Université IBN TOFAIL – Kénitra
ECOLE NATIONALE DES SCIENCES APPLIQUEES

Cours Sécurité des Systèmes Embarqués et IoT

CH1: Introduction et Généralités

Par:

Hassan EL FADIL

elfadil.h@gmail.com

1. Définition et Enjeux de la Sécurité dans les Systèmes IoT

1.1. Définition:

- La sécurité des systèmes IoT et embarqués vise à protéger ces systèmes contre les attaques, la compromission des données, et les dysfonctionnements dus à des accès non autorisés ou malveillants.
- Les systèmes IoT (Internet of Things) connectent des dispositifs intelligents via des réseaux, tandis que les systèmes embarqués incluent des composants matériels et logiciels intégrés pour effectuer des tâches spécifiques

1.2. Enjeux:

- **Protection des données sensibles** : Les systèmes IoT collectent et transmettent souvent des données personnelles ou critiques.
- **Continuité de service** : Les systèmes embarqués sont souvent utilisés dans des infrastructures critiques (santé, énergie, transports), où les interruptions peuvent être catastrophiques.
- **Respect des réglementations** : Les normes (ex. **RGPD** en Europe) imposent des mesures de sécurité pour protéger les utilisateurs.
- **Augmentation des surfaces d'attaque** : Avec la connectivité accrue, les systèmes IoT sont plus vulnérables aux cyberattaques.

RGPD : Règlement Général sur la Protection des Données

2. Différences entre Sécurité des Systèmes Classiques et des Systèmes Embarqués

Sécurité classique : Ordinateurs et serveurs peuvent utiliser des solutions lourdes comme des antivirus et des pare-feux complexes

Sécurité embarquée : Nécessite des algorithmes légers adaptés aux contraintes matérielles (ex. cryptographie légère).

Contraintes des systèmes embarqués :

- **Ressources limitées** : Contrairement aux systèmes classiques, les systèmes embarqués disposent souvent de peu de puissance de calcul, de mémoire, et d'énergie, ce qui complique l'implémentation de mesures de sécurité avancées.
- **Durée de vie étendue** : Les dispositifs IoT et embarqués sont souvent déployés pour des années, nécessitant des mises à jour de sécurité sur le long terme.
- **Connectivité étendue** : Les dispositifs IoT sont souvent exposés à des réseaux publics, augmentant leur vulnérabilité par rapport aux systèmes classiques souvent cloisonnés.

3. Concepts de Base de la Sécurité

Ces concepts fondamentaux sont souvent désignés par l'acronyme **CIAAN** (Confidentiality, Integrity, Availability, Authentication, Non-repudiation).

Confidentialité (Confidentiality) :
- Assurer que seules les entités autorisées peuvent accéder aux données sensibles.
- Méthodes : Cryptographie (AES, RSA), protocoles sécurisés (TLS).

Intégrité (Integrity) :
- Garantir que les données ne sont ni altérées ni modifiées pendant leur stockage ou transmission.
- Méthodes : Hashage (SHA-256), signatures numériques.

Disponibilité (Availability) :
- Assurer que les systèmes sont accessibles et fonctionnels à tout moment, même en cas d'attaque.
- Méthodes : Tolérance aux pannes, protection contre les attaques DDoS.

Authentification (Authentication) :
- Vérifier l'identité des utilisateurs ou des dispositifs accédant au système.
- Méthodes : Mots de passe, biométrie, certificats numériques.

Non-répudiation (Non-repudiation) :
- Empêcher une entité d'annuler ou de nier une action effectuée (ex. un envoi de données).
- Méthodes : Journaux d'audit sécurisés, signatures numériques.

4. Menaces et Vulnérabilités dans les Systèmes IoT et Embarqués

Les systèmes IoT et embarqués sont confrontés à des défis de sécurité importants en raison de leurs spécificités : connectivité étendue, ressources limitées, et déploiement dans des environnements variés

4.1. Analyse des menaces:

1. Attaques physiques:

- *Les attaques physiques ciblent directement les dispositifs IoT ou embarqués via un accès physique.).*
- **Exemples courants :**
  - **Injection de fautes :** Modification intentionnelle des paramètres d'un dispositif (ex. tension ou température) pour provoquer un comportement anormal.
  - **Extraction des clés :** Utilisation d'attaques par analyse de canaux auxiliaires (Side Channel Attacks) comme l'analyse de puissance ou d'émissions électromagnétiques.
  - **Sabotage matériel :** Remplacement ou destruction de composants physiques.
- **Mesures d'atténuation :** Boîtiers sécurisés, chiffrement des données sensibles, détection de manipulation.

