TELECOM SudParis

IP PARIS

VAP SEM
CSC5032 : Mobilité et Objets Communicants

Sécurité Systèmes de Embarqués

Jose Manuel Rubio Hernán
Email: jose.rubio_hernan@telecom-sudparis.com

Département Électronique et Physique

Plan

Plan

Sécurité & sûreté (définition 1)

Sécurité (*Safety*)

La sécurité consiste à prévenir contre les accidents, donc par définition involontaire (liés à des évènements fortuits ou des actes sans intention de nuire).

Sûreté (*Security*)

La sûreté consiste à prévenir contre les actes de malveillance (liés à des actes délibérés ou à la négligence avec intention de nuire)

Sécurité & sûreté de fonctionnement (définition 2)

Sécurité (security)

La sécurité consiste à prévenir contre les actes de malveillance (liés à des actes délibérés ou à la négligence avec intention de nuire)

Sûreté de fonctionnement (safety)

La sûreté consiste à prévenir contre les accidents et erreurs, donc par définition involontaire (liés à des évènements fortuits ou des actes sans intention de nuire).

Definitions

Sécurité des Systèmes d'Information (SSI)

Ensemble des mesures techniques et non techniques de protection permettant à un système d'information de résister à des événements 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 [1].

Definitions

Sécurité des Systèmes d'Information (SSI)

Ensemble des mesures techniques et non techniques de protection permettant à un système d'information de résister à des événements 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 [1].

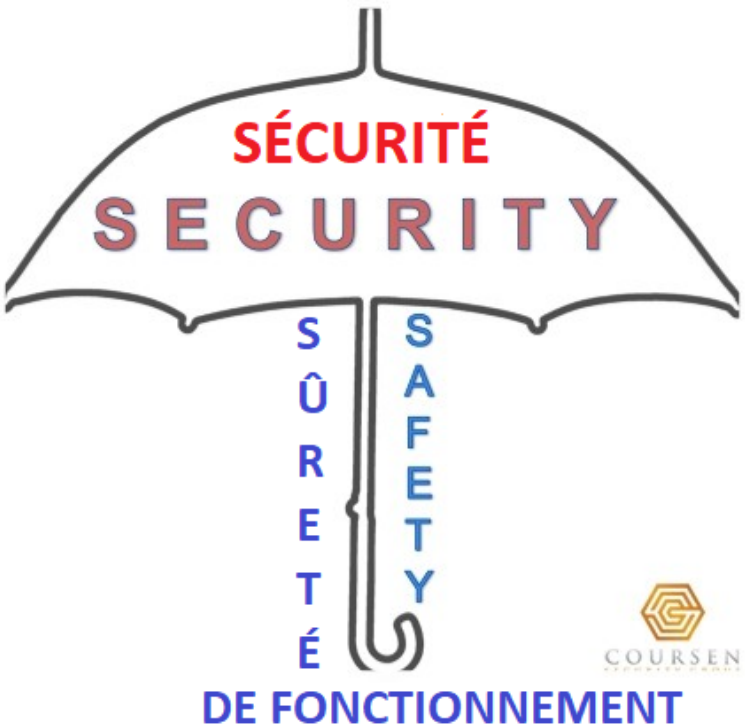
Sécurité de l'information

Protection de la confidentialité, de l'intégrité et de la disponibilité de l'information. En outre, d'autres propriétés, telles que l'authenticité, l'imputabilité, la non-répudiation et la fiabilité, peuvent également être concernées [*Source : ISO/IEC 27000 :2014*].

Sécurité & sûreté

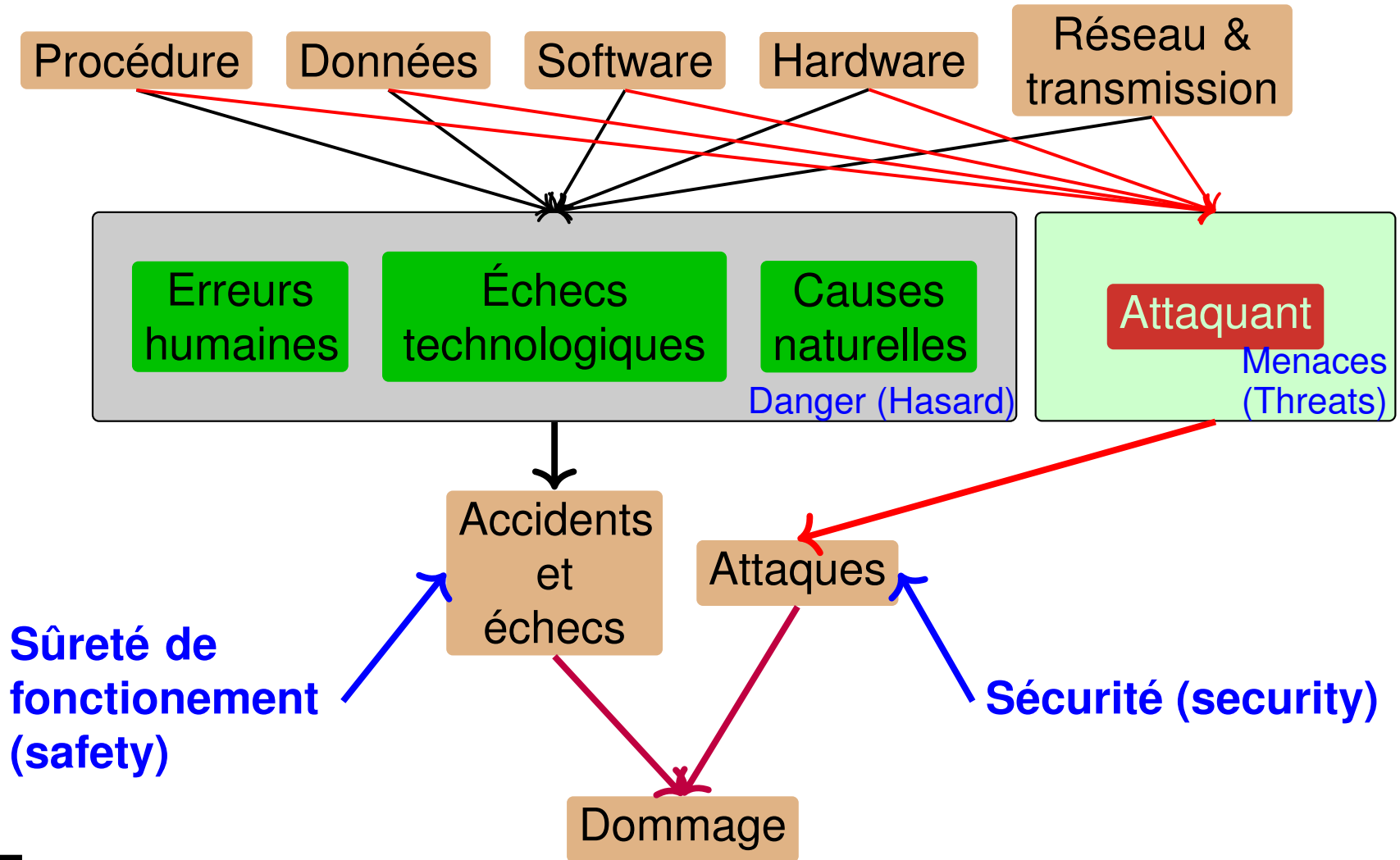
Pensez à la sécurité (*security*) comme si elle était le parapluie lors d'une tempête qui vous protège de la pluie. Votre sûreté de fonctionnement (*safety*) réside dans l'importance de rester au chaud et au sec. La sécurité (*security*) est la garantie qui garantit que notre sûreté de fonctionnement (*safety*) reste constante.

- Si les variables risquant de nuire à notre sûreté de fonctionnement (*safety*) **peuvent être prédites**, elles peuvent être évitées.
- Les variables risquant de nuire à notre sécurité (*security*) **ne sont pas faciles à prédire**.



Source : Coursen security group

Sécurité & sûreté de fonctionement



Accident vs. Attaques

Sécurité (*Security*)

Cybersecurity [2] :

- *The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.*

Domaines de la sécurité :

- **Sécurité physique** (eg. physical access to the servers or insertion of malicious hardware)
- **Sécurité de réseaux et de l'information** :
  1. Sécurité des communications,
  2. Sécurité opérationnelle,
  3. Sécurité de l'information.
- **Public/National Security** (infrastructures critiques attaques via cyberspace. L'objetive peut être physique ou cyber) **sécurité cyber-physique**

Propriétés de sécurité de l'information

Propriétés :

- **Confidentiality** - *confidentiality* - est la propriété qui permet d'empêcher les informations sensibles d'atteindre les mauvaises personnes (parties non autorisées) , tout en veillant à ce que les bonnes personnes (parties autorisées) puissent les obtenir.
- **Integrity** - *integrity* - est la propriété qui permet de maintenir la cohérence, l'exactitude et la fiabilité des données tout au long de leur cycle de vie.
- **Disponibilité** - *availability* - est la propieté qui permet que l'informatisons soient accessibles aux utilisateurs autorisés.
- Authentification - traçabilité - est la propriété qui permet de légitimer la demande d'accès au système, réseau ... faite par une entité externe.
- Non-répudiation de l'origine assure que l'émetteur du message ne pourra pas nier avoir émis le message dans le futur.

Plan

Système embarqué

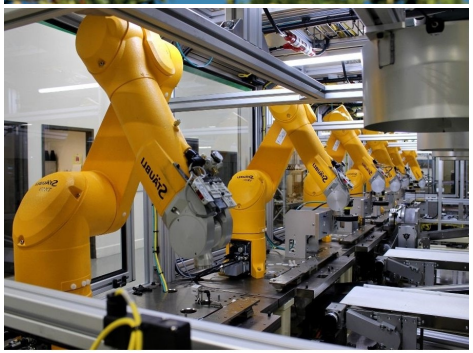
Système embarqué (définition)

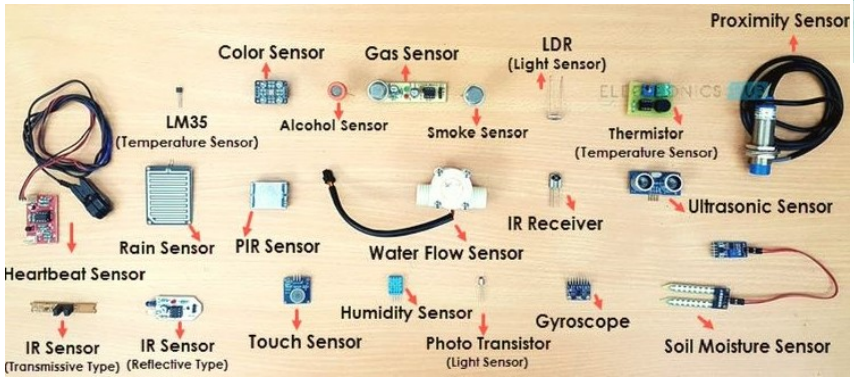
Un système embarqué peut être défini comme un **système électronique et informatique autonome**, qui est **dédié à une tâche bien précise, souvent en temps réel**, possédant des ressources d'ordre spatial (taille limitée) et énergétique (consommation restreinte) limitées.
Le terme de *Système Embarqué* désigne aussi bien le matériel que le logiciel utilisé.

