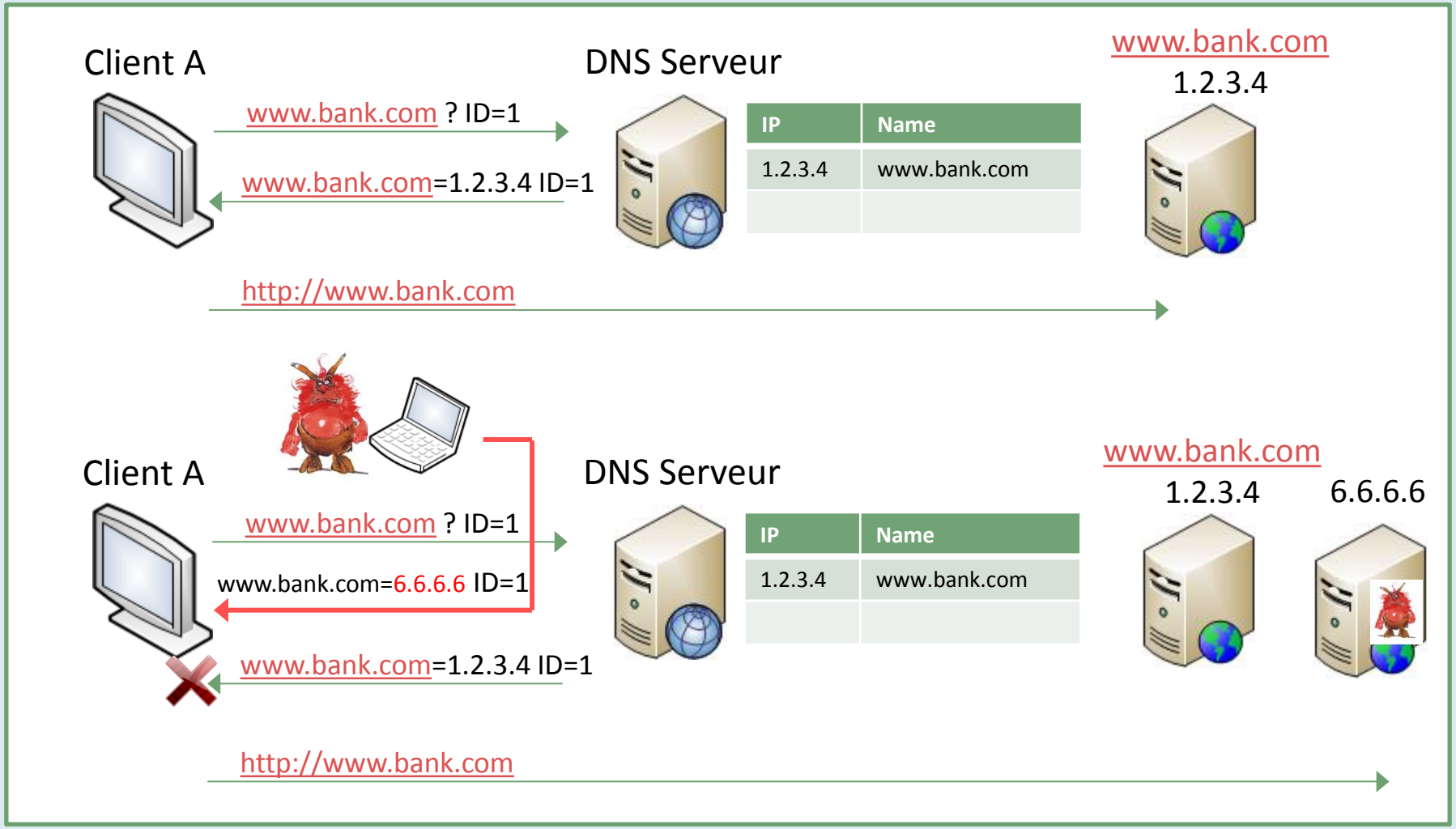
Les enjeux de la sécurité

- **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



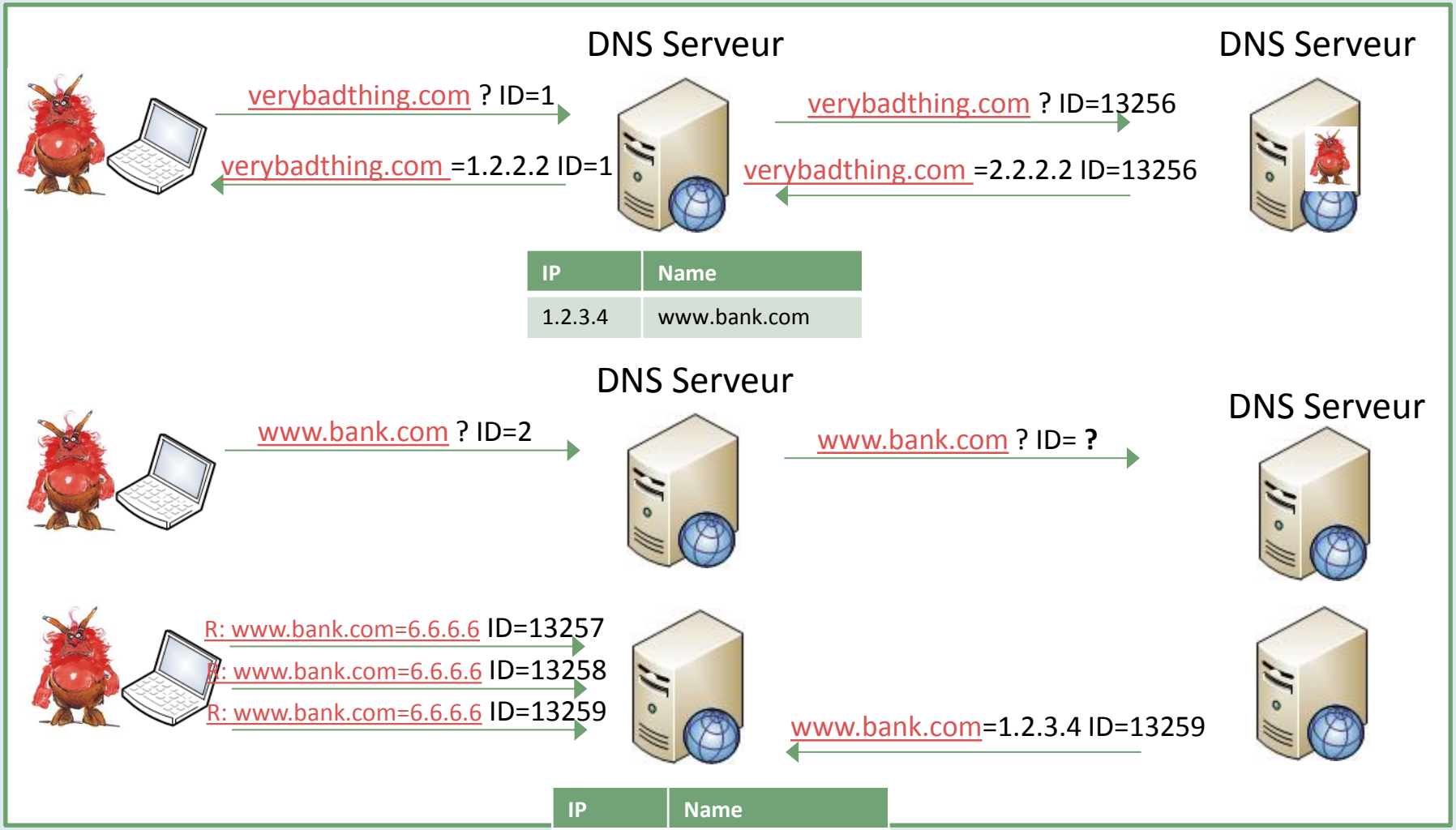
Les enjeux de la sécurité

- **DNS Spoofing : DNS Id Spoofing**



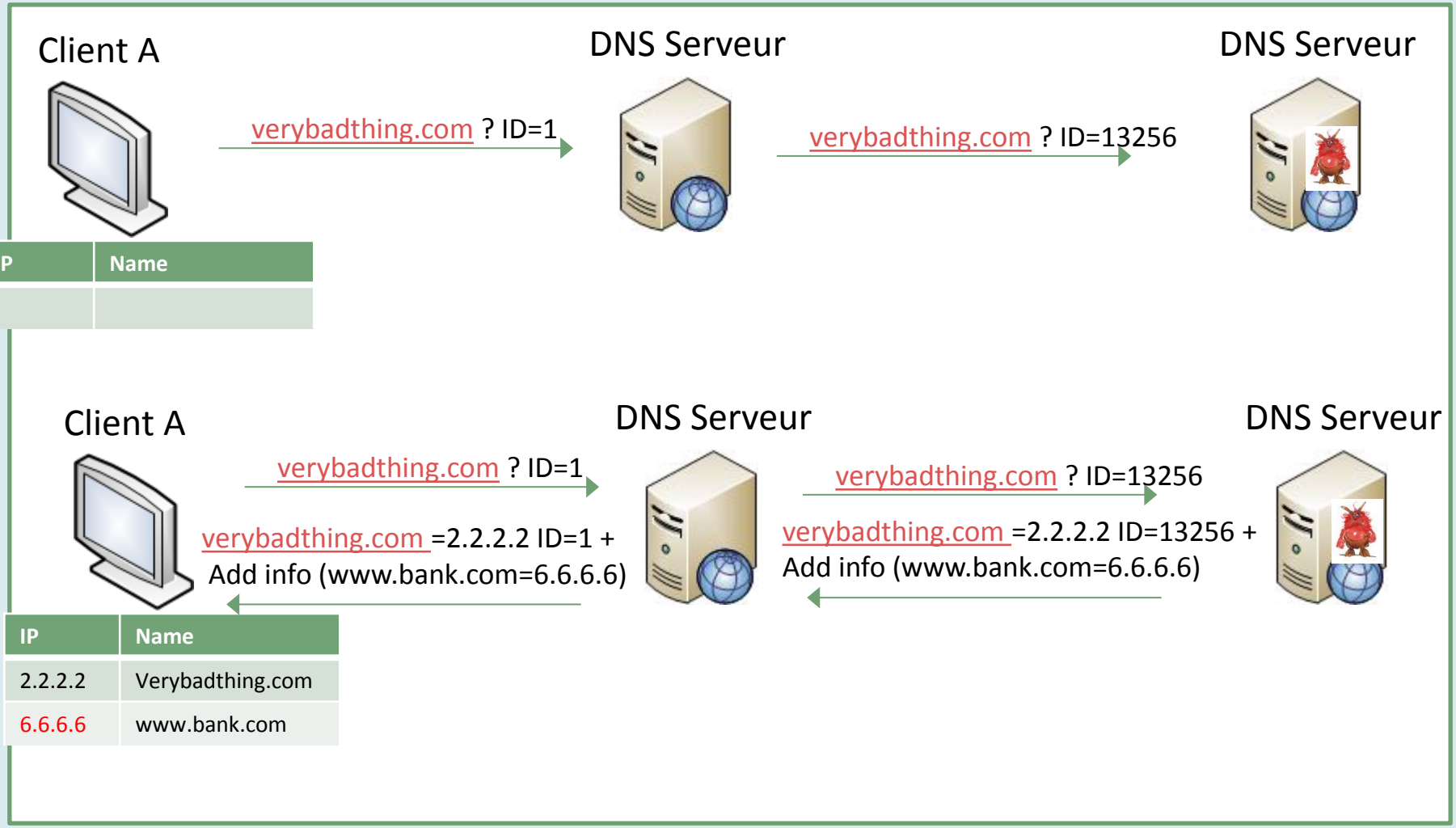
