R5.cy.12-Norme
Normes, standards et analyse de risque

Année 2024-25

jean-marc.thiriet@univ-grenoble-alpes.fr

Condensed CV

jean-marc.thiriet@univ-grenoble-alpes.fr

UGA Université Grenoble Alpes

Docteur (Ph.D.) Université Henri Poincaré Nancy 1: février 1993

* Maître de Conférences Université Henri Poincaré Nancy 1 1993-2005
* Professor d'Université, Univ. Grenoble Alpes depuis 2005
    * Recherche en cyber-security of cyber-physical systems (smart grids, drones)
    - Cybersecurity risk assessment for Unmanned Aircraft Systems, TRAN Trung Duc, 2021
    - Détection d'intrusions pour les systèmes de contrôle industriels, Oualid KOUCHAM, 2018
    - Diagnostic en réseau de mobiles communicants, stratégies de répartition de diagnostic en fonction de contraintes de l'application, Insaf SASSI, 2017
    - Cyber Sécurité des systèmes de contrôle de smart grid : détection d'intrusion dans les réseaux de communication IEC 61850, Maëlle KABIR-QUERREC, 2017
    * Enseignement en réseaux, cyber-sécurité, traitement du signal, Automatique et diagnostic : DUT/BUT, LPRO, master
    * Chargé Mission RI IUT1, Directeur-Adj. EUT RSE
    * Projets dans le cadre éducatif
        - Asean-Factori 4.0 (Europe-Asie du Sud-Est)

1. Cyber-sécurité

Année 2024-25

jean-marc.thiriet@univ-grenoble-alpes.fr

Qu’est-ce que la cyber-sécurité ?
Brainstorm

Qu'est-ce que la cyber-sécurité ?

- **Cybernetics** from Greek κῠβερνήτης (*kubernêtês*) => Used 19th and 20 century => ideas of control and communication
- **Cyber** : Greek *kubernân,* to govern
- Today used for everything relative to the « digital » world (internet, web…)
- **Cyber-security**:
  - Cyber security comprises technologies, processes and controls that are designed to protect systems, networks and data from cyber attacks. Effective cyber security reduces the risk of cyber attacks, and protects organisations and individuals from the unauthorised exploitation of systems, networks and technologies (https://www.itgovernance.co.uk/what-is-cybersecurity)
  - État recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense. (ANSSI, https://www.ssi.gouv.fr/entreprise/glossaire/c/)

Les enjeux de la sécurité des S.I.

Impacts financiers

Impacts sur l'image
et la réputation

Sécurité
des S.I.

Impacts juridiques
et réglementaires

Impacts
organisationnels

Organisation de ce cours

- Chap. 1: Cyber-sécurité, environnement
- Chap. 2: Analyse de risques
- Chap. 3: Outils spécifiques de cyber-sécurité
- Chap. 4: Stratégie et politique de sécurité, audits

DS : Vendredi 20 décembre 2024 de 10 à 12

1.1 Convergence entre Informatique et monde des Systèmes Cyber-physiques

1.1.Convergence between IT and cyber-physical systems

US Black-out, 2003

INFRASTRUCTURE

IT

Industrial Control Systems (ICS)

Smart grids

Cyber attack ukrainian power network, Dec. 2015

- Integrity of the information and communication infrastructure

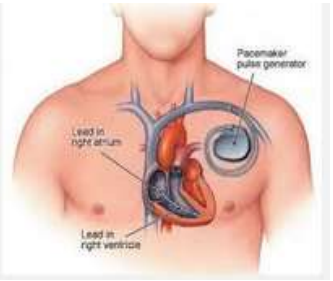
→ Challenge: DEPENDABILITY (RAMS Reliability, Availability, Security & Safety, Maintainability)

EMBEDDED SYSTEMS

Drones

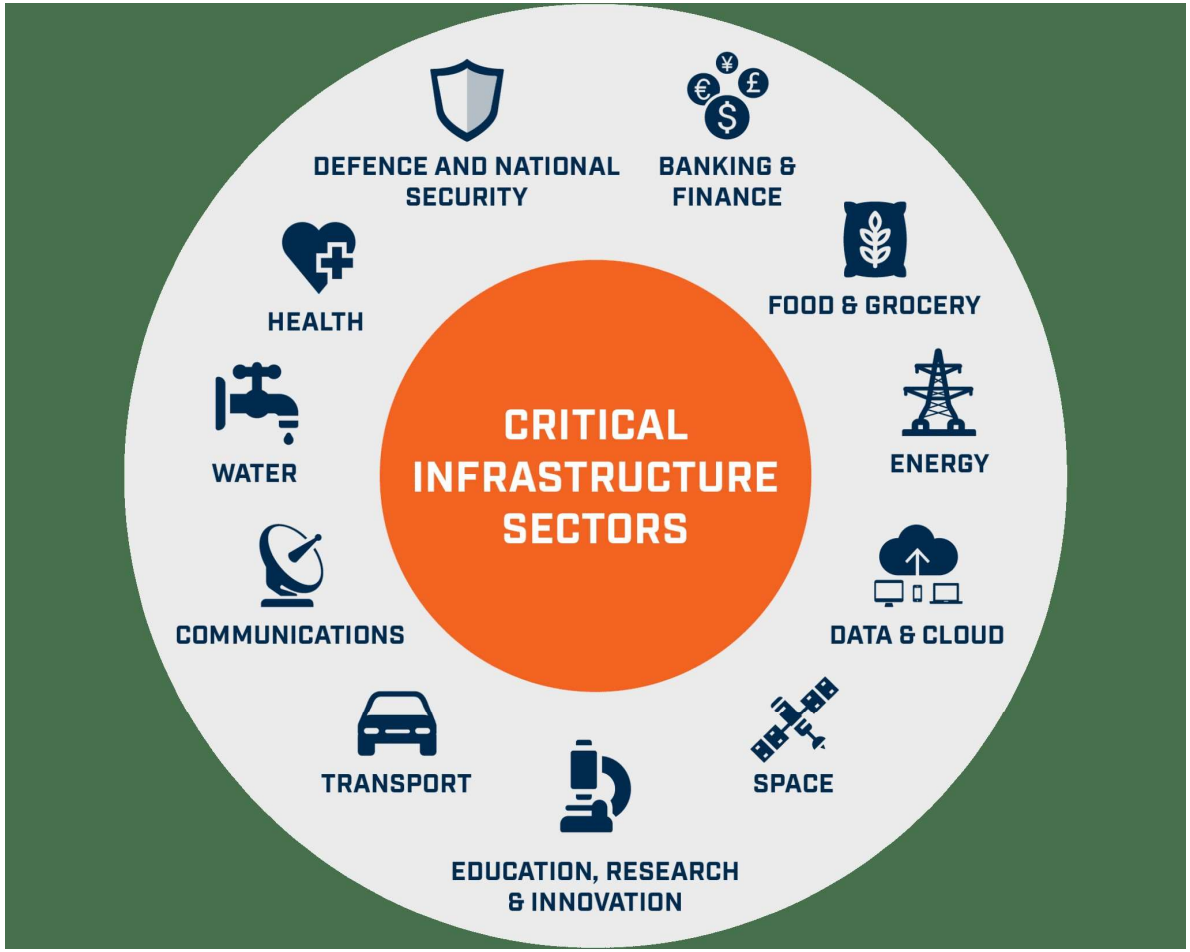
Autonomous vehicles

Connected objects, IoT



Maroochy shire, Stuxnet, CrashOverride

Des domaines d'application pour les Systèmes Cyber-Physiques
Brainstorm



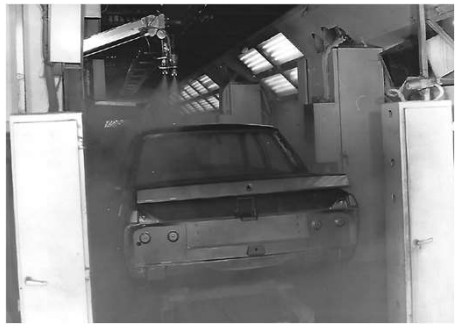
https://huntsmansecurity.com/industries/critical-infrastructure/

En France Secteurs d'Activités d'Importance Vitale (SAIV)

From Industry 1.0 to Industry 4.0…

Industry 1.0 : mechanization, mechanical energy (water, steam), ex: agriculture , XIXth century

Industry 2.0 : mass production, electricity, ex: car factory ~from 1920s to 1970s



Industry 3.0 : automation (robots) => First PLCs (Programmable Logic Controllers) computer, ex: pharmacy, food, 1980

Industry 4.0 : Cyber-physical systems, communication (virtual tools: Cloud), ex: smart cities, Nowadays

Industry 4.0: some challenges

PARCE QUE CERTAINS SYSTÈMES SONT CRITIQUES
NOS SERVICES DATACENTER AFFICHENT 100% DE DISPONIBILITÉ DEPUIS 10 ANS

Certification ISO 27001 pour les services Datacenter, Cloud, hébergement, supervision NOC/SOC, administration, innovation, commercialisation

Certification Hébergeur de données de santé sur les 6 périmètres

Certification

Organisation

L'usine du futur devrait faire la part belle à la 5G plutôt qu'aux réseaux LPWAN. Ces derniers pourront servir cependant à l'optimisation des bâtiments.

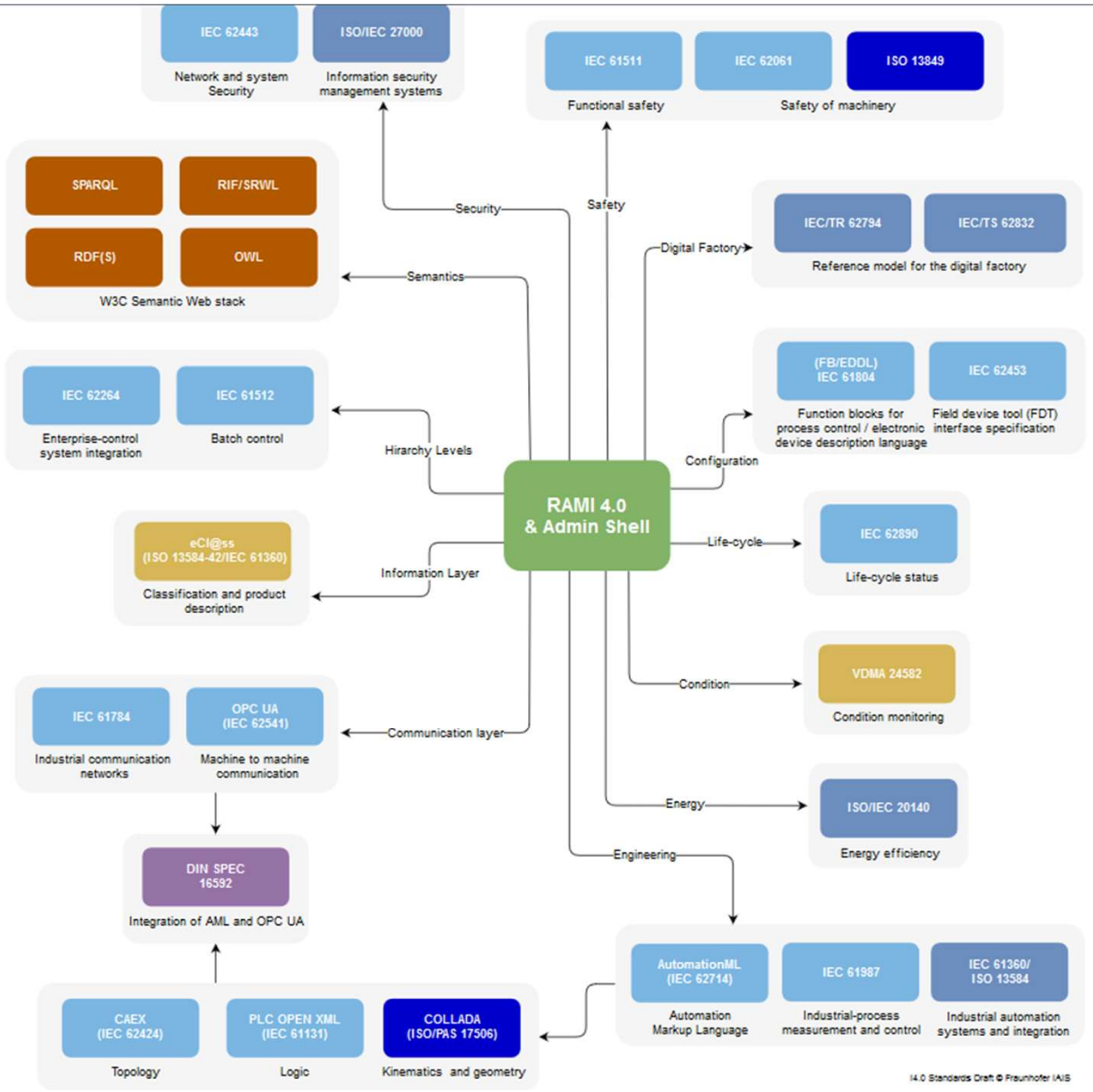
« New » networks: 5G

Certification

Standards…

State of the Art
Best practises
In security

Quality
Assurance
processes



Comparison between ICS and classical IT systems

IT Information Technogy

ICS Industrial Control System

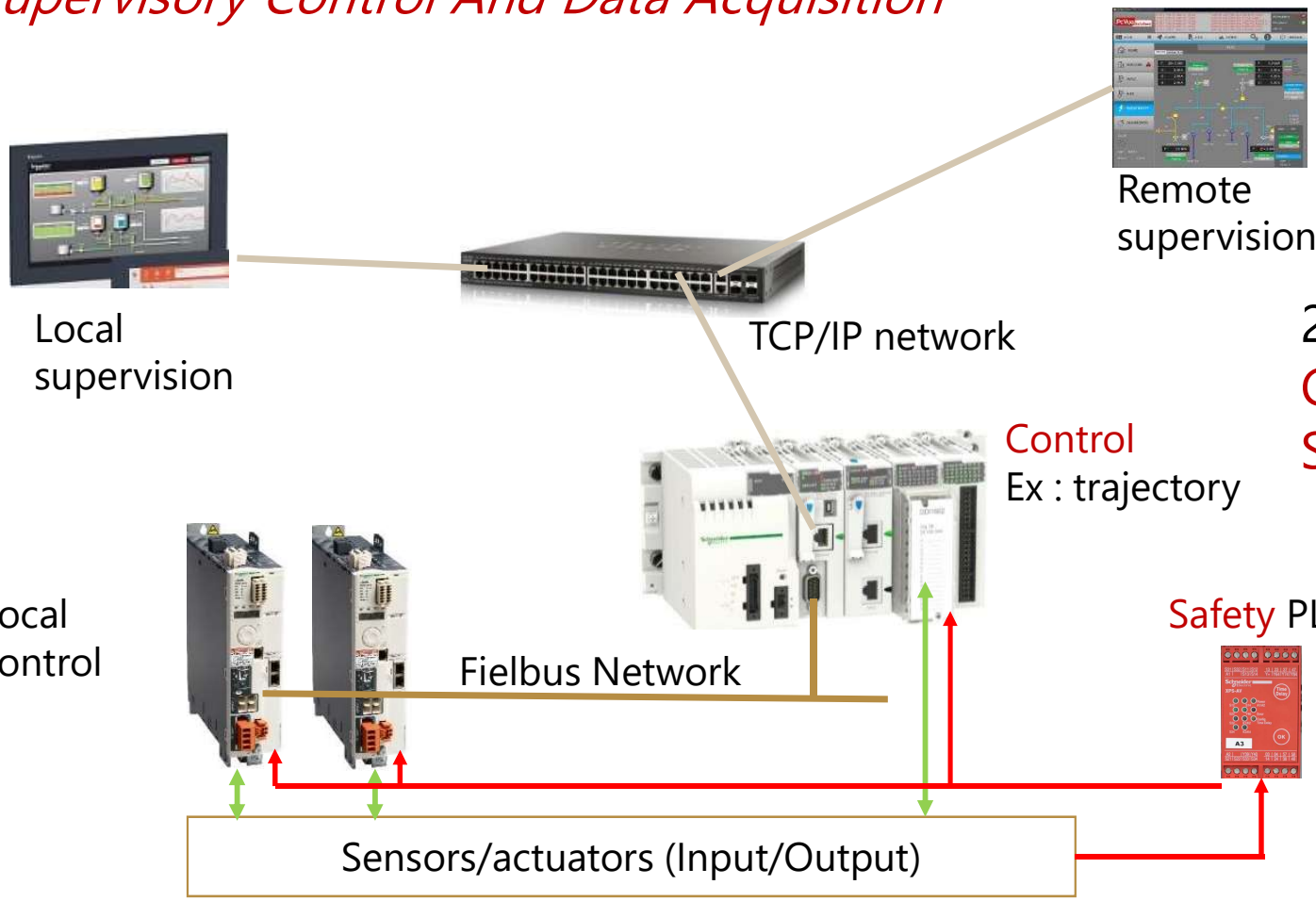
Category	IT systems	ICS systems
Cyber security culture	Awareness of risks Methods and tools	Recent
Life duration	3-5 years	> 20 years
Performance	Throughput	Latency Real-time constraints
Resources	Abundant	Limited
Networks Protocols topologies	Numerous connection points Dynamic topologies	Fixed topologies “Simple” protocols Defined communication strategy, scheduling
Performances	Delays and jigs acceptable	Real time, critical time Strict time constraints
Availability	Some tolerance on degradations, depending on situations	High availability Inacceptable loss of connection (depends) Advance planning
Resource constraints	Available resources	Design for industrial processes Limited processing and memory resources
Targeted properties	Confidentiality Integrity Availability	Timeliness Availability Integrity Confidentiality

Comparison between ICS and classical IT systems

Category	IT systems	ICS systems
Targeted properties	Confidentiality Integrity Availability	Timeliness Availability Integrity Confidentiality

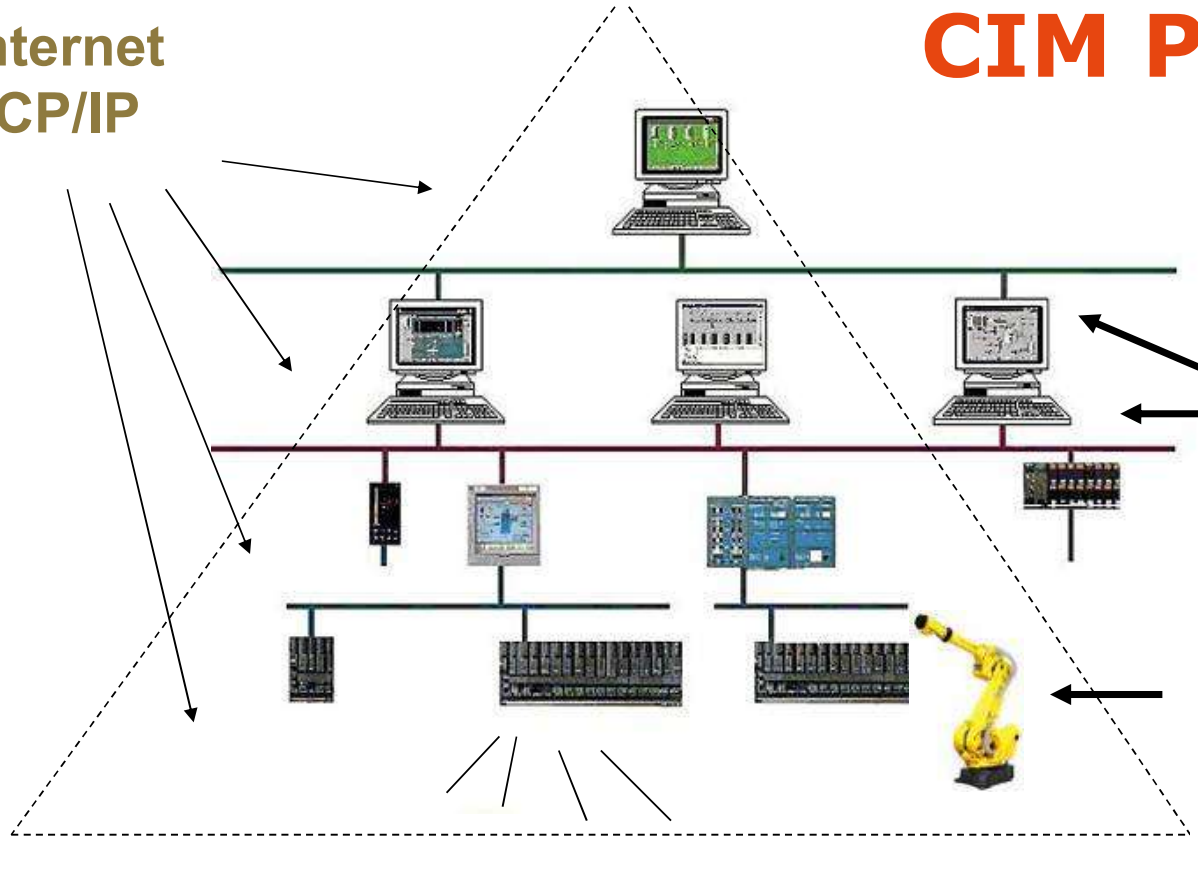
An example

SCADA: Supervisory Control And Data Acquisition



2 important aspects:
Control
Safety

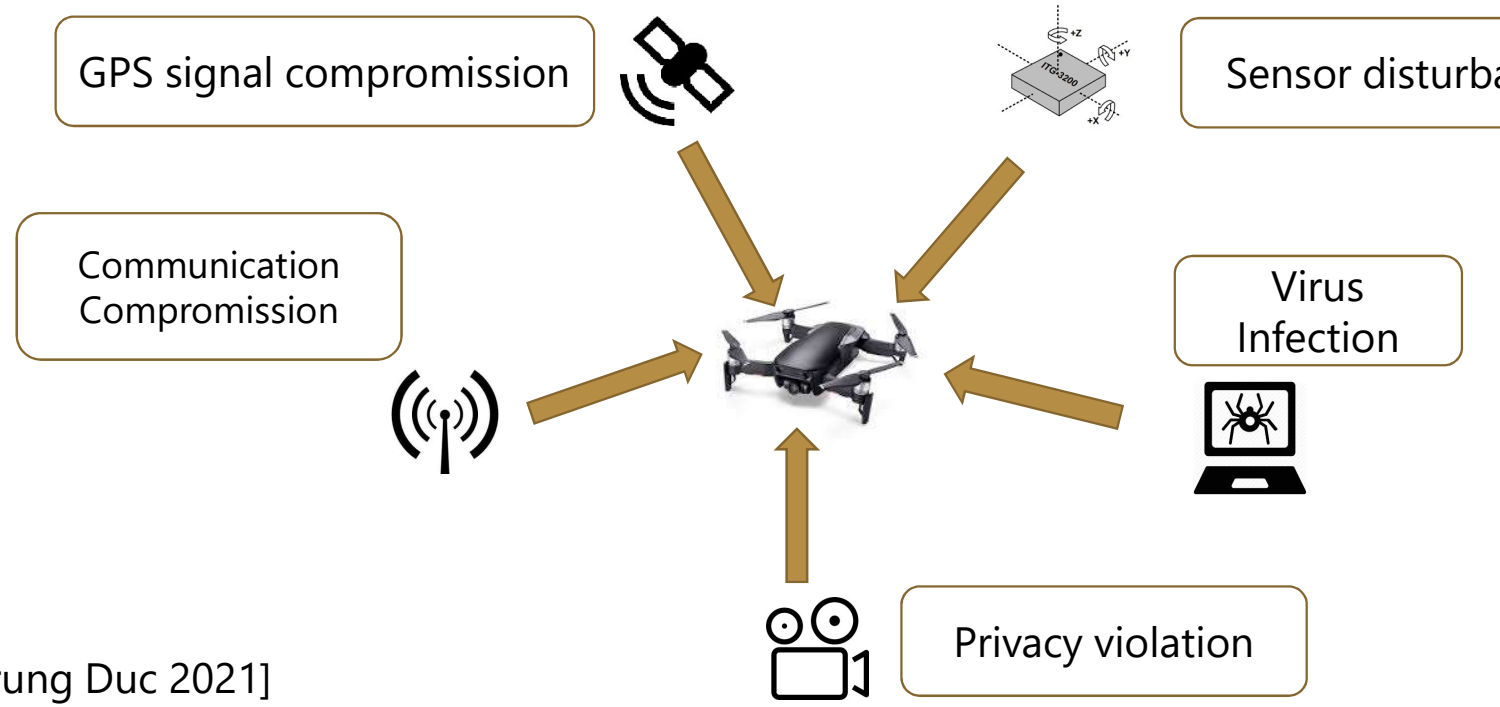
CIM Pyramid



Computer-integrated manufacturing (**CIM**)
Describe the complete automation of manufacturing processes
Several network layers

1. Cyber-security of flying drones: Risk analysis

Vulnerability of the drone:



[Phd TRAN Trung Duc 2021]