Caractéristique

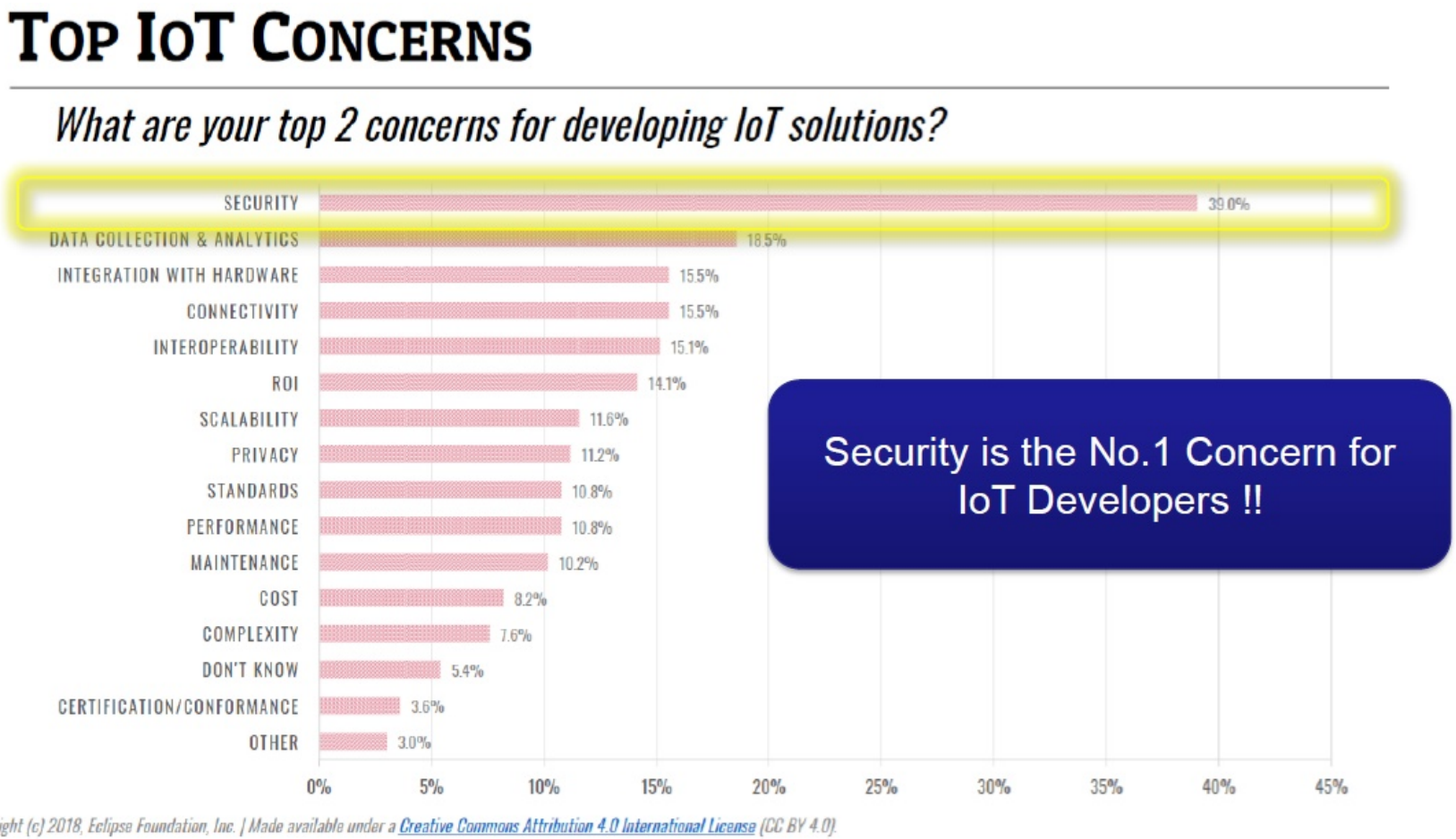
1. Fiable :
   - robustesse
   - maintenance
   - disponibilité
   - **sûreté de fonctionnement**
   - **sécurité**
2. Efficace :
   - consommation énergétique
   - faille du code / hardware
   - le poids et la taille
   - coût de fabrication, de conception et de design

Exemples de systèmes embarqués





Inquiétude des développeurs IoT



Source : IOT Developer Survey -2018 https://www.slideshare.net/kartben/iot-developer-survey-2018.

Source : Microchip

Types d'attaques

Hardware

1. **Intrusif**
   - **Accès physique au secret**
   - **Attaques par observation** (Anglais-> Side channel)
     - **Attaques laser**
     - **Attaques par potence**
     - **Attaques par temperature**
     - **Attaques par fréquence**
2. **Attaques logicielles**
   - BIOS hacking
   - Rootkits / Rooting
   - Jail breaking
   - VM escapes
   - Hardware Reflected Injection
3. **Non intrusif**
   - **Attaques par perturbation (pas d'accès physique)**
     - Acoustic crypto analysis
     - DRAM attacks
     - Electromagnetic Radiation Monitoring
     - Remotely inducing an invalid low power state
   - **Accés physique**
     - Differential power analysis
     - Power consumption during crypto computations
     - Values of variables related to secret keys

Types d'attaques

Réseaux

- **Attaque man-in-the-middle**
- **Replay attack**
- **Dénégation de service (DDoS)**
- **ARP poissoning**
- **Phishing attacks**
- **Spoofing attacks**
  - IP Address Spoofing Attacks
  - ARP poissoning
  - DNS Server Spoofing Attacks.
- **Jamming attacks :** attaque radio

Logiciel (software)

- **Malware spreading**
- **Access through database links**
- **...**

Exercice : Choisir un attaque et expliquer comment ça marche, et les possibles contramesures.

Plan

Sécurité Hardware

Hardware security

Just as software can have exploitable flaws and vulnerabilities, hardware carries similar risks, but with one major setback : "patching" hardware vulnerabilities requires manual labor and much more time than software, which can be patched for millions of users with a click of a button. With billions of devices being created and released each year.
[CyLab Security and Privacy Institute]

Note

- **la sécurité matériel née avec les *Hardware Trojan***
- **maintenant tourne vers le développement de matériel digne de confiance (*trustworthly Hardware*) pour la construction d'une racine de confiance (*root-of-trust)***

Sécurité Hardware

Hardware security [3]

- Hardware Trojan Detection
  - **Test fonctionnel améliorée :** La méthode repose sur l'idée que les chevaux de Troie matériels reposent souvent sur des événements rarement déclenchés.
  - **Empreintes digitales sur les canaux latéraux :** l'efficacité de cette méthode repose sur la capacité de différencier les signaux des canaux latéraux des circuits infectés par des chevaux de Troie des circuits sans chevaux de Troie.
    Problème : Necesité d'un modèle très precis pour faire la comparaison.
  - **Renforcement des circuits :** ces techniques tentent de modifier la structure du circuit avec une logique supplémentaire.
- Fonction physiquement non clonable (PUF)
  - Cette fonction exploite les disparités de perturbations causées par les variations de processus (eg. **le bruit**) pour générer des identités uniques, souvent des paires défi-réponse.
  - Cette fonction a une caractère aléatoire, de unicité, et de sécurité renforcée Exemple : ChipDNA *Maxim Integrated*

Sécurité Hardware

Sécurité informatique assistée par matériel :

- **ARM Trustzone (eg. ARM cortex M23)**
  L'approche TrustZone est basée sur une plate-forme sécurisée, dans laquelle une architecture matérielle prend en charge et applique une infrastructure de sécurité dans l'ensemble du système.
- **Intel SGX (software guard extension)**
  Extensions ajoutées à l'architecture Intel pour appliquer des stratégies et des autorisations d'accès à la mémoire.

Sécurité Hardware

Sécurité informatique assistée par matériel :

- **CHERI (capability hardware enhanced RISC instruction)**
  L'extension fournir une compartimentation fine de la mémoire dans le matériel tout en maintenant la compatibilité logicielle. Son objectif est la protection de la mémoire *(via une granularité fine de la mémoire, contrôle d'accès, évolutivité de segment/domaine, sécurité du pointeur etc.)*.
- **LowRISC**
  Jeu d'instructions pour les SoCs, qui est construit pour atteindre la sécurité et la haute performance.
  Problème : Open hardware projet.

Sécurité Hardware

Fireware

- Le terme apparaît vers les année 60s (*Rudy Meléndez - Datamotion*
- C'est une code **intègre** directement dans le **hardware** (avec un **langage de programmation**)
- Il est le **lien entre le hardware et le software** avec 3 fonction principaux :
  1. Il parvient à **accorder au système les routines fondamentales de fonctionnement** et de réponse par rapport aux demandes.
  2. L'utilisation comme **interface simple** et pratique de manière à ce que la configuration du système puisse être rapidement et facilement effectuée.
  3. Le **contrôle et gestion du démarrage du système**.

Exemple : La BIOS du système

Sécurité Hardware

Secure Boot UEFI (Unified Extensible Firmware Interface)

- **Problème :** attaques appelées *malware injection*.
  - Récupérer des données confidentielles et sensibles.
  - Forcer le périphérique à fonctionner de manière incorrecte.
  - Induire un comportement imprévisible du périphérique.
- **Objectif :** protéger les systèmes embarqués depuis la conception (authentification et la intégrité)
- **Solution :**
  - Asymmetric cryptographic algorithms, spécifiquement le FIPS 186 Elliptic Curve Digital Signature Algorithm (ECDSA).
  - Caractéristiques
    - Algorithme publique
    - Le développeur de fireware signe avec la clés privée
    - Le système embarqué utilise et stocke la clés public pour faire la vérification de données reçu (Vérification de la signature ECDSA)
    - Taille de la clés 256 bits ou plus (SHA-256 hash)

Plus d'information :
`https://www.maximintegrated.com/en/app-notes/index.mvp/id/6426`