Les enjeux de la sécurité

- **DNS Spoofing : DNS Cache poisoning**



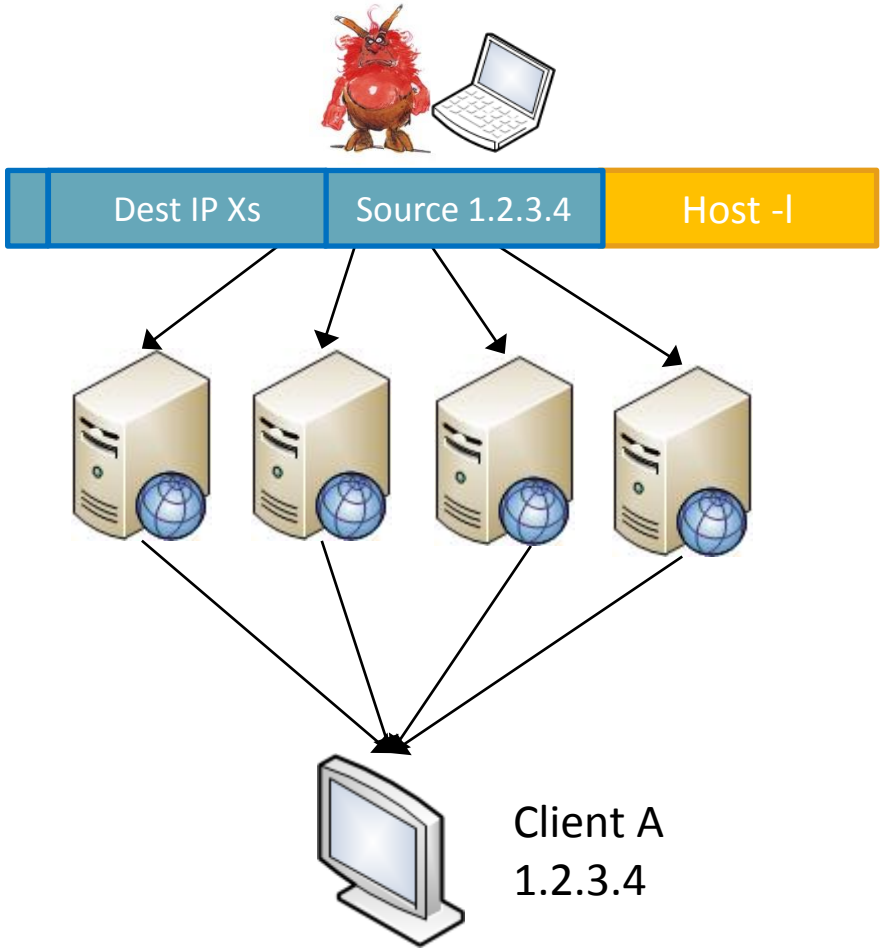
Les enjeux de la sécurité

- **DNS Spoofing : DNS Cache poisoning**



Les enjeux de la sécurité

- **DNS Spoofing : DOS using DNS**



Taille de la requête
27 octets