➡ Need of a methodology to get a cartography of the drone security in a systematic way and to ensure completude

Risk analysis

Aeronautics standards

Operational Technology (mission)

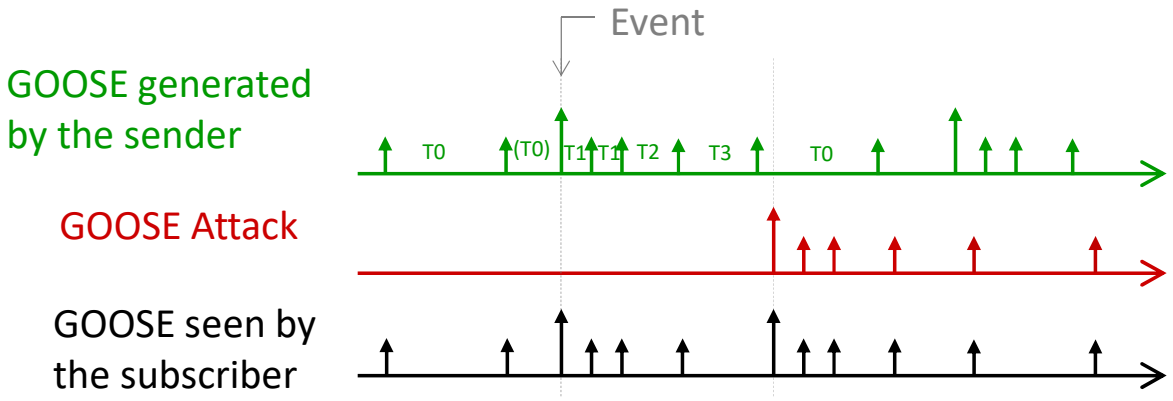
2. Reliability vs. injection of false GOOSE messages

[Phd Maëlle Kebir-Querrec 2017]

- Mechanism of GOOSE data transfer
  - Publisher / subscriber
  - Broadcast
  - Counters: *State number – StNum* and *Sequence Number - SqNum*)

Smart grids, IEC 61850

Protocol threats

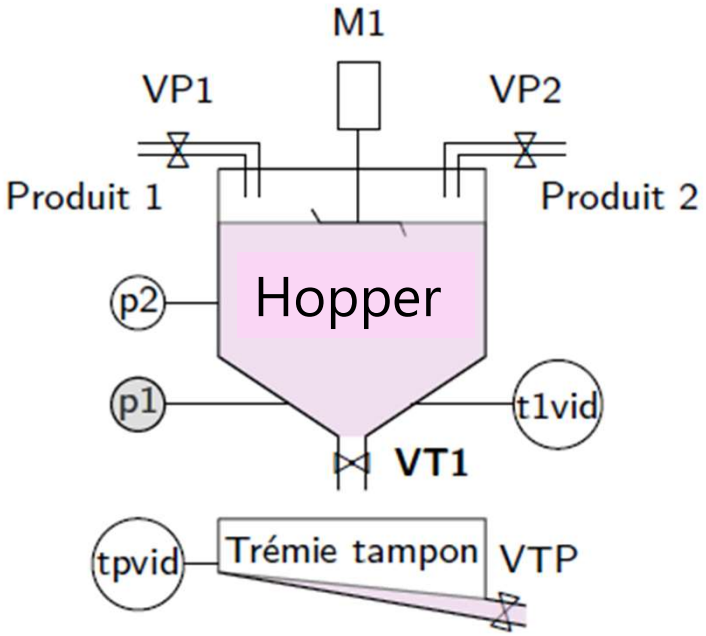


T0	Retransmission in stable conditions
(T0)	The retransmission cycle in stable conditions may be interrupted by an event
T1	The shortest retransmission time after an event
T2, T3	Retransmission time doubles up to T0

Transfer mechanism for the GOOSE protocole

… and exploit

3. ICS sequential system



[Phd Oualid KOUCHAM 2018]

Comportement séquentiel incorrect

$@t_0 : [vp1^{\uparrow}]$
$@t_1 : [t1vid^{\downarrow}]$
$@t_2 : [vt1^{\uparrow}]$
$@t_3 : [vt1^{\downarrow}, tpvid^{\downarrow}]$
$@t_4 : [p1^{\uparrow}, vp2^{\uparrow}, vp1^{\downarrow}]$
$@t_5 : [m1^{\uparrow}, p2^{\uparrow}, vp2^{\downarrow}]$
$@t_6 : [vt1^{\uparrow}, m1^{\downarrow}]$
$@t_7 : [p2^{\downarrow}]$

Focus on attacks designed to induce ***incorrect sequential behavior***

Operational Technology OT

Overview of cyber attacks against ICS systems (from PhD Peter Matousek)

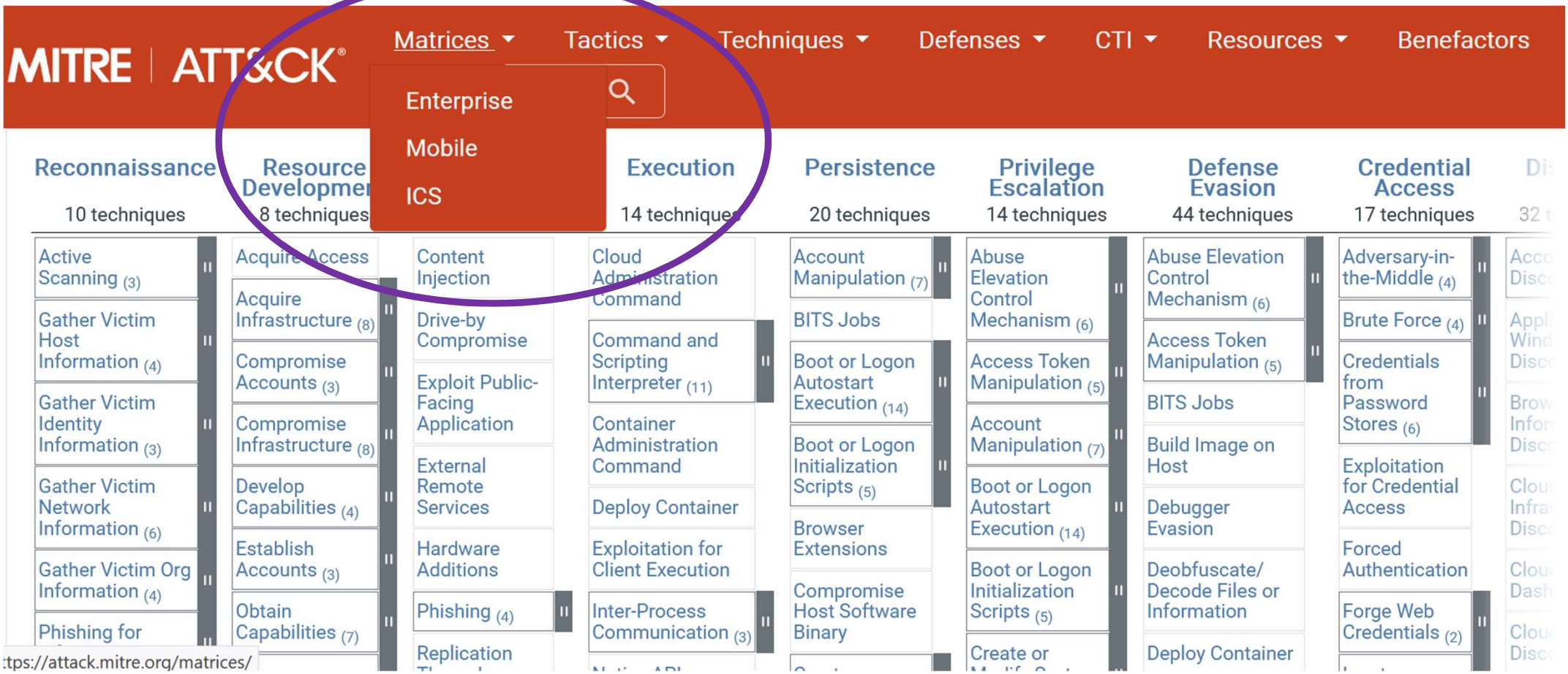
Year	Attack	Place
1982	Explosion of Siberian gas pipeline caused by a trojan which reset pump speeds and valve settings	Soviet Union
1997	Knock out of Worcester air traffic control communication	MA, USA
2000	Maroochy shire sewage spill	Australia
2003	Crash of the Safety Parameter Display System in Davis-Bess nuclear power plant by Slammer worm	OH, USA
2003	Shutting down of CSX train signaling system by Sobig virus	FL, USA
2005	Zotob virus knocked 13 of Daimler-Chrysler's manufacturing plants	USA
2010	Stuxnet virus damaged Iranian centrifuges by increasing and decreasing their speed and pressure beyond normal levels	Iran
2014	Disrupted control system in German steel mill	Germany
2015	Power outage off Ukrainian power plant distribution caused by BlackEnergy malware	Ukraine
2016	Industroyer malware attack on Ukrainian power grid	Ukraine
2017	Cyber-espionage attack against aerospace and energy industry by APT33 group	USA
2019	Cyber attack against chemical giant Bayer	Germany
2019	Intrusion attack against U.S. Energy sector by KAMACITE group	USA
2019	Cyber attack against Kudankulam nuclear power plant	India
2020	Compromising supply chain of Solarwinds software used in industrial environment	USA
2021	Ransomware attack against oil distribution company Colonial Pipeline	USA

Cyber-security of CPS

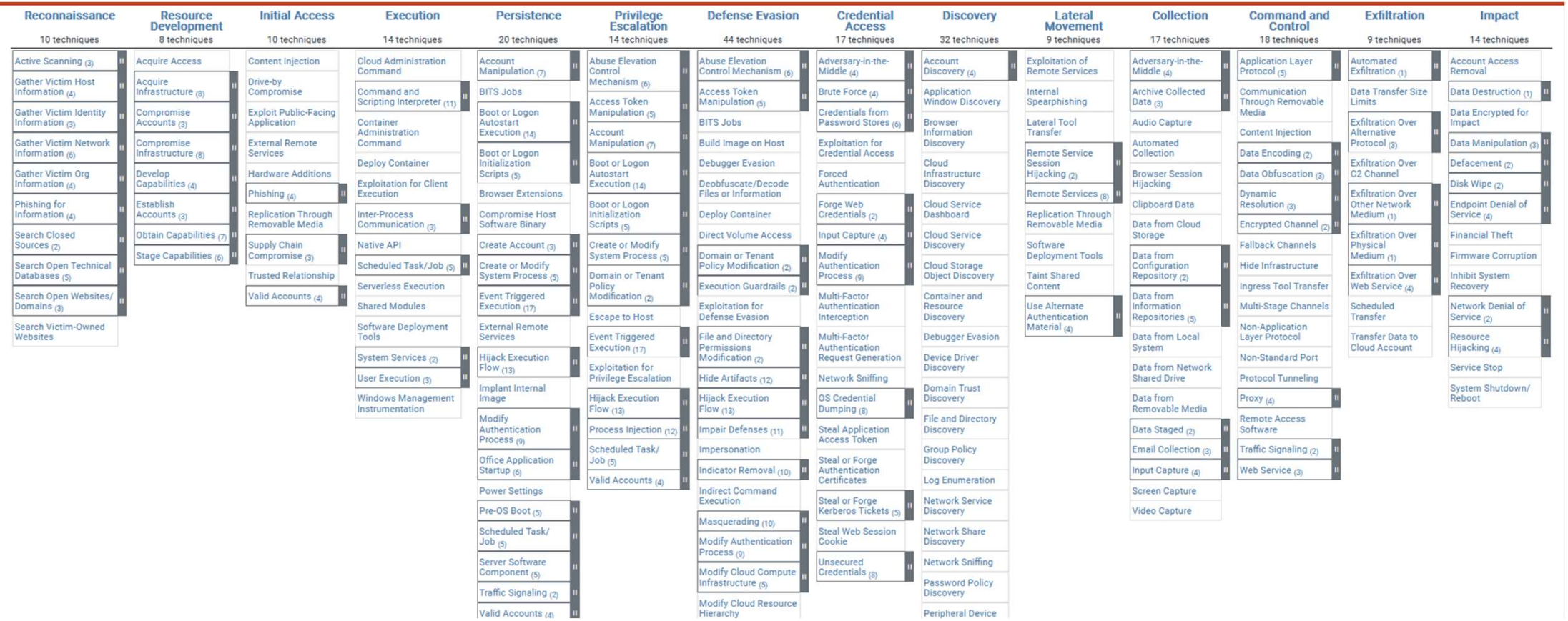
Methodology, standards **Science** **Applications** **Societal**

1. Dependability : Confidence in the system to ensure its mission without risk (or with a risk management)
   - => Co-design approach (Network QoS ⇔ System QoC)
2. Functional safety: part of the overall safety that depends on a system or equipment operating correctly in response to its inputs [IEC 61508]
3. Cyber-security: Cyber security is the protection of systems, networks and data in cyberspace [www.itgovernance.co.uk, www.ssi.gouv.fr]
4. Networked Control Systems: Control System closed through a network
5. Complex systems, infrastructure, distributed systems
6. Embedded system, autonomous system, connected objects
7. ICS : Industrial Control Systems
8. IoT: Internet of Things, IIoT: Industrial Internet of Things
9. Cyber-physical systems (CPS): Marrying physicality and computation [persyval-lab.org]
10. Our interest: To analyse CPS from the point of view of the potential impact of the system in the physical world (dependability point of view) due to a cyber-attack (attack in the digital world) and define the ways to protect it

https://attack.mitre.org/



https://attack.mitre.org/



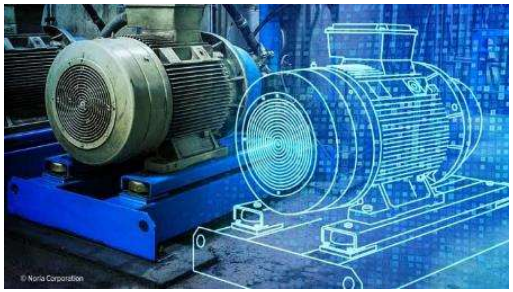
1.2 Réseaux, réseaux sans fil et réseaux industriels

Communication challenges

Data, I/O
Critical inf., Alarms

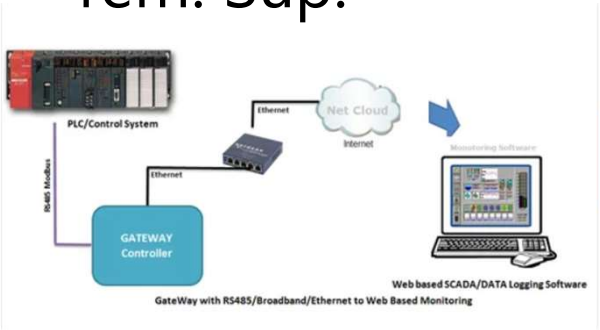
Industrial Internet Of Thing

Cloud



Digital Twin

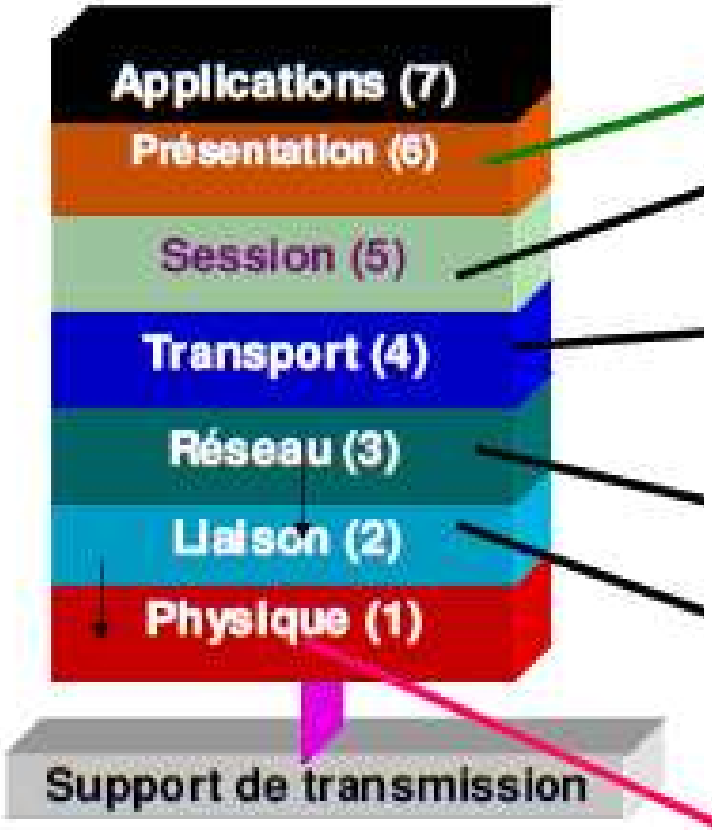
Remote SCADA, rem. Sup.

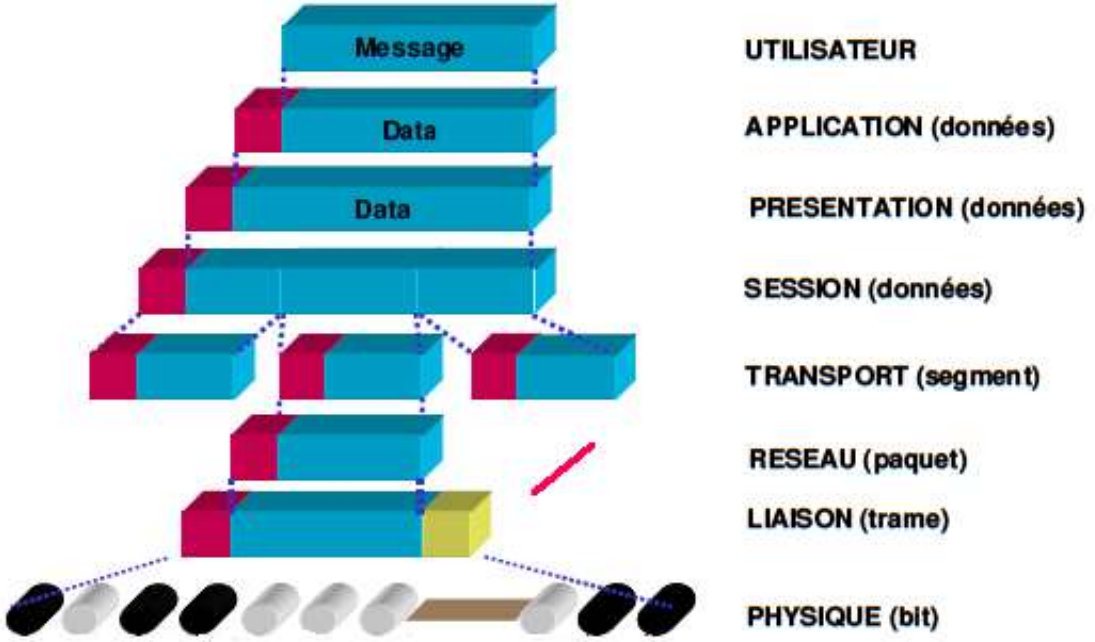


TCP/IP Networking
4G/5G/6G (LTE)
Wi-Fi, ZigBee
ModBus s., Profibus, CAN
Profinet, Modbus TCP
ProfiSafe, CANOpenSafe

Autonomous vehicles

Modèle OSI (Open Systems Interconnection / Interconnexion de Systèmes Ouverts) de l'ISO (International Organization for Standardization / Organisation internationale de normalisation)





Sécurité et réseaux

Protocole IP et les protocoles associés (TCP, UDP, ICMP, routage…) n'ont pas pris en compte la sécurité

- « Concept sécurité » inconnu à l'époque, personne n'imaginait que ces protocoles pourraient être détournés à des fins malveillantes ;
- **Aucun mécanisme de sécurité n'est donc implémenté au sein de ces protocoles.**

Ex:

- **Absence d'authentification des émetteurs et récepteurs** d'un datagramme : usurpation d'adresse IP possible ;
- **Absence de chiffrement des données**, celles-ci sont donc transmises en clair. Un hacker positionné sur un réseau peut donc écouter les connexions et accéder aux données ;
- **Le routage des datagrammes peut être modifié** de façon à rediriger les datagrammes vers un autre destinataire ;
- Note : l'exploitation de ces faiblesses nécessite des prérequis techniques, i.e. elles ne sont pas systématiquement applicables à tous les réseaux

Sécurité et réseaux

Mise en œuvre des mécanismes de sécurité complémentaires

- Chiffrement des communications
- Authentification des entités
- Cloisonnement réseau
- Filtrage
- Dimensionnement adapté des infrastructures
- Règles de renforcement des configurations des équipements
- Supervision des équipements
- etc.

Access Control Methodologies

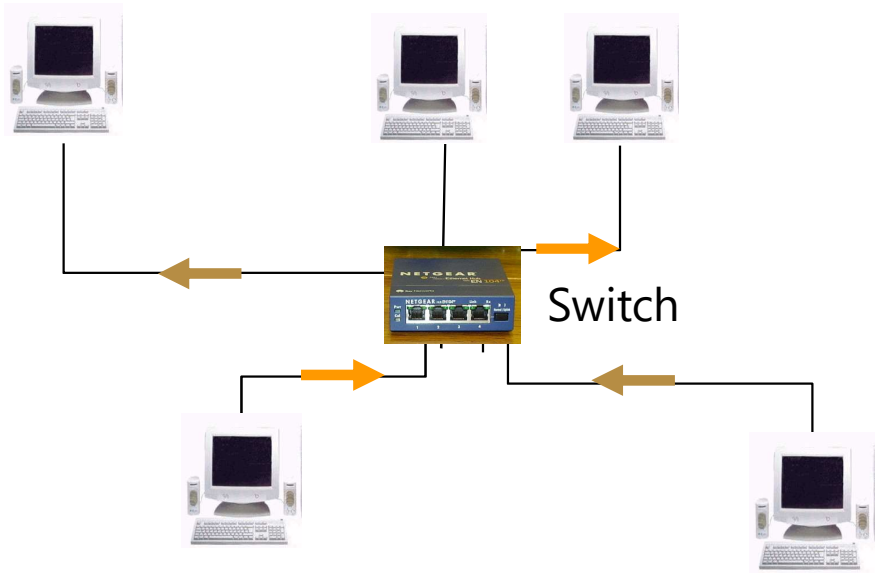
- Random access
  - Free access to the bus, as soon as the medium is free without prior authorization
  - Risk of collisions

Stochastic vs Determinist

- Principle: Competitive protocols
  - CSMA/CD (Carrier Sense Multiple Access / Collision Detection)
    - transmission as soon as the channel is free
    - in case of collision:
      - 1. transmission of a jamming sequence
      - 2. after a delay: new attempt
      - 3. abandonment after too many failures
- CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance)
  - Priority mechanism in case of simultaneous transmission

Switched Ethernet

- Ethernet = collisions
- Switches: delimitation of « free collisions » zones



Access Control Methodologies

- Controlled access
  - Waiting for a right to communicate (avoid any conflict)
  - Centralized management: 1 station controlling the accesses
  - Decentralized management: pl. stations controlling the accesses
- Centralized access by "polling"
  - Each subscriber can poll in turn according to a predefined order.
  - Requires:
    - 1. an access controller
    - 2. a polling table
- Bus token method
  - Creation of a logical ring in which a token rotates
  - Right to communicate and access control held by the owner of the token
  - Possession of the token limited in time

Stochastic vs Determinist

Sécurité Opérationnelle

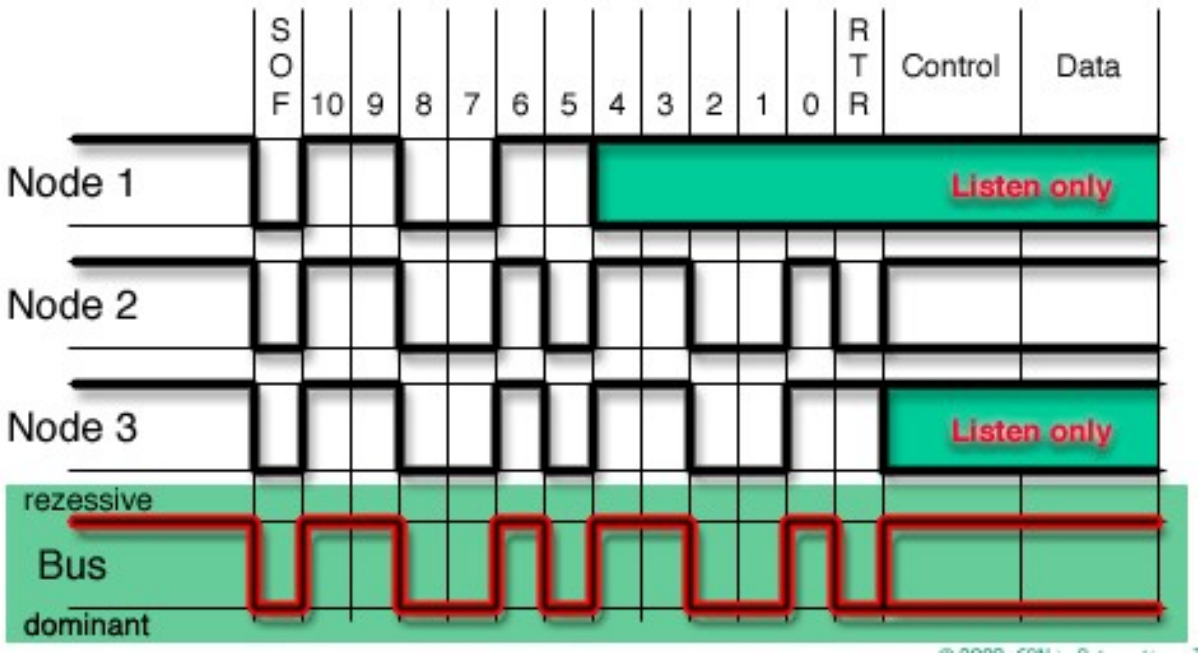
Example: Access mode: CSMA/AMP Arbitration by Message Priority

Ex. of Fieldbus networks

Scheduling of messages as a function of priorities

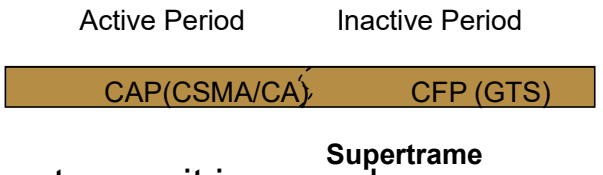
(ex : CAN network, Controller Area Network),

Partially determinist (configuration strategy)



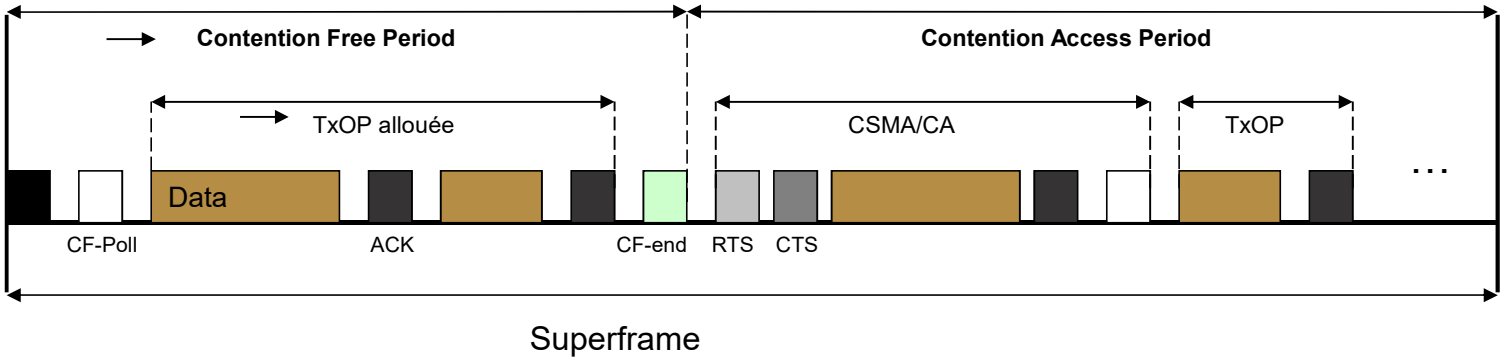
Real time (critical time)
Wireless network (if the physical layer works!)