Sécurité Hardware

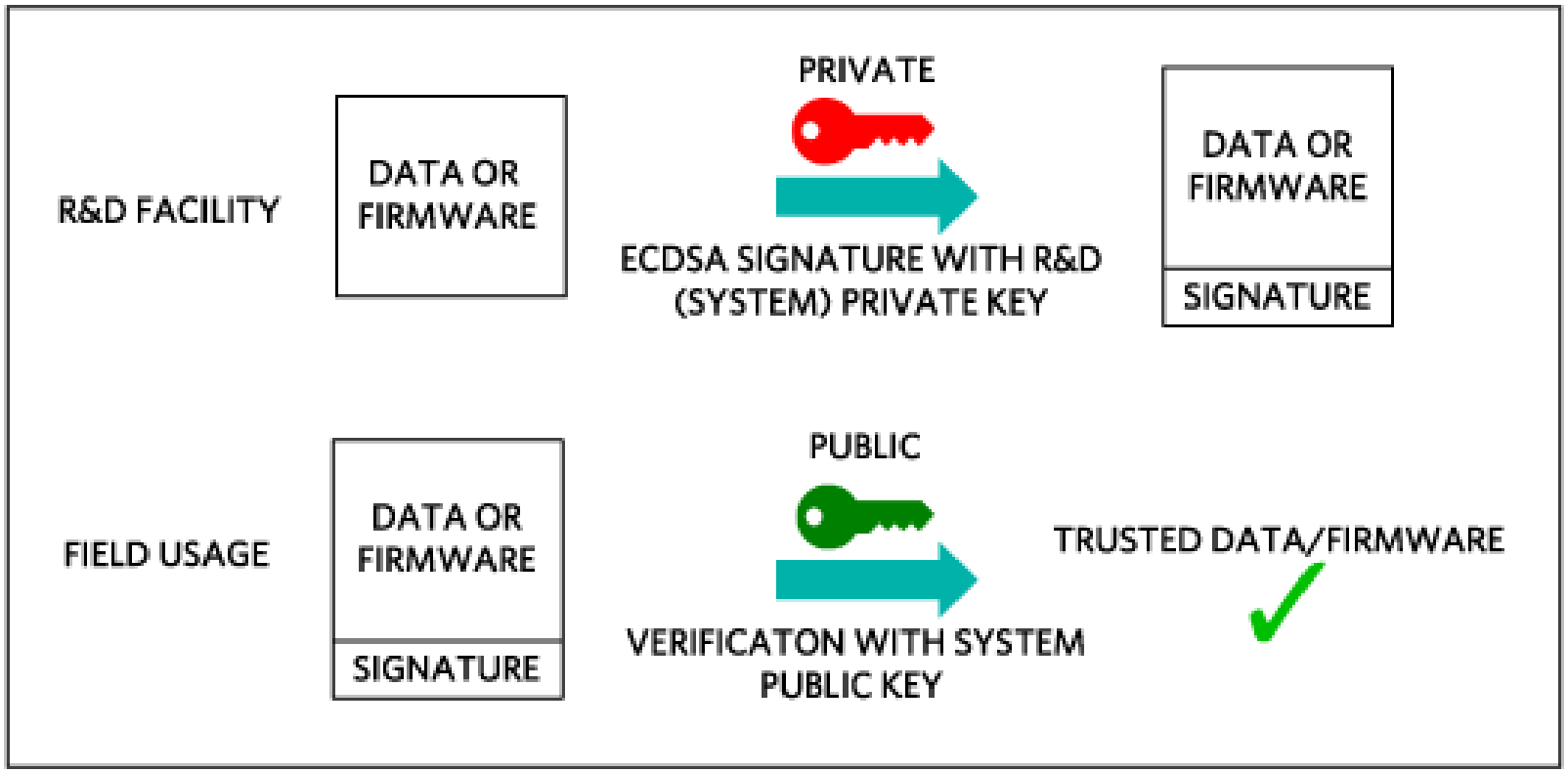


FIGURE – Use of ECDSA for secure boot and secure download.

Source : Maxime Integrated [4]

Sécurité Hardware

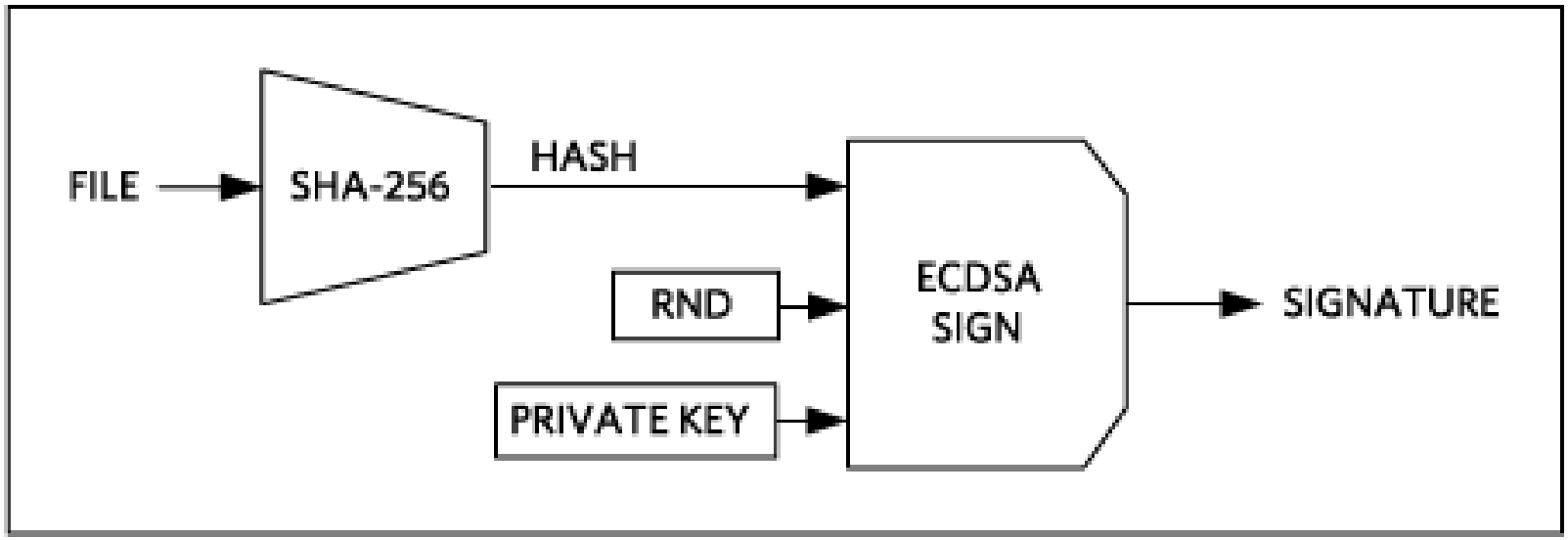


FIGURE – ECDSA signing of the firmware/data file

ECDSA : Elliptic Curve Digital Signature Algorithm **Signature :**
(r=x_{courbe},s) : $s = k^{-1}(hash(m) + rkey_{private})$

Source : Maxime Integrated [4]

Sécurité Hardware

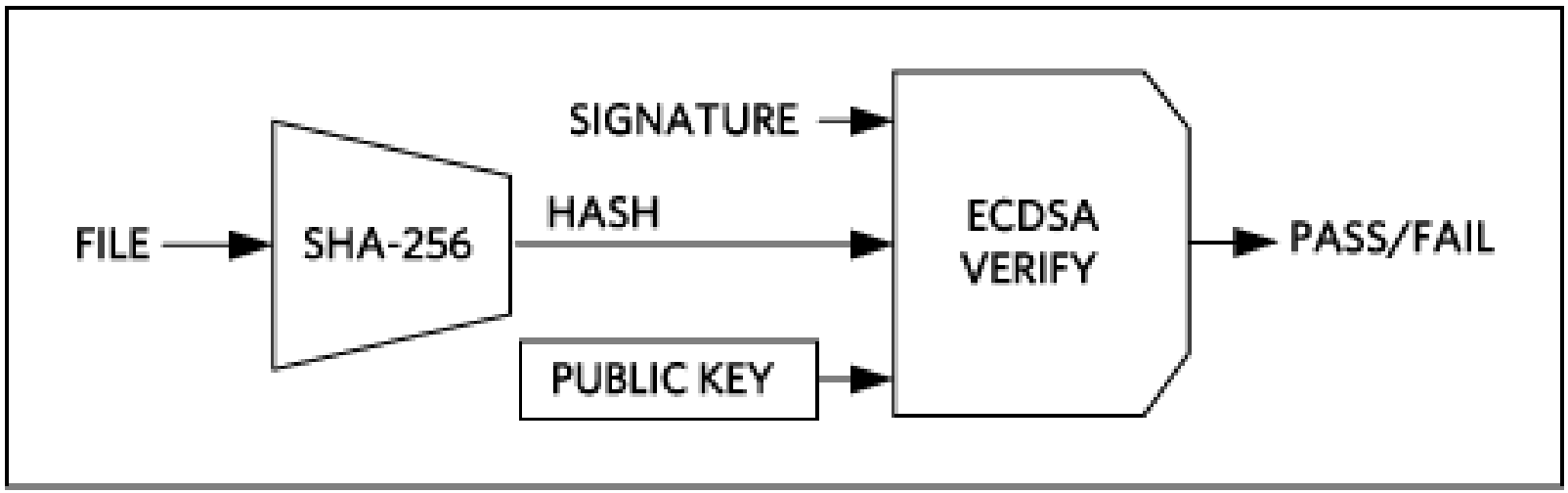


FIGURE – ECDSA verification of the firmware/data-file signature.

Source : Maxime Integrated [4]

Sécurité Hardware : RNG (sécurité dans les FPGAs)

Random Number Generator :

- Pseudo-RNG (PRNG)
  - Graine (*Seed*)
  - Algorithm
  - Problème : prévisibilité
- True-RNG (TRNG)
  - Pas de Graine (*Seed*)
  - Nombre aléatoire basé sur les phénomènes physiques
  - Sources :
    - Bruit thermique
    - Bruit atmosphérique
    - Bruit de grenaille (*Shot Noise*)
    - Bruit de scintillation (*flicker noise*)
    - Bruit radio
    - Gigue d'horloge (*Clock jitter*)
    - Bruit de phase (*Phase noise*)

Le **FPGA** est une plate-forme populaire pour la mise en œuvre de nombreux systèmes cryptographiques qui incluent les TRNG.

Hardware Hacking

Attaques

- Par des ingénieurs non électroniques
  - Amateurs de hackers / chercheurs
- Avec peu de connaissances sur la façon dont le produit était conçu
  - Pas d'accès à la fiche technique
  - Pas d'accès aux choix de conception ou à l'architecture
  - Pas d'accès au code source
- Avec des outils accessibles au public et bon marché (Ouvrir logiciels et outils Open Hardware)
- Sans l'utilisation d'électronique et de appareils de mesure. . . (attaques bon marché)

Mode d'emploi

- **Analyser, Exploitation, Destruction**

Différences avec les attaques software

Systèmes embarqués (Hardware)

- Aucune base de données de vulnérabilité disponible (ou peu) sur le l'Internet
- Chaque appareil est spécifique
- Protocoles de communication réseau plus obscurs
- Architecture décrit dans les fiches techniques
- Code source plus fermé
- Beaucoup de bibliothèques vulnérables ou anciennes
- Les périphériques matériels ne sont pas si souvent mis à jour

Plan

Comment sécuriser votre matériel

IMPORTANT

- Conception sécurisée et cycle de vie de développement (SDLC)
- Examen des meilleures pratiques de sécurité matérielle pour limiter les risques
- Limiter les accès JTAG et les vulnérabilités logicielles au niveau du système embarqué
- Examen des protections contre les attaques à canal latéral
- Contrôler l'accès via les différents bus de communication :
  - Bus de programmation
    - **JTAG** (Joint Test Action Group)
    - **SWD** (Serial Wire Debug
    - **ICSP** (In Circuit Serial programming)
  - Bus de communication
    - **SPI** (Serial Peripheral
    - **I2C** (Inter Integrated
    - **UART** (Universal Asynchronous Receiver Transmitter)

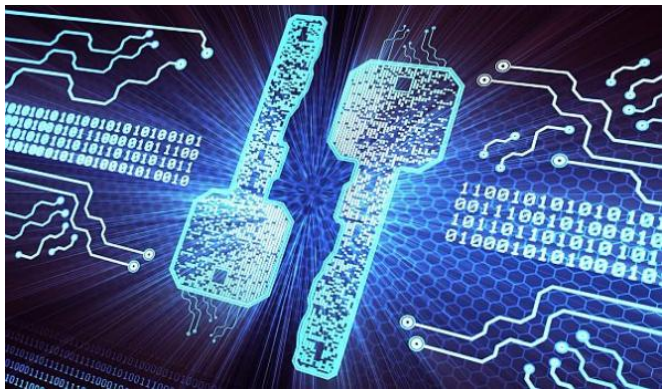
Comment sécuriser un système embarqué

- ISM Band
- One Time Programmable / One Time Password
- Crypto Hardware (Hardware Security Module (HSM) , SECURE ELEMENT , Trusted Platform Module (TPM))
- Datasheet
- Paradoxe des anniversaires
- Mise à jour des systèmes

Cryptographie

Cryptographie

Science des écritures cachées



Objectif

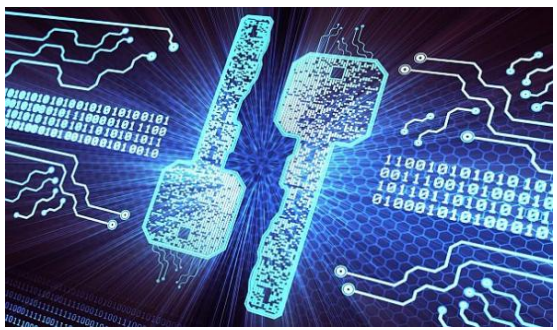
Garantir une communication sécurisée malgré les potentielles attaques extérieures

Cryptographie : principe général

Adversaire

Une entité malveillante dont le objectif est d'empêcher aux utilisateurs légitimes une bonne utilisation du système.

