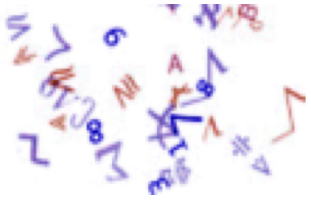
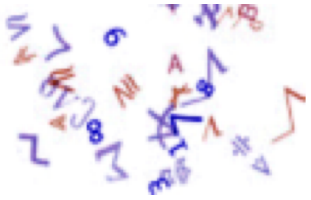


Information System Security

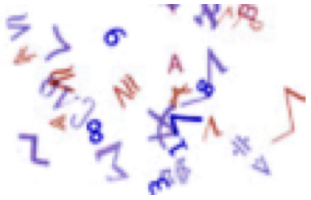
Ph. Jaillon

École des mines de St-Etienne



What is security?

- The state of being free from danger or threat
  - **Procedures** followed or **measures** taken to ensure the security
  - Security is more than 80% of managment and less than 20% of technologies



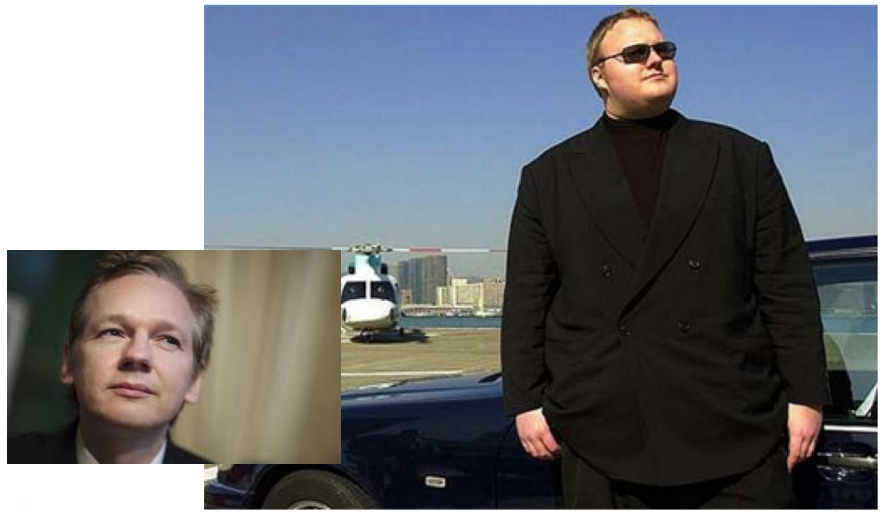
What is cyber-security?

- Ensuring security for all computers and networks supported activities

Every things used and done today!

  - From personal to industrial or state critical applications
    - your smart lock, a nuclear power plant…
  - It impact objects, communications, privacy, command, control…

Press review



2010 - 2012

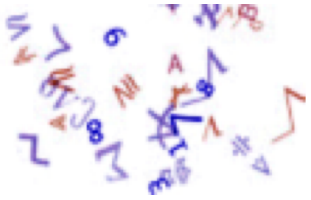
- Kerviel, Wikileaks, STUXNET, Hadopi …
- Comodo and Diginotar CA X509 compromised
- LulzSec and Anonymous
- MegaUpload,
- First Android malwares…
- First privacy leaks (iOS: 12 M, LinkedIn : 5.8M)

Press review

- 2013
  - Edward Snowden and the NSA
    - ➢PRISM : secret agreements with major operators
    - ➢Influence of the NSA on cryptographic standards
  - In short, unlimited means to do everything they wish
  - All knew it, but no one wanted to believe it

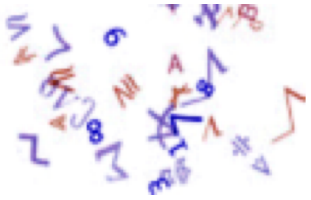
Press review

- 2014 -2016
  - More data leaks exposed: eBay, Dropbox, Yahoo…
  - First car, first TV operator (TV5 Monde) hacked
  - Sony hacked (100TO of corporate data exposed)
- 2017 - 2020
  - WannaCry and Petya: targeted ransomware campaign
  - IoT Security is a big challenge (Philips HUE, babyPhone, smart locks…)
  - Meltdown and Spectre: all computers in the world impacted
  - More cloud data leak: Amazon S3 Buckets Expose Data of Netflix, TD Bank…



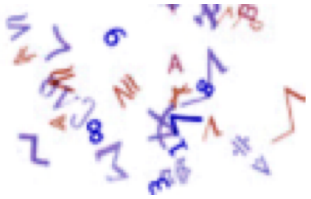
Tendencies

- Evolution of threats:
  - Criminal activities
  - Cyber-war, cyber-activism
  - Generalized Communications Monitoring
- New targets:
  - Phones, industrial systems, GAFA, Cloud
- New challenge:
  - Respect for privacy



Information System

- Today, all sectors of activity are very dependent on their information system.
  - Example: Sony, Orange, Aréva, the school ...
- It is everywhere
  - Procedures, humans, equipment, infrastructure, cloud
- It is essential
  - It must be permanently available, it contains sensitive information …

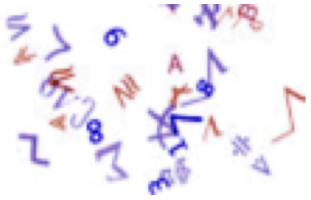


Report

- Importance of all the elements of the Information System for our economic world.

It must be protected.

- It is necessary to counteract all eventualities.
  - From earthquake to internal clumsiness