- Zig-Bee (on 802.15.4)
  - Superframes :



CAP (Contention Access Period) : all the nodes can transmit in a random way respecting the slot duration CSMA/CA
CFP (Contention Free Period) : Allow to garanty an access to a node during a certain amount of time (measured as a number of GTS slots)
GTS (Guaranteed Time slots) : Dedicated time slots (the coordinator can allocate one or several slots to a node, in particular for time garanties)

- Wi-Fi 802.11e

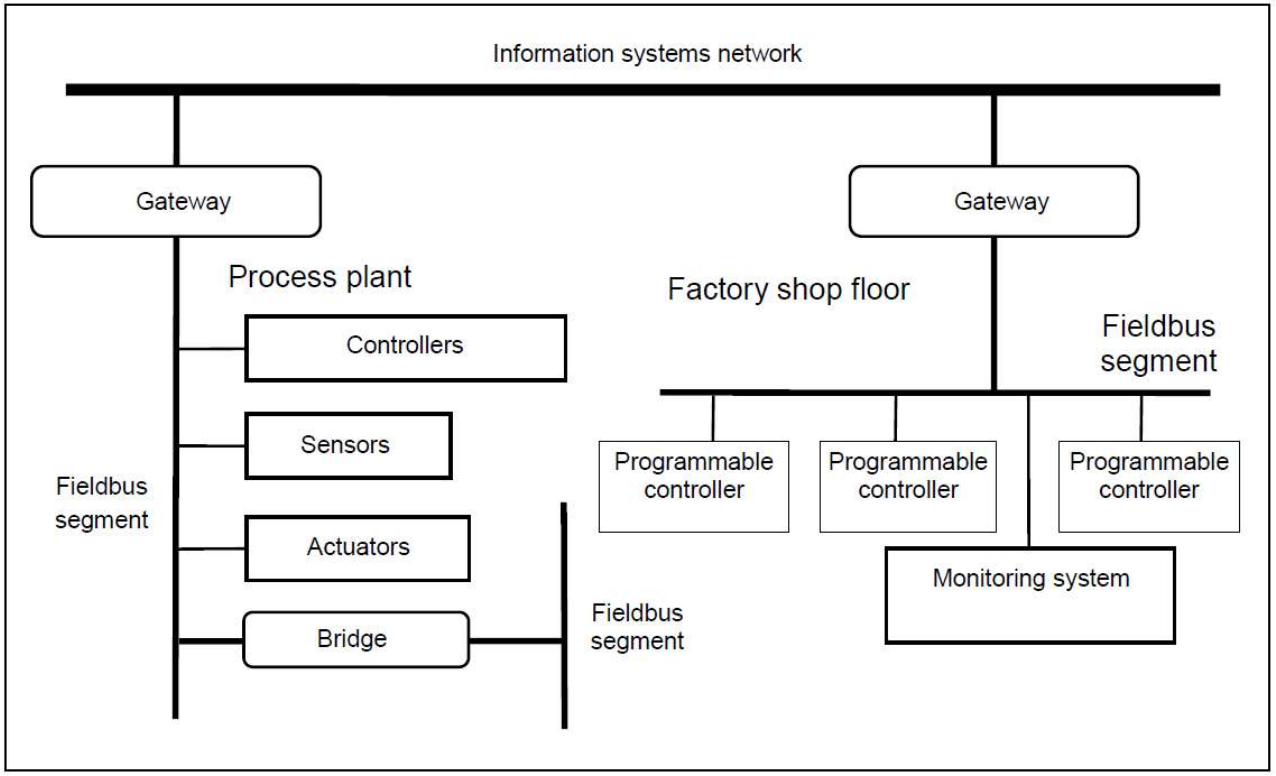


Fieldbus specifications : IEC 61158/ 61784 series
Industrial communication networks

Industrial process measurement and control

Data communication networks

Multilayer applications



Protocols normalized by IEC 61158/ 61784

	Name	Vendor
1.	Fieldbus Foundation,	EU
2.	ControlNet, EtherNet/IP, DeviceNet	ODVA
3.	PROFIBUS, PROFInet	Siemens
4.	P-Net,	Danmark
5.	WordFIP	Alstom, Cegelec
6.	INTERBUS	Phoenix Contact
7.	Swiftnet (retired)	Boeing
8.	CC-Link	Mitsubishi
9.	HART	Hart
10.	Vnet/IP	Yokogawa
11.	Tcnet	Japon
12.	EtherCAT	EtherCAT group
13.	ETHERNET Powerlink	Open source
14.	EPA	Chine
15.	MODBUS-RTPS	Schneider
16.	SERCOS	Sercos
17.	RAPIEnet	Korea
18.	SafetyNET p	Pilz Gmbh

All these protocols are incompatible each other
IP gateway is the solution to transfer data

Convergence Réseaux Industriels, réseaux IT

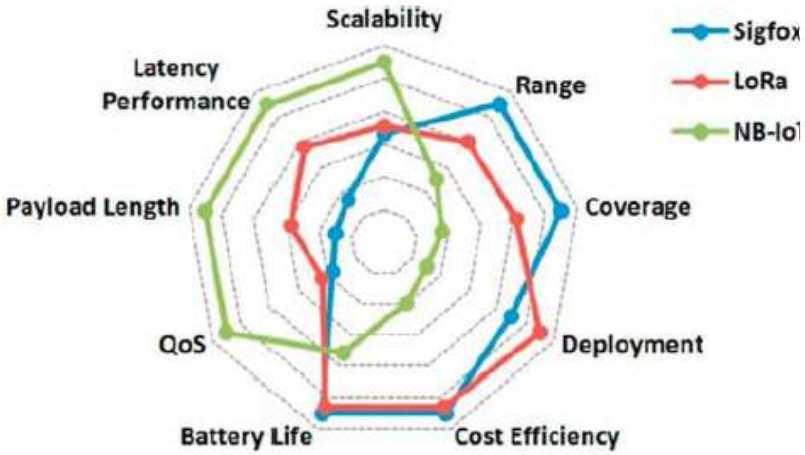
Ex :

- ProfiNet
- Can over Ethernet
- Modbus over TCP/IP

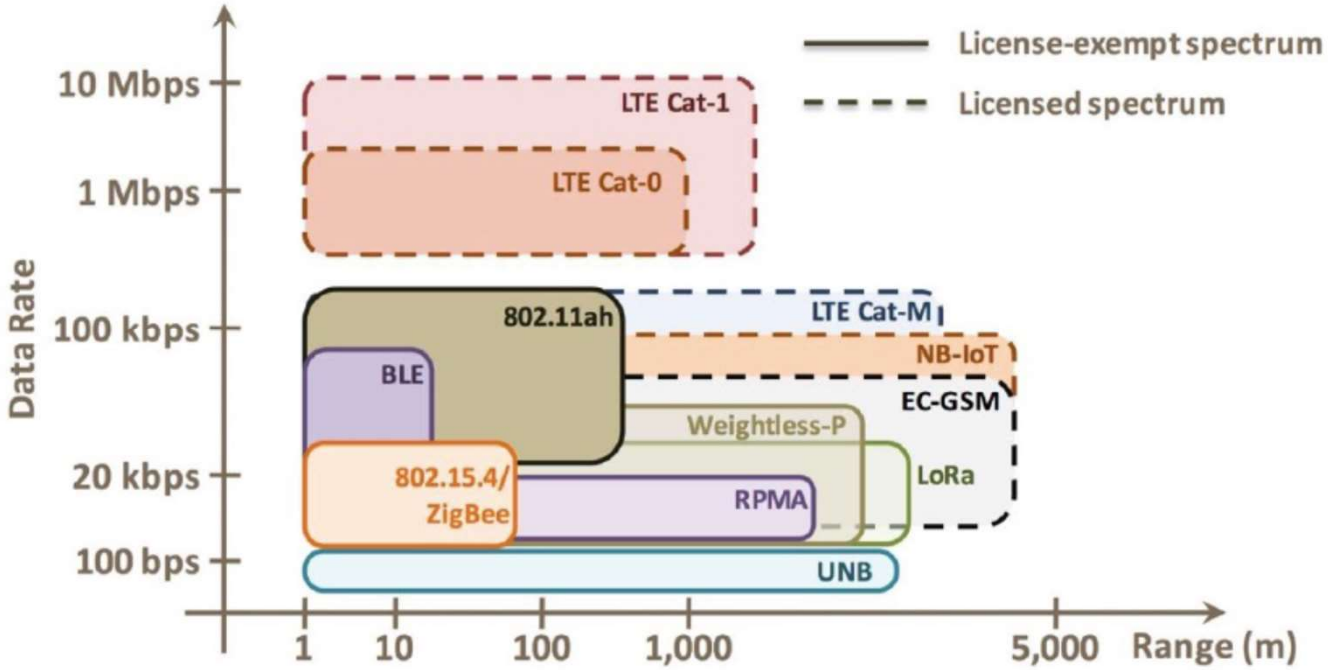
Wireless network

The main evaluation criteria for Low Power Wide Area Network - LWPAN:

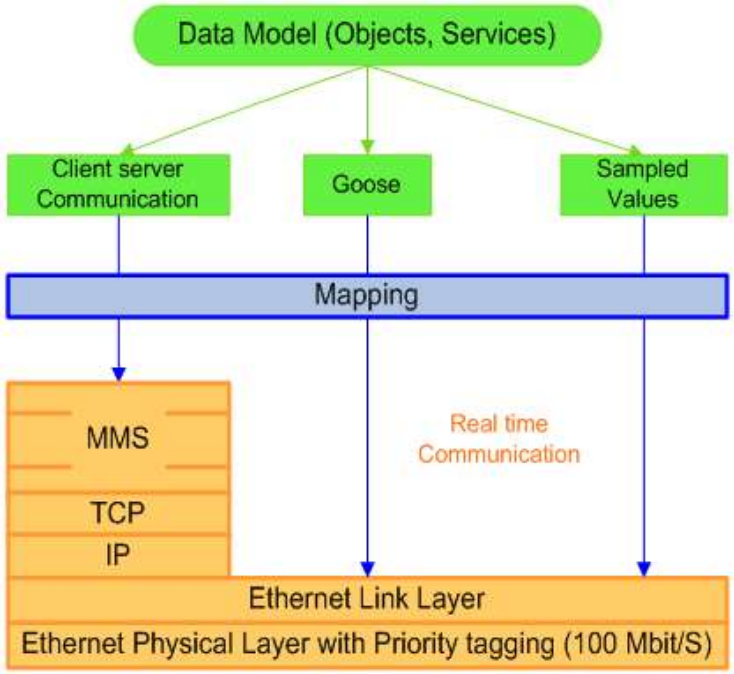
- Range / Coverage
- Deployment / infrastructure cost
- Payload / Latency / Performance
- Consumption (battery life)
- Quality of service / Latency



Source https://iotfactory.eu/



IEC 61850
Communications aspects based on Switched Ethernet => for Smart Grids



- Satisfying real time performance by the standard in developing extension cards that can transmit critical real-time signals at serial network level
- Development of a new appliction layer allowing to track the dialogue according to the IEC 61850 standard
- New equipment design playing the role of Ethernet switch/ IEC 61850 converter and data concentrator

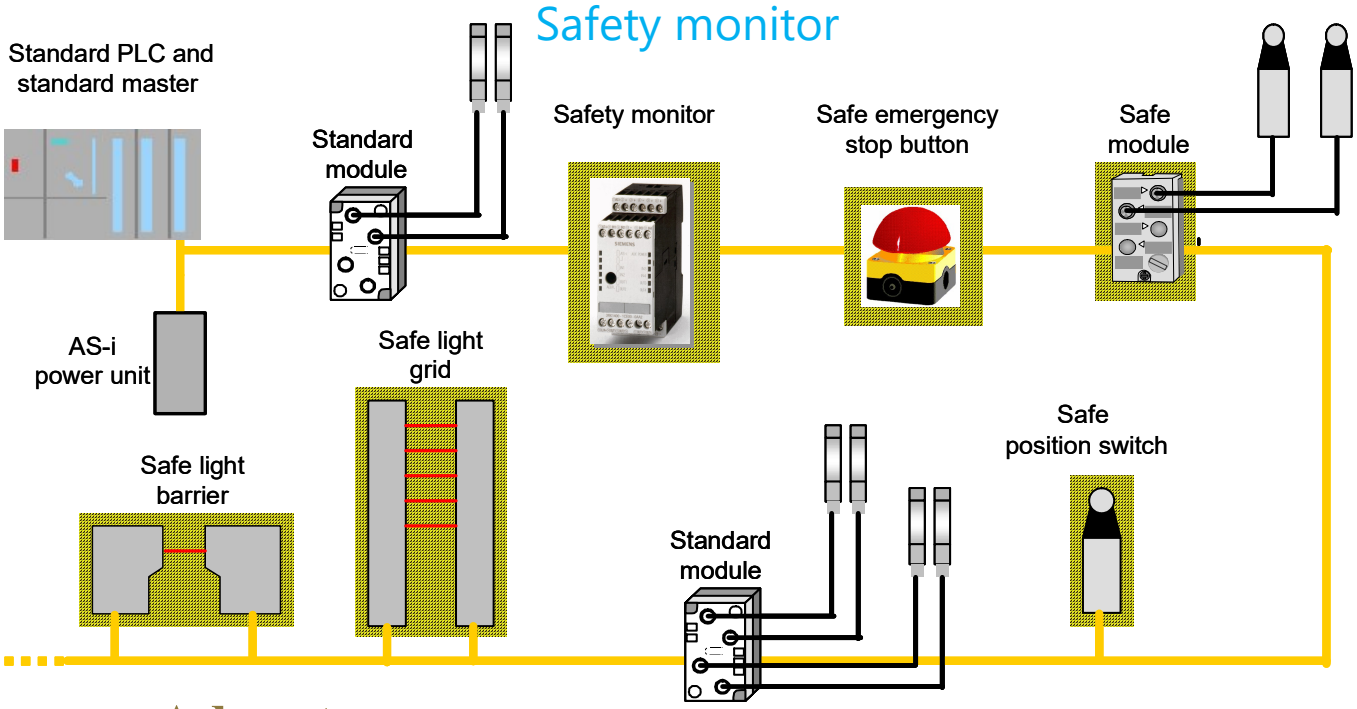
Safety networks

- 2 aspects of operational safety (see also IEC 61508)
  - Reliability, Maintainability, Availability
- For networks:
  - Offer network monitoring and administration services
  - Allow the implementation of redundancy mechanisms (master, medium…), watchdog…
- Safety
  - Ensure the non-occurrence of dangerous events

  - **Example of Safety networks**
  - ProfiSafe
  - CanOpenSafe
  - ASI Safety at Works
  - Device Net
  - …

Cat.	Prescriptions / Behaviour (EN 954)
B	a fault can lead to the loss of the safety function
A1	idem but with a lower probability thanks to proven principles
A2	a fault → loss of the safety function between control intervals
A3	for a single fault, the safety function is assured
A4	for several faults, the safety function is assured

ASI Safety at Works



Advantages

- cabling reduction
- Safety and non-safety on one bus
- Groups of safety signals
- EN 954 – 1 category 4 compliant
- Certified: TUV and BIA
- No AS-i wiring changes needed

1.3 Quelques considérations sur les stratégies d’attaques

Types of targets

- Convenient target *(cible opportune)*
  - By “chance”: detected by the pirates in the search of least protected machines or servers
  - What to do?: update the systems
  - To test the system (try to find faults)
- Chosen target *(cible de choix)*
  - Precise Target: strategic interest of the company …

Types of attacks

On classe les types d'attaques en deux catégories :

- Attaques passives
  - Interception, écoute, analyse
- Attaques actives
  - Modification, destruction
  - Interruption, perturbation
  - Dénis de service

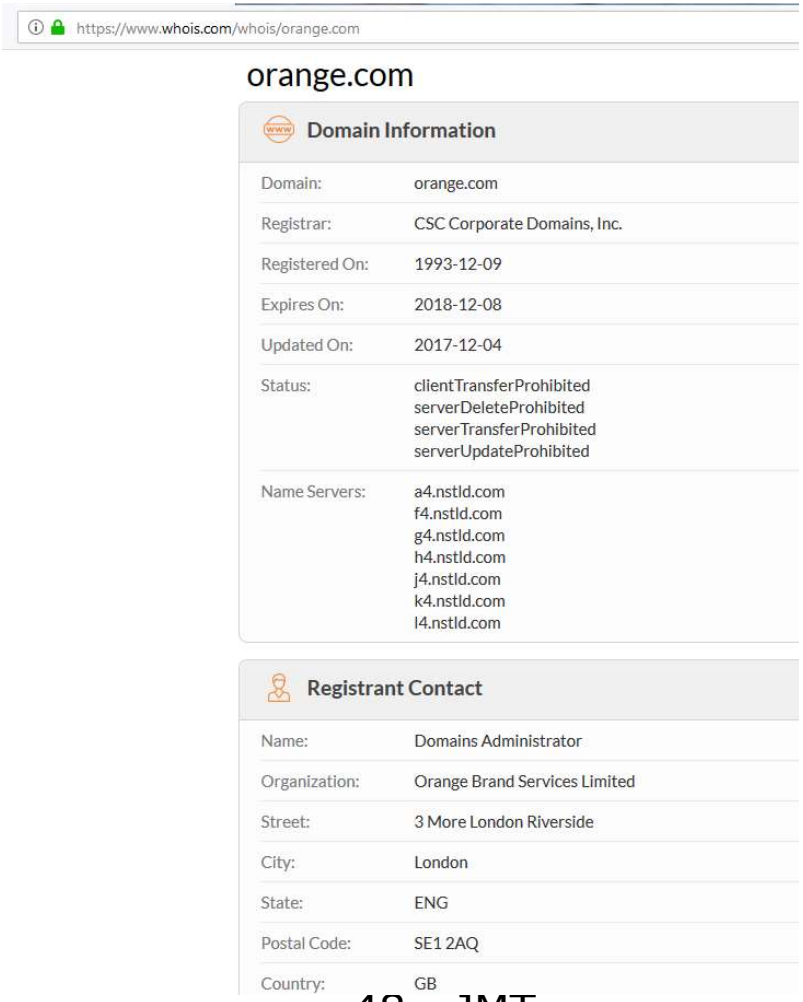
1 Reconnaissance et collecte de renseignements (1/4)

- Noms de domaine, serveurs DNS, blocs d'adresses IP assignés
- Adresses IP accessibles de l'extérieur
- Services présentant une cible valable
  - www, ftp, e-mail…
- Types de machines sur lesquels les services s'exécutent
  - Systèmes d'exploitation et numéro de version => utilisation des failles connues exploitables
- Mécanismes en place contrôlant l'accès au réseau
- Type de pare-feu et d'IDS (Intrusion Detection System)

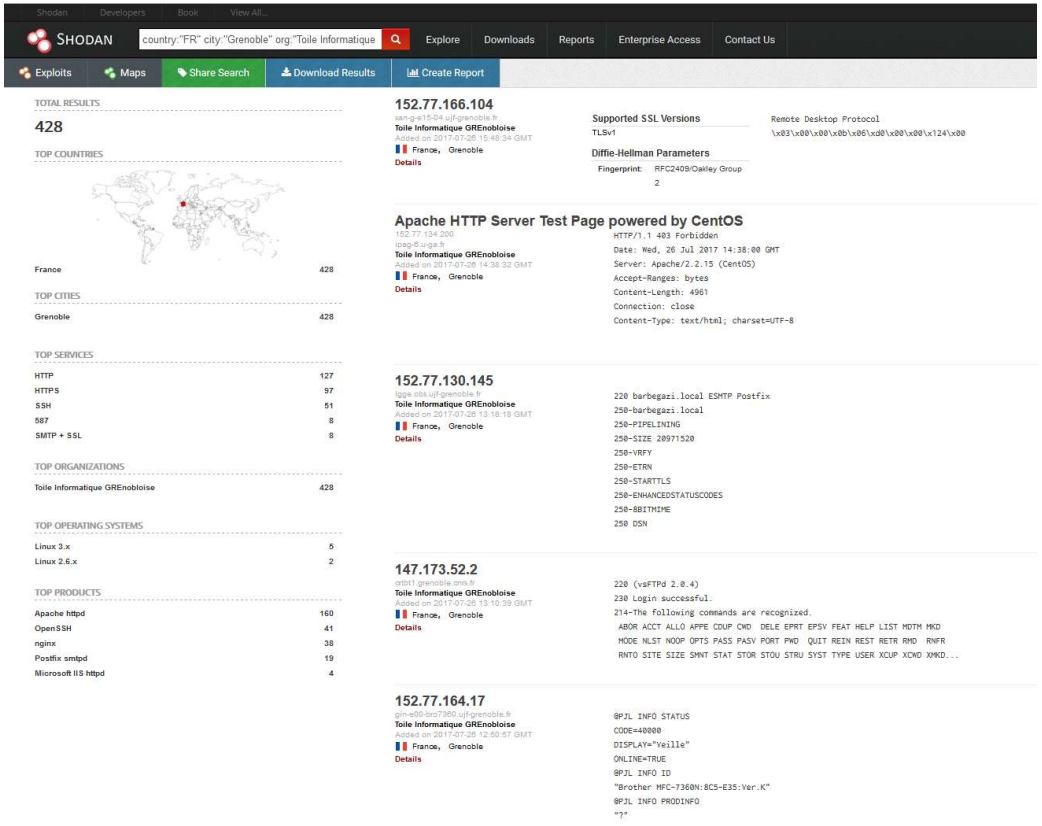
1 Reconnaissance et collecte de renseignements (2/4)

- Noms d'utilisateurs, groupes, tables de routage, informations SNMP (techniques d'énumération des sources du système)
- Emplacement physique des équipements et systèmes
- Protocoles de réseau utilisés (IP, IPv6, IPSec, SSL, OSPF (*Open Shortest Path First*), RIP (*Routing Information Protocol*))
- Cartographie du réseau
- Type de liaisons d'accès
  - Accès traditionnel (frame relay, large bande)
  - Accès par numérotation téléphonique (modem)
  - Accès par Wi-Fi
- Approche par « ingénierie sociale » (consiste à interroger des gens et à récupérer des informations en les piégeant)
  - Informations sur les personnes, leurs noms, numéros de téléphone, situation dans l'entreprise, adresse…

1 Reconnaissance et collecte de renseignements : WHOIS (3/4)



1 Reconnaissance et collecte de renseignements : Shodan (4/4)



2 Scan des services et des ports

- Scan détaillé d'une cible (NMAP = Network Mapper)

3 Enumération

- Extraction d'information sur les comptes valides et les ressources
  - ressources réseau et partages
  - utilisateurs et groupes (organisation fct du type de Système d'Exploitation)
  - applications
  - bandeaux envoyés en réponse par les équipements

4 Obtenir un accès

- Attaque de niveau système d'exploitation
  - Utilisation des fonctionnalités du S.E.
- Attaque de niveau application
  - Utilisation des fonctionnalités de l'application
- Attaque profitant d'une mauvaise configuration
  - Système "ouvert", configuration par défaut (nom et mot de passe administrateur !), nombreuses fonctionnalités activées
- Attaque utilisant des scripts hébergés
  - Scripts disponibles sur le système et quelques fois activés par défaut (Unix/Linux)
  - Détournement de requêtes SQL lors de l'interrogation d'une base de données via interface web
- Attaque automatisée (ex : scan du port 80 d'un bloc entier d'adresses de classe C afin de chercher une faille)
- Attaque ciblée : beaucoup plus rare mais difficile à détecter (pirates expérimentés)

5 Extension des privilèges acquis

- Si le pirate a réussi à entrer sur le système avec un mot de passe "faible" => extension des droits
  - Exécuter du code pour obtenir du privilège
  - Chercher à déchiffrer d'autres mots de passe
  - Rechercher des mots de passe enregistrés en clair
  - Rechercher d'éventuelles relations inter-réseaux
  - Identifier des permissions de fichiers ou de partages mal configurées

6 Couverture des traces

- Dissimuler à l'administrateur le fait que l'on ait pénétré le système
  - Windows : Eliminer les entrées dans le journal d'événements et le registre
  - Unix : vider le fichier d'historique (exécution du programme *log wiper*)

L'attaquant nettoie les journaux mais ne les supprime pas !

