Sécurité de la chaîne d'acquisition IoT

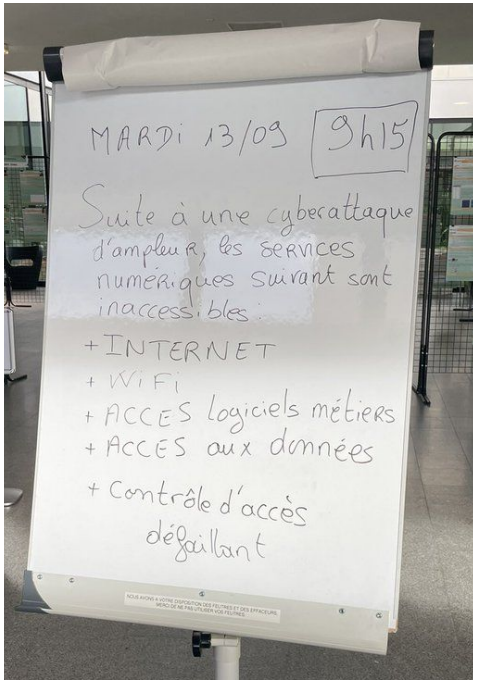
fcamps@laas.fr

Sécurité de la chaîne d'acquisition IoT

Agenda

Sécurité du transport de données
Notions de base
Sécurité au niveau du cloud
Synthèse
Les attaques
Outils de piratage et éthique
Auditer son système

Introduction



https://www.ladepeche.fr/2022/09/13/linstitut-polytechnique-de-toulouse-victime-dune-cyberattaque-dampleur-10541469.php
https://www.ladepeche.fr/2022/03/17/toulouse-lecole-nationale-de-laviation-civile-victime-dune-cyberattaque-10176877.php
https://www.lefigaro.fr/secteur/high-tech/assurance-maladie-les-donnees-de-plus-de-500-000-francais-derobees-20220317

Piratage dans la presse:

- **ENA L'ENAC, l'école nationale de l'aviation civile mars 2022**

- **Assurance maladie 17 mars 2022**

- **"Faute de rançon, les données volées dans un hôpital de l'Essonne se retrouvent mises en ligne" août 2022**

- **INP Toulouse septembre 2022,** "Dans la nuit du 12 au 13 septembre, l'ensemble des établissements de l'institut national polytechnique de Toulouse (INP) a fait l'objet d'une attaque informatique « d'ampleur » bloquant l'accès à un certain nombre de ses données. Une plainte a été déposée."

- **Les hôpitaux** ont comptabilisé 730 déclarations d'incidents en 2022 ! …

Introduction

https://actu.fr/ile-de-france/brunoy_91114/essonne-la-mairie-de-brunoy-victime-d-une-cyberattaque_54902613.html#:~:text=Le%20r%C3%A9seau%20informatique%20de%20la,par%20cet%20acte%20de%20malveillance.
https://www.seine-et-marne.fr/fr/actualites/cyberattaque-au-departement-de-seine-et-marne-le-point-sur-la-situation#:~:text=Conseil%20d%C3%A9partemental%2C%20D%C3%A9partement%20Cyberattaque%20au,le%20point%20sur%20la%20situation&text=Depuis%20le%206%20novembre%2C%20le,coup%C3%A9s%20par%20mesure%20de%20s%C3%A9curit%C3%A9.

Piratage dans la presse:

- **La mairie de Brunoy (Essonne) :** Une demande de rançon de 5 millions de dollars

- **Le conseil départemental de Seine et Marne en novembre**

- **Le conseil régional de Normandie en décembre**

…

Introduction

https://www.cybermalveillance.gouv.fr/ https://www.capital.fr/economie-politique https://www.usine-digitale.fr/

Le hacking en chiffre

- En 2018, les cyberattaques menées par des hackers contre les entreprises ont augmenté de 55%.
- En 2018, 28 855 victimes ont été recensées en 2018,
- En 2019, plus de 90 000 victimes ont été recensées, soit une augmentation de plus de 210% par rapport à 2018,