Facteur * 10 pour chaque requête

Taille de la réponse
312 octets

Comprendre les attaques

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

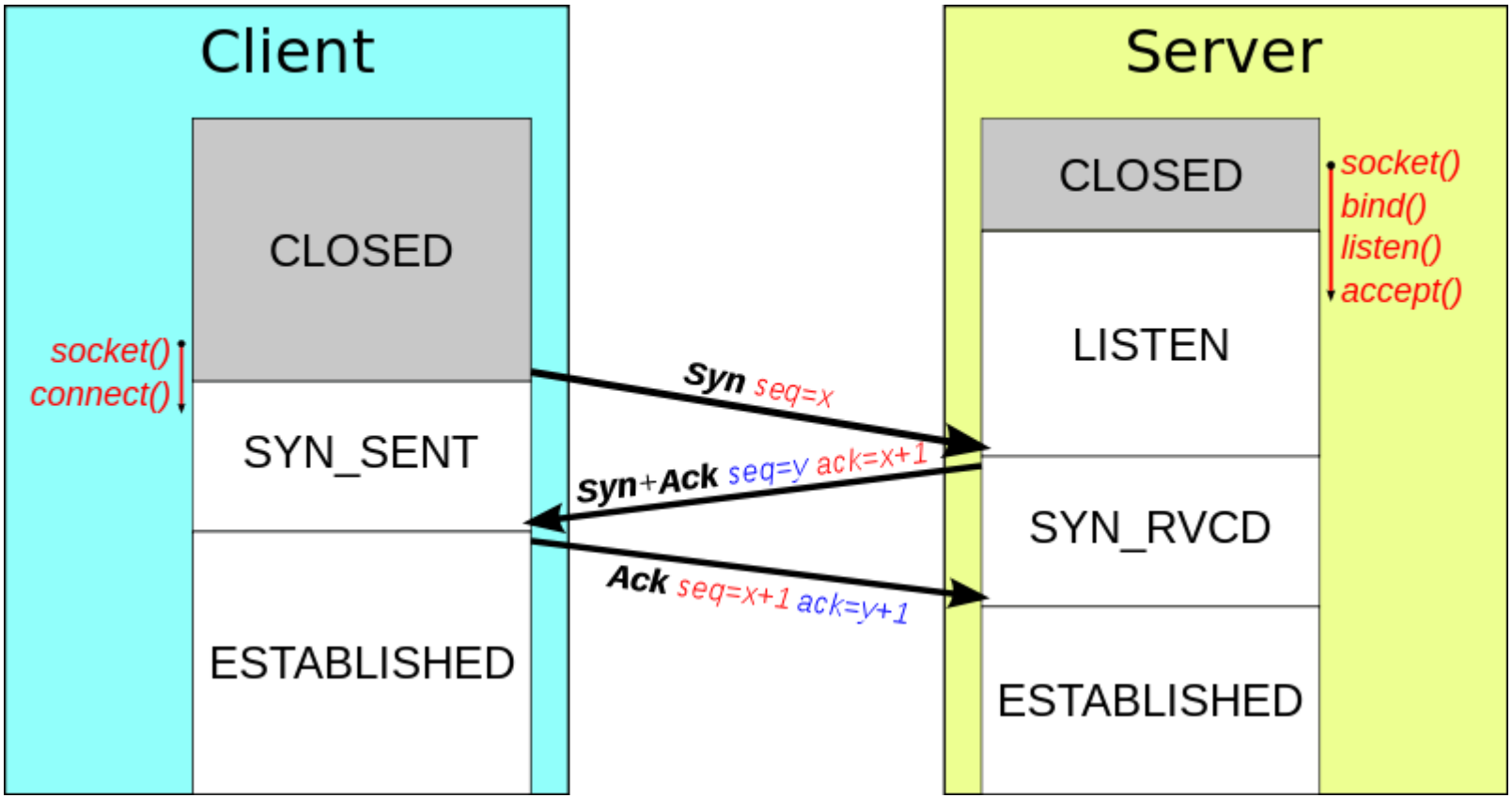
Les enjeux de la sécurité

- **TCP Session Hijaking**
  - 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