Types of attacks (1/3)

- DoS (Denial of service) : To decrease the system capabilities
  - DDoS (Distributed DoS) : idem but with an attack coming from several sites (http://grc.com/dos/grcdos.htm)
  - SYN Flood: the attacker floods a system with SYN synchronization packets in order to initiate connection requests (these requests are never finished) => strong exploitation of the processor resources, memory, network cards => Denial of service
  - UDP Flood: attack which submerges a system with UDP packets => prevent it from treating the valid requests for connection (often on the DNS port 53) (ICMP Flood: idem to submerge a system with ICMP messages (Internet Control Message Protocol) by using the Ping utility)
  - Ping of Death: possibility to "ping" with a too huge packet which can cause a whole range of uncontrolled reactions on the targeted system: Denial of service, shut down, freezing or restarting

Types of attacks (2/3)

- Scan of ports: Packets sent by using the port numbers in order to scan available services, hoping that a port answers
- Eavesdropping: the goal is to violate the confidentiality of the communication (by sniffing packets on the local area network or by intercepting wireless communications)
- Man-in-the-middle: the attacker acts between the two ends of the communication as if he were the awaited interlocutor: harmful effects on the confidentiality and possibly the integrity

Types of attacks (3/3)

- Java/ActiveX/ZIP/EXE: dangerous Java components or Active X hidden in Web pages, Trojan dissimulated in a ZIP/TAR or EXE file
- Breaking into a system: by violating the authentication or the access control, the attacker obtains the possibility of controlling the communication: effects on the confidentiality and the integrity
- Virus: shortcuts the authentication and the access control with the aim of carrying out destroying code: effects on the availability of the machine and/or the network
- Trojan: virus hidden in a function usually used, program being carried out on the pirated machine to send information to the pirate
- Worm *(ver)*: explore and automatically exploits the faults of a system, without action of the user => problems of availability

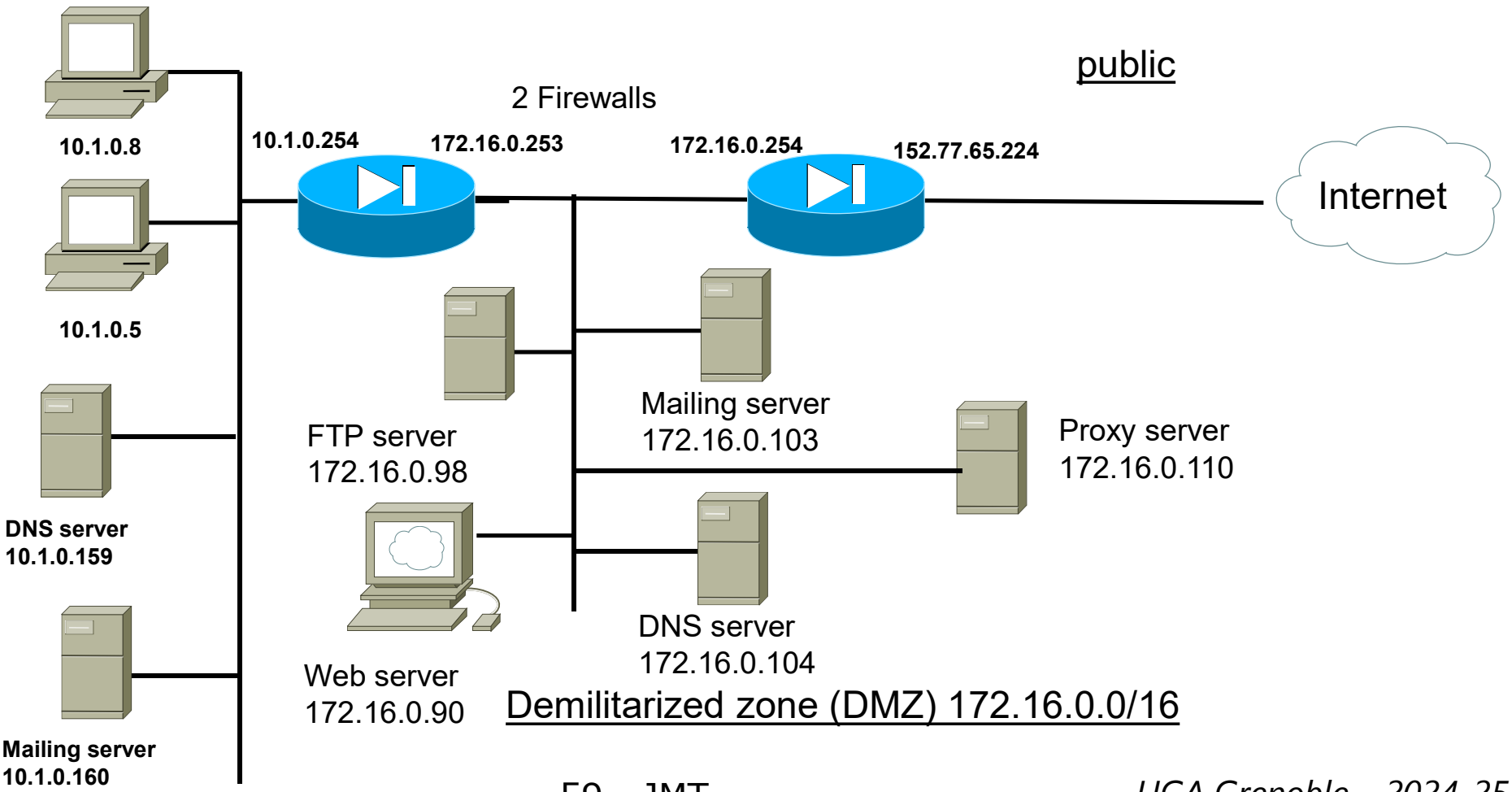
Detection of attacks

- By human beings (culture)
- By specialised software or hardware (anti-virus, firewalls)
- By ports normally non open (alert scans)
- By abnormal reactions
  - During connections, when you are absent
  - Of the applications (slow, double validation)
- By abnormal overloads
  - Network resources
  - Processor, disk, memory resources
- By invalid data
- By data losses

Every abnormal event should incitate to remain very “attentive” !

1.4 Pare-feu, Zone démilitarisée

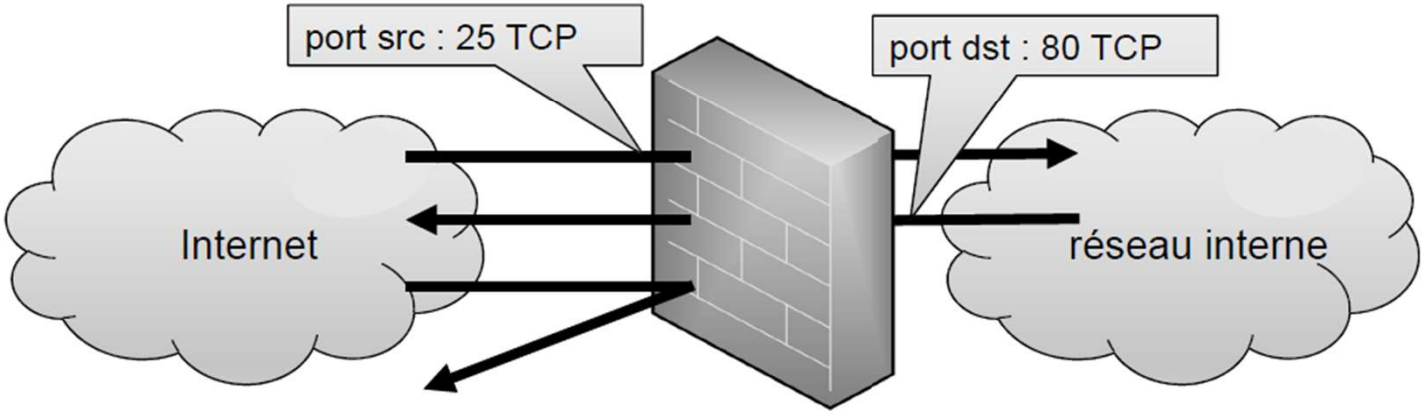
DMZ


Internal Corporate network (private) 10.1.0.0/16
public
2 Firewalls
10.1.0.254
172.16.0.253
172.16.0.254
152.77.65.224
Internet
10.1.0.8
10.1.0.5
DNS server 10.1.0.159
Mailing server 10.1.0.160
FTP server 172.16.0.98
Mailing server 172.16.0.103
Proxy server 172.16.0.110
Web server 172.16.0.90
DNS server 172.16.0.104
Demilitarized zone (DMZ) 172.16.0.0/16

Filtrage stateless

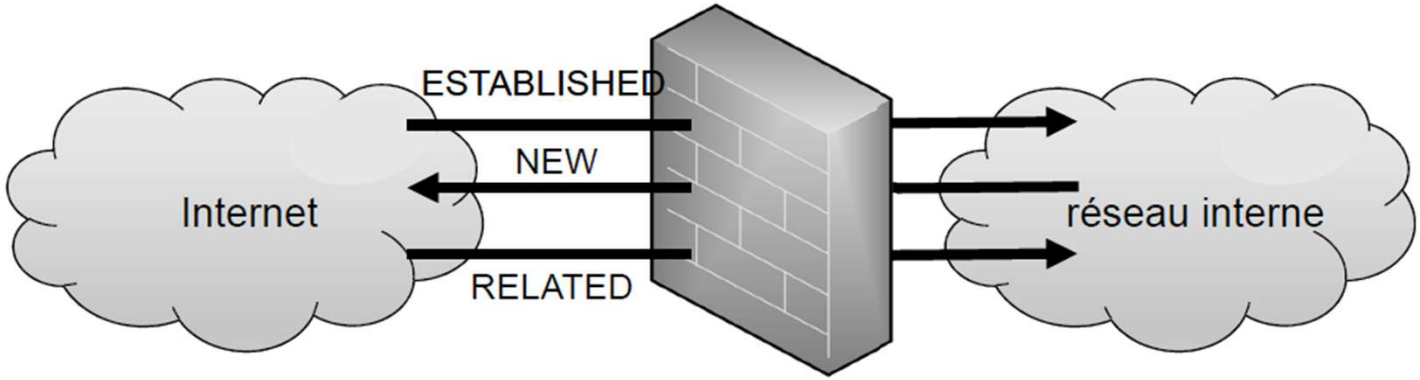
- Le filtrage ne prend pas en compte l'état du paquet

```
access-list 101 permit tcp any eq 25 host 195.83.80.5
access-list 102 permit tcp any any eq 80
access-list 101 deny ip any any log
```



Filtrage stateful

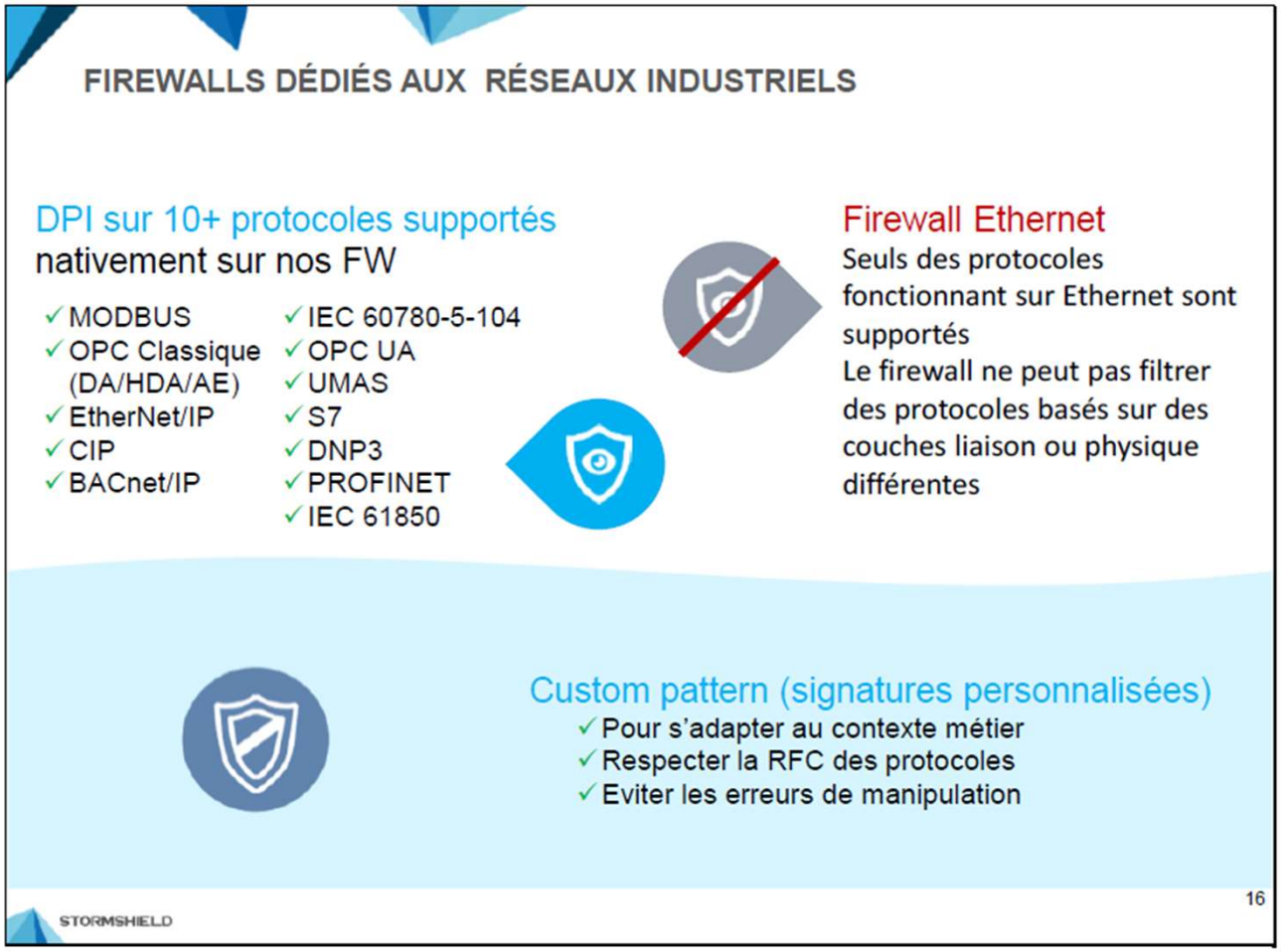
- Le filtrage prend en compte l'état du paquet
  - ESTABLISHED
    - Paquet associé à une connexion déjà établie
  - NEW
    - Paquet demandant une nouvelle connexion
  - INVALID
    - Paquet associé à une connexion inconnue
  - RELATED
    - Nouvelle connexion mais liée



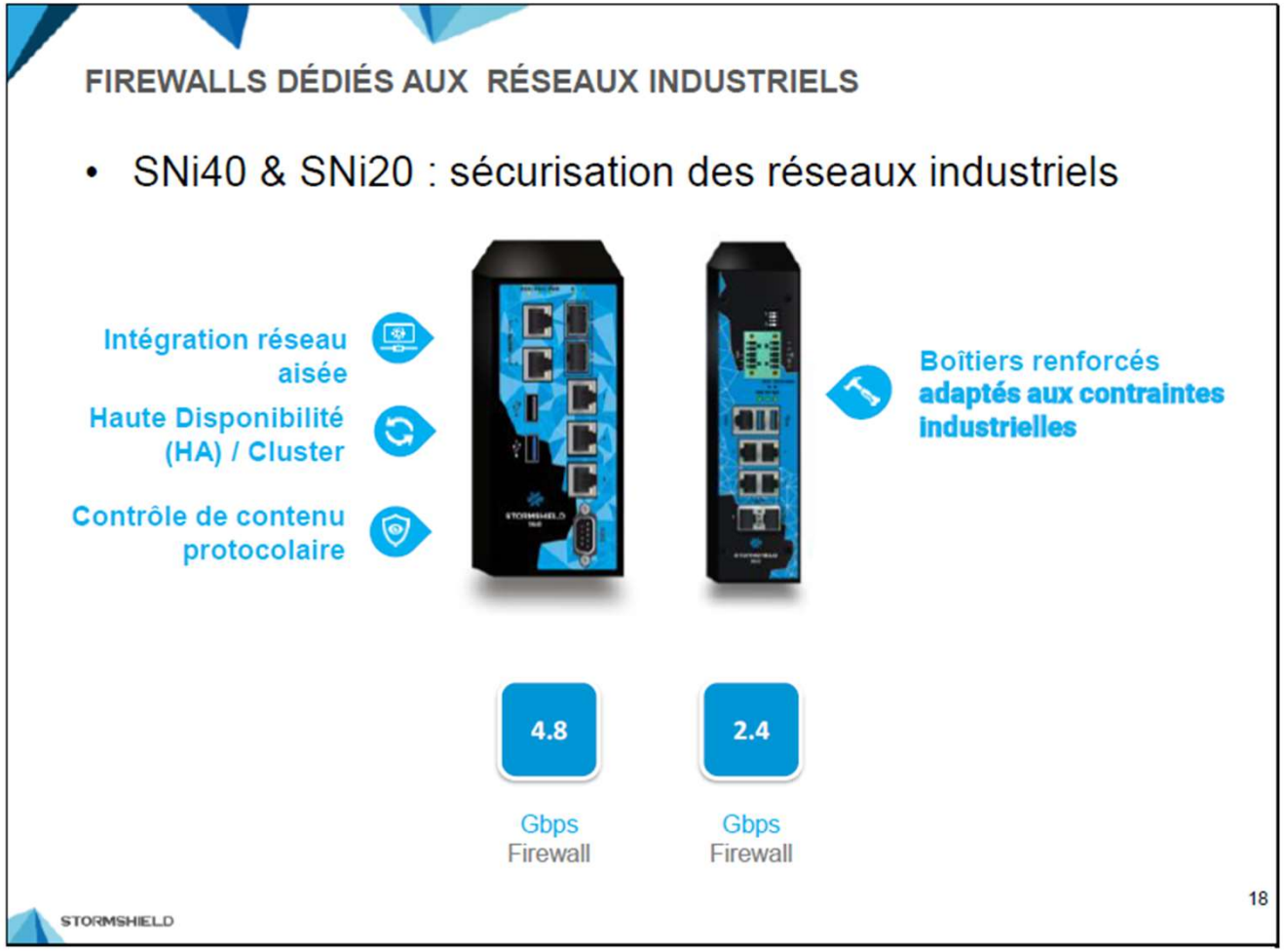
Pare-feu nouvelle génération

- *Next Generation FireWall* (NGFW)
- Centré sur le **type d'application** et **l'identité de l'utilisateur**
  - +800 protocoles, des milliers d'applications Web
  - S'ajoute au durcissement la politique de filtrage classique : fermeture de ce qui est interdit
  - Sur ce qui est ouvert : identification des applications (*application awareness*)
    - Exemple : autoriser l'accès au Web mais interdire Facebook

Pare-feu industriel (ex : Stormshield)



Pare-feu industriel



Exercise 1

- We use a stateful firewall
- The machines from the inside network should be able to reach any machine in the DMZ or outside (for the mail)
  - Access-list 1 permit mail 10.1.0.0/16 any eq 25
- The machines from the DMZ should be able to reach any machine in outside BUT NOT inside (for the mail)
  - Access-list 1 deny mail 172.16.0.0/16 10.1.0.0/16 eq 25 (should be before !)
  - Access-list 1 permit mail 172.16.0.0/16 any eq 25
- Concerning http
  - Any machine from inside should NOT reach directly an http somewhere, but the request should be sent to the proxy machine (using the 3128 port)
  - Access-list 1 permit tcp/udp 10.1.0.0/16 172.16.0.110 eq 3128
  - Any machine from the DMZ should NOT reach directly an http somewhere, but the request should be sent to the proxy machine (using the 3128 port)
  - No rule
  - The proxy should be able to reach any http server (port 80) everywhere
  - Access-list 1 permit tcp 172.16.0.110 any eq 80
- We should not forget the DNS aspects (port 53)
  - Access-list 1 permit tcp/udp 10.1.0.159 172.16.0.104 eq 53
  - Access-list 1 permit tcp/udp 172.16.0.104 a_specific_DNS_Server_outside eq 53
  - Access-list 1 deny any any any eq any

Exercice 2

- Soit une architecture autour d'un pare-feu à états
- On souhaite mettre en place :
  1. Toutes les machines du réseau interne doivent pinguer la DMZ ou l'extérieur.
  2. Toutes les machines de la DMZ doivent pinguer l'extérieur mais pas le réseau interne.
  3. Toutes les machines de l'intérieur doivent pouvoir sortir en http ou https en passant par le proxy
  4. Le serveur DNS du réseau interne doit pouvoir joindre le DNS de la DMZ sur le port 53.
  5. Le serveur DNS de la DMZ doit pouvoir joindre un DNS externe (IP: 143.210.47.211).
- Actions à mener
  - Si besoin, mettre en place des règles de translation
  - Ecrire les règles de filtrage et les commenter
- Audit de notre stratégie de sécurité
  - Toutes les machines du réseau interne doivent pinguer la DMZ ou l'extérieur. Est-ce une bonne stratégie ? Pourquoi ?
  - Toutes les machines de la DMZ doivent pinguer l'extérieur mais pas le réseau interne. Pourquoi cette stratégie ?