Introduction

https://www.cybermalveillance.gouv.fr/ https://www.capital.fr/economie-politique https://www.usine-digitale.fr/

Le hacking en chiffre

- 2020: La cybercriminalité coûte 1.000 milliards de dollars par an à l'économie mondiale
- Deux tiers des entreprises interrogées ont subi une cyberattaque en 2020 …
- Une entreprise française sur deux est victime d'une cyberattaque en 2022, selon le baromètre du CESIN (Club des Experts de la Sécurité de l'Information et du Numérique).

Introduction

https://www.novencia.com/

Le hacking en chiffre

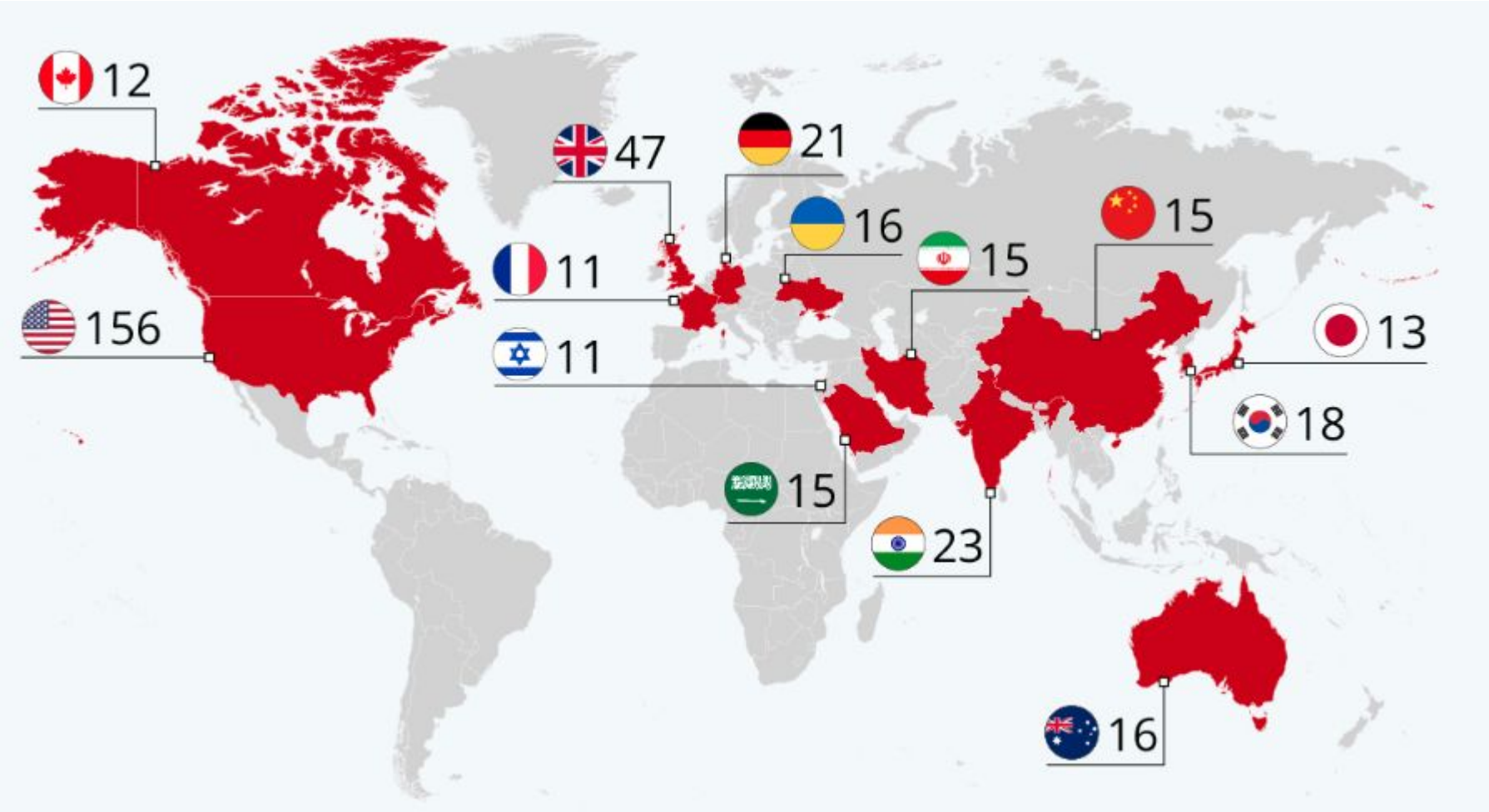
- Entre 30min et 10 jours, c'est le temps moyen pour s'introduire dans un réseau d'entreprise. **La réussite est au rendez-vous dans 93% des cas**.
- Pour une entreprise, pas moins de 13 vecteurs de pénétration (réseau, mail, web, réseaux sociaux …) ont été recensés.
- Interpol a recensé 907 000 spams, 737 incidents liés à un malware et 48 000 URL malveillantes, de janvier à avril 2020.