- Adversaire passif
- Adversaire actif



Principe

Transformer le contenu de l'information. Contenu indéchiffrable à toute personne extérieure.

Cryptographie

Cryptographie

- La Cryptographie est une des disciplines de la cryptologie. Le mot cryptographie viens du Grecque **kruptos** $\kappa\rho\upsilon\pi\tau$ός (caché ou secret) et **graphein** $\gamma\pi\alpha\phi\eta$ (écrire).

Terminologie

- CRYPTOLOGIE
- CRYPTOGRAPHIE
- CHIFFREMENT
- CHIFFRER
- DÉCHIFFRER
- DÉCRYPTER
- CHIFFRAGE
- CHAÎNES DITES *CRYPTÉES*
- CRYPTER / CRYPTAGE
- ENCRYPTER / DÉENCRYPTER

Cryptographie

Cryptographie

- La Cryptographie est une des disciplines de la cryptologie. Le mot cryptographie viens du Grecque **kruptos** $\kappa\rho\upsilon\pi\tau$ός (caché ou secret) et **graphein** $\gamma\pi\alpha\phi\eta$ (écrire).

Terminologie

- CRYPTOLOGIE ✓
- CRYPTOGRAPHIE ✓
- CHIFFREMENT ✓
- CHIFFRER ✓
- DÉCHIFFRER ✓
- DÉCRYPTER ✓

- CHIFFRAGE ✗
- CHAÎNES DITES *CRYPTÉES* ✓
- CRYPTER / CRYPTAGE ✗
- ENCRYPTER / DÉENCRYPTER ✗

Terminologie (1/3)

- ✓ **Cryptologie :** la science du secret, JUsqu'à les année 80's reservé aux militaires et diplômâts. Cette science englobe : la cryptographie - l'art de communiquer de manière confidentielle via un canal non sécurisé -, la cryptanalyse - l'art de déchiffrer ces communications quand on n'est pas le destinataire légitime-, et la stéganographie – l'art de la dissimulation.
- ✓ **Cryptographie :** La cryptographie est l'art de communiquer de manière confidentielle via un canal non sécurisé. Elle est une des disciplines de la cryptologie s'attachant à protéger des messages en s'aidant souvent de secrets ou clés.

Terminologie (2/3)

✓ **Chiffrement ;** Le chiffrement est un procédé de cryptographie qui consiste à transformer un message à transmettre, dit *message clair* , en un autre message, inintelligible pour un tiers, dit *message chiffré*, en vue d'assurer le secret de sa transmission.

✓ **Chiffrer :** L'action de procéder à un chiffrement.

✓ **Dechiffrer :** En informatique et en télécommunications, déchiffrer consiste à retrouver le texte original d'un message chiffré dont on possède la clé de (dé)chiffrement.

✗ **Chiffage :** Action de chiffrer, de calculer

Terminologie (3/3)

✗ **Décrypter :** Décrypter consiste à retrouver le texte original (clair) d'un message chiffré, sans connaître la clef ayant servi à le transcrire.
Note : Décrypter ne peut accepter d'antonyme (**Crypter**) : il est impossible de créer un message chiffré sans posséder de clé de chiffrement.

✓ **Chaines dites cryptées :** Dans le cadre de la télévision à péage, l'Académie Française accepte de parler de chaînes *cryptées*.

✗ **Cryptage :** Action de coder un fichier sans en connaître la clé et donc sans pouvoir le décoder ensuite. Le Référentiel Général de Sécurité de l'ANSSI qualifie d'incorrect *cryptage*, et elle n'est pas reconnu par le dictionnaire de l'Académie française.

✗ **Encrypter** / **Deencrypter :** Le terme *encrypter* et ses dérivés sont des **anglicismes**.

Un peu d'histoire

Stéganographie (dés le Ve siècle av JC) : cacher un message dans un autre.

Exemples :

- raser la tête d'un esclave,
- lire un paragraphe différèrent,
- lire les lsb ou les msb d'une figure.

Cover image

message to be hide

stegnographic image

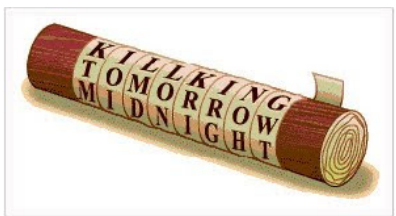
extracted message image

Source : https ://fr.mathworks.com/matlabcentral/fileexchange/41326-steganography-using-lsb-substitution by Ashish Soni

Un peu d'histoire

Cryptographie :

Scytale spartiate



Origine de la cryptographie :
Ve siècle av JC

Jeux de lettres :

- chiffre de César (Substitution, Permutation),
- chiffrement de Vigenère (Substitution, Permutation, une lettre puisse être codée de plusieurs façons),

Un peu d'histoire

Cryptographie :

Avant le XXème siècle :

- très simple : chiffre manuellement,
- attaque : Analyse de fréquence des lettres dans l'alphabet

Entre 1900 et 1970 :

- plus élaborés : chiffre manuellement,
- apparition de machines chiffrantes (automatisation)
  Ex. machine Enigma

Aujourd'hui :

- mécanismes complexes pour assurer la confidentialité, et authenticité sans révéler la moindre information sur le secret ni l'envoyer sur un canal,
- Année 70 démocratisation de sa utilisation.

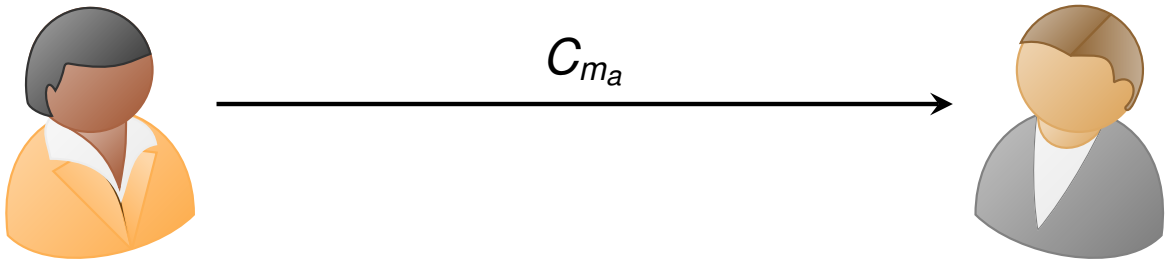
Principe de Kerckhoffs (1883)

Les axiomes fondamentaux de la cryptographie sont :

- **L'adversaire possède tous les détails de l'algorithme**
- Il y a **seule un élément secret, la clef**.

Chiffrement symétrique

Comme fonctionne ?

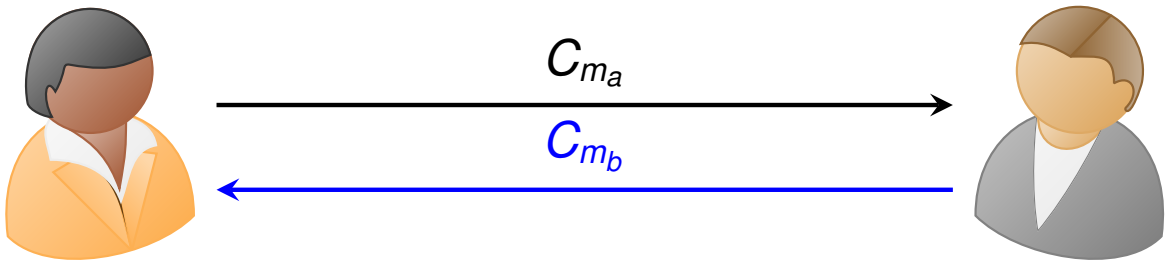


Alice : C_{m_a} = Chiffre(m_a, k)

Bob : m_a = Déchiffre (C_{m_a}, k)

Chiffrement symétrique

Comme fonctionne ?



Alice : C_{m_a}= Chiffre(m_a, k)

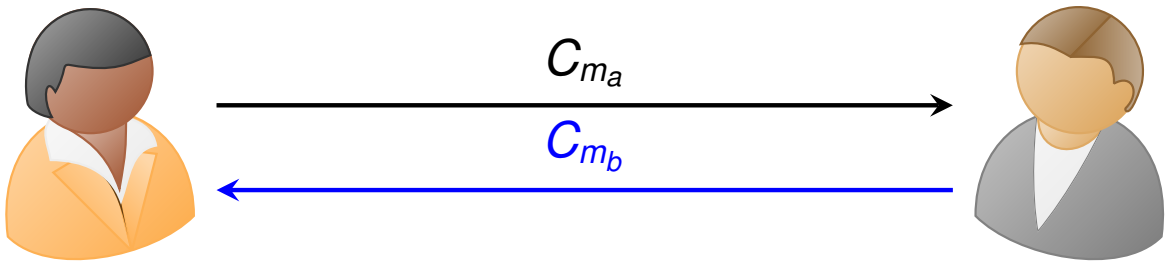
m_b= Déchiffre (C_{m_b}, k)

Bob : m_a= Déchiffre (C_{m_a}, k)

C_{m_b}= Chiffre(m_b, k)

Chiffrement symétrique

Comme fonctionne ?



Alice : C_{m_a}= Chiffre(m_a, k)

Bob : m_a= Déchiffre (C_{m_a}, k)

m_b= Déchiffre (C_{m_b}, k)

C_{m_b}= Chiffre(m_b, k)

Inconvénients

- **Nombre de clés très important : Une clé pour un chaque couple d'utilisateurs** (par exemple, difficile à gérer pour des groupes de partage)
- **Echange de clés difficile à mettre en place :** Transmission d'une nouvelle clé **oblige les deux parties à se rencontrer**

Système de chiffrement à clés secrète

Cryptographie à clés secrète

- **Opération simple :** utilisation des bits,
- Système de chiffrement **par flot (stream cipher)**,
- Système de chiffrement **par bloc (block cipher)**.