Les enjeux de la sécurité

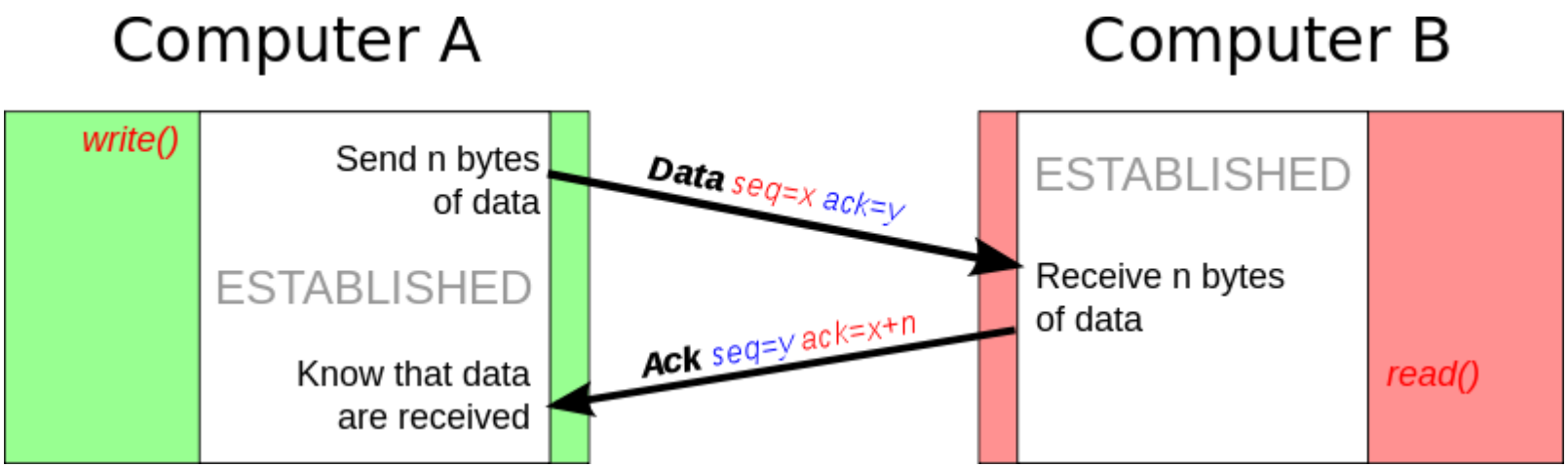
- **TCP protocol**



http://fr.wikipedia.org/wiki/Transmission_Control_Protocol

Les enjeux de la sécurité

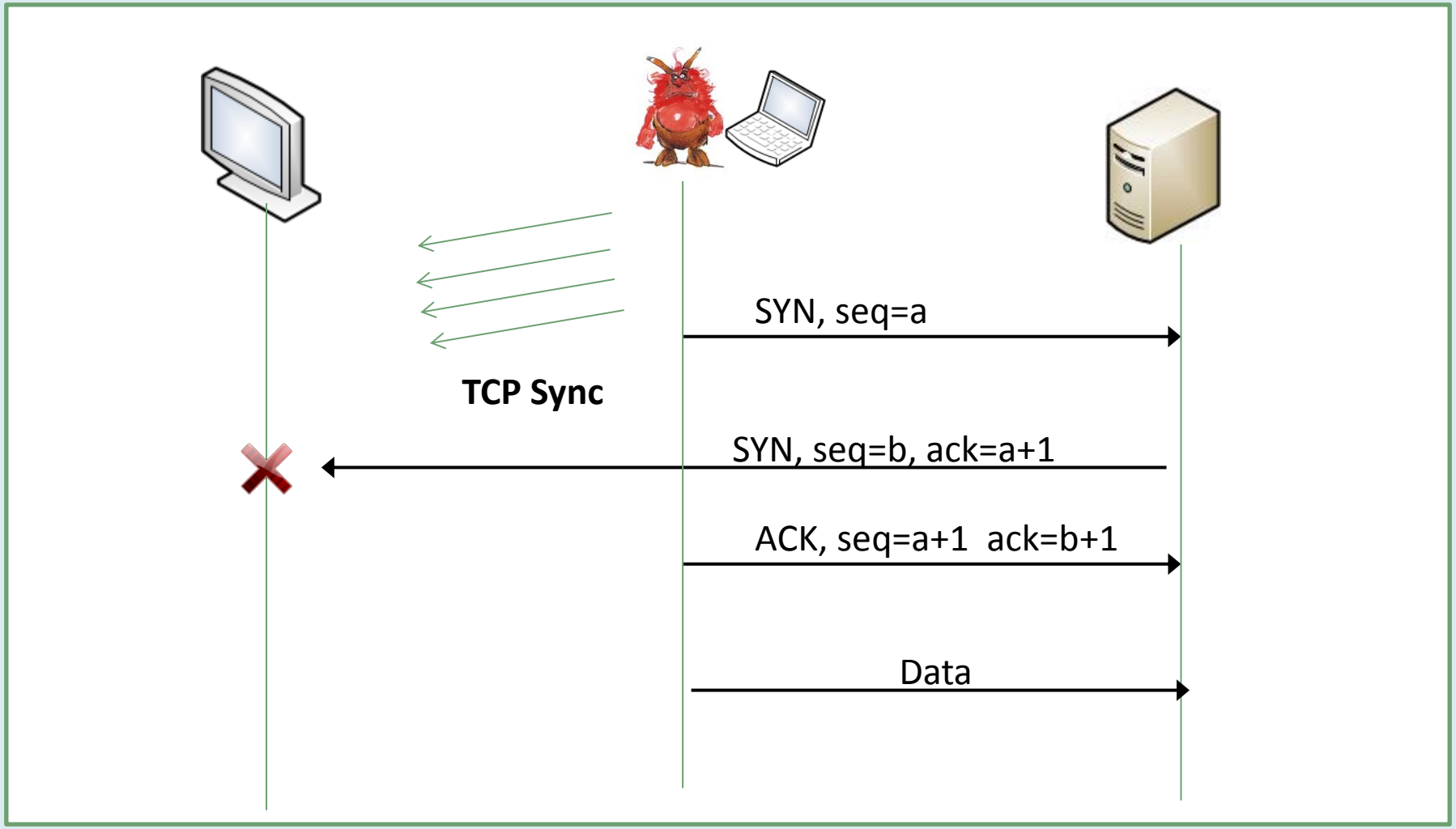
- **TCP protocol**