2. Attaques logiques:

- Exploitation des failles logicielles dans le code ou les protocoles.

- **Exemples courants :**
  - **Injection de code :** Exploitation de failles comme les débordements de tampon (Buffer Overflow).
  - **Exploitation des failles d'authentification :** Attaques par force brute ou contournement des mécanismes d'authentification.
  - **Malwares embarqués :** Infections par des logiciels malveillants.

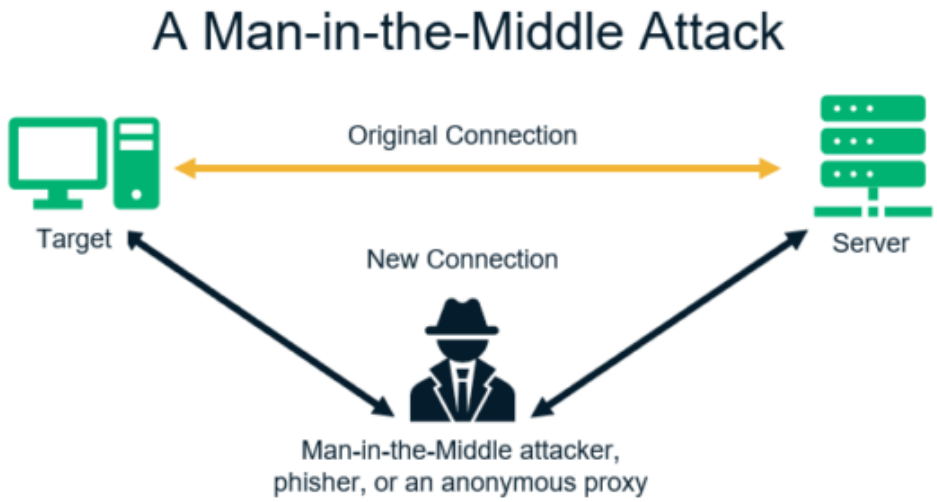
- **Mesures d'atténuation :** Validation des entrées, tests de pénétration, mise en place de mécanismes de détection d'intrusion.

3. Attaques réseau:

- Menaces ciblant les communications réseau entre dispositifs IoT.

- **Exemples courants :**
  - **Interception des communications :** Attaques de type Man-in-the-Middle (MITM).
  - **Déni de service (DoS/DDoS) :** Saturation des ressources réseau pour les rendre inaccessibles.
  - **Exploitation de protocoles faibles :** Failles dans des protocoles comme MQTT ou CoAP.

- **Mesures d'atténuation :** Chiffrement des communications (TLS/DTLS), segmentation réseau, détection et prévention des intrusions (IDS/IPS).



- Interception
- Écoute et modification
- Vol de données sensible
- Diffusion de logiciels malveillants, …

IDS : Intrusion Detection System
IPS :Intrusion Prevention System

3. Attaques réseau:

- Le groupe de cyberpirates marocain appelé Moroccan Soldiers a affirmé avoir ciblé, le dimanche 16 Février 2025, plusieurs sites Internet institutionnels en Tunisie par des attaques de type déni de service (**DDoS:** Distributed Denial of Service).
- Sans viser à voler des données personnelles, les attaques **DDoS** permettent à leurs auteurs de saturer les sites Internet ciblés pour les rendre inaccessibles.
- Précédemment, des hackers marocains ont mis hors service plusieurs sites institutionnels de pays ou encore des plateformes du Polisario.

🚨 DDoS Alert 🚨

Moroccan Soldiers claims to have targeted multiple websites in Tunisia.