Remember

(Cyber-)Security must protect

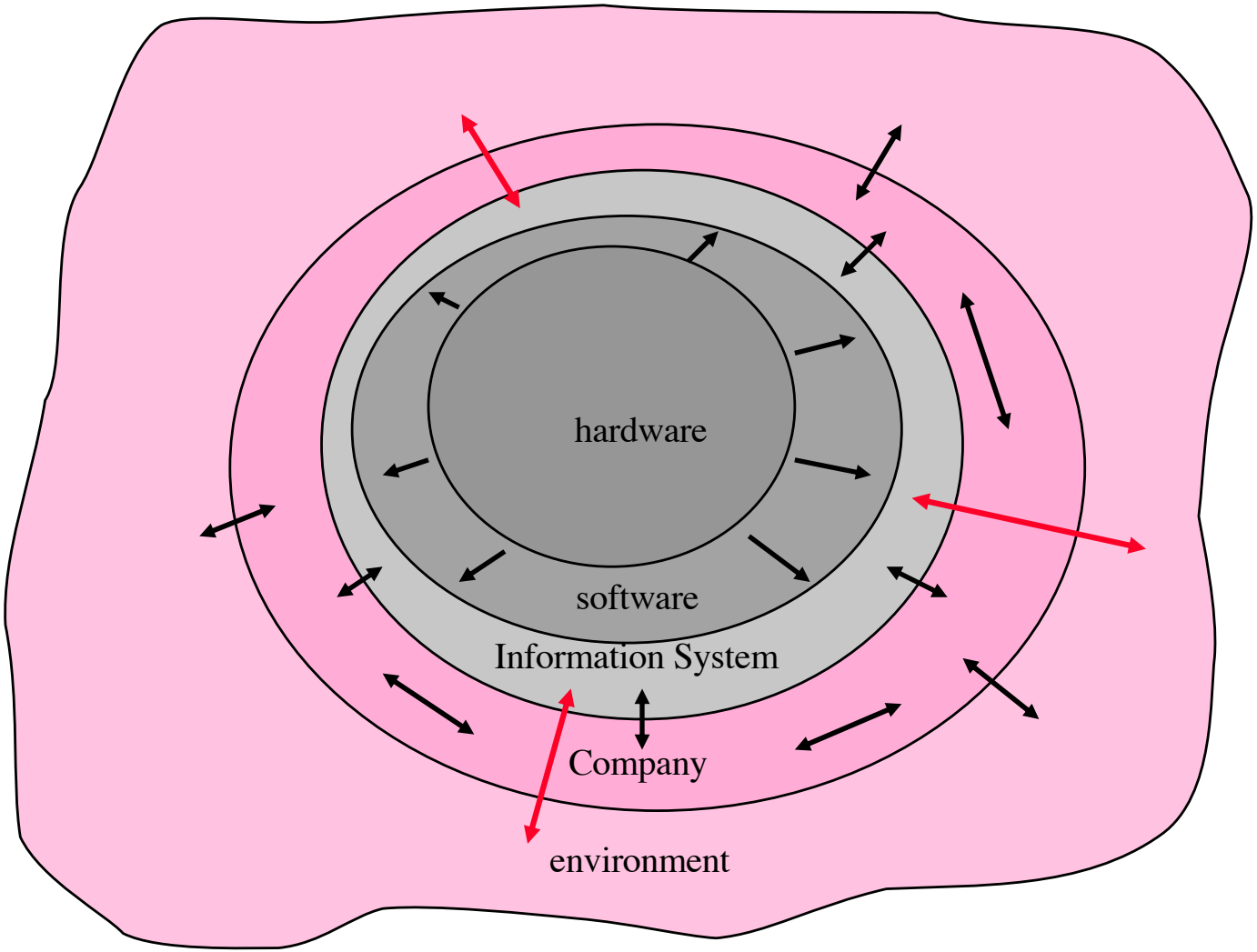
Disponibility

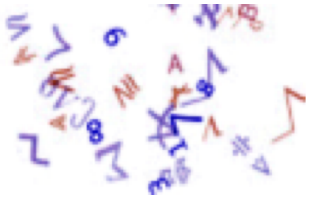
Integrity

Confidentiality

of every things in your system

Information System

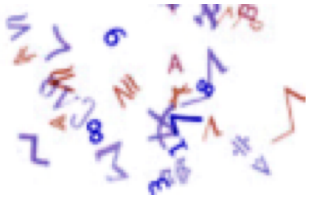




Security of an Information System

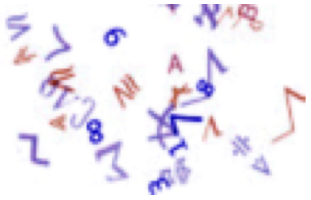
- The level of security achieved is that of the weakest element.
  - Hardware, Software, Network…
    - ➢Bugs, misconfigurations…
  - Procedures
  - Human/users behavior
  - …
- Result in lost of

DISPONIBILITY, INTEGRITY, CONFIDENTIALITY



Risk

A risk arises from the fact that the entity, the company or the organization has *assets*, physical or not, that could be *degraded* or *damaged*, with impairment having *consequences* for the entity.

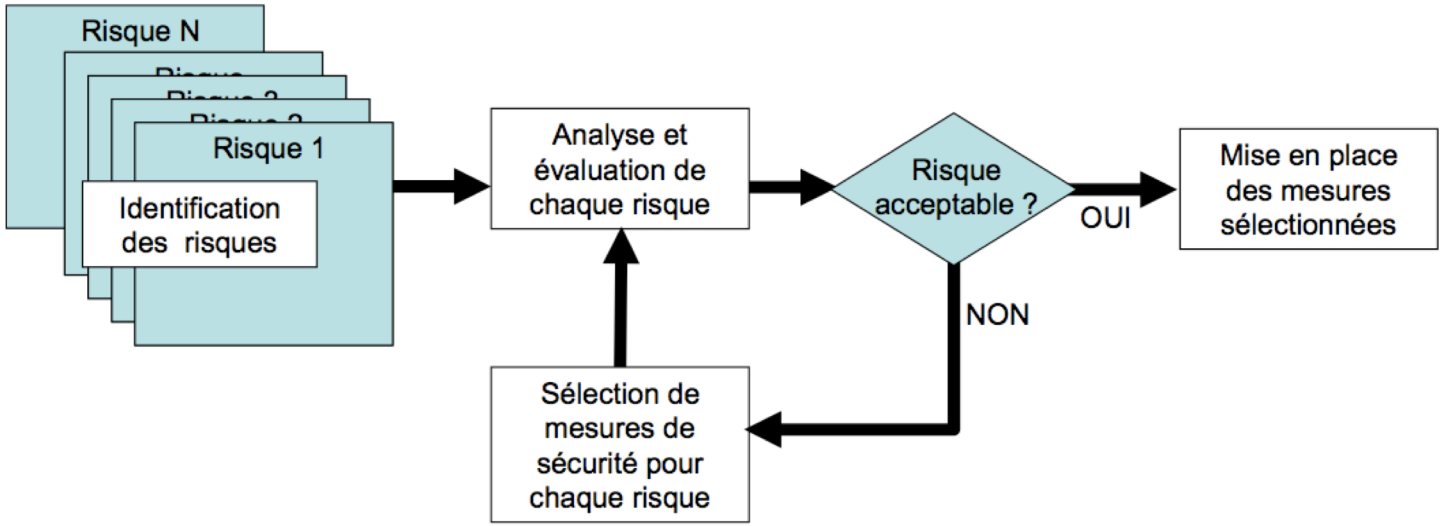


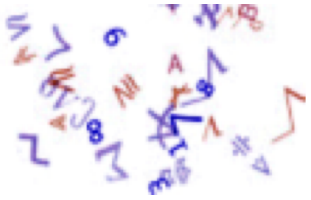
Threats and vulnerabilities

- The notion of threat:
  - Causing damage to assets such as information, processes or systems and therefore to organizations (ISO 27005).
- The concept of vulnerability:
  - Characteristic of a system, object or asset that is a potential point of application for threats.

Risk management

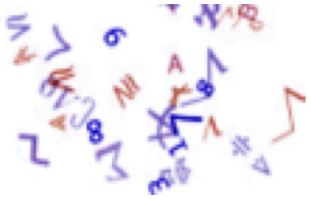
- Risk is the conjunction of an *asset*, a *threat* that may cause damage to that asset, and *vulnerabilities* exploited by the threat to cause the asset to suffer such damage.





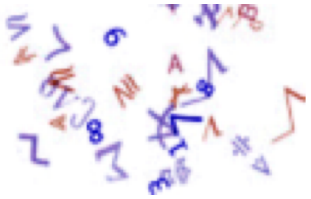
Inventory: Business premises

- Access to buildings
  - Vulnerability, circulation, prevention equipment (theft, fire).
- Access to materials
  - Physical access to computers, contents.
- Access to communications
  - Telephones, computer networks.
  - Internet ?