Chiffrement Vernam *One time Pad*

Cryptosystème développe par Gilbert Vernam en 1918

Schéma à clé secrète : Parfaitement sûr

- Chiffrement

Clair : 0100100001101001 = Hi (ASCII)
Clé $\oplus$ 1001110100110101
Chiffré = 1101010101011100 = Õ\ (ASCII)

- Déchiffrement

Chiffré : 1101010101011100 = Õ\ (ASCII)
Clé $\oplus$ 1001110100110101
Clair = 0100100001101001 = Hi (ASCII)

Chiffrement Vernam *One time Pad*

Cryptosystème développe par Gilbert Vernam en 1918

Schéma à clé secrète : Parfaitement sûr

- Chiffrement

Clair : 0100100001101001 = Hi (ASCII)
Clé $\oplus$ 1001110100110101
Chiffré = 1101010101011100 = Õ\ (ASCII)

- Déchiffrement

Chiffré : 1101010101011100 = Õ\ (ASCII)
Clé $\oplus$ 1001110100110101
Clair = 0100100001101001 = Hi (ASCII)

Caractéristiques :

1. Clé totalement aléatoire,
2. Taille de la clés égal au message en clair,
3. Utiliser a chaque fois une clé diffèrent,
4. Garder la clés toujours en secret.

Chiffrement Vernam *One time Pad*

Utilisé pour chiffrer les messages du téléphone rouge

Avantages

- Sécurité inconditionnelle
- Aucune information ne peut être déduite sur le clair, à partir du chiffré

Inconvénients

- Gestion difficile des clés : les clés sont aussi longues que les messages
- Renouvellement de la clé pour chaque nouveau message

Système de chiffrement par flot (stream cipher)

Même principe que le chiffrement de Vernam

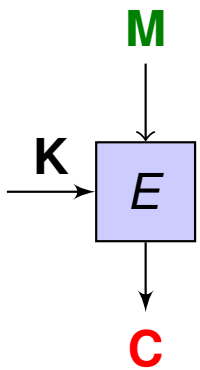
Idée : une clé plus courte

- On en dérive une suite de bits **pseudo-aléatoire** de longueur voulue
- Cette suite est l'équivalent de la clé du chiffrement de Vernam

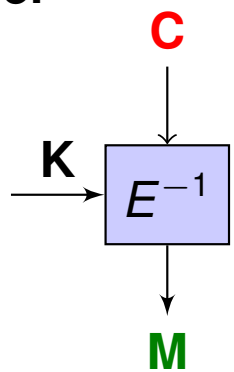
Système de chiffrement par block (block cipher)

Principe : Le calcul est réalisé sur un bloc de taille fixe

Chiffrer



Déchiffrer



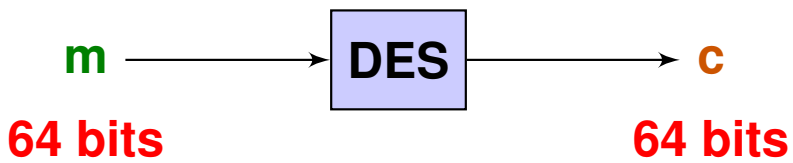
Exemples :

1. **DES (1977) :** blocs de 64 bits, clés de 56 bits
2. **AES (2000) :** blocs de 128 bits, clés de 128, 192 ou 256 bits

Data Encryption Standard (DES)

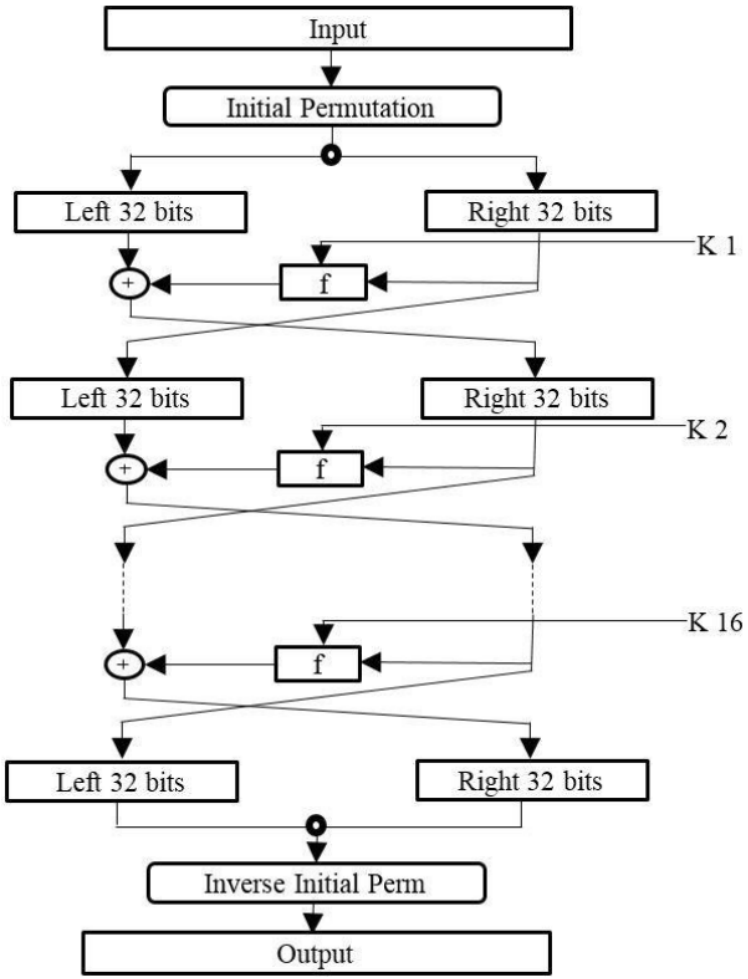
Algorithme de chiffrement symétrique par bloc

1. Une clé maître : Clé K = 56 bits
2. Bloc de taille 64 bits



3. 16 sous clés de 48 bits générés à partir de K : K1, K2, . . . , K16

DES : Mode de fonctionnement



Source : A Survey on the Cryptographic Encryption Algorithms [5]

Utilise les schémas de Feistal

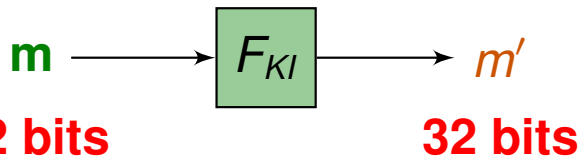
Idée : 16 tours avec les sous clés K1, K2, . . . , K16

Opérations :

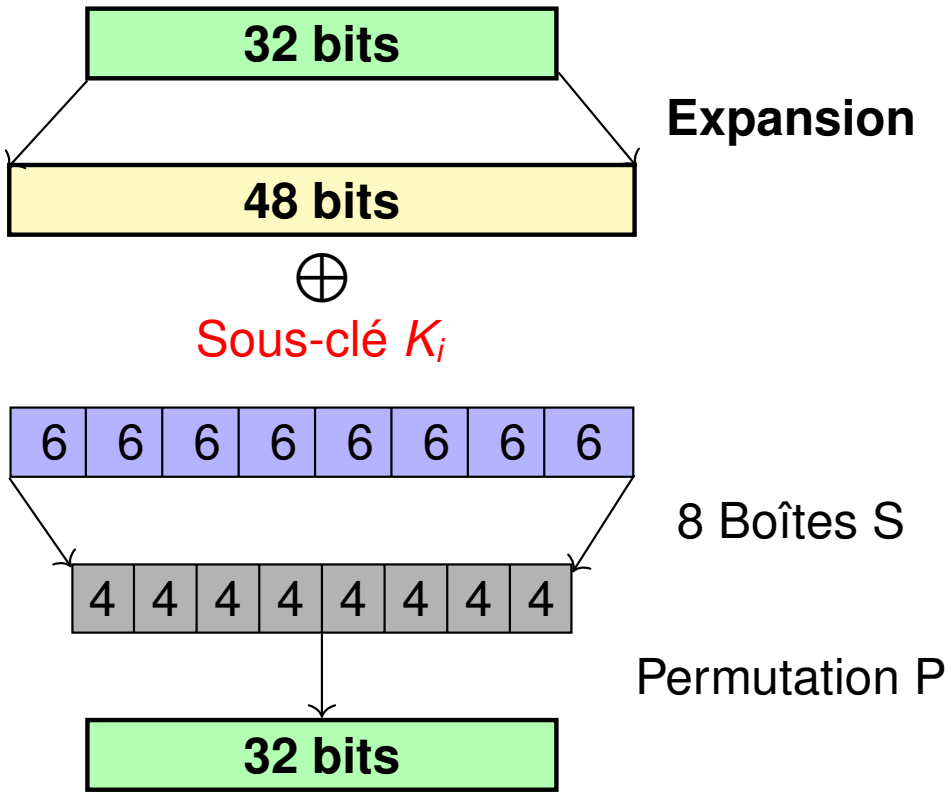
- Permutation initiale
- 16 tours de Feistal
- Permutation Inverse

DES : Mode de fonctionnement

Fonctions Feistal :



Principe :



Sécurité du DES

Attaque : DES a été cassé par recherche exhaustive :
18 Janvier 1999, Electronic Frontier Fundation (EFF), 100000 PC, 22h15

Idée : Utiliser le double DES :

- DESK1(DESK2(m))
- Attaque par le milieu : DES K1 (M) = ? DES-1 K2 (C)

Solution :

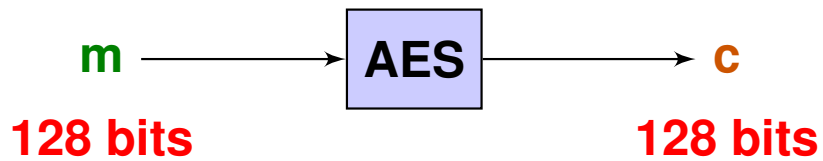
- Utilisation du triple DES (3 clés différentes)

Advanced Encryption Standard (AES)

Algorithme de chiffrement symétrique par bloc

Composé par :

1. Une clé maître : Clé K de 128, 192, ou 256 bits (découpés en octets)
2. Bloc de taille 128 bits

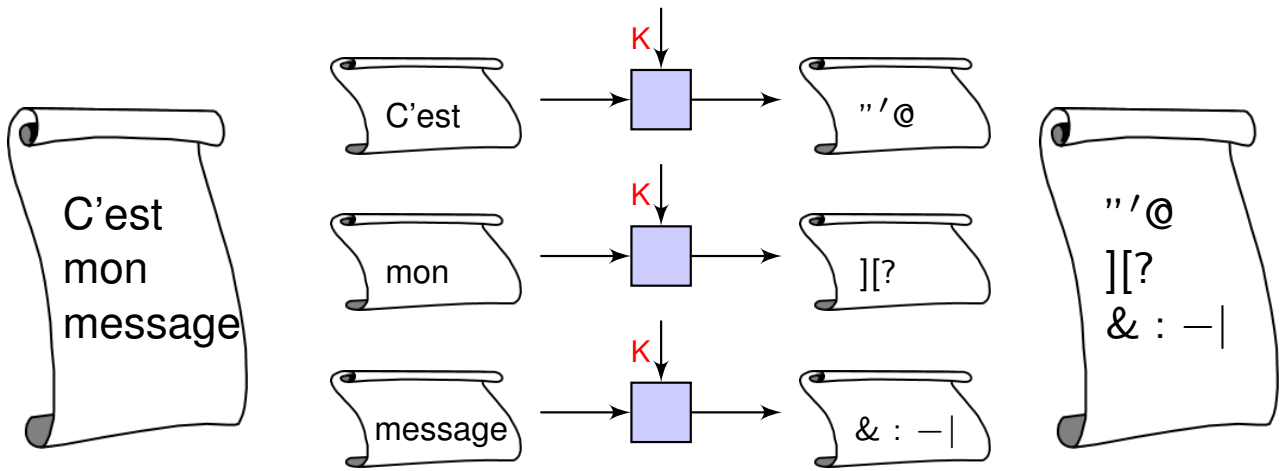


3. Des sous clés de 128 bits générés à partir de K : Le nombre des clés dépend du nombre des tours

Modes de chiffrement

Le mode ECB (Electronic Code Book) : *Dictionnaire de codes*

- Le message est découpé en plusieurs **blocs de taille fixe**
- Chaque bloc est chiffré séparément