http://fr.wikipedia.org/wiki/Transmission_Control_Protocol

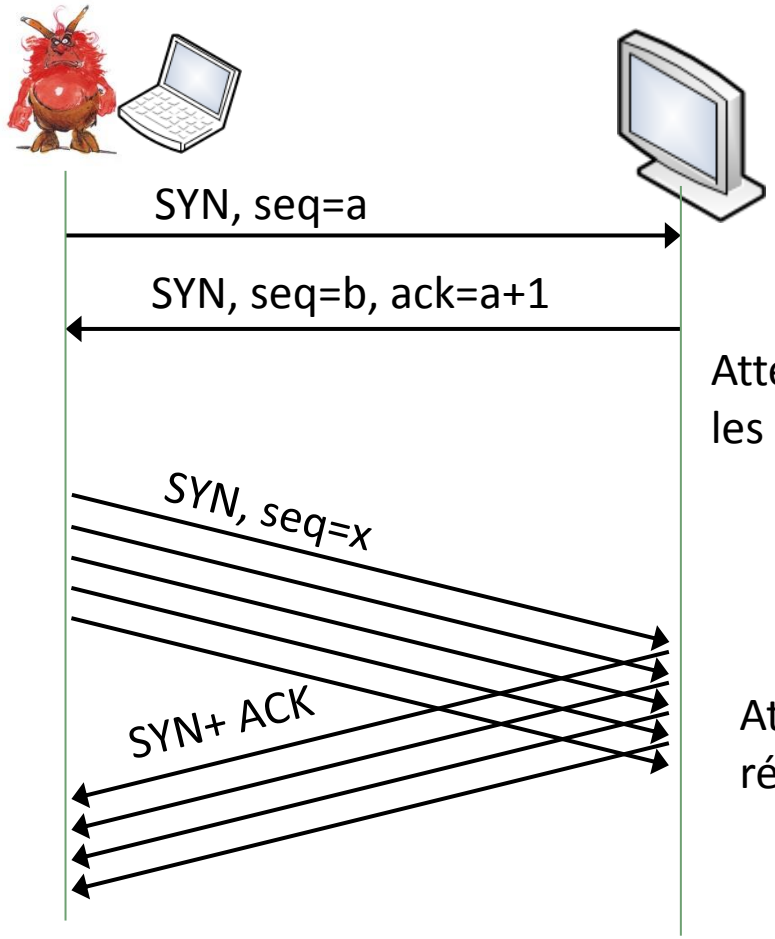
Les enjeux de la sécurité

- **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-persistant
    - 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**