Introduction

https://fr.statista.com/

Le hacking en chiffre

Pays les plus ciblés par les cyberattaques majeures (2006-2020)



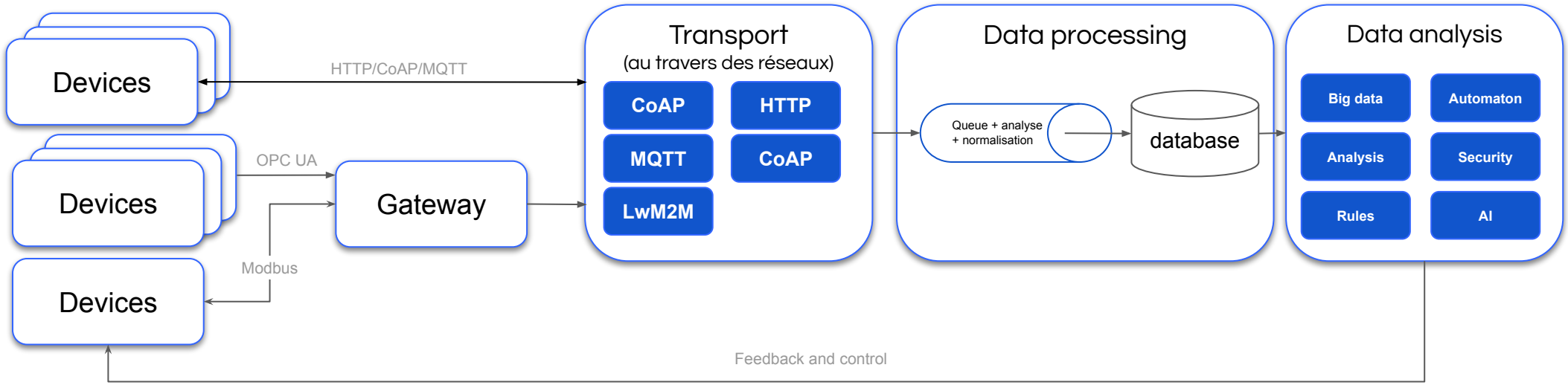
Sécurité du transport de données / Introduction

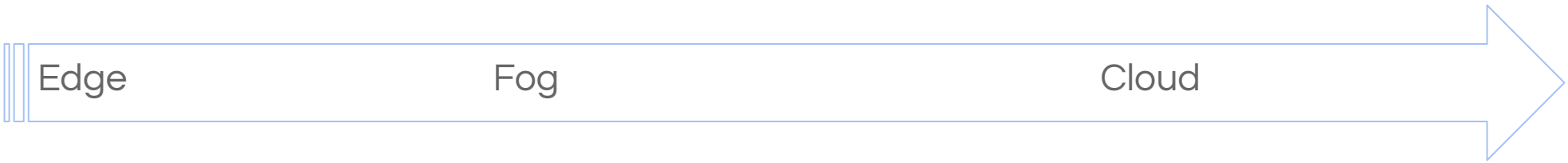
Service de sécurité pour le transport des données IoT:

Notion d'architecture système

IEEE INTERNET OF THINGS JOURNAL, VOL. 7, NO. 10, OCTOBER 2020 - P10091 /
Landscape of Architecture and Design Patterns for IoT Systems - https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9120234

Les 4 composants majeurs d'une plateforme IoT (simplifiée)





Architecture

IoT DEVICES

Edge / Fog

Cloud
Architecture style: Saas, PaaS …

Notion d'architecture système

https://www.etsi.org/technologies/consumer-iot-security
https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf
https://ec.europa.eu/commission/presscorner/detail/fr/ip_21_5634
https://fr.wikipedia.org/wiki/Directive_RED

L'architectures d'une plateforme IOT (simplifiée) / Normalisation

Normes de sécurité IoT - (documents payants/gratuits)

- ETSI EN 303 645 (Cyber Security for Consumer Internet of Things: Baseline Requirements. European Standard)
- La directive RED (directive européenne 2014/53/UE1)
- ISO/IEC 29181-5:2014 (Future Network -- Problem statement and requirements)
- X.1362 (Simple encryption procedure for IoT environments)
- Y.4102/Y.2074 (Requirements for IoT devices and operation of IoT applications during disasters)
- Y.4455 (Reference architecture for IoT network service capability exposure)
- Y.4118 (IoT requirements and technical capabilities for support of accounting and charging)
- Q.3952 (The architecture and facilities of a model network for IoT testing)
- Y.4702 (Common requirements and capabilities of device management in the IoT)
- Q.3913 (Set of parameters for monitoring IoT devices)

Sécurité du transport de données / Introduction

- Le but du cloud est d'offrir des services pour réduire les coûts, éviter des infrastructures non maîtrisées, objectifs:
  - Se concentrer sur son activité en utilisant des services clés en main,
  - Stockage massif de données des IoT,
  - Processing des données (analyse, IA …),
  - Concentration des flux …
- Les données doivent transiter par de nombreux supports physiques et utiliser des protocoles parfois différents pour arriver au point de stockage,
- Les protocoles utilisent des supports filaires, optiques, radios,
- Le transport pose forcément des problèmes de sécurité parfois complexes à résoudre.