- ISIE
- Ministry of Agriculture
- Ministry of Communication Technologies
- Ministry of Social Affairs-Tunisia
- Ministry of Health-Tunisia
- Ministry of Higher Education and Scientific... Voir plus

Source: Yabiladi 17/02/2025

DDoS vise perturber le trafic normal d'un serveur, service ou réseau en le submergeant d'un flot massif de trafic Internet

4.2. Résumé des principales menaces:

Phishing
Email frauduleux: L'attaquant se fait passer pour une entité de confiance (banque, administration,..)

Keylogger
Type de logiciel ou de matériel malveillant conçu pour enregistrer en secret les frappes effectuées sur un clavier.

Stealer
Type de malware conçu pour voler des informations sensibles d'un système infecté

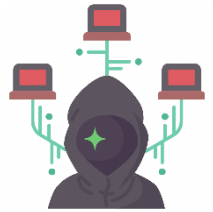
Malware
(malicious software):
Tout programme ou code conçu pour endommager, perturber ou voler des données sur un système informatique

Backdoor
(**porte dérobée**) est un accès caché dans un système informatique, un logiciel ou un réseau qui permet à un attaquant de contourner les mécanismes de sécurité et d'accéder discrètement à l'appareil infecté.

Ransom
Un ransomware (rançongiciel) est un type de malware qui chiffre les fichiers d'un système et demande une rançon en échange de la clé de déchiffrement.

RAT apps
RAT (Remote Access Trojan) est un type de malware qui permet à un attaquant de prendre le contrôle total d'un appareil à distance sans le consentement de l'utilisateur

DDoS
(Distributed Denial of Service) est une attaque informatique visant à surcharger un serveur, un site web ou un réseau en envoyant un énorme volume de requêtes



Botnet
Un botnet est un réseau d'ordinateurs infectés (appelés bots ou zombies) contrôlés à distance par un cybercriminel (botmaster)

4.3. Principales vulnérabilités des systèmes IoT:

1. Mots de passe faibles:

- **Description :** Les mots de passe par défaut ou faibles sont facilement devinés ou accessibles publiquement.
- **Impact :**
  - Prise de contrôle des dispositifs.
  - Utilisation des dispositifs dans des botnets (ex. Mirai).
- **Bonnes pratiques :**
  - Forcer le changement des mots de passe par défaut.
  - Imposer des politiques de mots de passe robustes.
  - Implémenter une authentification multi-facteurs (MFA).

2. Absence de mise à jour

- **Description :** Les dispositifs IoT ne reçoivent souvent pas de mises à jour logicielles, laissant des failles exploitées par les attaquants.
- **Impact :**
  - Exploitation de vulnérabilités connues.
  - Risques croissants au fil du temps.
- **Bonnes pratiques :**
  - Intégration d'un mécanisme de mise à jour OTA (Over-The-Air).
  - Notification aux utilisateurs des mises à jour disponibles.
  - Conception d’un plan de maintenance à long terme.

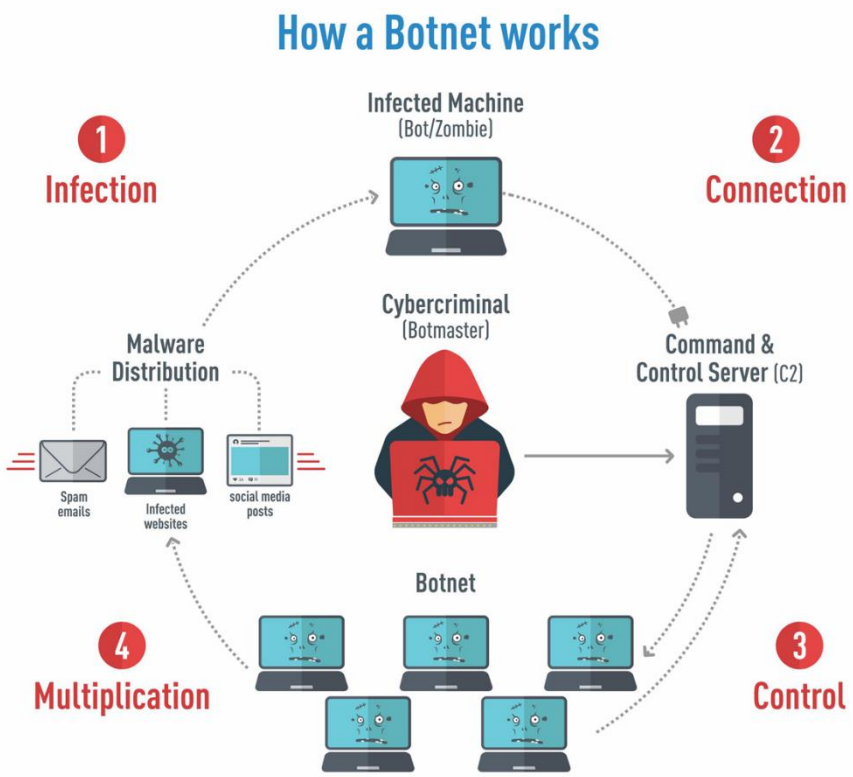
3. Exposition des interfaces:

- **Description :** Les interfaces accessibles (ex. API, ports, Wi-Fi non protégé) peuvent être exploitées par des attaquants.
- **Impact :**
  - Accès non autorisé aux fonctions critiques.
  - Possibilité d'injection de commandes malveillantes.
- **Bonnes pratiques :**
  - Réduction de la surface d'attaque (désactivation des interfaces inutilisées).
  - Authentification stricte pour l'accès aux interfaces.
  - Mise en place de pare-feu applicatifs et de surveillance réseau.

4.4. Études de cas d'attaques réelles sur des dispositifs IoT

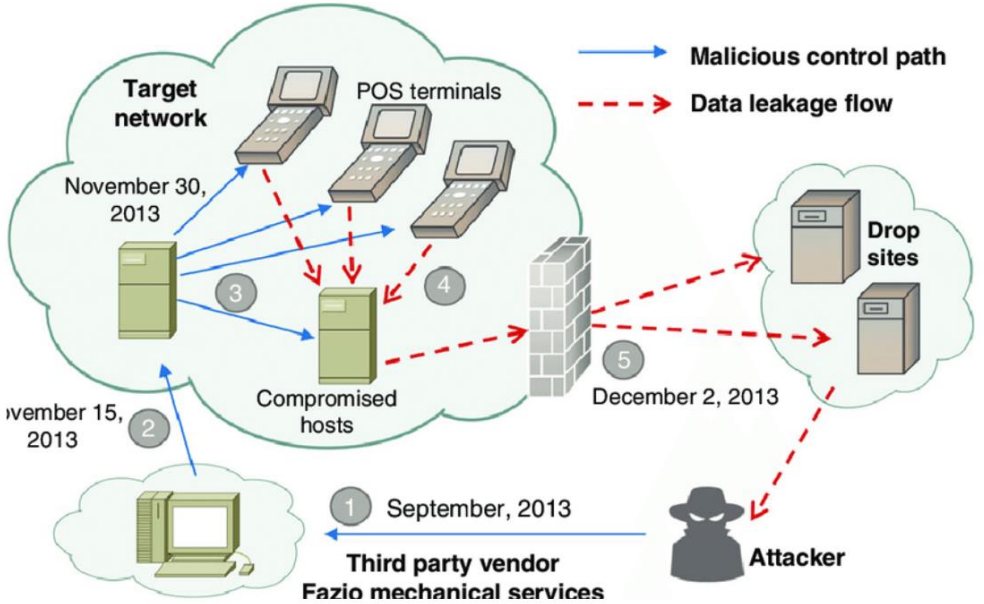
Botnet Mirai:

- **Description :** Botnet constitué d'appareils IoT infectés, utilisé pour lancer des attaques DDoS massives.
- **Vulnérabilités exploitées :**
  - Mots de passe par défaut non changés.
- **Impact :**
  - Paralysie de services majeurs (ex. Les serveurs DNS de l'entreprise **Dyn**, un fournisseur de services DNS majeur en 2016).
- **Leçons apprises :**
  - Importance de changer les mots de passe par défaut.
  - Nécessité de surveiller les comportements anormaux.



Violation des données de cartes de crédit de Target:

- En 2013, des pirates informatiques ont réussi à pénétrer le réseau de Target et ont volé des informations de cartes de crédit issues de millions de transactions.
- Comment ont-ils procédé ? Ils ont volé les identifiants de connexion d'un fournisseur de systèmes de chauffage, ventilation et climatisation (CVC), qui utilisait des capteurs IoT pour aider Target à surveiller sa consommation d'énergie et à rendre ses systèmes plus efficaces.