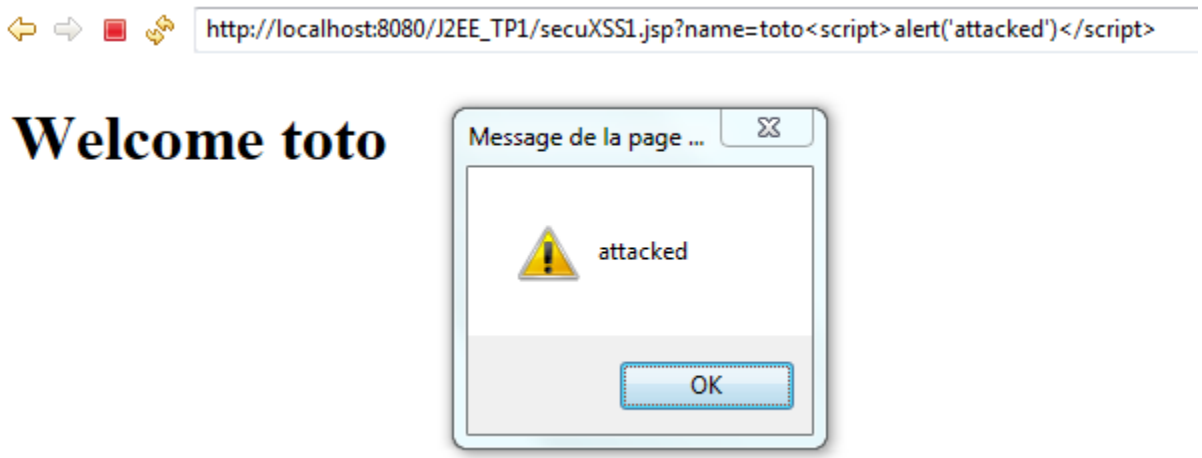
```
<%@ page language="java" contentType="text/html;
    charset=ISO-8859-1"
    pageEncoding="ISO-8859-1"%>
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
        "http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<meta http-equiv="Content-Type"
    content="text/html; charset=ISO-8859-1">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

Les enjeux de la sécurité