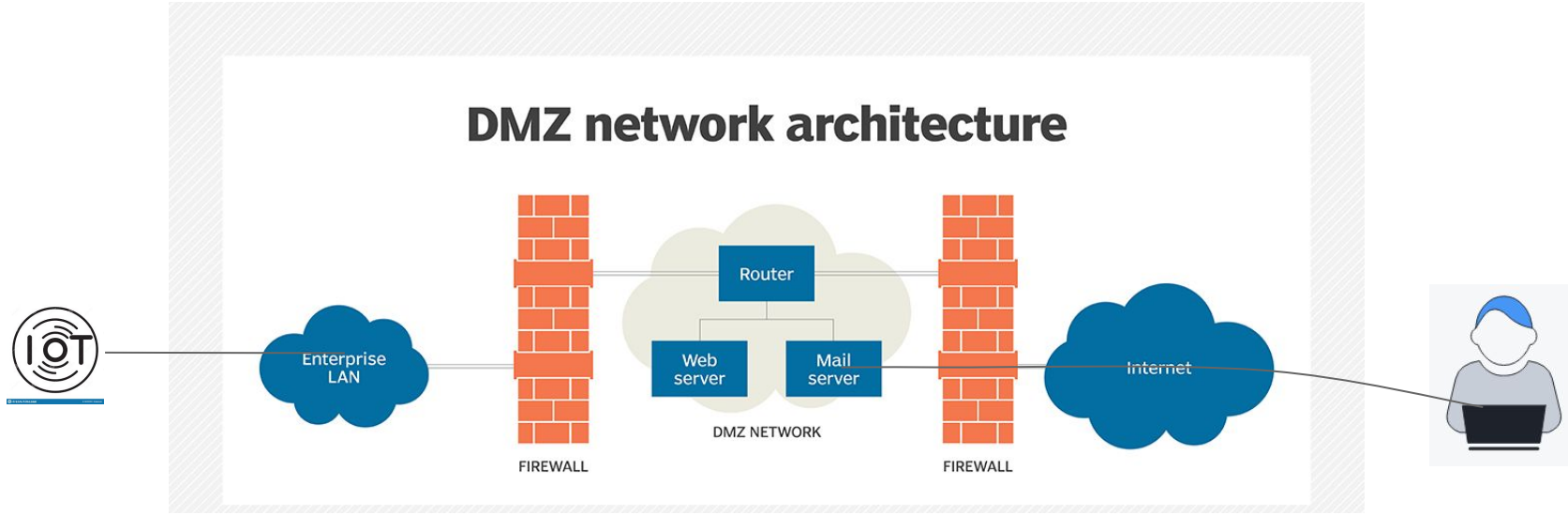
Sécurité au niveau du cloud

Sécurité du transport de données / Protocole TCP et UDP

- L'utilisation de TCP UDP/IP sans sécurité n'est pas possible,
- Rappels du comportement de TCP/IP UDP/IP:
  - Les données de TCP ou UDP sont en claires sur le réseau,
  - Il est possible d'espionner et de récupérer les données, mot de passe …