Règles de filtrage

Protocole	Source	Destination	Service (numéro port)	Action	Commentaire
ICMP	10.1.0.0/16	Any	Any	Pass	Réseau interne ping partout
ICMP	172.16.0.0/16	10.1.0.0/16	Any	Block	Pas de de DMZ vers réseau interne
ICMP	172.16.0.0/16	Any	Any	Pass	DMZ pingue partout
TCP	10.1.0.0/16	172.16.0.110	Httpproxy	Pass	Passage flux TCP réseau interne => proxy
TCP	172.16.0.110	Any	http, https	Pass	Passage flux TCP du proxy vers les serveurs http partout
TCP,UDP	10.1.0.159	172.16.0.104	Dns (port 53)	Pass	DNS Passe du réseau interne => DMZ
TCP,UDP	172.16.0.104	143.210.47.211	Dns (port 53)	Pass	DNS passe de DMZ vers DNS externe

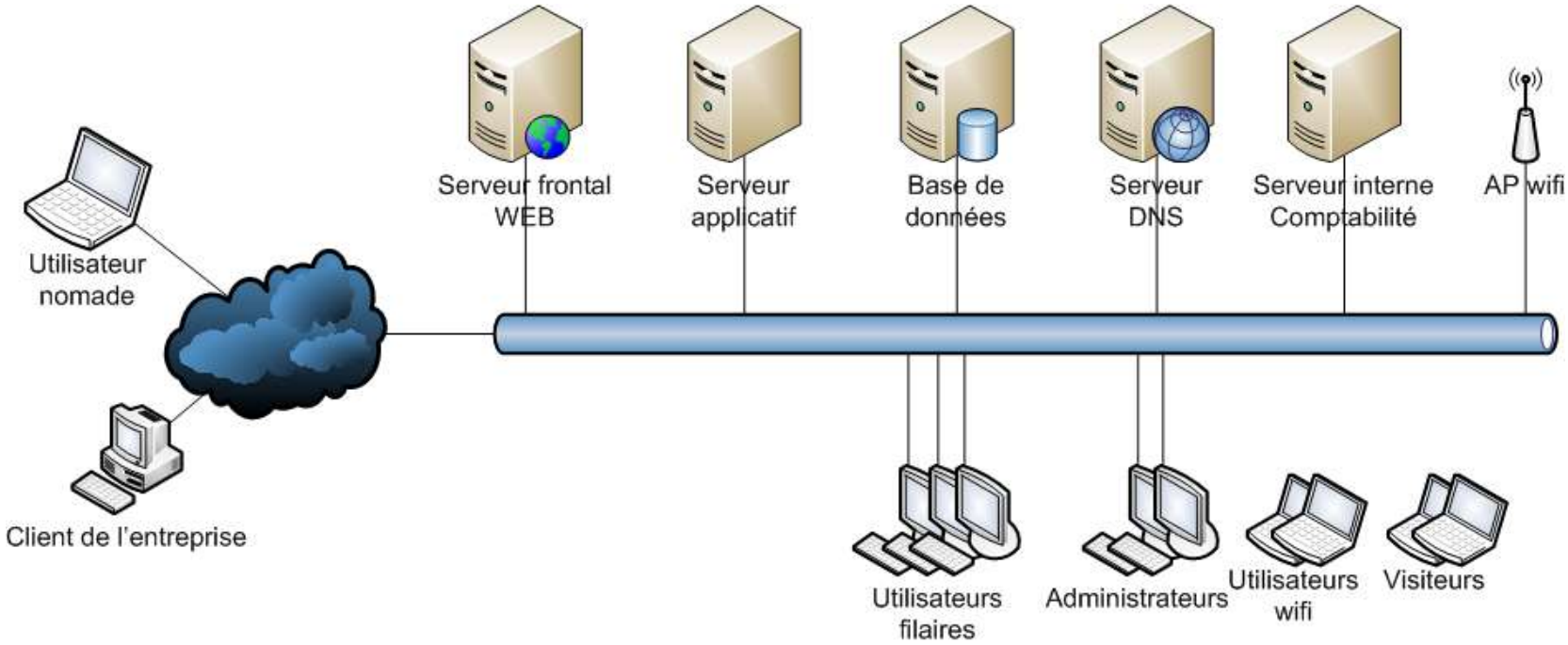
Ex : Sécurisation d'un réseau simple : D'après Cyril Bras

1.4.5 Exemple pratique de sécurisation avec un réseau simple

Prenons l'exemple d'un réseau d'entreprise « à plat ». Caractéristiques de cette entreprise :

- Elle fournit un **site WEB de e-commerce** ;
- Certains employés se connectent sur le **réseau local filaire**, d'autres se connectent en **wifi** ;
- Certains employés sont **nomades** et doivent donc se **connecter à distance** ;
- Il existe deux catégories principales d'utilisateurs : les **utilisateurs « standard »** et les **administrateurs** du S.I. ;
- Afin de fonctionner, l'entreprise possède également des **serveurs internes** (comptabilité, wiki, etc.) ;
- L'entreprise souhaite permettre à ses **visiteurs** de se connecter en **wifi** afin de naviguer sur internet.

Exemple pratique de sécurisation avec un réseau simple



Réseau « à plat », avant sécurisation

Exemple pratique de sécurisation avec un réseau simple

Voyons comment nous allons pouvoir sécuriser ce réseau.

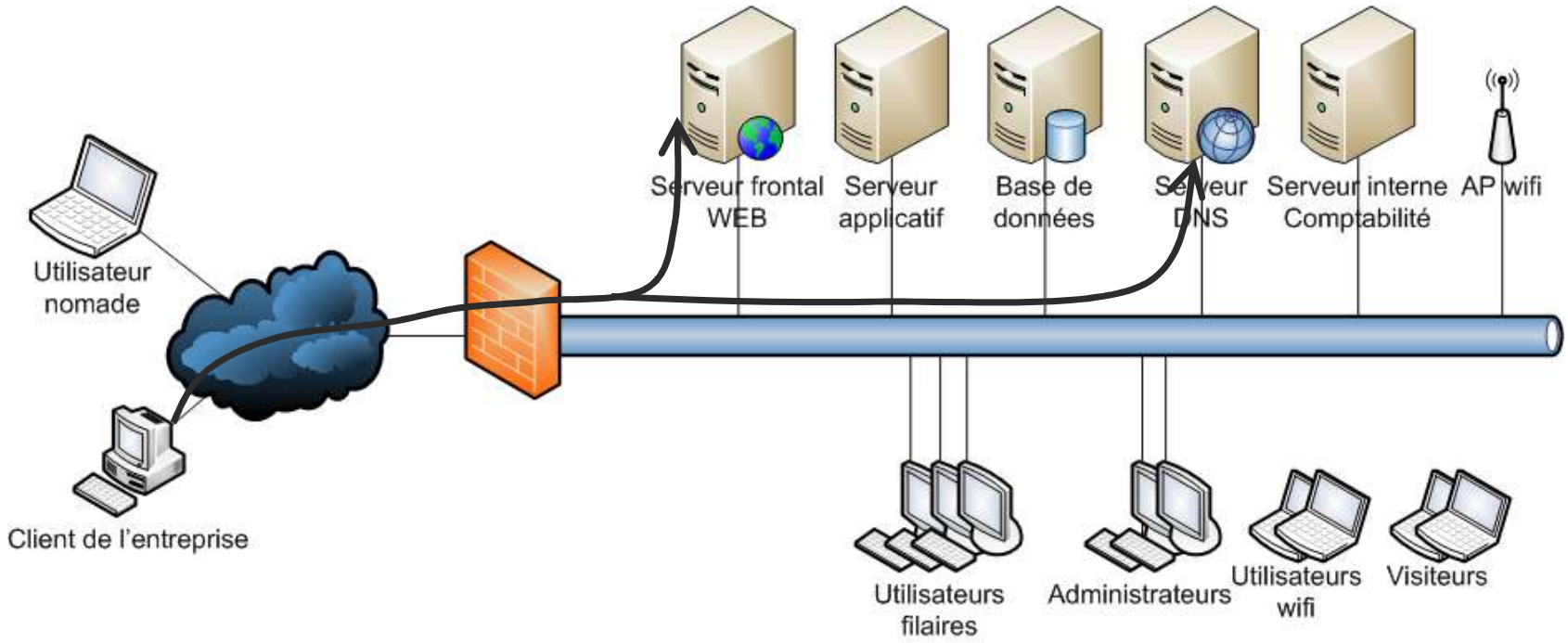
•Note : il existe plusieurs façons d'améliorer la sécurité de ce réseau, nous en présentons ici uniquement les grandes lignes. Cet exercice n'est ni exhaustif ni la seule solution possible.

Parmi les nombreuses faiblesses architecturales de ce réseau, nous pouvons identifier au moins le problème suivant :

•Le réseau est **directement connecté à Internet**, i.e. tous les systèmes et utilisateurs et systèmes peuvent communiquer avec l'extérieur (attention aux **fuites de données !**) et **tout Internet peut se connecter sur notre réseau interne.**

Corrigeons cela en implémentant un **pare-feu** en frontal qui va autoriser uniquement les flux entrants vers le serveur WEB (TCP/80 et TCP/443) et le serveur DNS (UDP/53 et TCP/53). Ainsi, Internet ne pourra plus accéder au reste du réseau interne

Exemple pratique de sécurisation avec un réseau simple



Réseau « à plat », avec un pare-feu en frontal

Exemple pratique de sécurisation avec un réseau simple

Le pare-feu empêche – certes – la connexion directe entre internet et le réseau interne, mais :

•Au cas où le serveur WEB présente une **vulnérabilité**, un hacker présent sur Internet peut potentiellement **prendre la main sur ce serveur**, puis **rebondir ensuite sur le réseau interne.**

Nous allons donc **segmenter** notre réseau en **différentes zones de criticité**, notamment :

•Une **DMZ (zone démilitarisée)** destinée à héberger tous les serveurs qui doivent être accessibles depuis internet, et uniquement ceux-ci. Ainsi, en cas de faille dans le serveur web, un attaquant aurait plus de difficultés pour rebondir sur le réseau interne ;

•Une zone destinée aux **serveurs internes** de l'entreprise ;

•Une zone pour les **postes de travail filaires des utilisateurs ;**

•Une zone pour les **postes de travail wifi des utilisateurs ;**

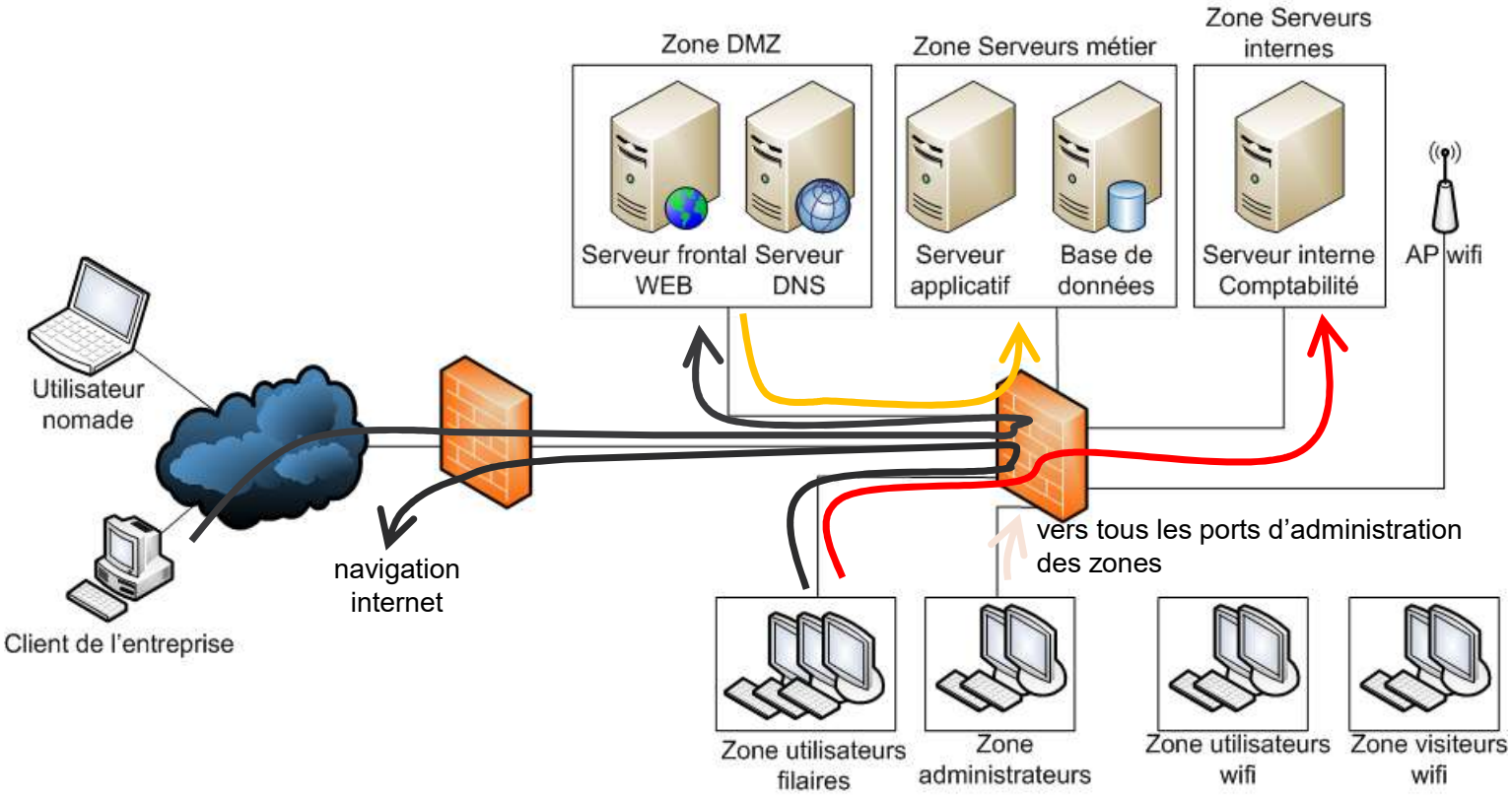
•Une zone pour les **postes wifi des visiteurs ;**

•Une zone pour les **postes de travail des administrateurs**, car ceux-ci ont besoin d'accéder à des interfaces d'administration (RDP, SSH…).

Afin que cette segmentation réseau soit efficace, nous faisons **passer tous les flux** (y compris internes) **par un deuxième pare-feu (interne)** afin que seuls les flux que nous allons configurer soient autorisés.

•Note : on observe malheureusement souvent des réseaux segmentés mais non filtrés. Cela ne sert à rien en terme de sécurité, car toutes les zones peuvent communiquer entre-elles.

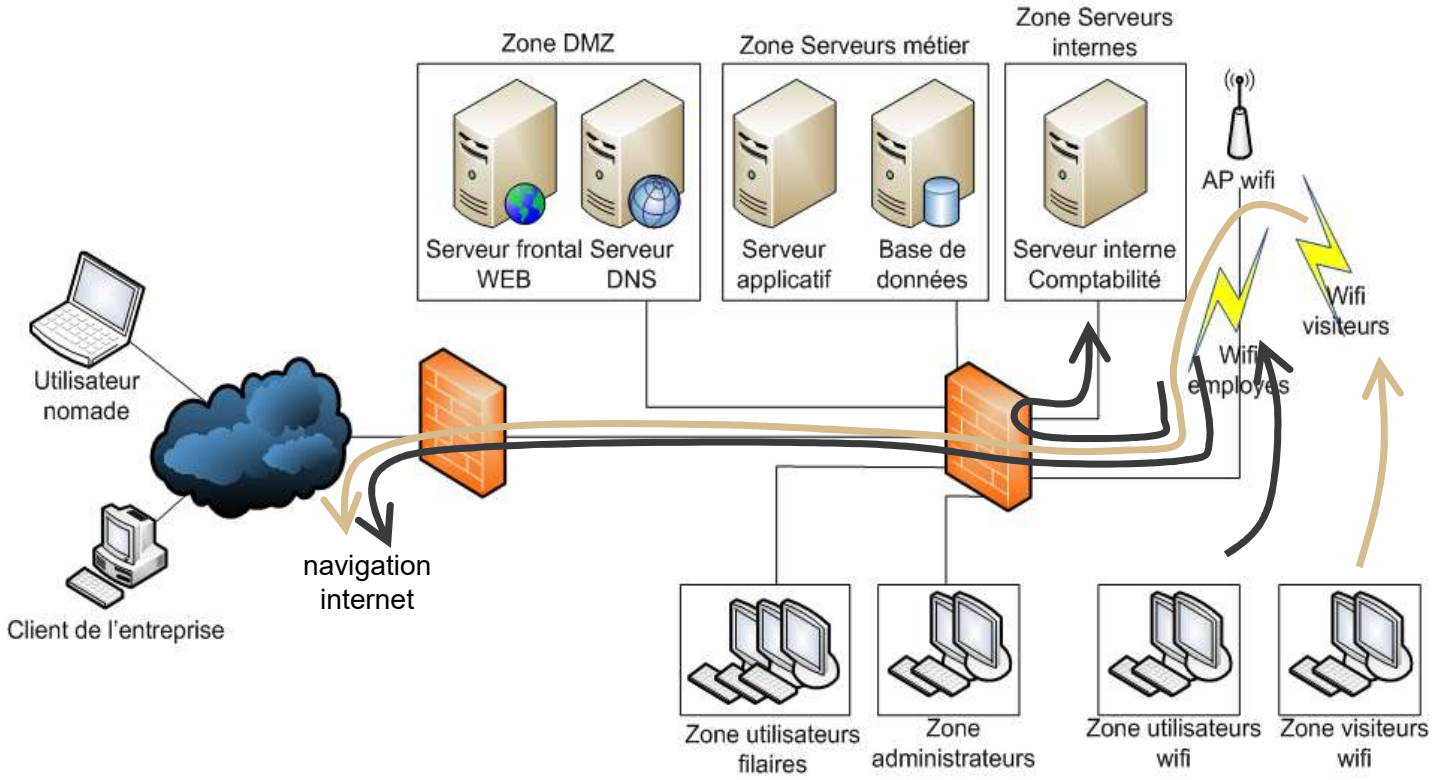
Exemple pratique de sécurisation avec un réseau simple



Réseau avec des zones segmentées, et un filtrage systématique via le pare-feu, y compris pour les flux internes.

Exemple pratique de sécurisation avec un réseau simple

Le point d'accès wifi doit être accessible aux visiteurs et aux employés internes. Puisque le besoin d'accès aux ressources est différent pour ces 2 populations, nous allons donc implémenter deux SSID (**deux réseaux wifi distincts**, portés par le même point d'accès, et dont le pare-feu filtrera les flux).



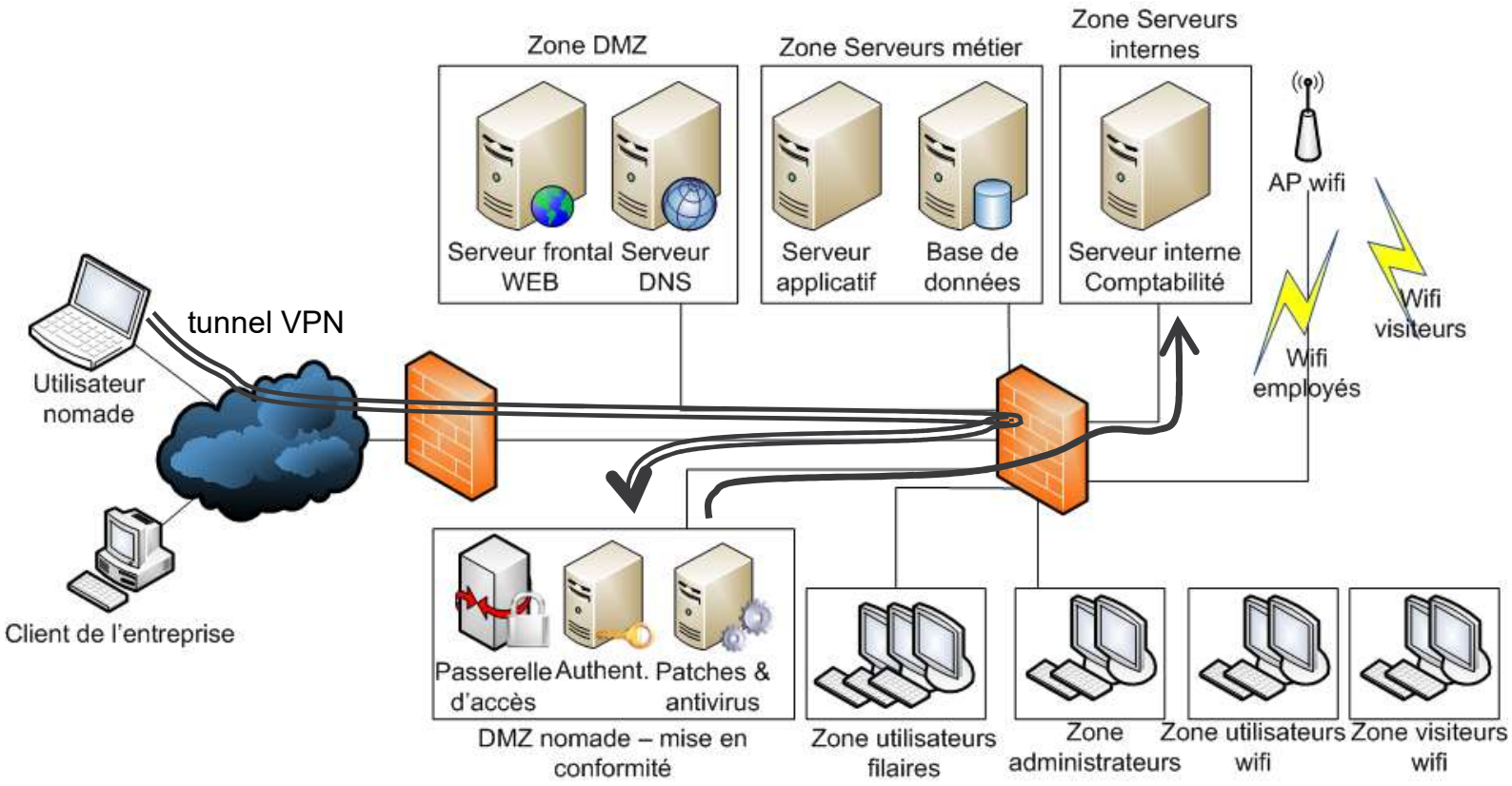
Deux réseaux wifi, dont les flux sont filtrés différemment.

Exemple pratique de sécurisation avec un réseau simple

Nous devons également permettre aux **utilisateurs nomades de se connecter** au réseau interne depuis internet. Cela se fait via une DMZ spécifique, appelée zone de mise en conformité, dont le rôle est le suivant :

- Fournir l'interface d'accès au réseau interne depuis internet, en général via un **tunnel VPN** ;
- **Vérifier que le poste nomade et son utilisateur sont habilités** pour se connecter à distance ;
- **Vérifier le niveau de sécurité du poste** avant d'autoriser la connexion (**patches et anti-virus à jour** notamment) ;
- Si tout est OK, alors **autoriser les flux vers les zones internes** (et seulement celles qui sont nécessaires pour le métier), toujours en passant par le **pare-feu**.

Exemple pratique de sécurisation avec un réseau simple



Réseau avec DMZ de mise en conformité pour les postes nomades.

Exemple pratique de sécurisation avec un réseau simple

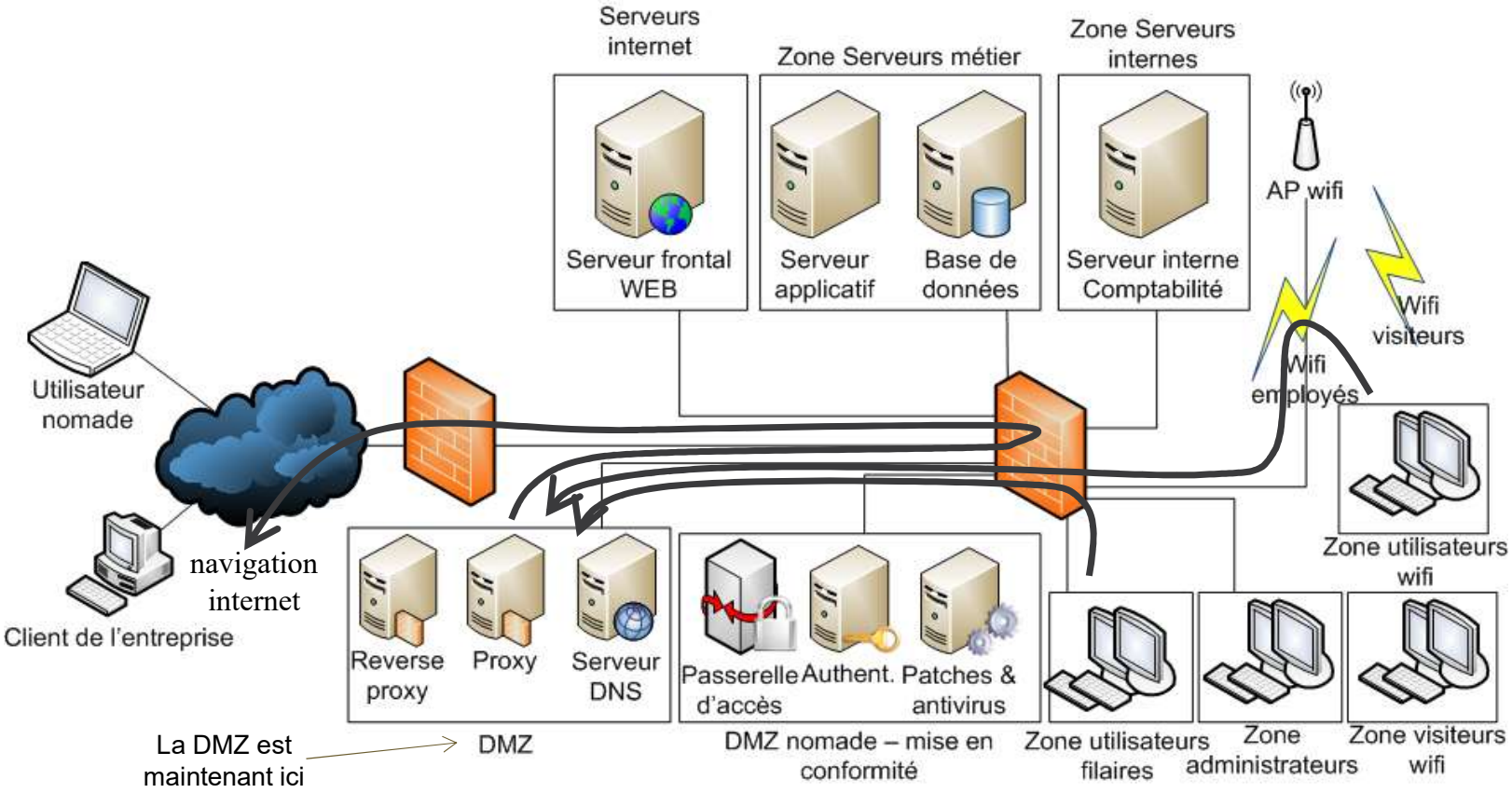
Enfin, il serait souhaitable de **mieux filtrer le trafic WEB** entrant et sortant :

- **Trafic sortant** : définir les catégories de sites WEB que les employés sont autorisés à naviguer, implémenter une liste blanche ou noire de sites autorisés/interdits ;
- **Trafic entrant** : analyser les requêtes WEB d'internet vers le serveur de e-commerce afin d'intercepter les requêtes malveillantes (injection, malware, etc.).