Piratage d'une voiture connectée:

- **Description :** Prise de contrôle à distance des fonctions critiques d'un véhicule (accélérateur, freins, etc.).
- **Vulnérabilités exploitées :**
  - Failles dans les systèmes de communication interne du véhicule.
- **Impact :**
  - Risque pour la sécurité des passagers.
- **Leçons apprises :**
  - Isolation des systèmes critiques.
  - Tests de sécurité sur tous les protocoles de communication.

Exemple emblématique de piratage de voitures connectées qui s'est produit en **juillet 2015**, lorsque des chercheurs en cybersécurité ont démontré la vulnérabilité d'un véhicule **Jeep Cherokee** à une attaque à distance

Les stimulateurs cardiaques de St. Jude Medical

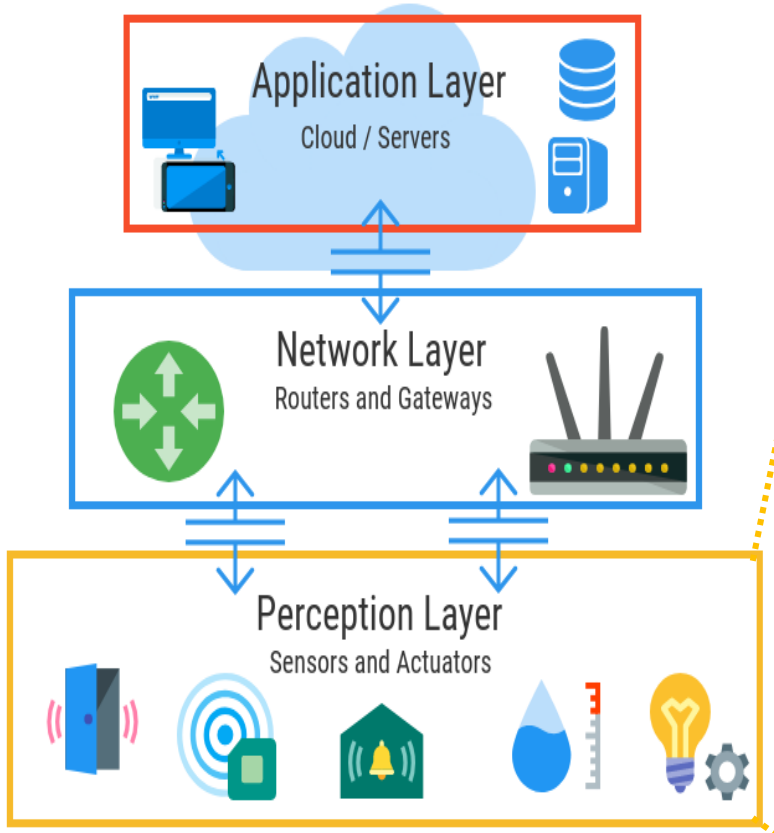
- En 2017, la FDA (Food and Drug Administration) a annoncé que plus de 465 000 stimulateurs cardiaques implantables étaient vulnérables au piratage.
- En prenant le contrôle de l'un de ces dispositifs, un pirate informatique pourrait littéralement tuer quelqu'un en épuisant la batterie, en modifiant le rythme cardiaque ou en administrant des chocs.
- Une faille de sécurité liée à l'IoT a transformé un dispositif conçu pour sauver des vies en une arme potentiellement mortelle.

Attaque sur les caméras de surveillance:

- **Description :** Piratage de caméras de surveillance pour espionner les utilisateurs ou lancer des attaques.
- **Vulnérabilités exploitées :**
  - Interfaces non sécurisées exposées à Internet.
- **Impact :**
  - Atteinte à la vie privée.
  - Compromission des infrastructures de sécurité.
- **Leçons apprises :**
  - Limiter l'accès aux dispositifs via des VPN ou des pare-feu.
  - Mise à jour régulière des firmwares.