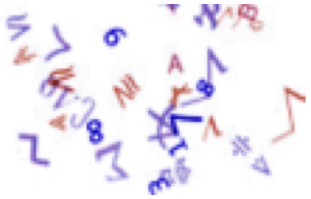
Inventory: People

- The problems are mainly due to errors of manipulation and lack of sensitization (example of viruses)
- Internal malicious activity
- External malicious activity
  - Destructions, theft, ...
  - A very small part through the network



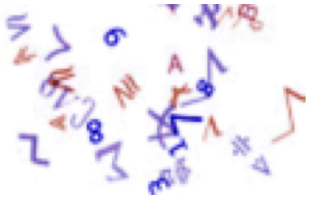
Inventory: The Information System

- Production management
- Customer management
- Personnel management and accounting
- R & D activity
  - Sensitive information
  - Information vital to the company's activity



Inventory: information

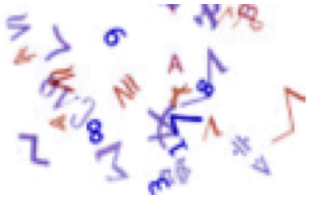
- What information is strategic
- Assess the criticality of the data?
  - Impact of unavailability, disclosure and alteration of information
  - Managing Data Access



Inventory

- Relations with the environment
- Relations with suppliers, contractors, subcontractors
- Imposed technical solutions

- Internet : e-mail, WEB servers …

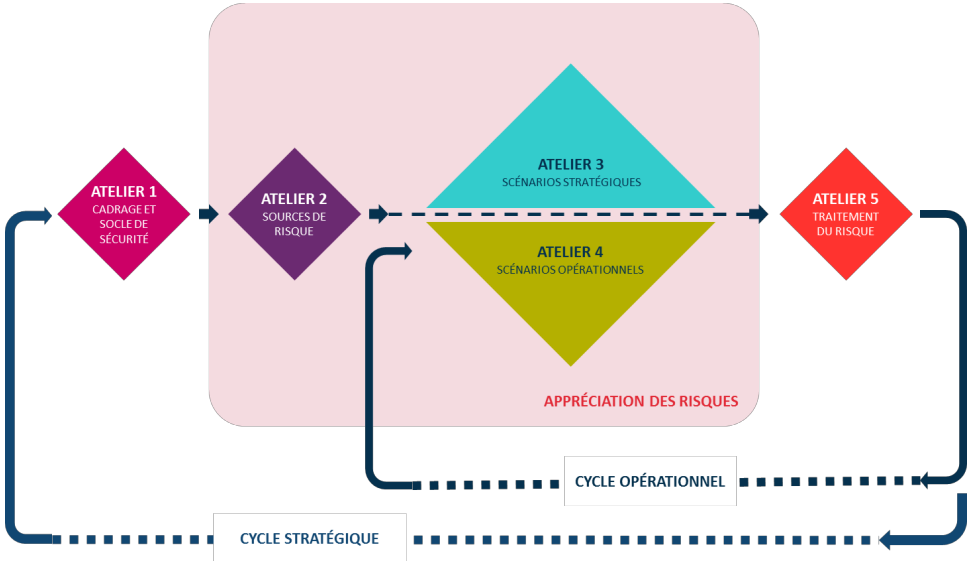


Inventory: don’t forget anything

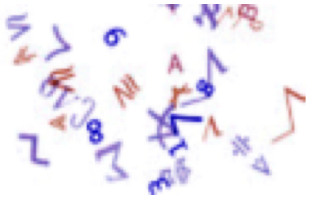
- Methodological tools:
  - EBIOS (anssi), MEHARI (clusif), …
- Criteria and evaluation methods :
  - TCSEC : *Trusted Computer System Evaluation Criteria (EU).*
  - ITSEC : *Information Technology Security Evaluation Criteria (EC 1991).*
  - ISO/CEI 15408-1:1999(E) : *Common Criteria for Information Technology Security Evaluation.*
  - ISO/CEI 27002:2005 : *Information technology - Security techniques - Code of practice for information security management.*
  - ISO/CEI 27001:2005 : *Information technology - Security techniques - Information security management systems - Requirements* (ISO/CEI 27002 enforcement).
  - ISO/CEI 27005:2008 : *Information technology - Security techniques - Information security risk management.*

EBIOS (in brief)

- Method based on 5 workshops,
  1. Framing and security base
  2. Sources of risk
  3. Strategic Scenarios
  4. Operational scenarios
  5. Risk Management



Source: https://www.ssi.gouv.fr/administration/management-du-risque/la-methode-ebios-risk-manager/

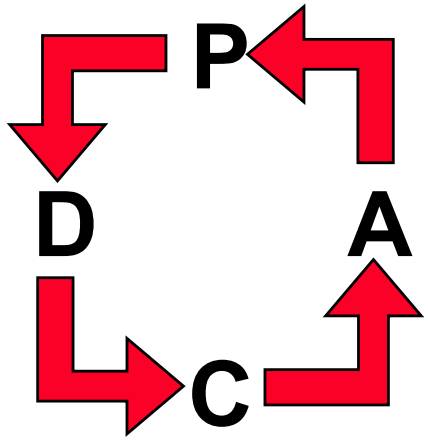


Commun Criteria
Evaluation Assurance Level (EAL)

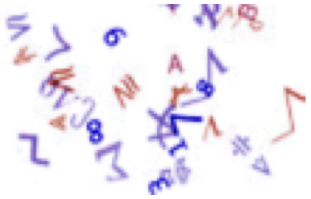
7 levels of assurance:

EAL1 : functionally tested
EAL2 : structurally tested
EAL3 : methodically tested and checked
EAL4 : methodically designed, tested, and reviewed
EAL5 : semi-formally designed and tested
EAL6 : semi-formally verified design and dested
EAL7 : formally verified design and tested

ISO/CEI 27001:2005



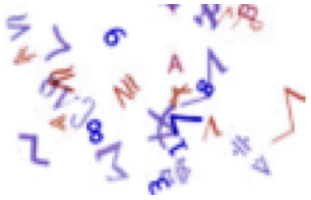
- Information security management systems
  - PDCA model (Plan, Do, Check, Act - Deming Wheel) already used for quality management (ISO 9001)
    - Plan: we say what we do
    - Do: we do what we say
    - Check: we check that it works
    - Act: we make adjustments or corrective actions if required
  - Continuous process improvement
  - ISO 27001 describes what it is essential to take into account at each of these stages



ISO/CEI 27002:2005

- Good Practice Guide from BS 7799-1
- Catalog of security objectives and technical measures to achieve them.
  - 39 objectives, 133 measures.
- The use of ISO 27002 derives from the security requirements expressed by the management system (ISO 27001).
- Examples:
  - Purpose: *user access management*
  - Measures: *user registration*, *privilege management*, *user password management*, ...