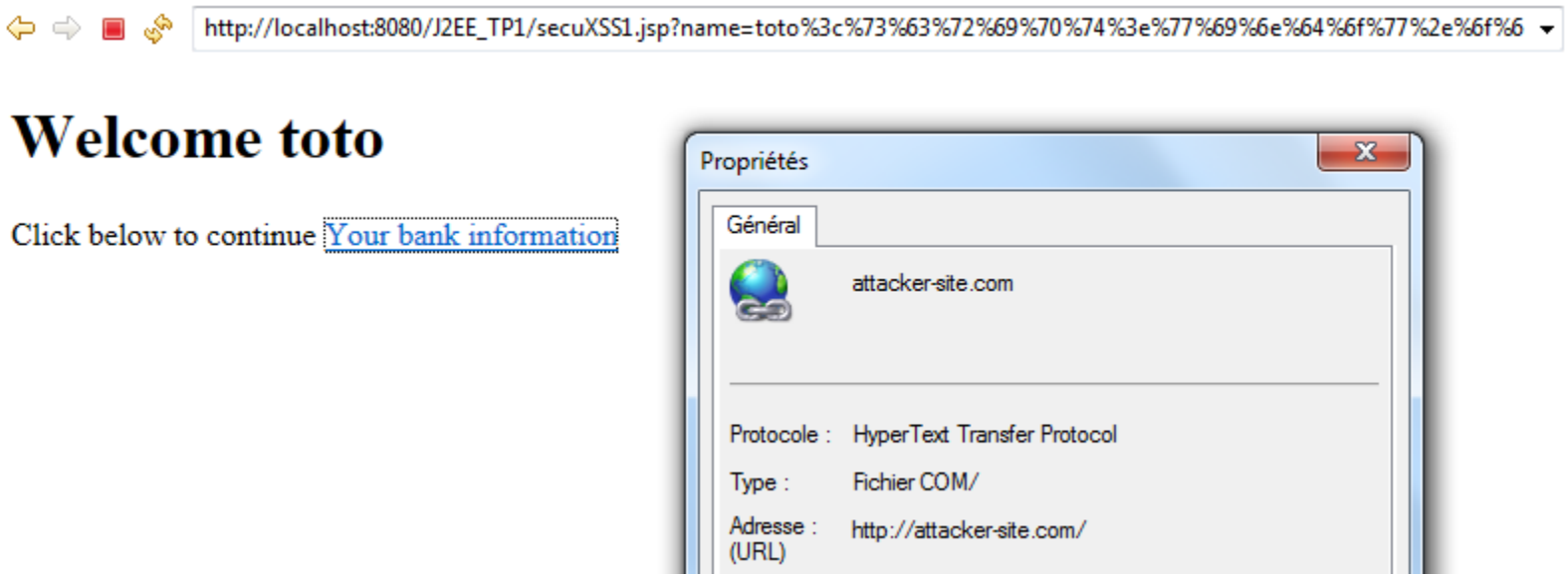
- **XSS non persistant**



Les enjeux de la sécurité

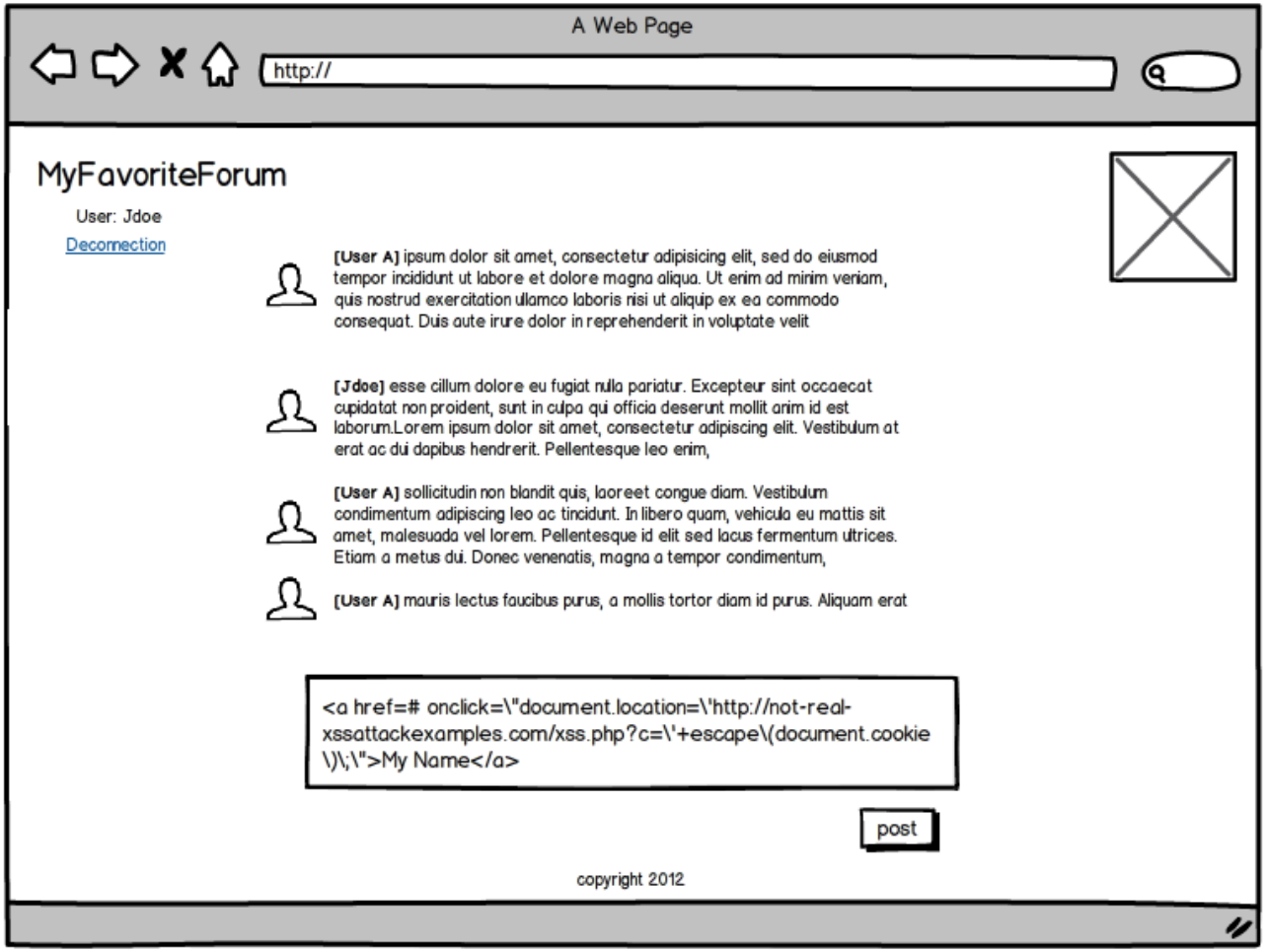
- **XSS non persistant**

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>



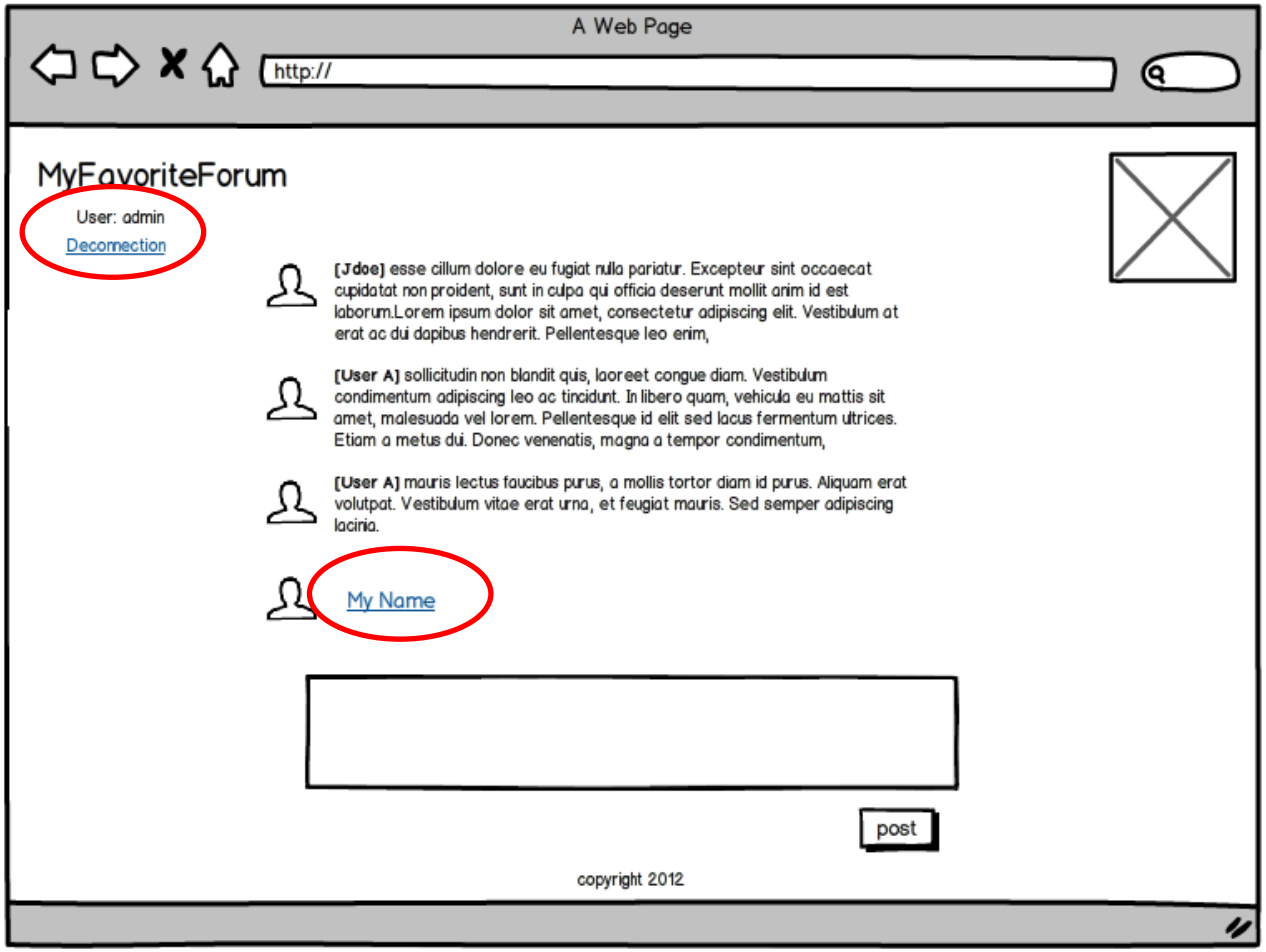
Les enjeux de la sécurité

- **XSS persistant**



Les enjeux de la sécurité

- **XSS persistant**



Comprendre les attaques

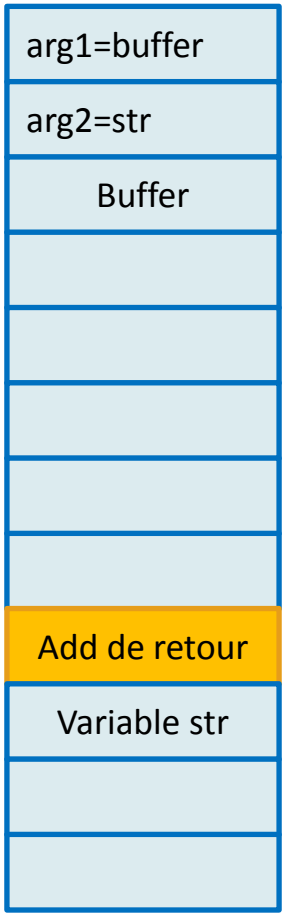
- ARP Spoofing