  - De nombreuses failles de sécurité sont possibles,
  - TCP/IP et UDP/IP sont les seuls protocoles possibles sur Internet,
- Il faut utiliser des mécanismes de sécurité avec TCP/UDP

Notions de base

DMZ



sous contrôle — flux 1 →

sous contrôle important — ← flux 2

← flux 3 — sous contrôle important

sous contrôle — flux 4 →

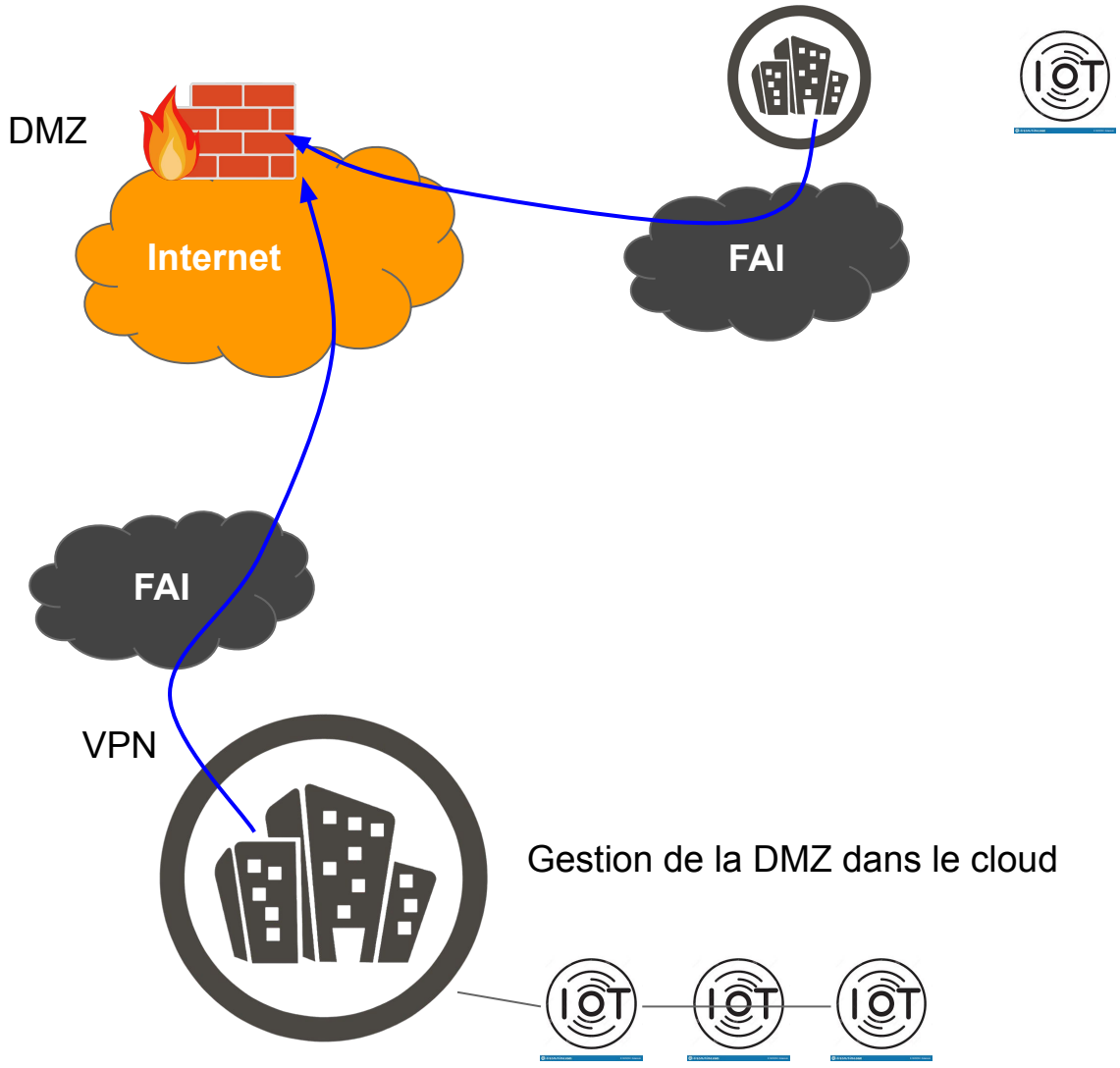
DMZ de type cloud (hybrid)