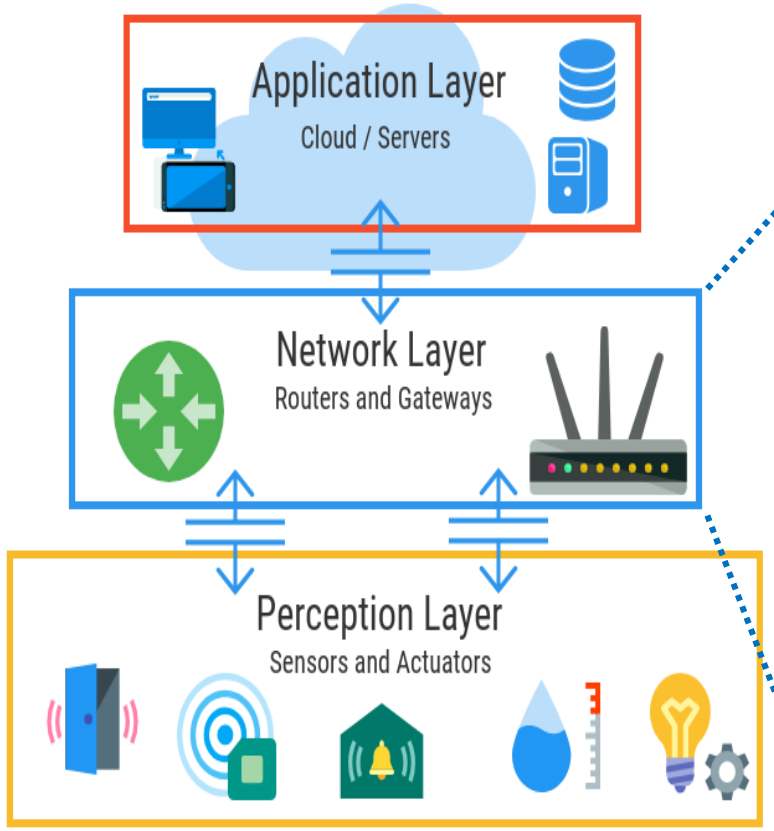
A eu lieu en **novembre 2021**, avec le piratage de l'entreprise **Verkada**, spécialisée dans les systèmes de vidéosurveillance connectés

5. Principales Solutions de Sécurité pour l'Architecture IoT



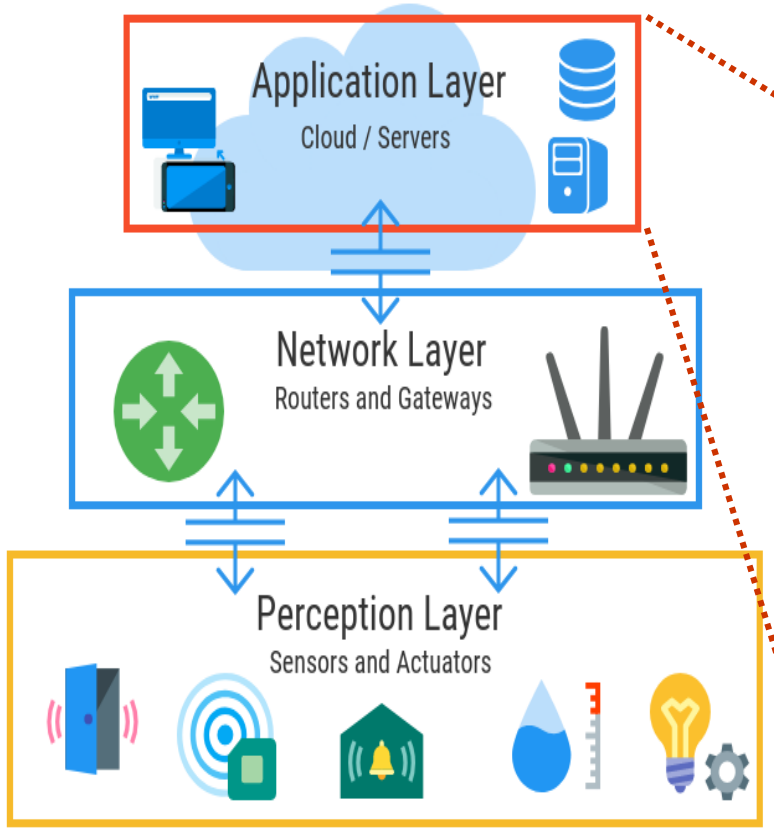
Couche de perception (Capteurs et dispositifs embarqués)