Nous allons donc recourir à un **proxy pour analyser les flux sortants**, et **un reverse-proxy pour analyser les flux entrants**. Ces équipements étant en coupure, ils empêchent donc les postes de travail des utilisateurs d'être connectés directement à Internet tout en leur permettant de naviguer sur les sites autorisés. Même remarque pour le serveur WEB : celui-ci n'est plus connecté directement sur Internet, c'est le reverse-proxy qui est maintenant en frontal.

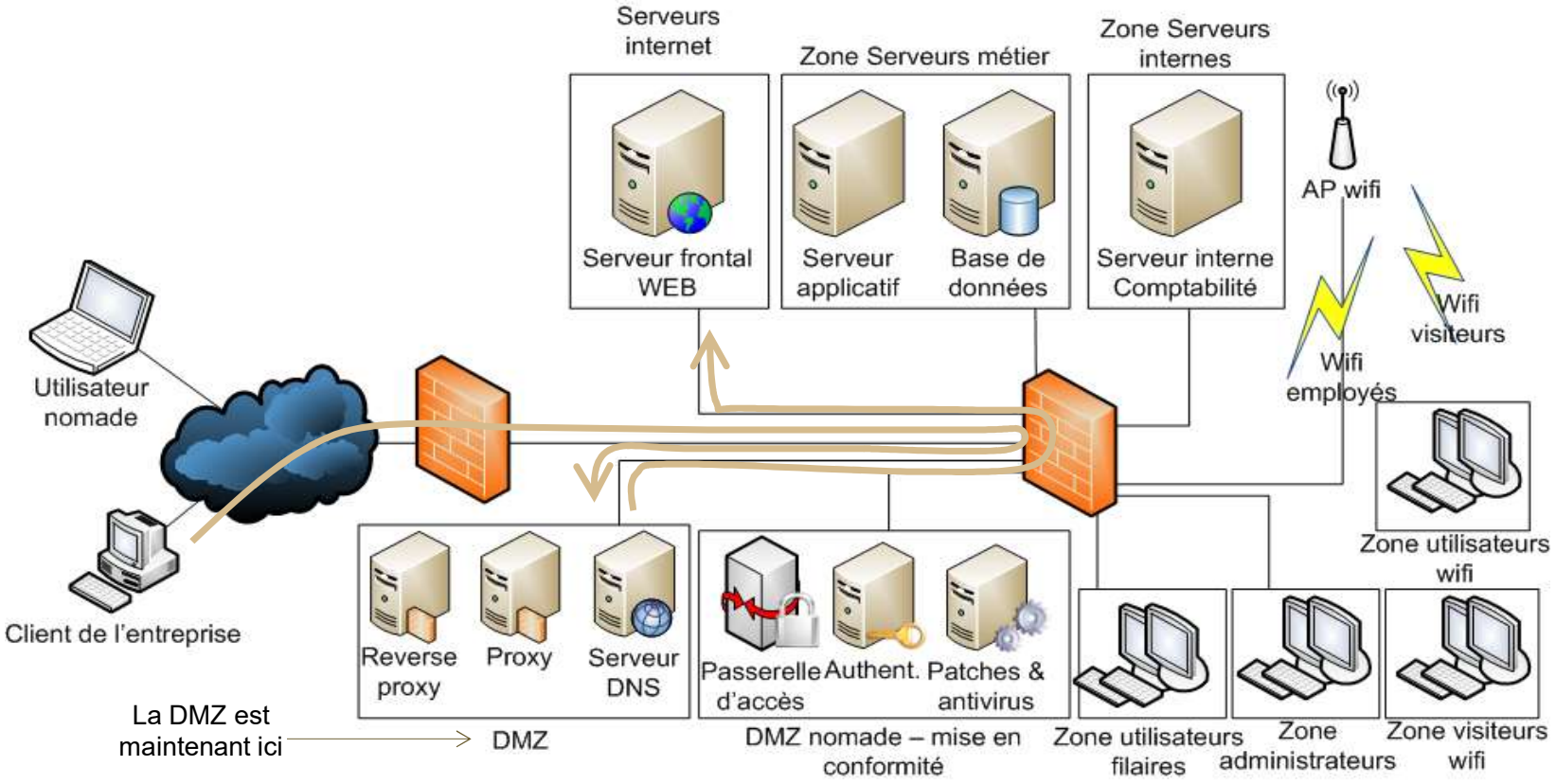
Puisque les proxies et reverse-proxies sont en frontal Internet, ce sont donc eux qu'il faut **placer dans la DMZ** maintenant.

Exemple pratique de sécurisation avec un réseau simple



Réseau avec un proxy et un reverse-proxy en coupure des flux de/vers Internet

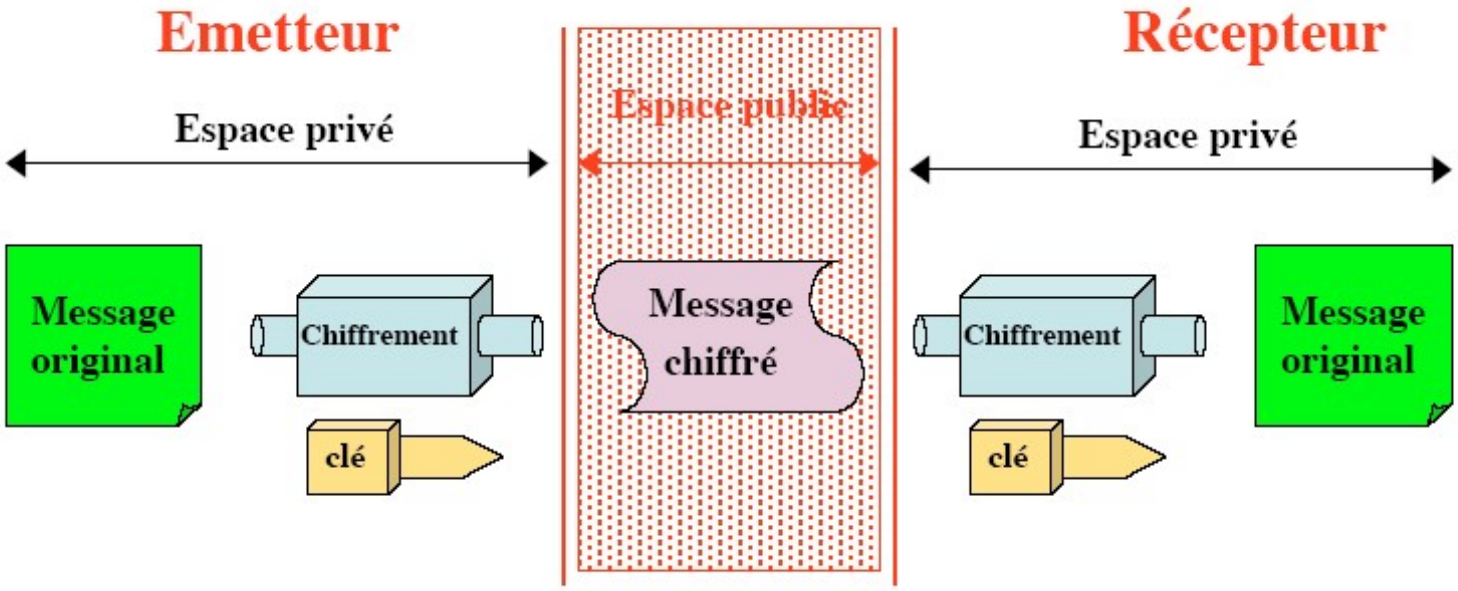
Exemple pratique de sécurisation avec un réseau simple



Réseau avec un proxy et un reverse-proxy en coupure des flux de/vers Internet.

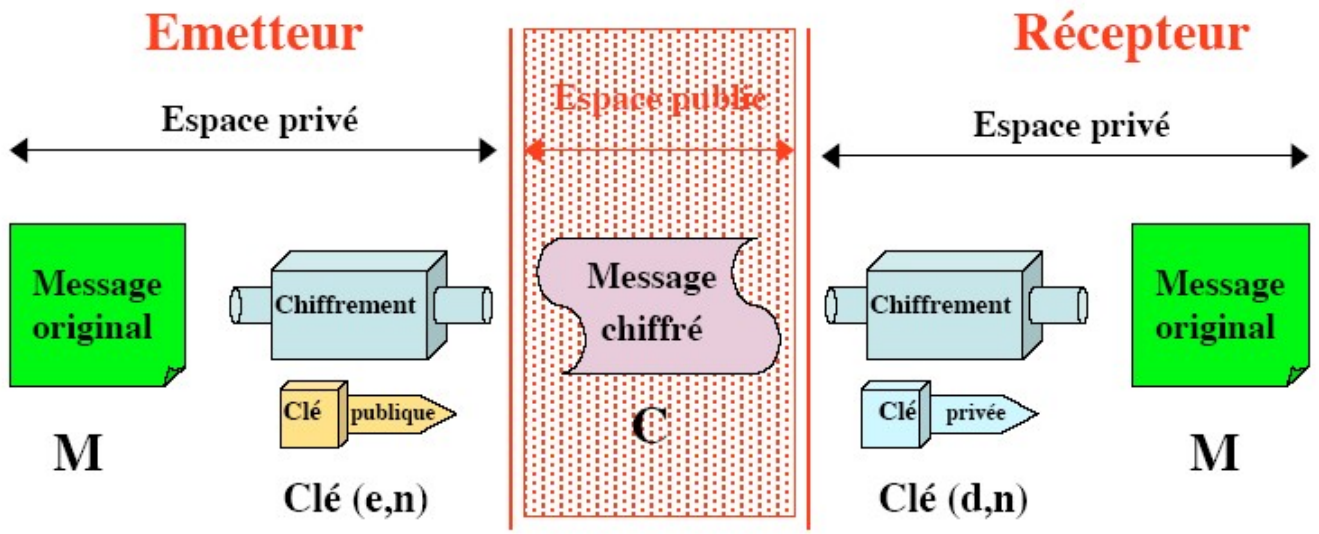
1.5 Enjeux de cryptographie

Chiffrement symétrique



- ✓La même clé est utilisée pour chiffrer et déchiffrer
- ✓Problème : TRANSFERT de la clé

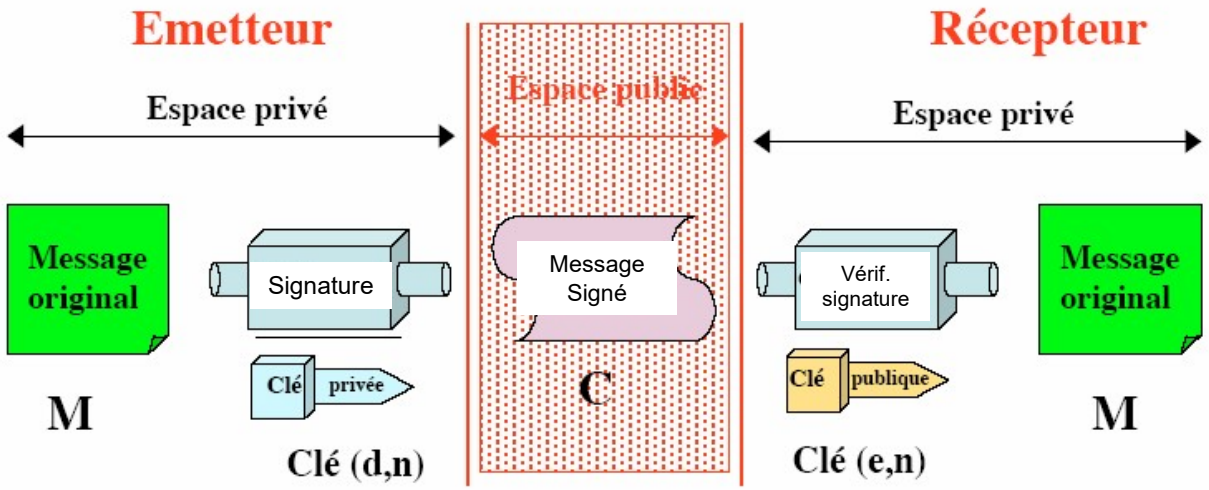
Cryptage asymétrique, protection de la confidentialité



✓Le chiffrement est effectué avec la clé publique

✓Garantie : que « SEUL » le détenteur de la clé privée peut lire le message

Cryptage asymétrique, principe de signature



✓Pour signer un message, on peut le chiffrer avec la clé privée !

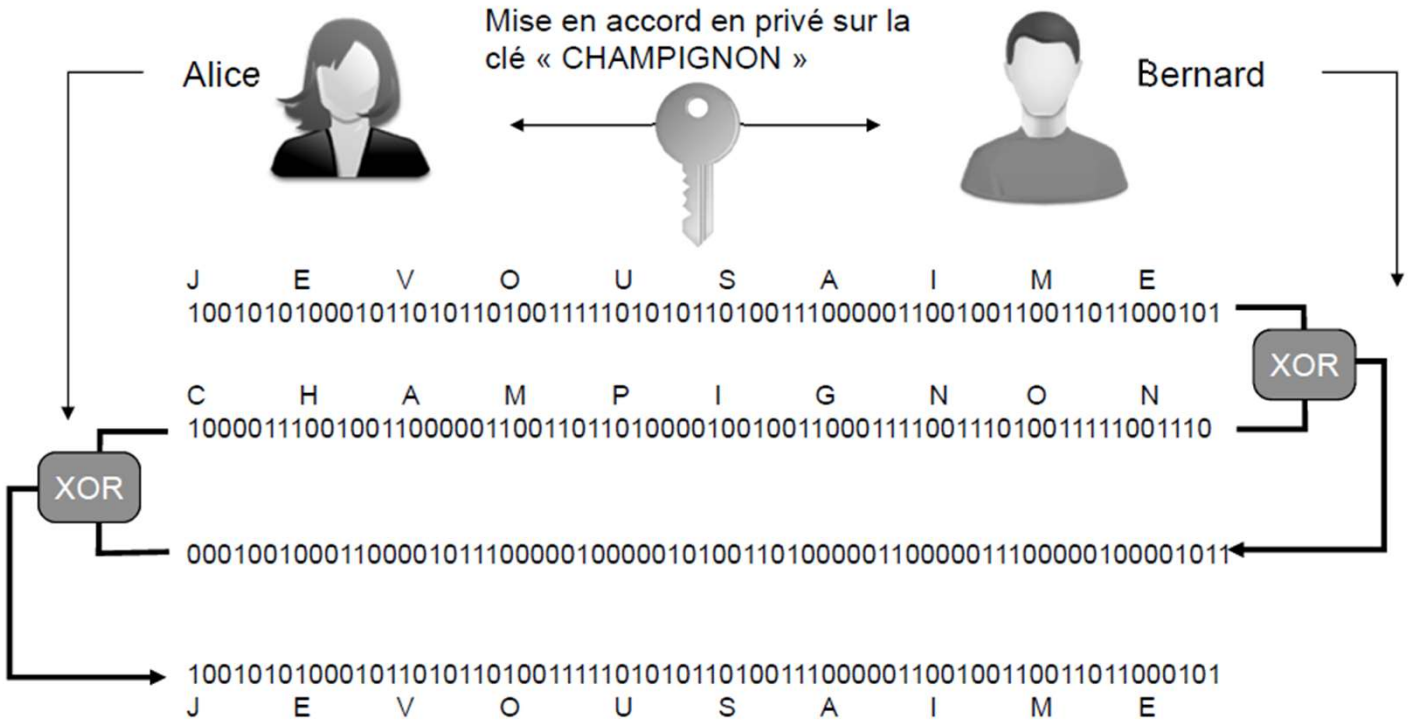
✓Le déchiffrement avec la clé publique prouve que seul le détenteur de la clé privée a pu créer la signature.

✓Signer un message = chiffrer un message

Robustesse du système de cryptage

- Puissance de l'algorithme (algorithme non secret)
- Taille de la clé utilisée
- Capacité à garder les clés secrètes de façon sécurisée
- Un système de chiffrement est dit fiable, robuste, sûr, sécurisé s'il reste inviolable indépendamment de la puissance de calcul ou du temps dont dispose un attaquant
- Il est dit opérationnellement sécurisé (*computational secure*) si sa sécurité dépend d'une série d'opérations réalisables en théorie, mais irréalisables pratiquement (temps de traitement trop longs…)
- Il faut changer fréquemment la clé de chiffrement

Chiffrement symétrique : Exemple fonction XOR

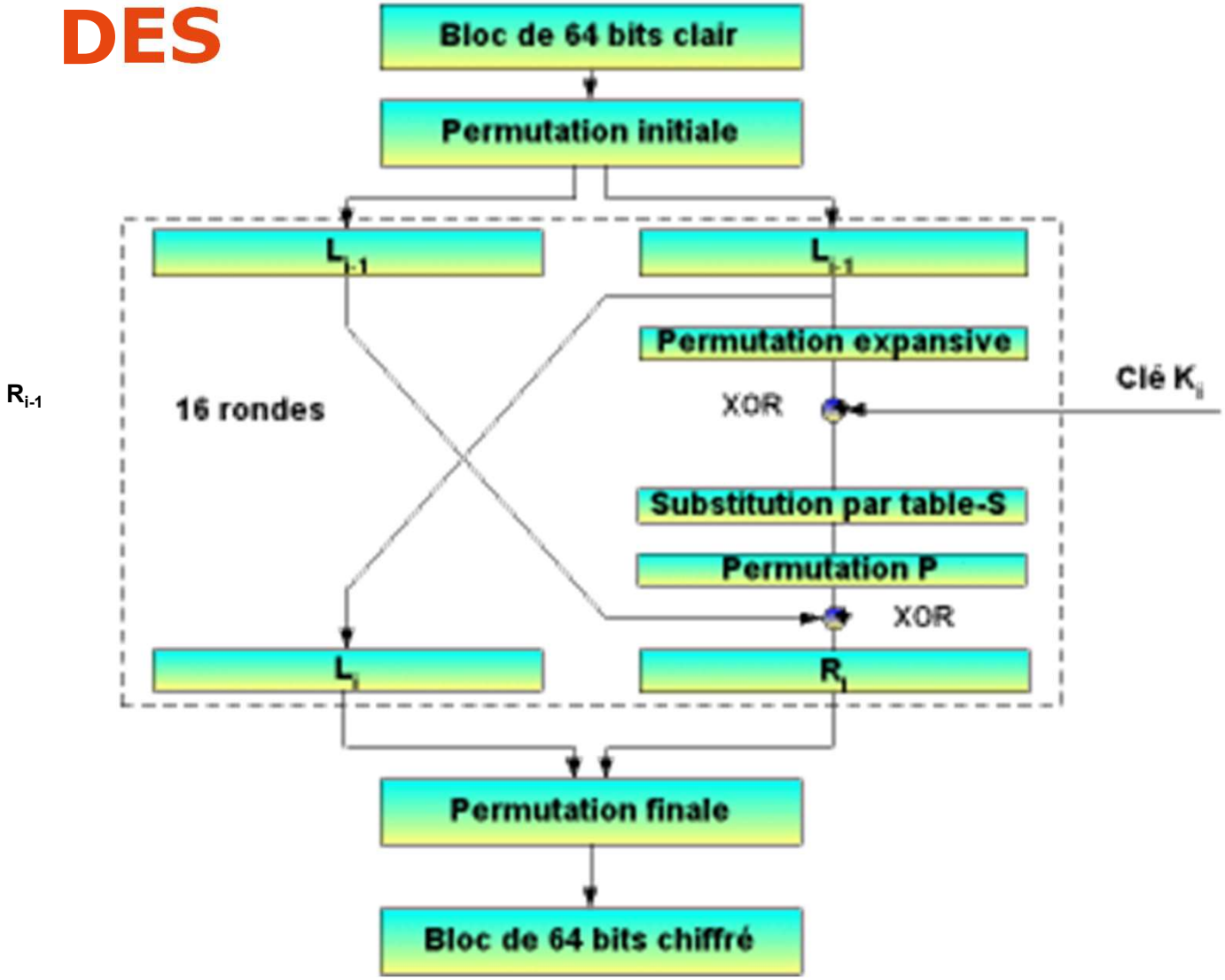


XOR	0	1
0	0	1
1	1	0

Le standard des algorithmes de cryptage symétrique : le DES (Data Encryption Standard) d'IBM

- Date de 1977
- Algorithme de chiffrement par bloc
- A l'origine pour documents classés ou secrets
- Aujourd'hui industrie du logiciel et cartes à puce
- DES signifie "norme de cryptage des données"
- Rapidité de chiffrement et de déchiffrement
  - Peut être développé en moins de 200 lignes de programme
  - Très rapide sur des cartes électroniques dédiées
    - Cartes à puces
    - Systèmes électroniques de télécommunications
- Implémentation du DES pour les systèmes Unix, Windows et MacOs disponibles sur internet

DES


Bloc de 64 bits clair
Permutation initiale
L_{i-1}
L_{i-1}
R_{i-1}
16 rondes
Permutation expansive
XOR
Clé K_i
Substitution par table-S
Permutation P
XOR
L_i
R_i
Permutation finale
Bloc de 64 bits chiffré

Autres algorithmes symétriques

- 3DES (triple DES, clé de 168 bits)
  - On utilise trois fois l'algorithme DES avec trois clés k_1, k_2 et k_3 : $m' = DES_{k1}(DES_{k2}(DES_{k3}(m)))$
  - Variante avec 2 clés et en utilisant deux fois l'algo de cryptage et une fois l'algo de décryptage : $m' = DES_{k1}(DES^{-1}_{k2}(DES_{k1}(m)))$, cette variante est réputée plus sûre
- DESX (DES XORed),GDES (Generalized DES), RDES (Randomized DES) : sont issus de l'algorithme DES, en utilisant des clés plus longues.
- AES (Advanced Encryption Standard), publié en 1998, standard recommandé depuis 2002
  - A été développé pour remplacer DES et offrir une meilleure sécurité
  - Utilise des clés de 128, 192 ou 256 bits
  - N.B. Fin 2003, le département américain de la défense a approuvé son autorisation
  - Utilisé dans IPSec (IP sécurisé) et IKE (Internet Key Exchange)
  - A ce jour demeure incassable et le plus sûr des systèmes de chiffrement symétriques

AES (quelques points)

- DES retraite méritée fin des années 90 :
  - taille de clé trop faible,
  - temps d'exécution trop long (accentué avec triple-DES),
  - existences de portes dérobées de la part de la NSA (?)
- 1997 : compétition pour AES par NIST (National Institute of Standards and Technology, USA)
  - Pouvoir utiliser des clés de 128, 192 ou 256 bits
  - Taille de blocs d'au moins 128 bits
  - Exécution rapide sur un maximum de plates-formes
- Algorithme Rijndael conçu par Daemen et Rijmen, UC Louvain (BE) en 2000
- Les cryptanalystes travaillent constamment à l'attaque des algorithmes pour détecter des vulnéabilités. Par exemple, sur les 10 tours (rondes) que compte l'AES-128, s'il est facile de casser en un seul tour l'AES, il n'existe pas aujourd'hui (2016) de résultats significatifs sur plus de 6 tours.