- Une solution de sécurité à base d'équipement physique, n'est pas toujours économiquement viable: coût des équipements + maintenance + configuration
- De plus en plus d'entreprises couplent l'hybridation de leur réseau à la transformation de leur solution de sécurité vers un modèle cloud.
- Le modèle SaaS est utilisé pour les plateformes de sécurité car le SaaS est également dans le cloud.
- Une DMZ est implémentée entre le réseau sur site d'une organisation et le réseau virtuel.
- Cette méthode est généralement utilisée dans les situations où les applications de l'entreprise s'exécutent en partie sur site et en partie sur le réseau virtuel.

DMZ de type cloud (hybrid)

La DMZ est dans le cloud comme un SaaS. La sécurité est assurée par ce point, on y trouve tous les services : HTTP, MQTT, CoAP

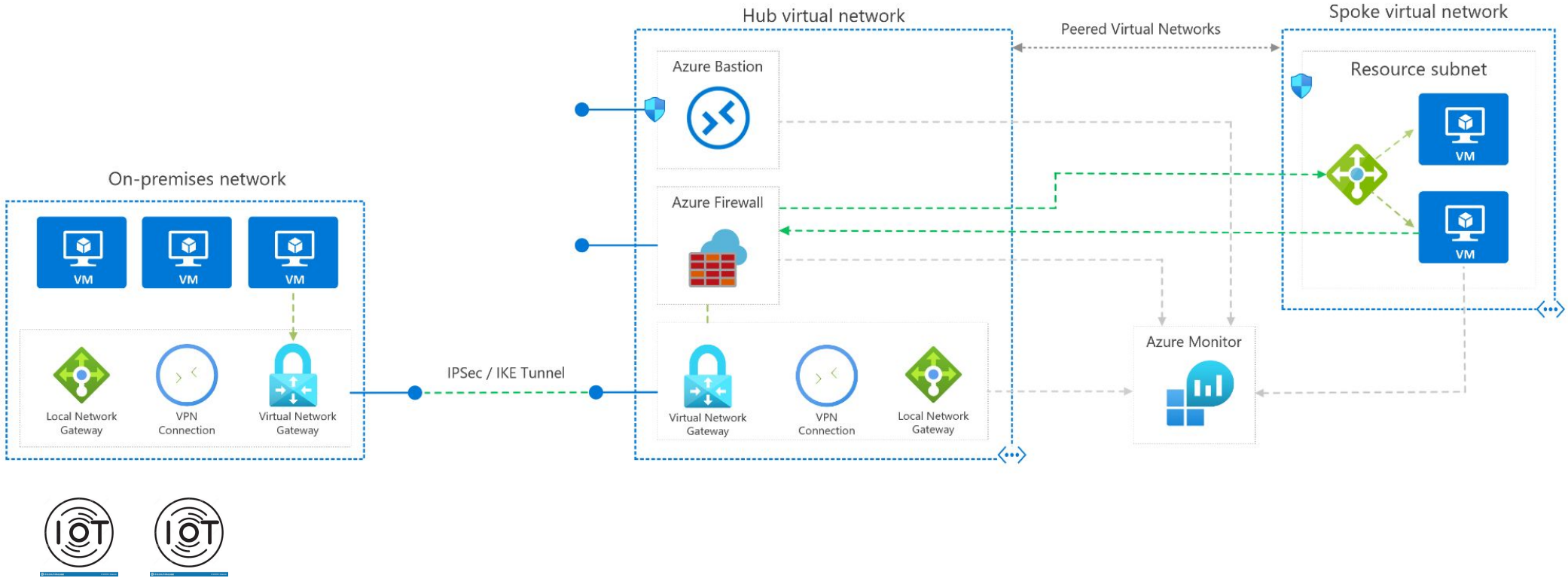
Connexion locale au fournisseur Internet



https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/dmz/secure-vnet-dmz?tabs=portal

DMZ de type cloud (hybrid)

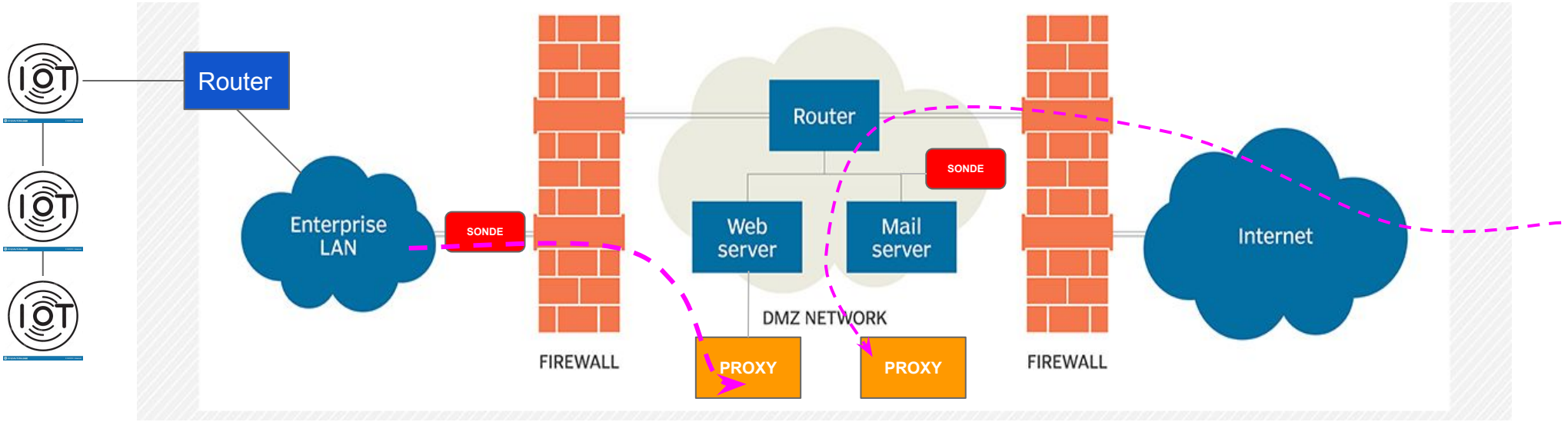
Exemple avec Azur



https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/dmz/secure-vnet-dmz?tabs=portal