- DNS Spoofing
- TCP Flooding / TCP Session Hijacking
- XSS
- Bufferoverflow

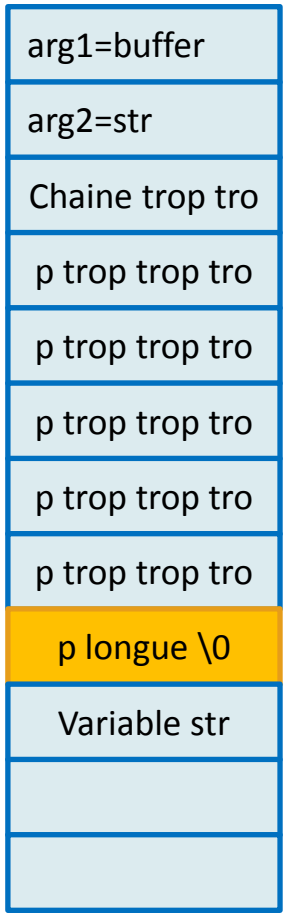
Les enjeux de la sécurité

- **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**





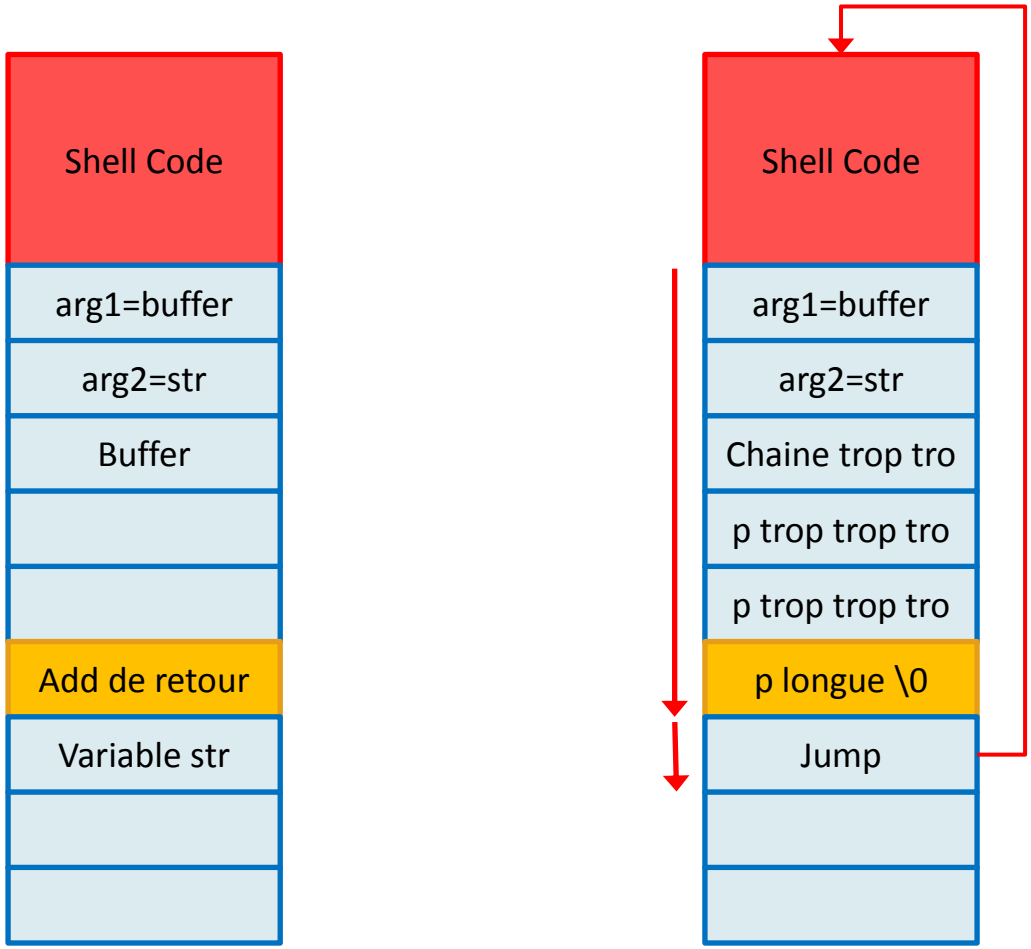
Exécution de la commande strcpy()

Exécution de la commande

Puis exécution du code dans str

Les enjeux de la sécurité

- **Buffer Overflow**



Les enjeux de la sécurité

Questions ?