Autres algorithmes symétriques

- RC (Rivest Cipher) de RC2 à RC6
  - Algorithmes propriétaires à clés symétriques diffusés par RSA Security Inc. (www.rsasecurity.com)
  - Utilisent une clé de longueur variable (jusqu'à 2048 bits)
  - Utilisés pour rendre confidentiels des flux applicatifs
- IDEA (International Data Encryption Algorithm)
  - Clé de 128 bits pour coder des blocs de données de 64 bits
  - Utilisé par le protocole de messagerie sécurisé PGP (*Pretty Good Privacy*) http://sebsauvage.net/logiciels/pgp.html
- Twofish
  - Clés jusqu'à 256 bits
- Blowfish
  - Algorithme de chiffrement symétrique développé en 1993, largement remplacé par AES

Conclusion sur les systèmes symétriques

- Sûrs
- Rapides (pourquoi ?)

  mais
- Nécessité de s'échanger la clé
  - Problème de sécurité lors de la transmission de la clé
- Problème de la gestion des clés (nombre de clés à gérer)

Ex 1 : Recherche exhaustive (attaque par force brute) de clefs symétriques

Sachant que la machine spécialisée "DES cracker" met en moyenne 4,5 jours pour retrouver par une recherche exhaustive une clé de 56 bits, combien de temps mettrait-elle pour trouver une clé de 40 bits ? une clé de 112 bits ?

Size of the key (Example)

- Knowing what the specialized machine "DES cracker" spent on average 4,5 days to find by an exhaustive research (brute force attack) a 56 bits-key
- how long will it take to find a 40 bits-key?
  - $4,5 * 2^{40}/2^{56}=4,5*2^{-16} =5,93$ seconds

- a 112 bits-key?
  - $4,5 * 2^{112}/2^{56}=4,5*2^{56} =887 * 10^{12}$ years
  - ~= 60 000 Big bangs !

Some considerations on breaking a 768-bit RSA key

- From an Inria document, 2010.
- Key used for bank cards
- To break the key, find the prime numbers which compose the key: it is a number composed of 232 figures (2^{768})…
- Need efficient algorithm
- Need large calculation capacities: use of Grid'5000 => 1544 computers with more than 5000 cores.
- Collaboration with CH, JP, NL, DE : on average 1700 cores used during one year of calculation…
- One week by using the supercomputer *Jaguar* (from *Oak Ridge National Laboratory*) if available (not such computers in Europe…)
- The purpose was to show if it is possible to break using grid of « classical » computers
- Next step: to break a 1024 bit-key => it should be possible around 2020
- Advise from ANSSI (2010):
  - Use at least 1536 bit-keys for applications until 2010
  - Use at least 2048 bit-keys for application beyond 2010

Systèmes asymétriques : principes

- Permettre d'échanger des informations cryptées sans se rencontrer pour échanger les clés
- La sécurité est basée sur l'impossibilité pratique de résoudre un problème informatique « difficile », pour lequel la recherche d'une solution se chiffre en milliers, voire milliards d'année.

Systèmes asymétriques : quelques concepts (1/2)

- Fonctions à sens unique
  - D'après la théorie de la calculabilité et la complexité algorithmique, une fonction est à sens unique si :
    - La fonction f est calculable rapidement
    - Son inverse f^{-1} se calcule en un temps très long
  - Exemple de fonction à sens unique :

    $a^p \bmod n$ => appelées exponentielles modulaires de la variable ***p***

    Base a fixée

    n est le produit de deux « grands » nombres premiers

    La fonction inverse (appelée logarithme discret) est « difficilement » calculable

Systèmes asymétriques : quelques concepts (2/2)

- Fonctions « trappe » ou à brèche secrète
  - Fonction à sens unique sauf pour toute personne connaissant un secret, ou une brèche, permettant de calculer un algorithme d'inversion rapide
  - Exemple de fonction à brèche secrète :

    $a^p \bmod n$ => appelées exponentiation modulaire de la variable ***a***

    Exposant p fixé, n produit de deux nombre premiers

    L'existence d'un algorithme réciproque qui permet le calcul des racines p-ièmes modulo n de a est démontrée, mais on ne connaît pas cet algorithme

    Par contre, si on connaît la factorisation de n (la brèche), on peut très facilement inverser l'exponentiation modulaire

Les nombres premiers

- **Plus grand nombre premier :**
- $2^{136\,279\,841} - 1$
- **Trouvé le 11/10/24, confirmé le 12/10/14, composé de** 41 024 320 chiffres
- $2^{82\,589\,933} - 1$
- **Trouvé en décembre 2018, composé de** 24 862 048 chiffres
- 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223…

Principe de la cryptographie asymétrique

- Utilise des fonctions mathématiques faisant offices de cadenas
  - Faciles à utiliser dans un sens
  - Très difficile à inverser à moins de connaître un paramètre secret
- Problème de la factorisation des nombres premiers
  - Facile dans un sens
    - 13×17 = 221
    - 10 247×17 159 = 175 828 273
  - Difficile dans l'autre
    - 209 = 11×19
    - 7 321 010 267 = 55 487×131 941

Le RSA (cryptage, confidentialité)

- L'algorithme est remarquable par sa simplicité. Il est basé sur les nombres premiers.
- Pour encrypter un message, on fait:

  c = m^e mod n

- Pour décrypter: **m = c^d mod n**
  - **m** = message en clair
    c = message encrypté
    (e,n) constitue la clé publique
    (d,n) constitue la clé privée
    n est le produit de 2 nombres premiers
    ^ est l'opération de mise à la puissance (a^b : a puissance b)
    mod est l'opération de modulo (reste de la division entière)

Le RSA (signature numérique pour protéger intégrité et authenticité)

- L'algorithme est remarquable par sa simplicité. Il est basé sur les nombres premiers.
- Pour **signer** un message, on fait:

s = m^d mod n

- Pour « dé-signer » (vérifier la signature):

m = s^e mod n

  - **m** = message en clair
    s = message **signé**
    (e,n) constitue la clé publique
    (d,n) constitue la clé privée
    n est le produit de 2 nombres premiers
    ^ est l'opération de mise à la puissance (a^b : a puissance b)
    mod est l'opération de modulo (reste de la division entière)

RSA : Règles opératives

- On travaille à partir de messages codés numériquement (par exemple ASCII)
- On découpe le message en blocs qui comportent moins de chiffres que **n** (on complète par des zéros s'il le faut pour obtenir le dernier bloc)

Principe de fonctionnement

Choisit deux grands entiers naturels premiers **p** et **q** et fait leur produit **n = p×q**
n=5141=53×97

Choisit un entier **e** premier avec **(p-1)(q-1)**
e=7, premier avec 52×96=4992

Publie sa clé publique (n,e)
(5141,7)

Calcule sa clé privée **d** telle que **e×d mod ((p-1)(q-1)) = 1**
d=4279

Transforme en nombre son message en remplaçant par exemple chaque lettre par son rang dans l'alphabet

J E V O U S A I M E
10 05 22 15 21 19 01 09 13 05

Découpe son message chiffré en blocs de même longueur représentant chacun un nombre plus petit que **n**

010 052 215 211 901 091 305

Chiffre à l'aide de la clé publique d'Alice chaque bloc B par la formule $B^e \bmod n$

(5141,7)

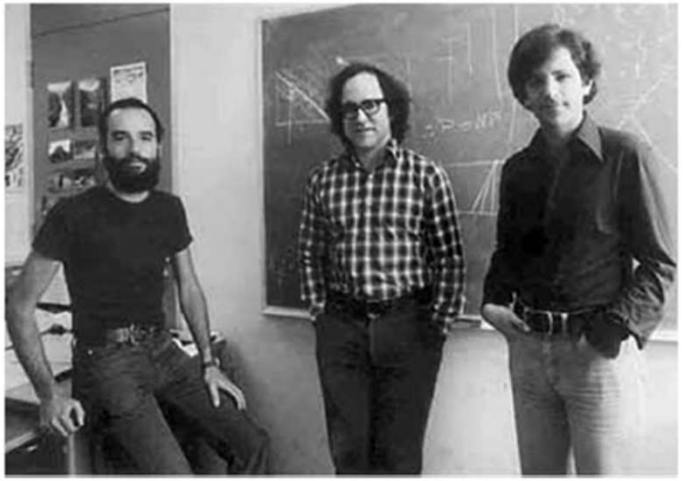
0755 1324 2823 3550 3763 2237 2052

Déchiffre chaque bloc C du message chiffré par la formule $C^d \bmod n$

4279

RSA, 1er protocole à clé publique

- 1975
  - Diffie, Hellman et Merkle inventent le principe de la cryptographie à clé publique
  - Mais aucun exemple concret n´est proposé
- 1977
  - Ronal Rivest, Adi Shamir et Leonard Adleman inventent le premier protocole de cryptographie à clé publique : RSA
  - Basé sur le problème de la factorisation



RSA : Exemple (1/4)

- https://www.cs.drexel.edu/~jpopyack/IntroCS/HW/RSAWorksheet.html
- Commençons par créer notre paire de clés:
  - Prenons 2 nombres premiers au hasard: **p = 127**, **q = 167**
  - Calculons **n = pq = 127 * 167 = 21209**
- On doit choisir **e** au hasard tel que **e** n'ait aucun facteur en commun avec r=**(p-1) (q-1)**:
  - **r=(p-1) (q-1) = (127-1) (167-1) = 20916**
- Il faut trouver deux nombres **e** et **d** tels que leur produit (**modulo r**) soit égal à 1. Il faut choisir e "aléatoirement" mais de telle manière que e n'ait aucun facteur en commun avec r.
- Les nombres possibles sont du type (a.r+1), avec a appartenant à N*.
- 20917 41833 62749 83665 104581 125497 146413 167329
- 188245 209161 230077 250993 271909 292825 313741 334657
- 355573 376489 397405 418321 439237 460153 481069 501985
- 522901 543817 564733 585649 606565 627481

RSA : Exemple (2/4)

- Etape 2. Choisir un des nombres du tableau précédent (nombres égaux à 1 modulo r):
  - Prenons par exemple 20917
- Il faut factoriser ce nombre (voir https://www.cs.drexel.edu/~jpopyack/IntroCS/HW/RSAWorksheet.html)
  - 13*1609
- On prend **e = 13**
- On choisit **d** tel que **13*d mod 20916 = 1**
  - On teste **d = 1609**
- On a maintenant nos clés :
  - La clé publique est **(e,n) = (13,21209)** (=clé d'encryptage)
  - La clé privée est **(d,n) = (1609,21209)** (=clé de décryptage)

RSA : Exemple (3/4)

- https://www.cs.drexel.edu/~jpopyack/IntroCS/HW/RSAWorksheet.html
- On va encrypter le message '**HELLO**'. On va prendre le code ASCII (en décimal) de chaque caractère et on les met bout à bout:
  - **m = 72-69-76-76-79 (en base 10)**
- Ensuite, il faut découper le message en blocs qui comportent moins de chiffres que **n**.
- **n** comporte 4 chiffres, on va donc découper notre message en blocs de 3 chiffres:
  - 726 976 767 900
    (on complète avec des zéros)
- Ensuite on encrypte chacun de ces blocs:
  - 726^13 mod **21209** = 11600
    976^13 mod **21209** = 5705
    767^13 mod **21209** = 16590
    900^13 mod **21209** = 3565
    Le message encrypté est **11600.5705.16590.3565**. On peut le décrypter avec d:
  - 11600^1609 mod **21209** = 726
    5705^1609 mod **21209** = 976
    16590^1609 mod **21209** = 767
    3565^1609 mod **21209** = 900
- C'est à dire la suite de chiffre **726976767900**.
  On retrouve notre message en clair **72 69 76 76 79** : '**HELLO**'.

RSA : Exemple (4/4)

- https://www.cs.drexel.edu/~jpopyack/IntroCS/HW/RSAWorksheet.html
- On va encrypter le message '**HELLO**'. On va prendre le code ASCII (en décimal) de chaque caractère et on les met bout à bout:
  - **m = 72-69-76-76-79 (en base 10)**
- Ensuite, il faut découper le message en blocs qui comportent moins de chiffres que **n**.
- **n** comporte 4 chiffres, on va donc découper notre message en blocs de 3 chiffres:
  - 726 976 767 900
    (on complète avec des zéros)
- Ensuite on encrypte chacun de ces blocs:
  - 726^13 mod **21209** = 11600
    976^13 mod **21209** = 5705
    767^13 mod **21209** = 16590
    900^13 mod **21209** = 3565
    Le message encrypté est **11600.5705.16590.3565**. On peut le décrypter avec d:
  - 11600^1609 mod **21209** = 726 (si 1 bit est corrompu 11601^1609 mod 21209 = 6051)
    5705^1609 mod **21209** = 976
    16590^1609 mod **21209** = 767
    3565^1609 mod **21209** = 900
- C'est à dire la suite de chiffre **726976767900**.
  On retrouve notre message en clair **72 69 76 76 79** : '**HELLO**'.

Remarques sur le RSA

- Dans la pratique, ce n'est pas si simple à programmer : Il faut trouver de grands nombres premiers (ça peut être très long à calculer)
- Il faut obtenir des nombres premiers **p** et **q** *réellement* aléatoires (ce qui est loin d'être évident)
- On n'utilise pas de blocs aussi petits que dans l'exemple ci-dessus: il faut être capable de calculer des puissances et des modulos sur de très grand nombres
- En fait, on n'utilise jamais les algorithmes asymétriques pour chiffrer toutes les données, car ils sont trop longs à calculer : on chiffre les données avec un simple algorithme symétrique dont la clé est tirée au hasard, et c'est cette clé qu'on chiffre avec un algorithme asymétrique comme le RSA

D’autres algorithmes asymétriques

- gpg (GNU Privacy Guard)
- **ECC** (Elliptic Curve Cryptosystems, Encryptage par Courbe Elliptique). Ce système est basé sur une courbe paramétrique qui passe par un certain nombre de points de coordonnées entières. Ce n'est pas encore très développé, mais il est prometteur
- **Diffie-Hellman** (Utilisé dans les négociations IKE (Internet Key Exchange)), de plus en plus préféré à RSA. (Diffie-Hellman avait rapidement été adopté par la communauté opensource quand RSA n'était pas encore dans le domaine public)
- **El Gamal** : basé sur le calcul de logarithmes discrets

Comparaison des systèmes de cryptage

- Cryptage asymétrique utile
  - Elimine le problème du transfert de la clé (d'une clé secrète)
  - Permet la signature numérique
  - Possibilité de gérer une Infrastructure à clés publiques (Public Key Infrastructure, PKI)
- Cryptage symétrique plus rapide (La Recherche, juin 2018)
  - AES permet de chiffrer plusieurs gigaoctets par seconde sur un processeur récent
  - Standards de cryptographie asymétrique atteignent moins d'un megaoctet par seconde (1000 à 10000 fois plus lent !)
- On combine souvent les 2 types de cryptage pour bénéficier des avantages de chacun
  - Intérêt : Utiliser un protocole à clé publique pour transmettre la clé du AES(symétrique) => cryptographie hybride
    - In this situation, the AES key is called "symmetric" key, "common" key, "session" key or "shared" key

Cryptographie hybride (Diffie-Hellman) : génération d'une clé de partage

- Deux utilisateurs vont concevoir une clé commune qui ne servira qu'à eux seuls

ASPECT ASSYMETRIQUE

- Ils choisissent n un nombre produit de deux nombres premier p et q et un entier a (a et n n'étant pas forcément confidentiels)
- Ensuite chacun choisit un entier X appartenant à [1, n-1] et calcule l'entier $Y=a^X \bmod n$
- On obtient deux couples (X_1,Y_1) et (X_2, Y_2) où les valeurs Y_1 et Y_2 vont être publiées

ASPECT HYBRIDE

- Chacun d'eux peut alors calculer la clé $c=a^{X1.X2} \bmod n$ car $c=(Y1^{X2} \bmod n)=(Y2^{X1} \bmod n)$
- R : Chacun ignore le X de l'autre
- La sécurité vient du fait qu'il est impossible en un temps raisonnable de découvrir la clé c par le calcul d'un logarithme discret (infaisable en un temps raisonnable compte tenu de la taille de n)

ASPECT SYMETRIQUE

- Les utilisateurs peuvent maintenant échanger leurs données de manière cryptée en utilisant un système symétrique grâce à la clé commune c

Application

- Utilisateur 1
- X1 : clé privée
- $Y1=a^{X1} \bmod n$: clé publique
- Envoi Y1 à util. 2
- Reçoit Y2
- $c=(Y2^{X1} \bmod n)$
- Clé « c » permettant l'usage d'un système de cryptage symétrique

n
a

- Utilisateur 2
- X2 : clé privée
- $Y2=a^{X2} \bmod n$: clé publique
- Envoi Y2 à util. 1
- Reçoit Y1
- $c=(Y1^{X2} \bmod n)$
- Clé « c » permettant l'usage d'un système de cryptage symétrique

Clé privée et clé publique

- La clé secrète est constituée de deux nombres p et q de plusieurs centaines de bits de longueur.
- La clé publique contient n =p*q.
- Comme n est très grand, il est impossible de trouver toutes les factorisations possibles.
- La connaissance de n ne permet pas d'en déduire celle de p et de q.

Exercice 2

- Amusez-vous avec votre voisin à générer une clé de partage
- (ex:
  - a=3 et n=14 (valeurs connues) (n=2*7)
  - X_1 = 4 (valeur secrète connue uniquement du voisin de gauche)
  - X_2 = 3 (valeur secrète connue uniquement du voisin de droite)

Exercice 2, correction

- Amusez-vous avec votre voisin à générer une clé de partage
- (ex:
  - a=3 et n=14 (valeurs connues) (n=2*7)
  - X_1 = 4 (valeur secrète connue uniquement du voisin de gauche)
  - X_2 = 3 (valeur secrète connue uniquement du voisin de droite)

  - $Y1=a^{X1} \bmod n = 3\text{^}4 \bmod 14 = 11$
  - $Y2=a^{X2} \bmod n = 3\text{^}3 \bmod 14 = 13$
  - $c=Y2^{X1} \bmod n = 13\text{^}4 \bmod 14 = 1$
  - $c=Y1^{X2} \bmod n = 11\text{^}3 \bmod 14 = 1$

Ex 3

- En 1883, Auguste Kerckhoffs a établi un principe fondamental de la cryptographie : "il faut qu'un système cryptographique n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi". Expliquer ce principe.

Ex 3, Corrections

- En 1883, Auguste Kerckhoffs a établi un principe fondamental de la cryptographie : "il faut qu'un système cryptographique n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi". Expliquer ce principe.
- RÉPONSES
- Le système (algorithme) doit être public, ce qui le rend invulnérable au vol
- La clé doit être secrète
- Le système doit être public afin de permettre à tout le monde de le tester. Cela permet de trouver des vulnérabilités et donc d'améliorer l'algorithme

Ex 4 : Gestion d'usagers

Un groupe de n personnes souhaite utiliser un système cryptographique pour s'échanger deux à deux des informations confidentielles. Les informations échangées entre deux membres du groupe ne devront pas pouvoir être lues par un autre membre. Le groupe décide d'utiliser un système de chiffrement symétrique.

1. Quel est le nombre minimal de clés symétriques nécessaires ?
2. Donner le nom d'un algorithme de chiffrement symétrique reconnu.

Le groupe décide ensuite de remplacer ce système par un système asymétrique.

3. Quel est le nombre minimal de couples de clés asymétriques nécessaires pour que chaque membre puisse envoyer et recevoir des informations chiffrées et/ou signées ? Si l'on considère que chacun peut communiquer avec tout le monde, combien de clés privées et publiques chaque utilisateur devra-t-il détenir
4. Bob souhaite envoyer des informations chiffrées et signées à Alice (Bob et Alice appartiennent tous les deux au groupe). Quelle(s) clé(s) Bob doit-il utiliser ?
5. Donner le nom d'un algorithme de chiffrement asymétrique reconnu.

Le groupe décide finalement d'utiliser un système hybride pour le chiffrement (c'est-à-dire qui utilise la cryptographie symétrique et asymétrique).

4. Donner les raisons qui ont poussé ce groupe à utiliser un tel système.

Ex 4 : Gestion d'usagers, correction

Un groupe de n personnes souhaite utiliser un système cryptographique pour s'échanger deux à deux des informations confidentielles. Les informations échangées entre deux membres du groupe ne devront pas pouvoir être lues par un autre membre. Le groupe décide d'utiliser un système de chiffrement symétrique.

1. Quel est le nombre minimal de clés symétriques nécessaires ?

n.(n-1)/2 clés secrètes sont nécessaires.

1. Donner le nom d'un algorithme de chiffrement symétrique reconnu.

DES par exemple

Le groupe décide ensuite de remplacer ce système par un système asymétrique.

3. Quel est le nombre minimal de couples de clés asymétriques nécessaires pour que chaque membre puisse envoyer et recevoir des informations chiffrées et/ou signées ? Si l'on considère que chacun peut communiquer avec tout le monde, combien de clés privées et publiques chaque utilisateur devra-t-il détenir n paires de clés, chacun aura sa clé secrète et distribuera sa clé publique à tous les autres. Donc chacun détiendra les n-1 clés publiques d'autrui.Le groupe décide enfin d'utiliser une infrastructure de gestion de clé (PKI, certificats).

1. Quel est l'intérêt d'utiliser un tel système ?
2. Combien de clés doivent finalement être gérées par chaque utilisateur ? Combien y a-t-il de clés en tout ?

4. Bob souhaite envoyer des informations chiffrées et signées à Alice (Bob et Alice appartiennent tous les deux au groupe). Quelle(s) clé(s) Bob doit-il utiliser ?

Pour chiffrer, Bob devra utiliser la clé publique d'Alice. Pour signer, il devra utiliser sa propre clé privée.

4. Donner le nom d'un algorithme de chiffrement asymétrique reconnu.

RSA par exemple

Le groupe décide finalement d'utiliser un système hybride pour le chiffrement (c'est-à-dire qui utilise la cryptographie symétrique et asymétrique).

4. Donner les raisons qui ont poussé ce groupe à utiliser un tel système.

$$C_n^2 = \frac{N!}{2!.(N-2)!} = \frac{N.(N-1).(N-2).(N-3).(N-4)\ldots}{2.(N-2).(N-3).(N-4)\ldots} = \frac{N.(N-1)}{2}$$

Ex 4, corrections

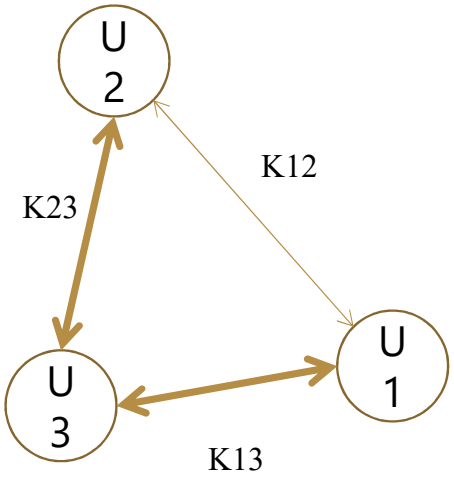
- 1. N personnes

est le nombre de clés symétriques (clés de session) nécessaires

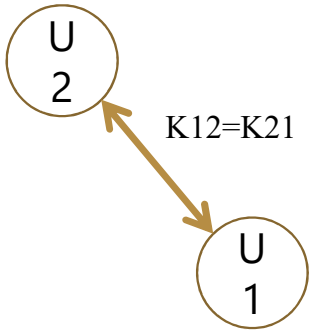
- 2. DES, AES, 3DES…
- 3. N paires de clés est le nombre de clés asymétriques nécessaires (soit 2.N clés)
- N+1 clés possibles sur un ordinateur (clé privée de l'utilisateur + clé publique de l'utilisateur (pour envoi aux autres utilisateurs) + N-1 clés publiques provenant des autres utilisateurs)
- 4. Pour crypter, Bob a besoin de la clé publique d'Alice, puis pour signer, Bob utilise sa propre clé privée.
  - (au-delà de l'exercice) : Après réception, Alice va d'abor vérifier la signature en utilisant la clé publique de Bob, puis pourra décrypter le fichier en utilisant sa propre clé privée.
  - (au-delà de l'exercice) : nous considérons ici que les utilisateurs ont échangé leurs clés publiques au préalable
- 5. RSA
- 6. Il est plus efficace de gérer un système asymétrique (par l'utilisation d'une PKI) pour lequel nous avons besoin globalement de 2.N clés (N paires de clés) que de gérer un système symétrique avec N.(N-1)/2 clés

Sym.