This is the new name of ISO / IEC 17799: 2005

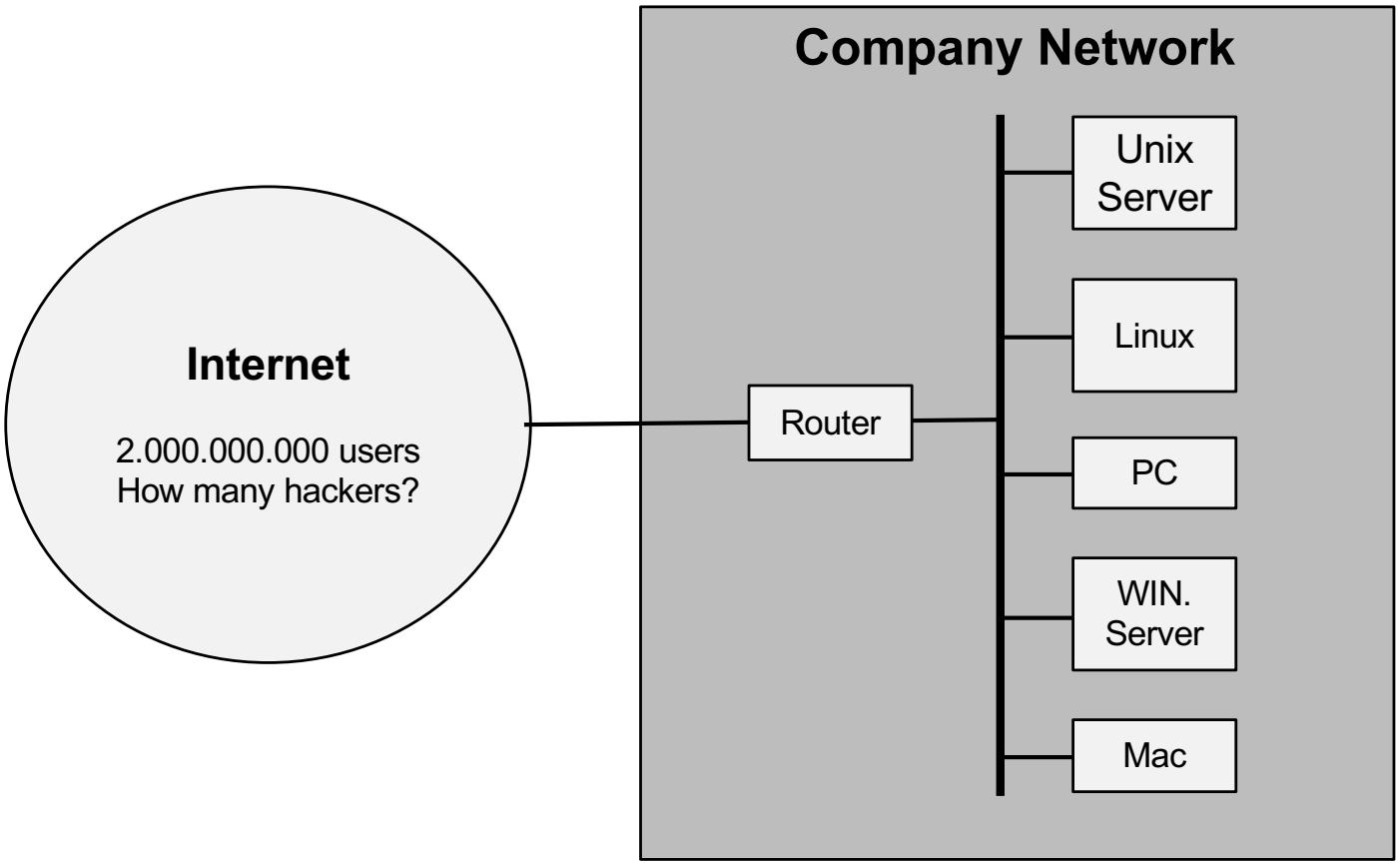


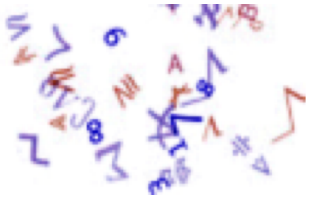
Why do we need Computer Security?

Protecting information, services, infrastructures is essential to any economical activities

- Ensuring availability
  - For infrastructure, services, information...
- Preserving Integrity and Confidentiality
  - For information, communications ...

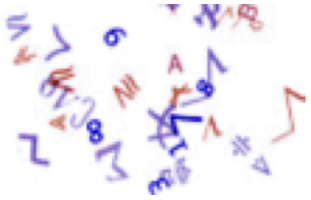
Threats


Company Network
Unix Server
Linux
PC
WIN. Server
Mac
Router
Internet
2.000.000.000 users
How many hackers?



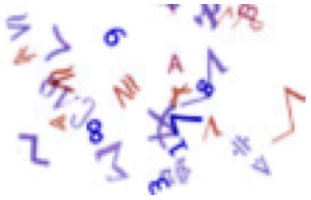
Threats

- Disponibility and Integrity
  - Services interruption
    - Impossible to establish contact with the remote correspondant of your choice
    - Physicaly break communication infrastructure
  - Data modifications
    - Unreadable data
    - Incorrect or false informations
  - Data destruction



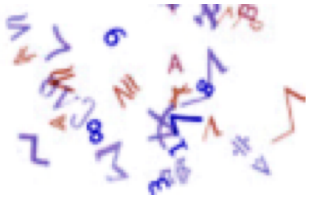
Threats

- Exchange confidentiality
  - Sniffers (on the local network)
  - Forwarders (on a computeur or by routing)
- Remote user authentication
  - Passwords or keys theft
  - Social ingineering
- Exchange integrity
  - Data modification during transit, TCP sessions theft (IP slicing)



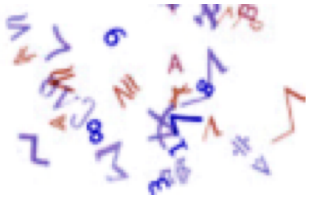
Threats

- Information leak by malicious insider
  - Standard protocols (FTP, HTTP...)
  - “tunneling” (TFTP over DNS)
- Attack by content (program, data)
  - End user is the major risk
    - More by lake of knowledge than illicite practices
  - Virus
  - Trojans
    - Dangerous or *bugged* applications
    - Dialup access software with routing options (connection sharing)
  - Application gateway (irc, ActiveX...)



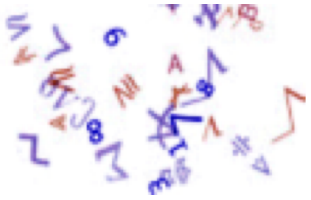
Vulnerabilities

- Applications and Internet services use generaly the Client / Server model
- Domain Name System (DNS)
  - Internet naming system (map name with IP address)
- E-mail (SMTP)
  - Frequently used for security alarms
  - Frequently used for binary files exchange
- File transfert (FTP)
  - Send and receive files of any type
  - Security of an FTP server is complex
  - FTP protocol itself is very dangerous



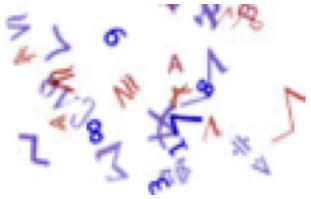
Vulnerabilities

- Illegal remote access using security flaw inside applications
  - Designed at a time when security was not a goal in the Internet (main goal was operational conectivity)
    - Sendmail bug of the month
    - IIS bug of the week
  - Sources disponibilities
    - For: source code can be verified by the community
    - Against: more easy to attack
  - Designers of protocol and applications of the Internet frequenly confused from simpicity and miss of security
    - But today, it's evolving



Vulnerabilities

- Illegal remote access (more)
  - Using weakness of IP protocols or of their implementation
    - IP spoofing
    - IP Fragmentation and overlapping
  - Impersonate users
    - From an remote correspondant
    - From an insider



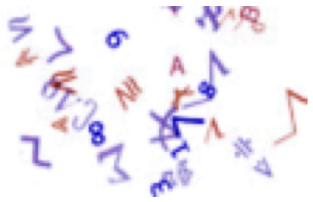
Vulnerabilities

- SMTP

```
From: root@public.com.fr
To: Joe.User@com.fr
Subject: Renew your password

    Dear Joe User,
  We have found your password for the computer named “public”
  is very easy to guess. For security purpose, please change
  it quickly by this one:
                              YugDiputs!

Syncerely,
Your system administrator          root@public.com.fr
```

De : S F R <services-bancaires@neufbox.fr>
Objet : **Incident bancaire**
Date : 27 décembre 2009 04:43:52 HNEC
À : Recipients <services-bancaires@neufbox.fr>

SFR **Incident bancaire**

Votre Reference Client : 1-QHF65I

Une defaillance technique au niveau de l'un de nos logiciels gerant les comptes clients SFR a causer malencontreusement L'impute la somme 167,98 euro, sur votre compte. En vue du remboursement de cette somme prelevee par erreur sur votre compte, et dans les plus brefs delais, nous vous prions de vous connecter sur le lien qui apparait en dessous de ce message. .