- **Chiffrement des données** : Protéger les données collectées avant leur transmission (ex. : AES, RSA).
- **Authentification et contrôle d'accès** : Utiliser des mécanismes d'authentification solides et des contrôles d'accès pour sécuriser les dispositifs.
- **Sécurisation physique** : Restreindre l'accès physique pour éviter toute manipulation des dispositifs IoT.
- **Sécurisation des interfaces sans fil** : Utiliser des protocoles sécurisés (HTTPS, TLS) pour éviter les attaques sur les interfaces non sécurisées.
- **Détection d'intrusion** : Déployer des capteurs ou systèmes de détection pour repérer toute tentative de manipulation physique ou logique.



Couche de réseau (Passerelles et réseaux)

- **Chiffrement de bout en bout** : Assurer la confidentialité et l'intégrité des données en transit (ex. : TLS/SSL).
- **Vérification des certificats** : Utiliser des certificats numériques pour authentifier les dispositifs et les passerelles.
- **Isolation des réseaux** : Séparer les réseaux internes des réseaux externes pour limiter les risques d'attaques.
- **Firewall et IDS** : Mettre en place des firewalls et des systèmes de détection d'intrusion pour surveiller et protéger le réseau.
- **VPN et tunneling sécurisé** : Sécuriser les canaux de communication via des VPN ou des mécanismes de tunneling.
- **Protocoles sécurisés** : Utiliser des protocoles de communication sécurisés comme MQTT avec TLS ou CoAP avec DTLS.



Couche d'application (Serveurs cloud et interfaces utilisateur)

- **Authentification forte (MFA)** : Imposer une authentification multifacteur pour les utilisateurs et les services cloud.
- **Sécurisation des API** : Utiliser des clés API, OAuth, et d'autres méthodes pour sécuriser les interfaces de programmation.
- **Protection contre les DDoS** : Mettre en place des mécanismes pour protéger contre les attaques par déni de service (ex. : CDN, Cloudflare).
- **Chiffrement des données au repos** : Chiffrer les données sensibles stockées dans le cloud pour éviter toute fuite d'informations.
- **Contrôle d'accès basé sur les rôles (RBAC)** : Limiter les permissions des utilisateurs pour éviter l'accès non autorisé à des informations sensibles.
- **Audits et mises à jour** : Effectuer des audits de sécurité réguliers et appliquer rapidement les mises à jour pour corriger les vulnérabilités.