⇒ Advantage : Le calcul est parallélisé

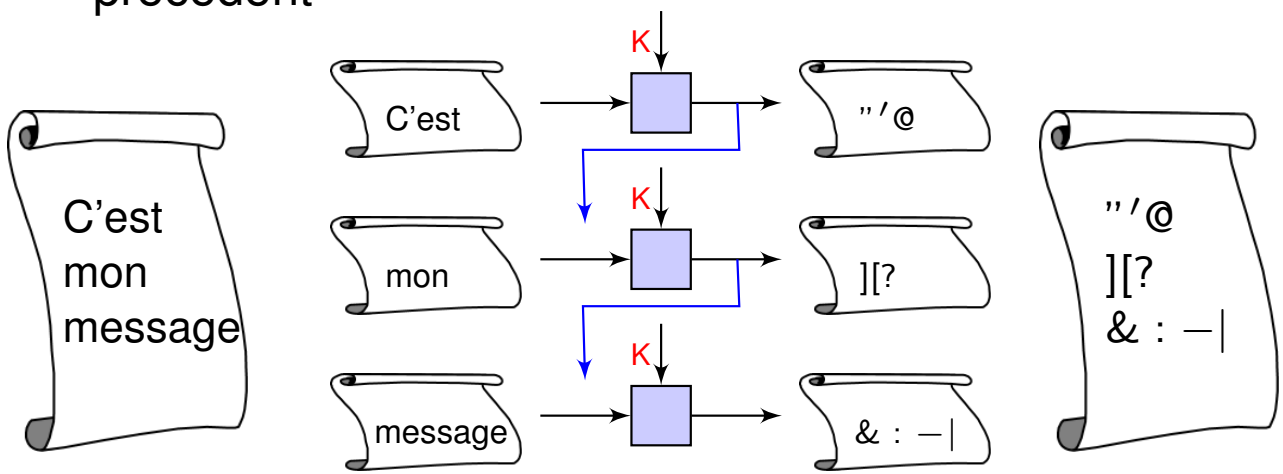
⇒ Inconvénient : Le chiffrement de deux blocs identiques

⇒ deux chiffrés identiques

Modes de chiffrement

Le mode CBC (Cipher Block Chaining) : *Enchainement de blocs*

- Le message est découpé en plusieurs blocs de taille fixe
- Le chiffré d'un bloc est obtenu en fonction du chiffré du bloc précédent



⇒ Advantage : Moins vulnérable que le mode ECB

⇒ Inconvénient : Pas de calcul parallélisé

D'autres modes de chiffrements par blocs le mode CFB (Cipher Feedback)

Chiffrement asymétrique

Question simple : Alice et Bob ont-ils besoin de partager la même clé pour pouvoir communiquer ?

Idée novatrice : Diffie et Hellman (1976) Les clés nécessaires au chiffrement et au déchiffrement peuvent être différentes

Chiffrement asymétrique

Question simple : Alice et Bob ont-ils besoin de partager la même clé pour pouvoir communiquer ?

Idée novatrice : Diffie et Hellman (1976) Les clés nécessaires au chiffrement et au déchiffrement peuvent être différentes

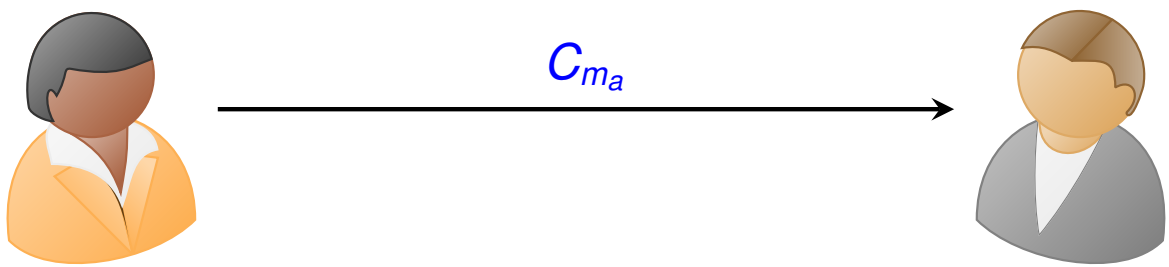
Le **chiffrement asymétrique** a une clé privée (secrète) et une clé publique.

Chiffrement asymétrique

Question simple : Alice et Bob ont-ils besoin de partager la même clé pour pouvoir communiquer ?

Idée novatrice : Diffie et Hellman (1976) Les clés nécessaires au chiffrement et au déchiffrement peuvent être différentes

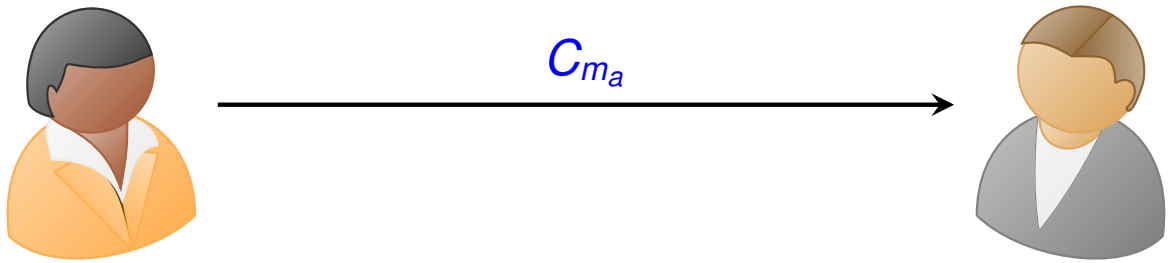
Le **chiffrement asymétrique** a une clé privée (secrète) et une clé publique.



Alice : C_{m_a} = Chiffre(m_a, p_{Bob})

Bob : m_a = Déchiffre (C_{m_a}, s_{Bob})

Chiffrement asymétrique



Alice : C_{m_a}= Chiffre(m_a, p_{Bob})

Bob : m_a = Déchiffre (C_{m_a}, s_{Bob})

Une paire de clés :

- tout le monde peut chiffrer avec la clé publique du destinataire,
- seul le destinataire peut déchiffrer avec sa clé privée.

Notion d'asymétrie :

- Les algorithmes de chiffrements et de déchiffrement ont des rôles fondamentalement différents

Systèmes de chiffrement à clé publique (1/2)

Propriétés

- **Clés :** La connaissance de la clé publique ne doit pas permettre de retrouver /déduire la clé privée.
  Comment faire étant donné le lien qui existe entre les deux clés ?
- **Schéma :**
  - Chiffrer un message doit être réalisable.
  - Déchiffrer, sans la clé, doit être difficile

Systèmes de chiffrement à clé publique (1/2)

Propriétés

- **Clés :** La connaissance de la clé publique ne doit pas permettre de retrouver /déduire la clé privée.
  Comment faire étant donné le lien qui existe entre les deux clés ?
- **Schéma :**
  - Chiffrer un message doit être réalisable.
  - Déchiffrer, sans la clé, doit être difficile

Relation entre la clé publique et la clé privée ?

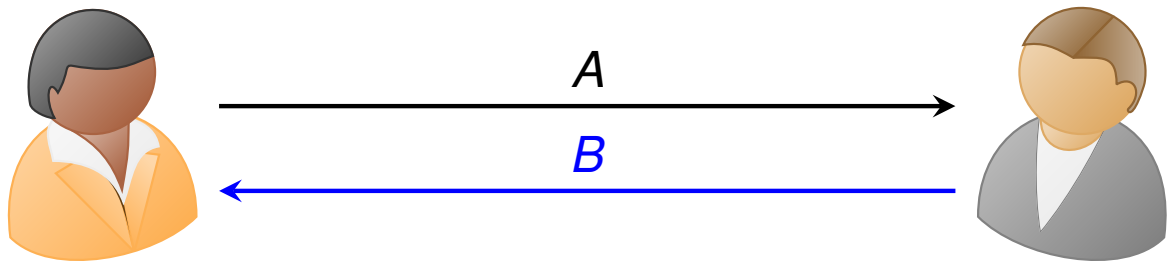
- Repose sur des **problèmes mathématiques difficiles à résoudre**.
  - Problème de **la factorisation d'entiers** en produit de facteurs premiers
  - Problème du **logarithme discret**
  - Problème de **la résolution d'un système quadratique aléatoire**

Systèmes de chiffrement à clé publique (2/2)

Objectif :

- **Retrouver la clé privée à partir de la clé publique** est aussi dur que résoudre le problème mathématique lui-même
- **Déchiffrer un message, sans la clé privée**, est aussi dur que résoudre le problème mathématique lui-même

Échange de clés Diffie Hellman



Alice (Secret a)

Bob (Secret b)

$A = g^a mod(p)$, $K = g^{ab} mod(p)$

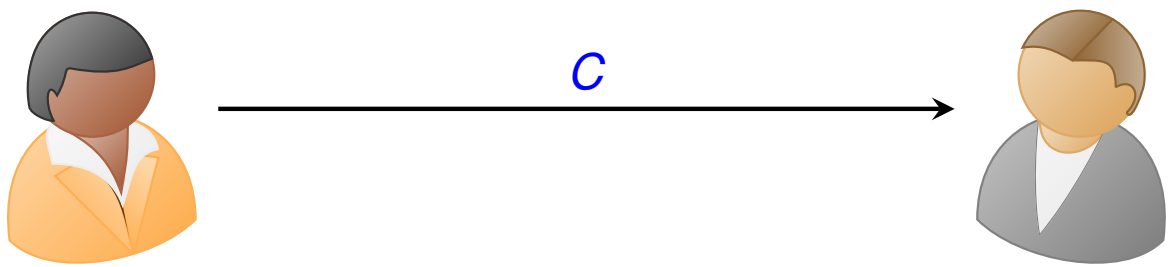
$B = g^b mod(p)$; $K = g^{ba} mod(p)$

- g sur groupe G mod(p)
- p nombre premier

Rivest, Shamir et Adleman (RSA)

Algorithme de **chiffrement asymétrique** très utilisé (1979) **Sécurité basée sur le problème de factorisation de numéros entiers**

- **Initialisation :**
  - **Nombres premiers p,q :** $n = pq$ (p, q taille similaire)
  - ϕ **(fonction d'Euler) :** $phi(n) = (p-1)(p+1)$
  - **Choisir deux entiers (e,d) :** $ed = 1 mod(p-1)(q-1)$
  - (n, e) est la clé privé et (n, d) est la clé publique.
- **Schéma :**