Cliquer ici pour proceder a l etablissement de votre fiche .

http://s-f-r-market.fr/espace-client/connexion/

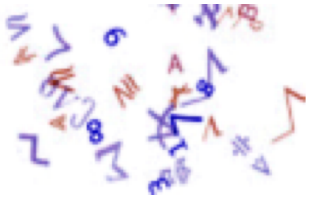
Nous vous remercions de votre fidelit

Dominique Delamarre
Directeur Service Client

Phishing

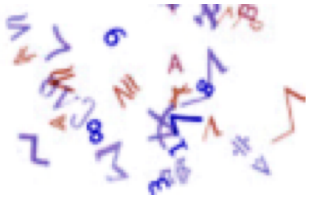
Phishing


EDF
bleu ciel
Avec la Facture Electronique,
toutes vos factures
sont disponibles en ligne
à tout moment !
Souscrivez dès maintenant
à la Facture Electronique
http://edf-tr.softmks.com/r/?id=h721214f,
711661f,71ab10f
Bonjour
Gratuite, pratique, sécurisée :
la Facture Electronique n'a vraiment
que des avantages !
Simplicité : réception d'un email d'alerte à l'arrivée de chaque facture.
Sécurité : accès unique depuis votre espace Client personnalisé et sécurisé.



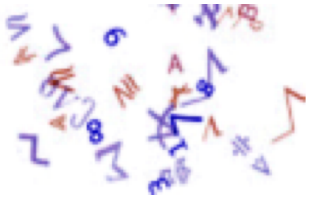
Vulnerabilities

- World Wide Web
  - Distributed, hyper-text and multimedia information service
  - Servers own application gateway(CGI), providing access to corporate databases, etc.
  - E-commerce base
  - PKI badly implemented and/or not well understood
- Remote connections
  - telnet: authentication is simple (cleartext password)
  - ssh: authentication using public key (RSA, DSA…), encrypted communications



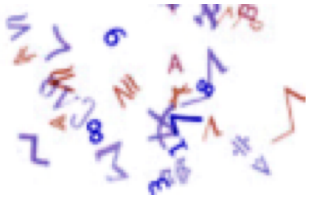
Vulnerabilities

- Tele-conference
  - UDP based applications
- Routing
  - Outside of the local network, routing is provided by the access provider
  - Static routing
  - Dynamique routing (EGP, IGRP...)
- Other services
  - rpc
  - IRC
  - ActiveX
  - Java
  - ...



Nimda virus

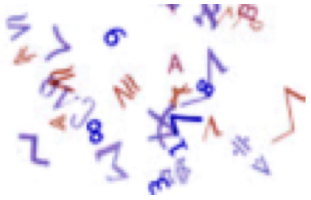
- september 18, 2001
  - 300 000 servers infected in less than 24 hours
- Spreading mecanism:
  - E-mail (attachement)
  - Web pages
  - Web serveurs (flaw in the IIS servers, backdoor from the CodeRed virus)
  - Infected computer look at new victims using all spreading methods available



Blaster worm propagation

```
HRESULT GetMachineName(WCHAR *pwszPath) {
   WCHAR wszMachineName[N+1];
   LPWSTR pwszServerName = wszMachineName;
   While( *pwszPath !=L'\\')
      * pwszServerName ++ = *pwszPath++;
      …
}
```

Source code from DCOM, Microsoft. Communication of the ACM, 2005



Using sockets

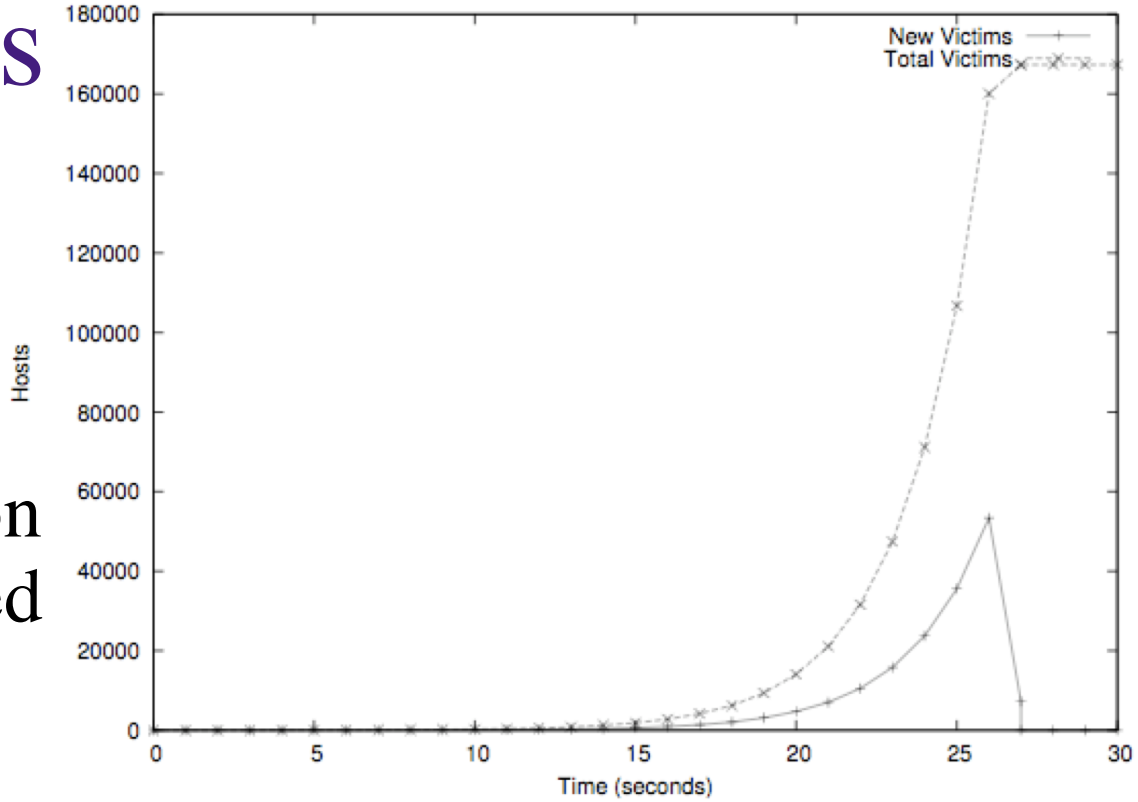
```
struct hostent *hp;
struct in_addr server;
hp = gethostbyname( hostname );

bcopy( hp->h_addr,
       &(server.sin_addr.s_addr),
       hp->h_length );

server.sin_family = AF_INET;
server.sin_port = htons( port );
...
```

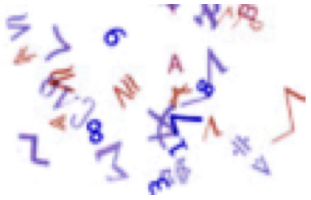

Perfect worms

- At an infection rate of 1 (each system infects one other system per second), a population of one million will be completely infected in under 20 seconds.