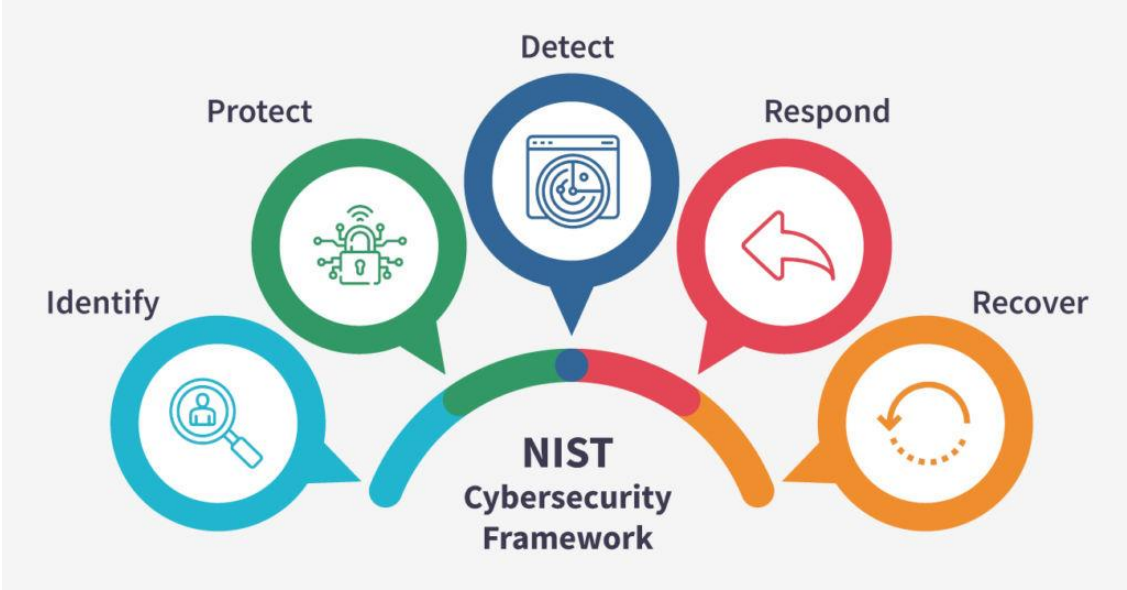
6. Normes et Réglementations

6.1. Normes de sécurité pour l'IoT

- **ETSI EN 303 645:** Cette norme, émise par l'ETSI (European Telecommunications Standards Institute), est l'une des normes les plus reconnues pour les dispositifs IoT.

- **NIST IoT Cybersecurity Standards (NIST SP 800-53, NIST SP 800-82):** Le NIST (National Institute of Standards and Technology) est un organisme américain qui publie des normes et des directives en matière de cybersécurité.

- Le NIST SP 800-53 et NIST SP 800-82 sont des documents clés pour la sécurité des systèmes IoT

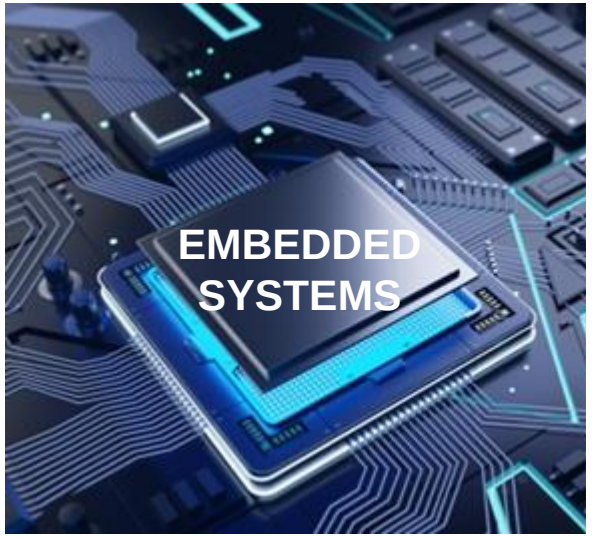


6.2. Réglementations sur la protection des données

- **RGPD (Règlement Général sur la Protection des Données)** : Le RGPD est un règlement de l'Union Européenne qui impose des règles strictes concernant la collecte, le stockage, et le traitement des données personnelles. Bien qu'il s'applique principalement aux entreprises opérant en Europe, il a des implications mondiales pour les entreprises traitant des données de citoyens européens.
- **CCPA (California Consumer Privacy Act)** : Le CCPA est une loi californienne qui protège la vie privée des consommateurs en Californie. Bien qu'il soit spécifique à cet état, il s'applique à toute entreprise traitant des données personnelles de résidents californiens, même si l'entreprise est située ailleurs.

6.3. Exigences sectorielles spécifiques

- **Secteur de la santé**
  - **HIPAA (Health Insurance Portability and Accountability Act)** : Aux États-Unis, la HIPAA réglemente la protection des informations de santé personnelles. Elle impose des règles strictes concernant la confidentialité, l'intégrité et la sécurité des données de santé électroniques.
- **Secteur du transport**
  - **ISO/IEC 27001** : Cette norme internationale est utilisée pour sécuriser les informations sensibles dans les systèmes de gestion de la sécurité de l'information (SMSI). Dans le secteur du transport, cette norme aide à protéger les systèmes embarqués (comme les véhicules autonomes) contre les cyberattaques.
- **Secteur industriel (Industrie 4.0)**
  - **IEC 62443** : Cette norme est spécifiquement conçue pour la sécurité des systèmes de contrôle industriels (ICS). Elle est essentielle dans les environnements IoT industriels où les dispositifs connectés interagissent avec des équipements critiques.



FIN !
Questions ?