Alice (m) : $C = m^e$ mod(n)

Bob (e,d) : $C^d = m$ mod(n)

Chiffrement hybride

Mélanger les deux systèmes de chiffrement

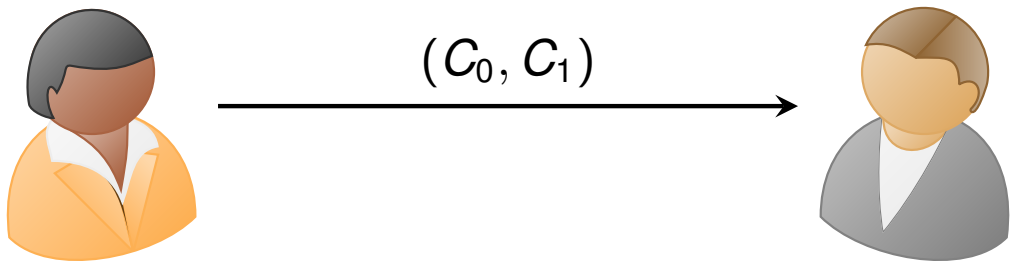
Principe

- Échanger une clé en utilisant la cryptographie asymétrique Utiliser ensuite un chiffrement symétrique, pour le chiffrement du message

Avantages des deux systèmes

- Gestion des clés plus aisée
- Rapidité des calculs

Schéma hybride



Alice (Générer aléatoirement K_s)

Bob (Secret b)

$C_0 = E_{RSA}(p_{Bob}], K_s$

$K_s = E^{-1}_{RSA}(s_{Bob}, C_0)$

$C_1 = E_{AES}(K_s, M)$

$M = E^{-1}_{AES}(K_s, C1)$

Taille des clé cryptographie

Grandes différences

Ne pas confondre les tailles de clés en cryptographie symétrique et asymétrique

Symétrique

- Recherche exhaustive
- Taille des clés (AES 256 bits)

Asymétrique

- Résolution d'un problème mathématique
- Taille des clés (RSA 3072 bits)

Cryptographie symétrique et asymétrique

Avantages/Inconvénients

Cryptographie symétrique

- Avantage : Très rapide
- Inconvénient : Gestion des clés

Cryptographie Asymétrique

- Avantage : Gestion des clés
- Inconvénient : Algorithmes relativement lents

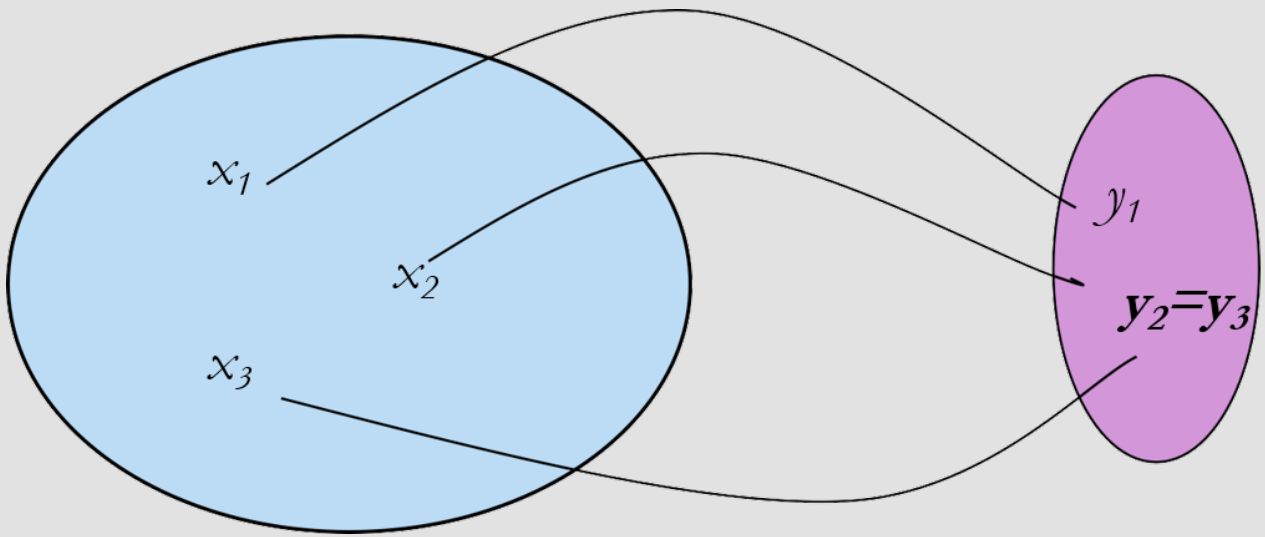
Comment tirer parti des avantages de chacun

Fonctions de hachage (hash or digest)

Définition

Les fonctions de hachage produisent une empreinte du message (haché du message) de petite taille (fixe) à partir d'un message trouver arbitrairement grand

Exemple : SHA-256 (sortie - 256 bits)



Note : Collisions inévitables ! !

Sécurité des fonctions de hachage (1/2)

Résistance aux collisions :

Il est difficile de trouver x et x' tel que $H(x) = H(x')$

Résistance à un deuxième antécédent :

Connaissant $H(x)$ et x, trouver x' différent de x tel que $H(x) = H(x')$

Paradoxe des anniversaires

Si D est la taille de l'ensemble d'arrivée, on trouve des collisions avec une probabilité $pr > \frac{1}{2}$ **en essayant** $\sqrt{D}$ **valeurs aléatoires**

Exemples : SHA2 (SHA-224, SHA-256, SHA-384, SHA-512), SHA-3

Signature électronique

Fonctionnement

- La clé privée sert à produire une signature

  Il ne faut pas que cette signature révèle la clé !
- La clé publique sert vérifier une signature

  Il ne faut pas que l'on soit capable de signer à partir de la clé publique d'Alice

Vérification de la Sécurité d'un système

Comment vérifier la sécurité du système ?

- déterminer ce à quoi l'attaquant a accès (passif, actif),
- proposer une preuve de sécurité,
- proposer une attaque du schéma.

Vérification de la Sécurité d'un système

Comment vérifier la sécurité du système ?

- déterminer ce à quoi l'attaquant a accès (passif, actif),
- proposer une preuve de sécurité,
- proposer une attaque du schéma.

Niveau de sécurité pour la cryptographie

2^{100} : opérations est aujourd'hui un niveau fort de sécurité

Vérification de la Sécurité d'un système

Comment vérifier la sécurité du système ?

- déterminer ce à quoi l'attaquant a accès (passif, actif),
- proposer une preuve de sécurité,
- proposer une attaque du schéma.

Niveau de sécurité pour la cryptographie

2^{100} : opérations est aujourd'hui un niveau fort de sécurité

Impose des recommandations sur :

- taille des clés,
- taille des paramètres des algorithmes,
- taille des entrées/sorties.

Vérification de la Sécurité d'un système

Comment vérifier la sécurité du système ?

- déterminer ce à quoi l'attaquant a accès (passif, actif),
- proposer une preuve de sécurité,
- proposer une attaque du schéma.

Niveau de sécurité pour la cryptographie

2^{100} : opérations est aujourd'hui un niveau fort de sécurité

Impose des recommandations sur :

- taille des clés,
- taille des paramètres des algorithmes,
- taille des entrées/sorties.

Permet de déterminer la faiblesse en termes de temps de calcul et/ou de complexité d'attaque

Plan

Sécurité Réseaux : *Checksum CRC*

Checksum

Les algorithmes de checksum sont utilisés pour assurer la sûreté de fonctionnement d'une communication, c-à-d. assurer qu'il n'a pas eu d'erreurs dans la transmission de l'information.

Sécurité Réseaux : *Checksum CRC*

Checksum

Les algorithmes de checksum sont utilisés pour assurer la sûreté de fonctionnement d'une communication, c-à-d. assurer qu'il n'a pas eu d'erreurs dans la transmission de l'information.

Fonctions CRC (contrôle de redondance cyclique) :

1. Crée un polynôme suivant une représentation big-Ending du message à transmettre. Par exemple : $M = 01001$ et $M(x) = 0 * x^4 + 1 * x^3 + 0 * x^2 + 0 * x^1 + 1 * x^0$.
2. Polynôme prédéterminé (connu pour l'émetteur et le récepteur) ; *polynôme générateur G(x)*. Par exemple : $G(x) = x^3 + 1$.
3. L'émetteur exécute un algorithme en utilisant les 2 polynômes, et transmet le résultat concaténé avec le message au récepteur.
4. Le récepteur vérifie s'il a eu des erreurs de transmission.

Sécurité Réseaux : *HMAC*

Un hachage est une fonction **à sens unique**.

- Elle prend un message d'entrée et produit une sortie
- Il n'est pas possible de déterminer quelle entrée correspond à une sortie donnée

Les propriétés du HMAC sont (elles qu'il est sécurisé) :

- Résistance à la collision (impossible de trouver deux entrées qui donnent la même sortie)
- Un attaquant qui ne connaît pas la clé K ne peut pas calculer la fonction $hash(K, x_0)$ correct pour les données x_0.

$$HMAC(k, m) = H\Big(\underbrace{\big(K \oplus opad\big)}_{\text{Inner clé}} \| H\big(\underbrace{(K \oplus ipad)}_{\text{Outer clé}} \| m\big) \Big)$$

Sécurité Réseaux : *WEP, WAP, WAP2, WPA3*

(WEP) Wired Equivalent Privacy :

utilisé dans tous équipement qui utilisent les protocoles 802.11a/b/g (medium access control *MAC* sublayer and physical layer)

Comment fonctionne le chiffrement WEP

1. **Séquence pseudo-aléatoire** utilisation de l'algoritme RC4 avec la clé symétrique et une vecteur d'initialisation,
2. **Données chiffrées :** Séquence aléatoire **RC4** $\oplus$ séquence de données en clair,
3. **Champ de contrôle d'intégrité (CRC)** calculé sur les données en clair.

Clés de 64-bit et 128-bit (256 bits possible mais très rare).

WEP a été officiellement abandonné par la Wi-Fi Alliance en 2004

Sécurité Réseaux : *WEP, WAP, WAP2, WPA3*

Wi-Fi Protected Access (WPA)

WAP est un système de chiffrement que la Wi-Fi Alliance a adopté officiellement en 2003 (pour remplacer le protocole WEP).

- La configuration WPA la plus courante est **WPA-PSK (clé pré-partagée)**.
- Les clés utilisées par WPA sont 256 bits.

Variantes selon les objectifs d'utilisation et les besoins de sécurité

1. **WPA-Personal :** il utilise un système de clés PSK ou pré-partagées
2. **RADIUS :** Centré sur les entreprises,
   - ce système de sécurité repose sur un serveur
   - les utilisateurs doivent s'authentifier auprès d'un utilisateur et d'un mot de passe différent pour chacun

WAP a été officiellement abandonné par la Wi-Fi Alliance en 2006

Sécurité Réseaux : *WEP, WAP, WAP2, WPA3*

Wi-Fi Protected Access II (WPA2)

WPA2 a deplacé officiellement WPA en 2006.
Changements les plus significatifs :

- l'utilisation obligatoire des algorithmes AES
- l'introduction du CCMP en remplacement de TKIP.