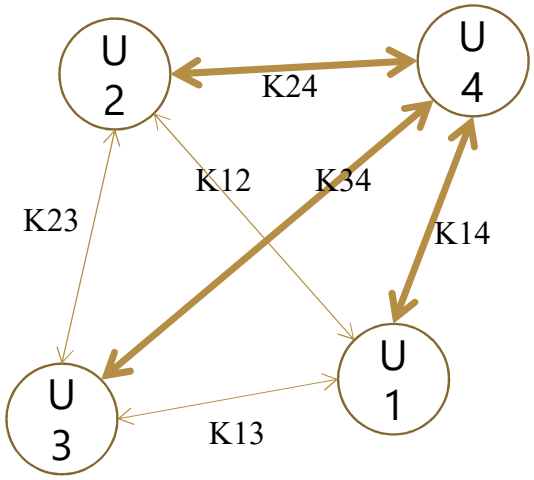
3 users, 3 keys



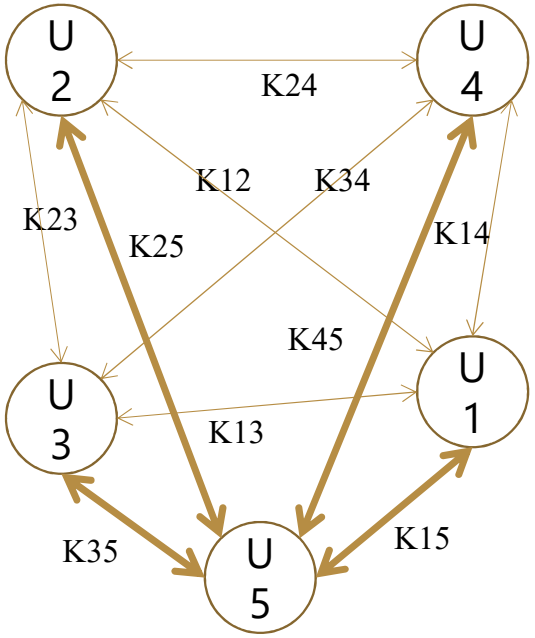
2 users, 1 key



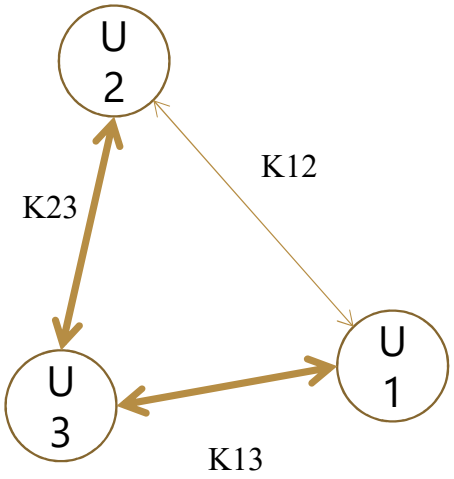
4 users, 6 keys



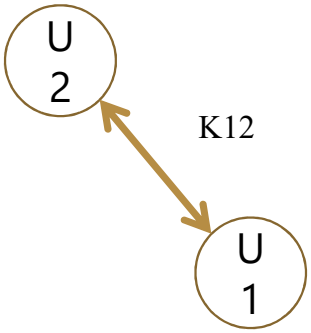
5 users, 10 keys



3 users, 3 keys



2 users, 1 key



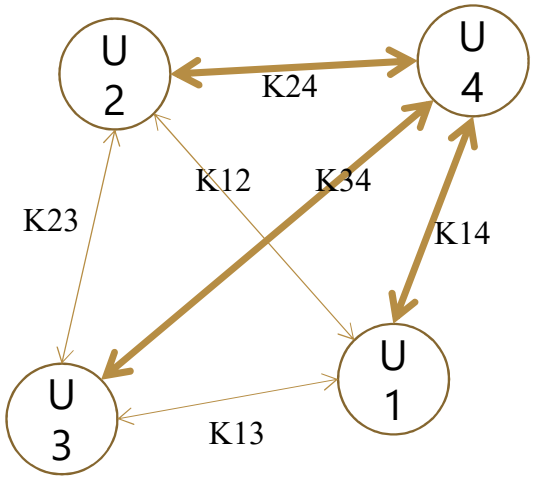
$$C_n^2 = \frac{N!}{2!.(N-2)!} = \frac{N.(N-1)}{2}$$

Pour 1000 utilisateurs :

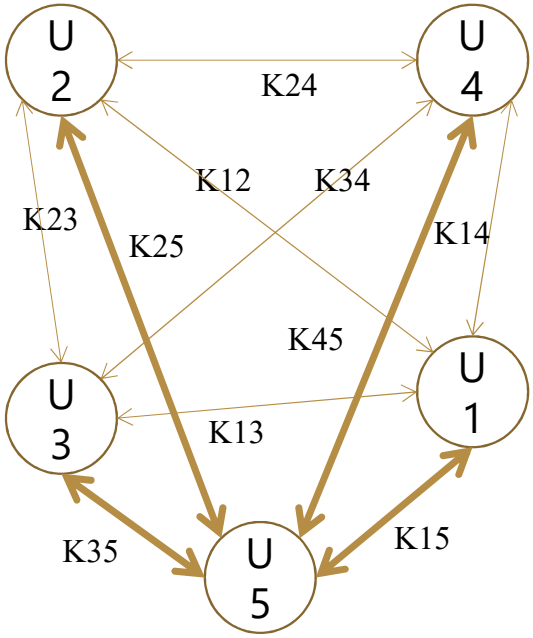
$C_n^2 == \frac{1000.(999)}{2} = 499.500$

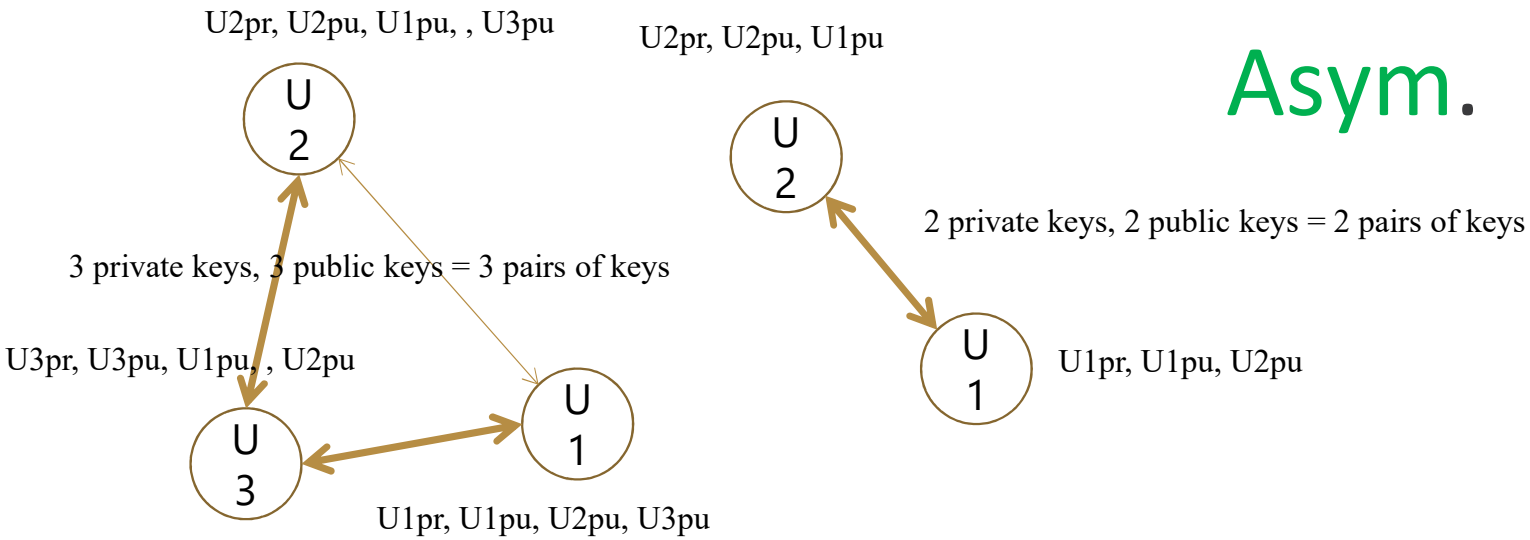
Ce qui veut dire environ un demi-million de clés pour 1000 utilisateurs …

4 users, 6 keys



5 users, 10 keys





Asym.

Pour 1000 utilisateurs, nous devons gérer globalement 2000 clés

Nous utilisons généralement une infrastructure à clés publiques (Public Key Infrastructure, PKI) dont le rôle est de gérer les clés publiques via un serveur

Ex 5

- **Perte d'une clé privée**

Un utilisateur, qui utilise souvent la messagerie sécurisée de son entreprise, vient de perdre sa clé privée, mais dispose encore de la clé publique correspondante.

1. Peut-il encore envoyer des courriers électroniques chiffrés ? Décrypter les messages reçus ?
2. Peut-il encore signer les courriers électroniques qu'il envoie ? Vérifier les signatures des courriers électroniques qu'il reçoit ?
3. A quoi peut encore servir la clé publique de notre utilisateur ?
4. Que doit-il faire pour être à nouveau capable d'effectuer toutes les opérations mentionnées ci-dessus ??

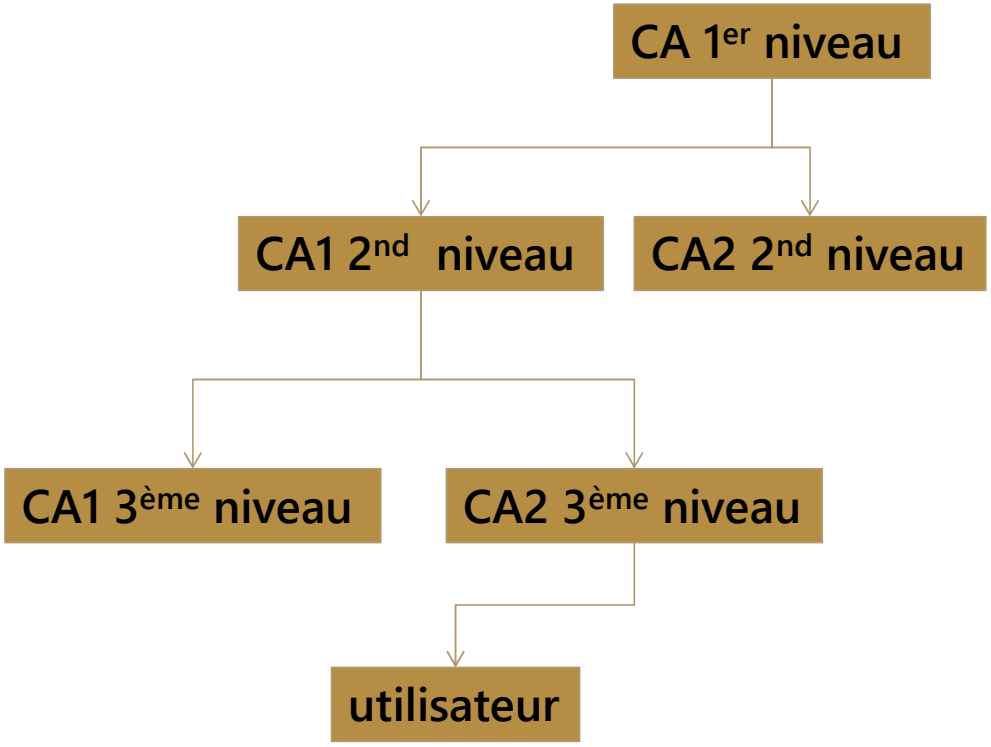
Ex 5, Corrections

1. Il peut encore envoyer des courriels cryptés puisqu'il utilise pour cela la clé publique de récepteur. Il ne peut plus décrypter les messages reçus puisqu'il a besoin de sa clé privée pour cela…
2. Il ne peut plus signer puisqu'il doit utiliser sa clé privée pour cela. Il peut vérifier la signature des courriels reçus puisqu'il utilise la clé publique de l'émetteur pour cela
3. Sa clé publique n'est plus utile puisque la clé privée liée n'est plus disponible
4. L'utilisateur doit renouveler sa clé privée et une nouvelle clé publique liée à cette clé privée

Certificats

- Document qui prouve que la clé publique appartient bien à son propriétaire
- Il contient au moins les documents suivants :
  - Clé publique
  - Identité de l'entité propriétaires du certificat
    - Nom, prénom
    - Adresse IP
    - Adresse E-mail
  - Date d'expiration (non obligatoire)
  - Signature du certificat par une tierce partie => c'est un partenaire de confiance (Entreprise connue avec une bonne réputation)
  - Ex: https://premium.wpmudev.org/blog/ssl-certificate-authorities-reviewed/

Autorité de Certification (Certification Authorities, CA)



Autorité de certification (CA)

- La CA crée et signe les certificats
- Chaque nouveau participant doit se présenter
  - La CA authentifie physiquement le participant
  - Elle fait générer une paire de clés publique/privée par le participant
  - Elle crée un certificat avec l'identité du participant, sa clé publique, une date d'expiration et la signature de la CA.
  - Elle fournit une copie de sa propre clé publique au participant.
- Muni de son certificat et de la clé publique de la CA, le nouveau participant peut communiquer avec tous les autres participants certifiés par la même CA.
- Une CA peut être une CA privée d'une entreprise ou une CA publique.
- Une CA peut faire certifier sa clé publique par une autre CA (hiérarchie).

Principaux paramètres d'un certificat numérique selon norme X509v3

1. Version du certificat
2. Numéro de série
3. Algorithme utilisé pour signer le certificat
4. Nom de l'organisme qui a géré le certificat
   - Le couple numéro de série-nom de l'organisme doit être unique
5. Période de validité
6. Nom du propriétaire du certificat
7. Clé publique du propriétaire
8. Informations additionnelles concernant le propriétaire ou les mécanismes de chiffrement
9. Signature du certificat
   - Algorithme et paramètres utilisés pour la signature ainsi que la signature

Validation du certificat

- Pour valider le certificat reçu, le client doit obtenir la clé publique de l'organisme qui a créé le certificat relatif à l'algorithme utilisé pour signer le certificat (champ 3) et doit déchiffrer la signature contenue dans le champ 9.
- A l'aide des informations également contenues dans ce champ, le client calcule la valeur du condensé (résumé ou *hash*) et compare la valeur trouvée à celle contenue dans le dernier champ => si les deux valeurs correspondent, le certificat est authentifié
- Ensuite, le client s'assure que la période de validité du certificat est correcte

L'annuaire de certificats

- ✓ Pour faciliter l'accès aux certificats, la CA met à disposition un annuaire (LDAP, HTTP)
- ✓ Pour envoyer un email à User1, User2 demande son certificat à l'annuaire, User1 n'a pas besoin d'être atteignable.
- ✓ L'annuaire fourni aussi la liste des certificats révoqués (Revoked List, CRL)
- ✓ Un certificat peut être révoqué avant son échéance pour cause de vol, de perte ou de changement de statut (User2 quitte son employeur)

Limites des certificats

- Diverses autorités de certification existent
  - Impossible qu'il n'y en ait qu'une (problèmes techniques et politiques/stratégiques)
  - Interopérabilité des autorités
  - Reconnaissance mutuelle
  - Compatibilité des certificats et de leur validité
  - Limites inhérentes aux infrastructures de gestion de clés
    - Complexité, coût du déploiement et de la gestion d'une infrastructure
    - Haut niveau de sécurité nécessaire à la réalisation des services
    - Validité, durée de vie, résiliation des certificats
  - Réel manque de confiance des utilisateurs dans les autorités de certification qui sont le plus souvent étrangères et les services offerts
    - Valeur des certificats
    - Mécanismes et procédures d'authentification
    - Protection des données personnelles, de leur identité, de leurs transactions

Infrastructure de gestion de clés

- Mise en œuvre de mécanismes nécessaires à la réalisation de systèmes de chiffrement asymétriques
  - IGC : infrastructure de gestion de clés (PKI : Public Key Infrastructure / Infrastructure à clé publique)
- Impossible de mémoriser l'ensemble des clés publiques de tous les correspondants potentiels d'un site internet
  - IGC (PKI) = répond à la nécessité de disposer des clés de chiffrement afin de mettre en œuvre un système de chiffrement asymétrique à clés publiques

Fonction d'une infrastructure à clé publique

- Génération d'un couple unique de clés (clé publique, clé privée)
  - Sauvegarde des informations nécessaires à sa gestion
    - Archivage des clés
    - Procédure de recouvrement en cas de perte par un utilisateur ou de demande de mise à disposition par les autorités judiciaires
- Gestion des certificats numériques
  - Création
  - Signature
  - Émission
  - Validation
  - Révocation
  - Renouvellement des certificats
- Diffusion des clés publiques aux ressources qui la solliciteraient et qui seraient habilitées à l'obtenir
- Certification des clés publiques (signature des certificats numériques)

Hardware security modules (HSM)

- For embedded systems for example:
- Cryptographic modules: specific hardware dedicated to cryptography
- May be certified on an international basis: (ex: Common Criteria, FIPS 140)
- Because cryptographic functions (especially asymmetric ones) are intensive regarding processing power and memory comsumption

Hardware security modules (HSM)

- Problem with « software-only » servers is they are general computers that aren't designed for security purposes
  - Many of their parts are « unsupervised »
  - Ex : shared memory
  - Not resistant against physical access
- A HSM is a physical computer that keeps, manages, and processes digital keys for authentication, signing, and verification and provides crypto-processing functions
- Exist in form of sole-appliance (used in networks) or as external attachments that re plug-able on a typical server to be used

Hardware security modules (HSM): characteristics

- Secure « crypto processor »: processor specified on small number of operations designed and dedicated for the crypto-processing
- Secure memory: accessible only through the defined channel (not under any condition through any other channel)
  - Should support fast and repetitive I/O
  - Caching operations should be handled with caution because of sensitivity of data
  - Optionally content of memory can be protected through mechanisms like
    - Virtual Addressing
    - ASLR (Address Space Layout Randomization)
    - W^X

Hardware security modules (HSM): characteristics

- Random number generator
  - Expected to be implemented in any HSM
  - Better to implement TRNG (True Random Number Generator) than PRNG (Pseudo-Random NG)
- Tamper-proof module
  - « resistance to tampering (intentional malfunction or sabotage) by either the normal users of a product, package, or system or others with physical access to it » (Wikipedia)
- Inter-component connections
  - HSMs consist of different units, connected to each other and all should be physically guarded by the tamper-proof module

HSM: standards

- FIPS 140 (Federal Information Processing Standards)
  - Standards for cryptographic modules which includes both hardware and software components
- PKCS #11 (Public-Key Cryptography Standards)
  - Maintained by OASIS PKCS #11 Technical Committee
  - Contains a very detailed and technical defined API (called « Cryptoki »)
    - For cryptographic tokens (HSM, cards…)
    - Includes mainly aspects (keys like RSA, certificates like X509)
  - Widely used by CA authority software and hardware

HSM: Usage

- PKI environments
- Banking and payment systems
- More recently
  - DNSSEC

Références bibliographiques

Some references

- S. Ghernaouti – Cyberssicurité : Analyser les risques, Mettre en œuvre les solutions
- J.F. Aubry, Nicolae Brinzei – Systems Dependability Assessment, Modeling with Graphs and Finite State Automata, Wiley, Fév. 2015.
- J.C. Laprie & al. – Guide de la sûreté de fonctionnement – Cépaduès, 1995.
- A. Villemeur – *Sûreté de fonctionnement des systèmes industriels* – Editions Eyrolles, Paris, 1988.
- C. Davis, M. Schiller, K. Wheeler - *IT Auditing: using control to protect assets* – 2007, Mc Graw Hill
- Cours Stéphane Mocanu, ENSE3, Industrial Communication Labs, 2016
- Cours Emmanuel Simeu, Polytech Grenoble, Supervision
- Patrick Monassier, cours CESI 2009, Informatique industrielle.
- Pierre Bonnet, cours Université de Lille, Introduction à la supervision, 2010
- EPFL, Industrial Automation course
- P_RAYMOND_BTS_MAI_Les_API
- Transmissions et réseaux, S. Lohier & D. Présent, Dunod, Paris, 2003.
- Cours Stéphane Mocanu, ENSE3, Industrial Communication Labs, 2016
- Cours Emmanuel Simeu, Polytech Grenoble, Supervision
- Cours de Blaise Conrard, Polytech Lille.
- Patrick Monassier, cours CESI 2009, Informatique industrielle.
- Pierre Bonnet, cours Université de Lille, Introduction à la supervision, 2010
- G. Boujat et P. Annaya, Automatique industrielle en 20 fiches, Dunod, 2007
- W. Bolton, Automates programmables industriels, Dunod, 2015.
- Duc Tran Trung , Cybersecurity risk assessment for Unmanned Aircraft System, PhD, Univ. Grenoble Alpes
- Cours Eric Gnaedinger, Université de Lorraine
- Automates programmables industriels – W. Bolton – Dunod, 2015.
- Networking courses of Denis Genon-Catalot, Asean-Factori project, 2022.

Some references

https://www.technologuepro.com/cours-automate-programmable-industriel/Les-automates-programmables-industriels-API.htm

http://www.est-usmba.ac.ma/coursenligne/GE-S2-M8.1-Automatismes%20logiques%20Industriels-CRS-El%20Hammoumi.pdf

http://colasapoil.free.fr/HEI/HEI5%20TC/Maintenance/h5_tc_maintenance_coursv2_coursv2_1783.pdf

https://www.cours-gratuit.com/cours-divers/cours-sur-les-definitions-methodes-et-operations-de-la-maintenance

https://www.manager-go.com/logistique/organisation-de-la-logistique.htm

https://www.lecoindesentrepreneurs.fr/logistique-entreprise/
https://d1n7iqsz6ob2ad.cloudfront.net/document/pdf/5346e085efe6e.pdf

https://www.icours.com/cours/economie/la-production

https://perso.imt-mines-albi.fr/~fontanil/THESE/5_Partie1_p13_43.pdf

Some references

- Cours réseaux et télécoms avec exercices corrigés, G. Pujolle, Eyrolles 2006
- SSL VPN, accès web et extranets sécurisés – J. Steinberg & T. Speed, Eyrolles, 2006.
- P. H. Oechlin, LASEC/EPFL
- http://sebsauvage.net/comprendre/encryptage/crypto_rsa.html
- S. Ghernaouti-Helie – *Sécurité informatique et réseaux, 4ème édition* – Dunod, 2013
- F. Halsall – Computer networking and the internet – Addison Welseley, 2005 + additional student support at www.pearsoned.co.uk/halsall
- D. Vergnaud – Exercices et problèmes de cryptographie, Dunod, 2015
- CEH, Certified Ethical Hacker, Matt Walker, McGrawHill, 2017
- L. Bloch & al. – Sécurité informatique pour les DSI, RSSI et administrateurs, Eyrolles, 2016.
- D. Genon-Catalot – Asean-Factori project Slides – 2021, 2022.
- C. Bras – Transparents LPRO RIMS/CNMS, 2022, 2023.
- Cours C. Bulfone
- Cyber-Edu - Sensibilisation et initiation à la cybersécurité – Module 1
- Les virus informatiques : théorie, pratique et applications, *E. Filiol*, 2004, Springer
- Computer networking and the internet, *F. Halsall*, Addison Welseley, 2005 + additional student support at www.pearsoned.co.uk/halsall
- Network security bible, *E. Cole, R. Krutz, JW Conley* , Wiley, 2005.
- Preventing Ransomware, *A. Mohanta M. Hahad K. Velmurugan,* 2018 Packt
- Sécurité et espionnage informatique : connaissance de la menace APT, Cédric Pernet, *Eyrolles*
- Hackers heroes of the computer revolution, S. Levy, 2010, *O'Reilly*
- Learn Social Engineering*, Dr E. Orzkaya,* 2018, *Packt*
- Cybersecurity – Attack and defense strategies, Y Diogenes E. Ozkaya, 2019, *Packt*
- Digital Forensics and incident response, G. Johansen, 2017, *Packt*
- Network scanning cookbook, S. Jetty, 2018, *Packt*

(rappels) le dénombrement

- Permutations
  - Tous les mélanges des objets
  - *Combien de jeux différents avec 6 cartes ? (ex : « 4,5,2,1, 3,6 » ou « 1,3,6,4,5,2 »)*
  - 6!=6*5*4*3*2*1 = 720
- Arrangements A_n^p=n!/(n-p)!
  - Tirage d'une quantité d'objets dans l'ordre
  - *Combien de fois 3 chevaux dans l'ordre avec 6 chevaux au départ ? (ex « 1,3,2 » et « 3,2,1 » sont deux **arrangements** différents, donc comptés deux fois)*
  - 6!/(6 – 3)! = 6*5*4=120
- Combinaisons C_n^p=n!/(n-p)!p!
  - Tirage d'une quantité sans ordre
  - *Combien de possibilités de trois numéros parmi 6 ? (ex « 1,3,2 » et « 3,2,1 » sont constitués (**combinés**) des trois mêmes chiffres, donc comptés une seule fois)*
  - 6!/(6 – 3)!3!=(6*5*4)/(3*2*1)=120/6=20

Merci pour votre attention
Merci pour votre attention

jean-marc.thiriet@univ-grenoble-alpes.fr

Université Grenoble Alpes

Merci pour votre attention