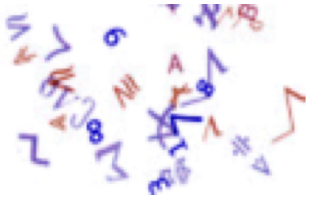
- Today, we don't know any methods to protect oneself again such attack.

Simulating and optimising worm propagation algorithms, Tom Vogt - 2003



Computer security aspects

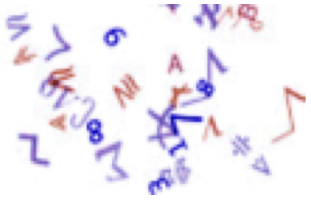
- Define a clear security policy supported by the entire hierarchy
- Common sense
  - Safe locations
  - Redundant hardware
  - Saving and preserving data
- Make it simple and auditable
- Raising users' awareness



Basic Principles

Simplicity and risks location

- For security point of view, complexity is the enemy
- A security architecture must help to concentrate all the securing efforts to a single point



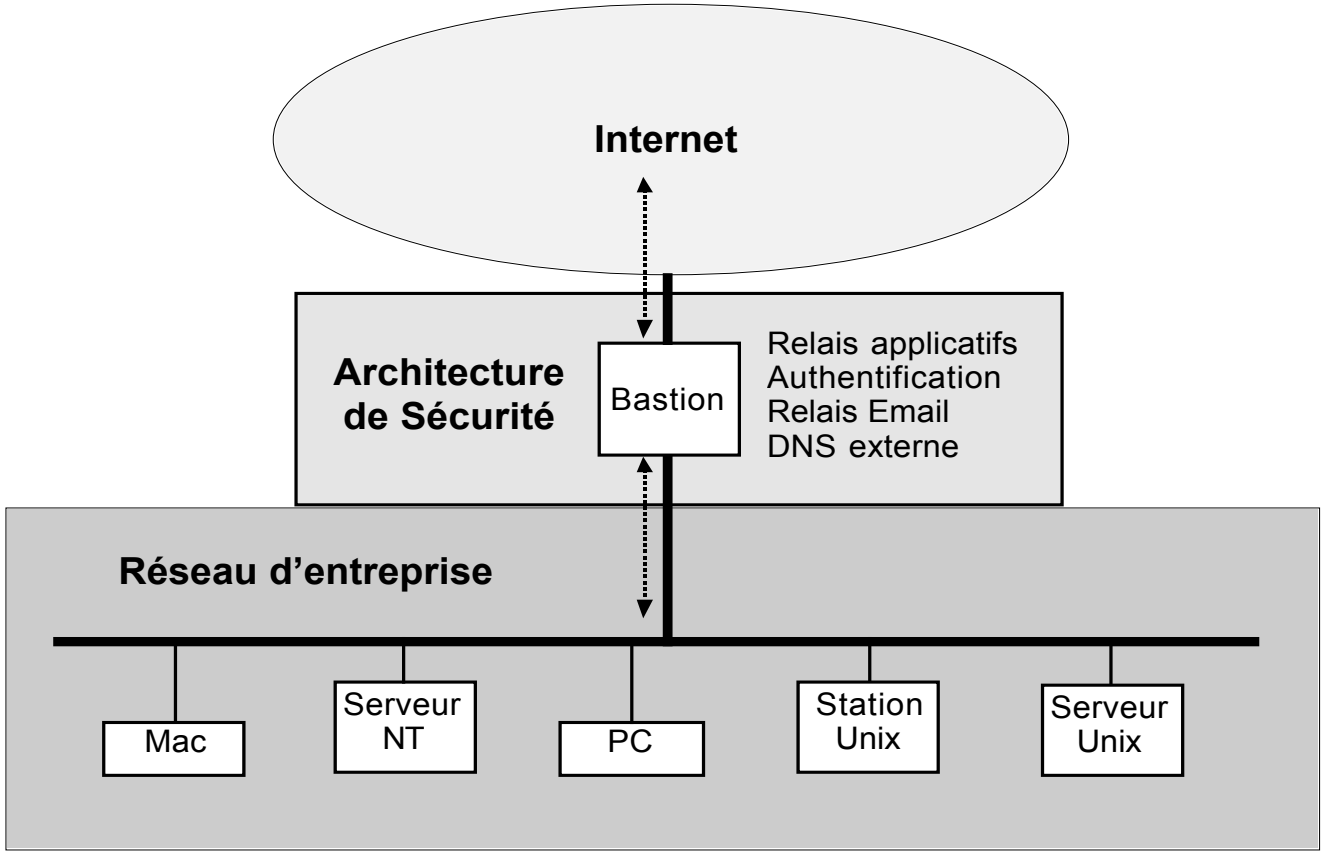
Which Solutions?

- Select the appropriate architecture:
  - Define zones with same confidence
  - Assess the sensitivity of services and data provided (external or local network)
  - Assess the consequences of a possible compromise of the different elements of the network architecture (security devices, servers, network devices, etc.)?

Each site has its own requierement and resources, it is often necessary to carry out arbitration involving many players (system, network, computer management teams…) before deciding on the architecture