TKIP est toujours conservé dans WPA2 en tant que système de secours et pour son interopérabilité avec WPA.

Type de chiffrement dans WPA et WPA2

- chiffrement TKIP :
  - système de clé par paquet compatibilité avec des appareils plus anciens
  - plusieurs vulnérabilités ont été détectées dans ce chiffrement
- chiffrement AES + CCMP :
  - amélioration de la sécurité,
  - vitesses plus élevées que TKIP.

Sécurité Réseaux : *WEP, WAP, WAP2, WPA3*

Liste basique des méthodes de sécurité Wi-Fi disponibles sur les routeurs postérieur à 2006, du meilleur au pire :

1. WPA2 + AES
2. WPA + AES
3. WPA + TKIP / AES (TKIP est là comme méthode de secours)
4. WPA + TKIP
5. WEP
6. Réseau ouvert (pas de sécurité du tout)

Toutes les méthodes ont une version personnel et une autre entreprise.

Sécurité Réseaux : *WEP, WAP, WAP2, WPA3*

Wi-Fi Protected Access III (WPA3)

Peut-être l'année prochain

1. S'appuie sur le succès généralisé et l'adoption du *Wi-Fi WPA2*
2. Simplification de la sécurité Wi-Fi
3. Authentification plus robuste
4. Renforcement de la capacité cryptographique (données sensibles)
5. Préservation la résilience des réseaux stratégiques.

Variantes selon les objectifs d'utilisation et les besoins de sécurité

1. **WPA3 personnel :** bénéficiera d'une protection renforcé contre les tentatives de recherche de mots de passe.
2. **WPA3 entreprise :** bénéficiera des protocoles de sécurité a très haut niveau pour proteger les données sensibles.

Plus d'information sur : `https://www.wi-fi.org/discover-wi-fi/security`

Sécurité Réseaux : *IPsec*

IPsec

IPsec est un IETF (Internet Engineering Task Force) standard pour la communication sécurisé en temps réel (*real-time communication security*). Ce standard travaille sur la couche IP (couche 3 du modelé OSI).

Les principaux composants d'IPsec sont :

- L' en-têtes **AH** : fournit uniquement une protection d'intégrité
- L' en-têtes **ESP** : fournit un chiffrement et/ou une protection de l'intégrité
- Protocole **IKE** : gère l'authentification et établisse une clé de section.

Sécurité Réseaux : *Kerberos*

Kerberos

Protocole de sécurité basé sur la cryptographie symétrique, développé par le MIT pour l'authentification des utilisateurs sur un réseau (le niveau de protection : authentification, intégrité et privacité).

Serveur Kerberos **KDC (Kerberos Distribution Center)** :

1. **L'authentification (AS, service d'authentification) :** authentifier les clients et leur fournir un ticket.
2. **Le service de ticket (TGS, service d'octroi de ticket) :** fournira les informations nécessaires pour communiquer avec un serveur.

L'architecture Kerberos repose sur trois objets de sécurité :

- **la clé de session**
- **le ticket**
- **l'authentificateur**

Sécurité Réseaux : *Secure Sockets Layer (SSL)*

Secure Sockets Layer (SSL) SSL est une norme de chiffrement pour la plupart des transactions Web. En fait, il est en train de devenir le type de chiffrement le plus populaire pour le commerce électronique. La plupart des applications intranet et extranet conventionnelles nécessiteraient généralement une combinaison de mécanismes de sécurité, notamment :

- Encryption
- Authentication
- Access control

SSL fournit des communications sécurisées client / serveur Web :

- chiffrement, Authentification et Vérification de l'intégrité sur la couche transport (TCP,UDP).

Développé par Netscape Communications : SSLv2, SSLv3

Sécurité Réseaux : *Transport Layer Security (TLS)*

Comment fonctionne le protocole TLS ?

TLS utilise une combinaison de cryptographie symétrique et asymétrique (bon compromis entre performance et sécurité).

Il utilise deux protocoles différentes :

a) **TLS Record Protocol :** l'authentification est effectuée de sorte que la transmission des données s'effectue via une connexion privée et fiable.

b) **TLS Handshake Protocol :** le message est négocié en toute sécurité. Chaque message est chiffré et conditionné avec un code d'authentification (ou MAC).

Sécurité Réseaux : *HTTPS*

Protocole HTTP

Protocole de communication utilisé par le World Wide Web. Ce protocole définit le format et la transmission des messages, ainsi que les actions que les serveurs et navigateurs Web doivent entreprendre en réponse à diverses commandes.

Protocole HTTPS

HTTPS (protocole de transfert hypertexte sécurisé ou protocole de transfert de données), est la version sécurisé du protocole HTTP. Ajoute le protocole TLS ou SSL pour :

- assurer la sécurité des données échanges entre le serveur et le client
- garantir l'identité du site web consulté

Gestion des clefs : Qu'est-ce qu'une PKI ?

PKI (Public Key Infrastructure) est un système de gestion des clefs publiques qui permet de gérer des listes importantes de clefs publiques et d'en assurer la fiabilité, pour des entités généralement dans un réseau.

On distingue 5 entités dans la PKI dont [6]

- **L'autorité de certification (AC)**
- **L'autorité d'enregistrement (AE)**
- **L'autorité de dépôt (Repository)**
- **L'entité finale (End Entity)**
- **L'autorité de séquestre (Key Escrow)**

Certificat électronique

Un certificat électronique est un fichier contenant des informations spécifiques telles que des données d'identification, un numéro de série, ainsi qu'une date d'expiration. Ce fichier inclut également la signature électronique de l'autorité de certification qui a généré le certificat, garantie de la validité de celui-ci, ainsi que la clé publique du détenteur du certificat. [Martin Furuhed]

Exemples de utilisation :

- signer une facture ou un bon de commande,
- signer des contrats de toute nature,
- répondre à des appels d'offres,
- signer des documents officiels (déclarations fiscales et sociales, par exemple),
- sécuriser l'accès à votre boîte mail ou un des sites internet.

Certificat électronique

Un certificat électronique est un fichier contenant des informations spécifiques telles que des données d'identification, un numéro de série, ainsi qu'une date d'expiration. Ce fichier inclut également la signature électronique de l'autorité de certification qui a généré le certificat, garantie de la validité de celui-ci, ainsi que la clé publique du détenteur du certificat. [Martin Furuhed]

Un certificat électronique es comme la carte d'identité :

- **infalsifiable :** il est chiffré pour empêcher toute modification,
- **nominatif :** il est délivré à une entité (comme la carte d'identité),
- **certifié :** il y a le "tampon" de l'autorité qui l'a délivré.

Plan

ystèmes et infrastructures critique (Sécurité)

Système ou infrastructure critique

Étymologiquement, le mot infrastructure vient du latin *infra-* structura de *struere* construire et signifie **au dessous de la construction** et le mot critique du grec *kritikos* de *krinein* discerner signifie **difficile, décisif**. Ainsi les infrastructures critiques sont les constructions décisives pour notre société [7].

On peut définir simplement les **infrastructures critiques** comme l'ensemble des systèmes essentiels.

1. Les réseaux électrique
2. Les réseaux télécommunication
3. Les réseaux d'eau
4. Les réseaux de gaz
5. Les réseaux d'égouts
6. Les réseaux de transports (ferrés, routiers, aériens ou fluviaux)
7. Les service d'urgences et médicaux

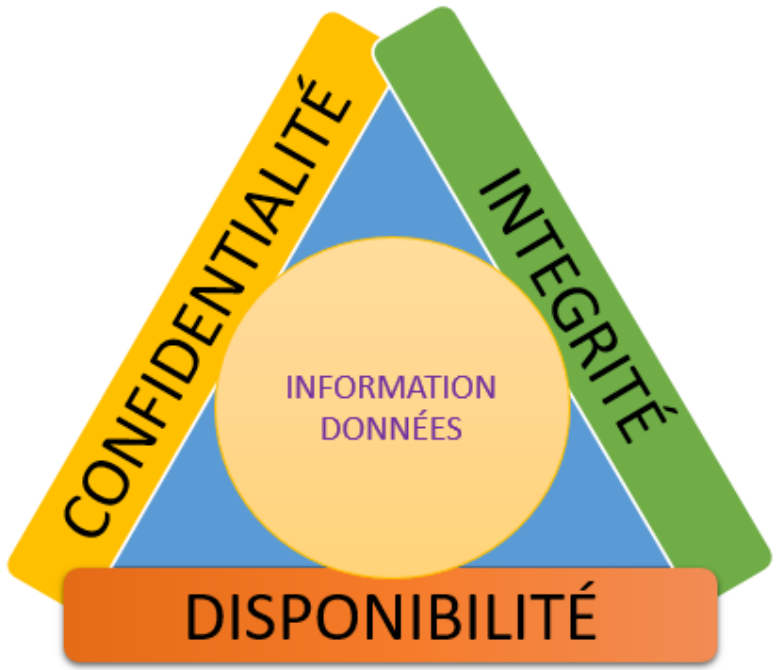
Propriétés de sécurité d'un système critique

Priorité dans les TICs et les systèmes embarqués non-critiques :

1. Confidentialité / privacité
2. Intégrité
3. Disponibilité

Priorité dans les systèmes embarqués critiques :

1. Disponibilité
2. Intégrité
3. Confidentialité / privacité



Résilience et systèmes critique

Résilience

La résilience d'un système réside dans sa capacité à continuer à bien fonctionner même s'il existe des conditions défavorables ou que des entités externes souhaitent perturber son fonctionnement.

La résilience de ces systèmes il faut la prévoir depuis la conception du système :

1. Il faut tenir en compte certains paramètres pour créer un système robust depuis un point de vue de la sûreté.
2. il faut aussi tenir en compte les vulnerabilités cyber et physiques.

Cela permet obtenir un systéme robust depuis un point de vue sûreté et sécurité. Cette robustesse donne une degrée de résilience au système conçu.

Bibliographie

[1] T. PERTUS, *Positionnement de la Cybersécurité entre Sécurité et Sûreté « faux-amis » ou vraies synergies ?*, Mars 2016 (dernier accès 08/07/2019).

[2] (CSCG) and ENISA, “Definition of Cybersecurity Gaps and overlaps in standardisation,” 2015.

[3] Y. Jin, “Introduction to hardware security,” *Electronics*, vol. 4, no. 4, pp. 763–784, 2015.

[4] S. Jones, C. Tremlet, and M. Jackson, “The fundamentals of secure boot and secure download : How to protect firmware and data within embedded devices.” https ://www.maximintegrated.com/en/app-notes/index.mvp/id/6426.

[5] M. Mushtaq, S. Jamel, A. Disina, Z. Pindar, N. Shakir, and M. Mat Deris, “A survey on the cryptographic encryption algorithms,” *International Journal of Advanced Computer Science and Applications*, vol. 8, pp. 333–343, 11 2017.

[6] H. Toutchkov. https ://www.oodrive.es/blog/security/que-es-una-pki-o-infraestructura-de-clave-publica/.

[7] B. Rozel, “La sécurisation des infrastructures critiques : recherche d’une méthodologie d’identification des vulnérabilités et modélisation des interdépendances,” *Thèse, Institut National Polytechnique de Grenoble - INPG*, July 2009.