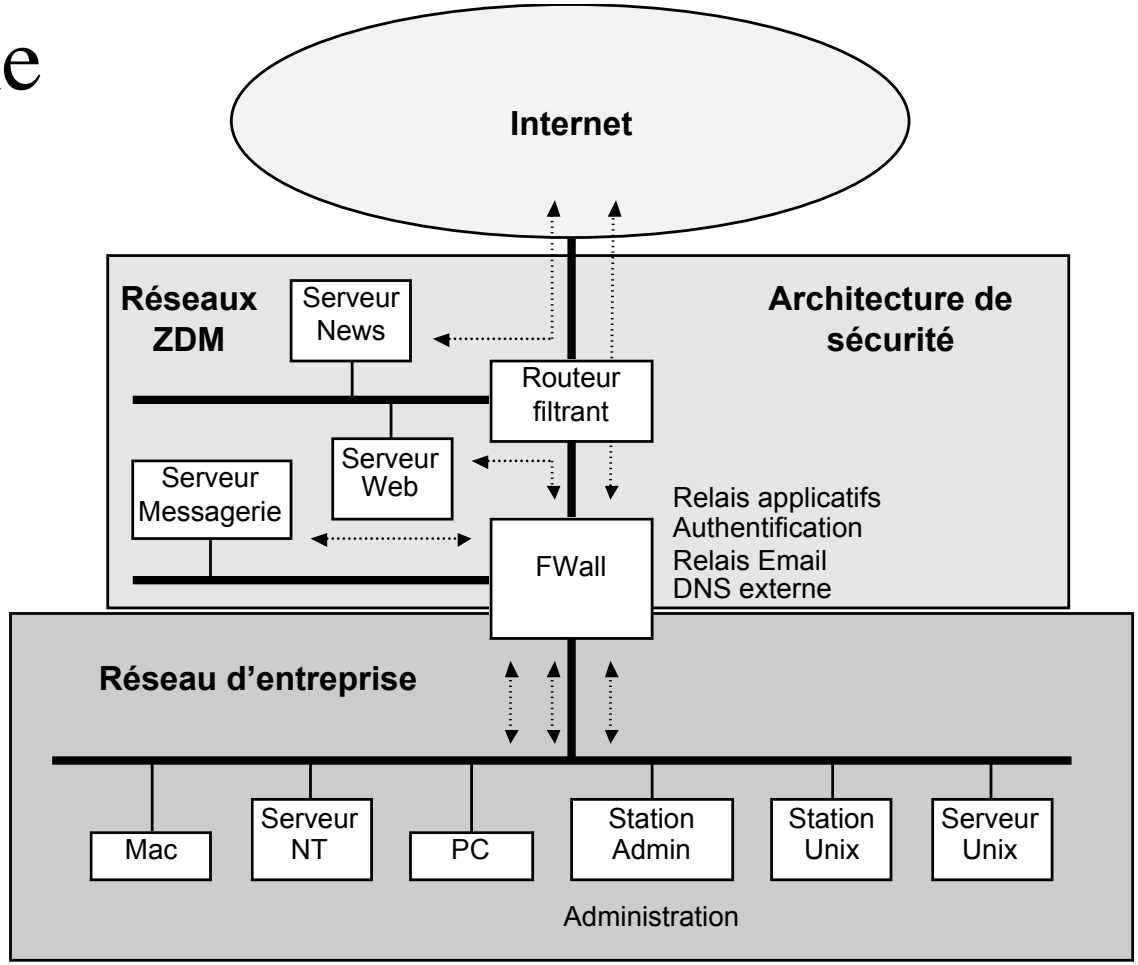
Which Solutions?

- Simple architecture: just one computer/router



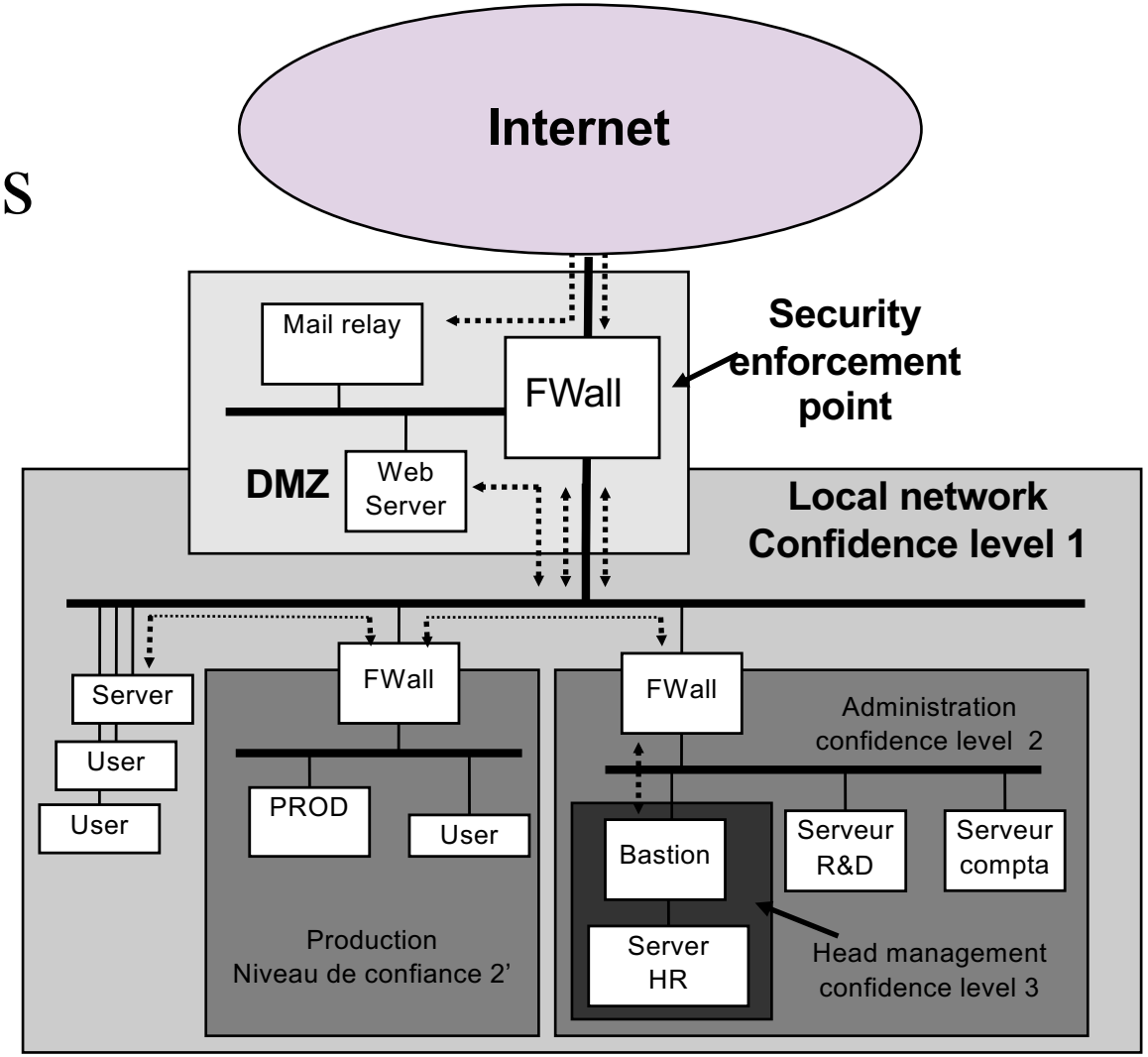
Which Solutions?

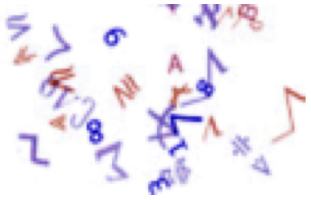
- Architecture example
  - Network with DMZ:
    - Public DMZ
    - Private DMZ



Which Solutions?

- Architecture examples
  - DMZ
  - Local networks with different confidence levels





Opérational objectives

Enforcing policy

- Controlling Access
  - hardware, network, application ...
- Detecting illegitimate access
  - Being able to react "in time"
- Controlling the exchange of information
- ...

Security Technologies

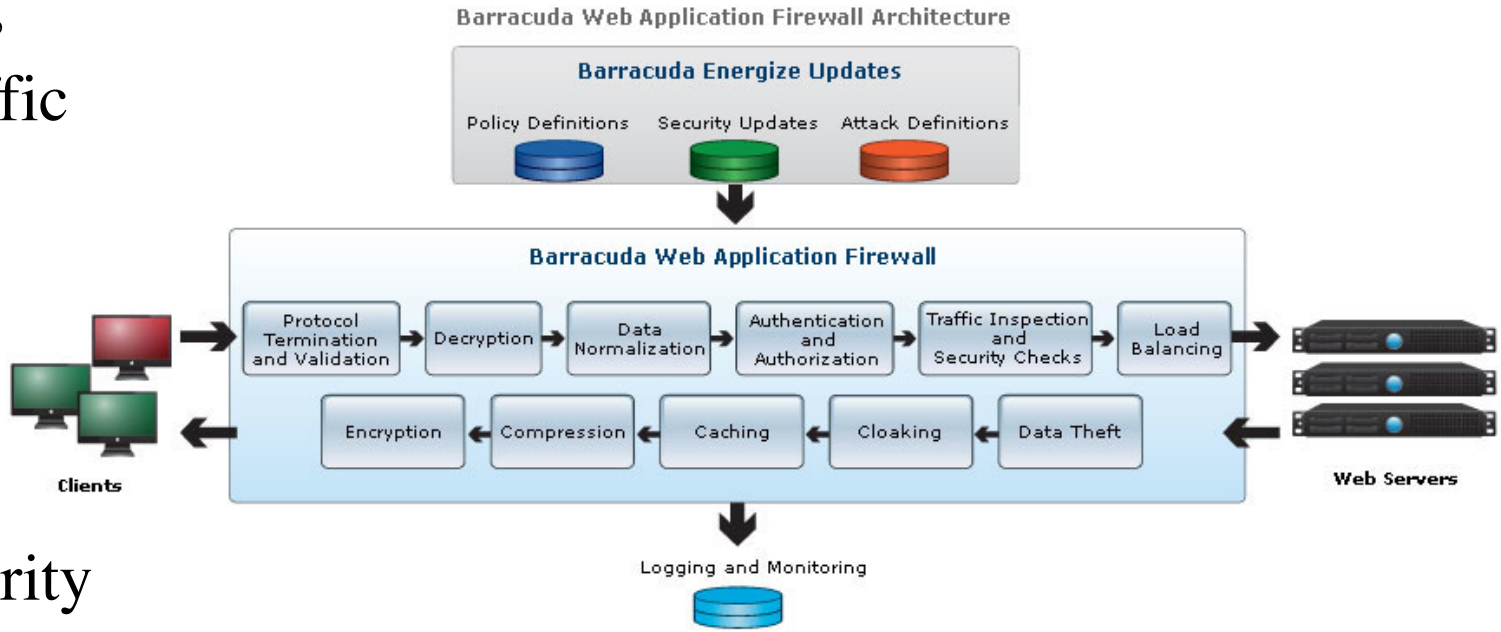
- IP Filtering
  - Determination of Flow
  - IP spoofing and other hazards
  - Configuring a Security Router

- Application Relay
  - Choice of relaying software: DNS, SMTP, other services
  - Example: TIS Firewall Toolkit
- Authentication
  - Authentication of incoming and outgoing accesses

A set of features grouped today under the term Firewall

Web Application Firewall (WAF)

- Protection against common attacks
- Outbound data theft protection
- Web site cloaking
- Secure HTTP traffic
- SSL Offloading
- SSL Acceleration
- Load Balancing



- Apache ModSecurity
- Check Point, Fortinet, Juniper Networks, McAfee, Palo Alto Networks, Barracuda …

IDS/IPS : Outils

- RealSecure, NFR, snort, bro…
  - http://www.iss.net/ *(IBM Internet Security System)*
  - http://www.nfr.net/ *(part of CheckPoint FW-1)*
  - http://www.snort.org/ *(SOURCEfire)*
  - http://bro-ids.org/ (*Lawrence Berkeley National Laboratory)*

  - Signatures based
    - Regular updates
    - Responsiveness to new threats

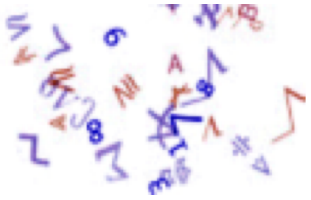
- Information
  - SANS Internet Storm Center (http://isc.sans.edu/)
  - Common Vulnerabilities and Exposures (http://cve.mitre.org/)

DLP : Data Lost Prevention

1 message out of 400 contains confidential data
1 file out of 50 is wrongly shared
1 in 10 laptops is stolen
1 USB key of 2 contains confidential information

- The cost of leaks can be in millions of euros
  - 1/3 of the losses are commercial (customer departures).
  - 1/3 of the losses are related to the theft of mobile phones or other mobile devices.
  - In any case, these loss of information cause prejudice in terms of images.
  - New legal constraints (CNIL in France).
- Tools
  - McAfee, RSA, Websence, Symantec…

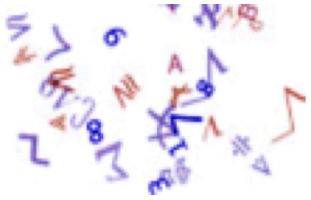
Etude Gartner, Forrester, FBI, Ponemon Institute (2008)



Cloud Computing

A new stakeholder to take into account in the security of the IS

- Industrialization and relocation of IT services
  - Software rental — SaaS (Software as a Service)
  - Systems rental — PaaS (Platform as a Service)
  - Hardware rental — IaaS (Infrastructure as a Service)
- Private, shared or public clouds?
- Nothing is in the clouds ☺

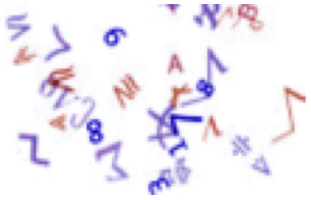


Cloud Computing

- SaaS
  - Storage services: Amazon S3, Dropbox, Google Drive…
  - Strategic business services: CRM, RH…
- PaaS, IaaS
  - Processing can be observed (industrial secrets)
  - Processing must take place on clear data

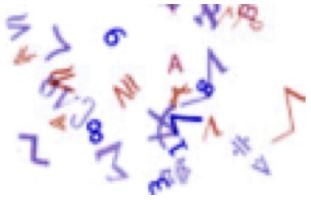
- Never forget the data transfert step.

Disponibility, confidentiality, integrity?



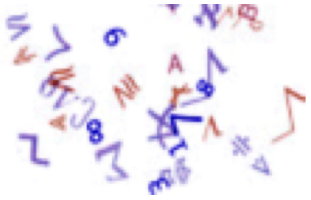
Management of the IS security

- Ensure that the required level of security is maintained
- Interest of ISO 27001: Management of Information Systems Security
  - Reflection on security policy
  - Implementation and operation
  - Incident management and control
  - Evolutions needed



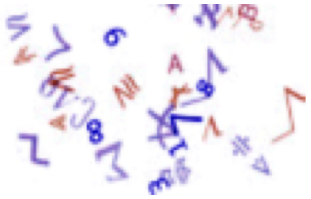
Bibliography

- Firewalls and Internet Security: Repelling the Wily Hacker
  William Cheswick & Steven Bellovin - Addison Wesley
- Building Internet Firewalls
  D. Brent Chapman & Elizabeth D. Zwicky - O'Reilly & Associates
- TCP/IP : Architecture, protocoles, applications - Douglas Comer - InterEditions – 1991
- Practical UNIX & Internet Security (2nd edition)
  Simson Garfinkel & Gene Spafford - O'Reilly & Associates



Online sources

- Mailing lists
  - CERTs
  - Firewalls
  - Bugtraq
  - Secunia
  - Full Disclosure
  - Oracle Security Alert, HP Security Info, Microsoft Security Announce, Cisco Security Announce, etc.
  - Clusif
  - sec@ossir.org



Online sources

- Electronic magazines
  - Phrack Magazine
- Web sites
  - Computer Security
  - Network Security
  - Exploits
  - Hacker's Sites
- Etc...