DMZ

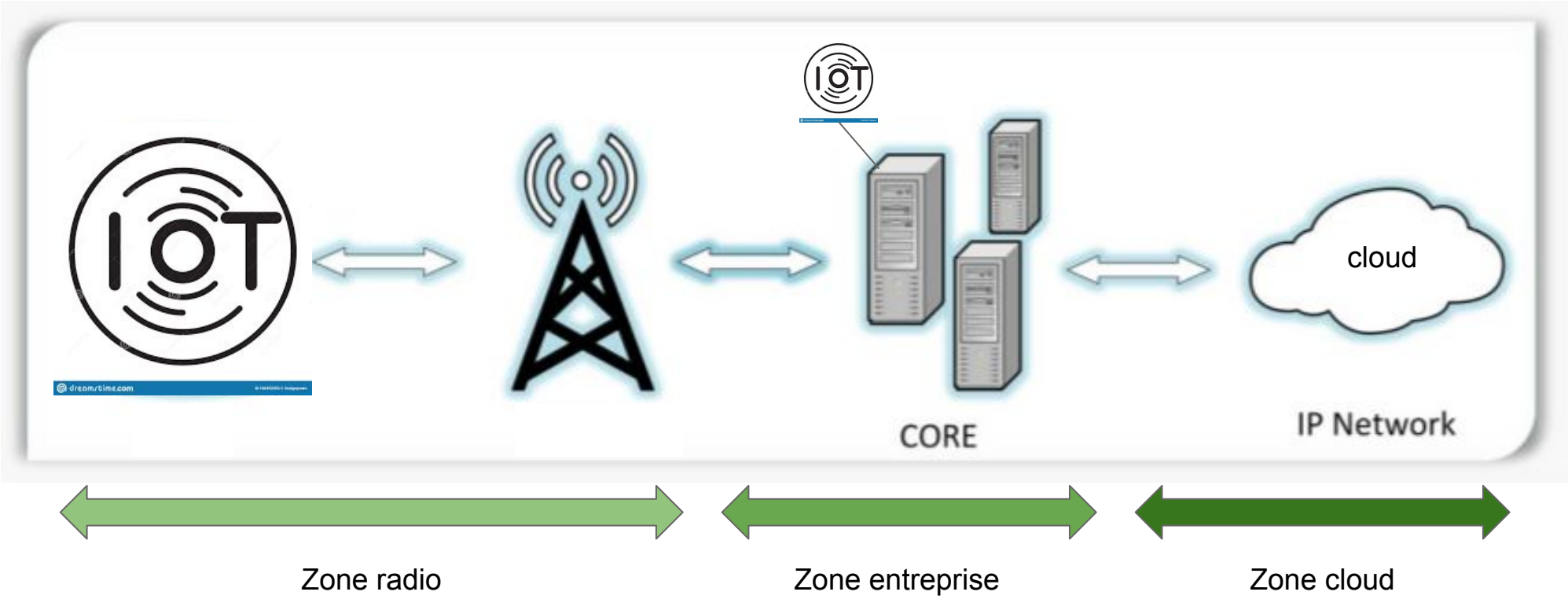
- Le deuxième niveau de sécurité permet d'intercaler **des sondes de sécurité** entre le firewall et le réseau local,
- Si un pirate arrive à passer alors la sonde peut le détecter,
- Tous les flux entrants et sortants passent par les proxies applicatifs.



Sécurité au niveau du cloud

https://csrc.nist.gov/CSRC/media/Presentations/LTE-Security-How-Good-is-it/images-media/day2_research_200-250.pdf

Sécurité du transport de données / Architecture commune



Sécurité au niveau du cloud

Sécurité du transport de données / Architecture commune

- **La zone radio entreprise est sécurisée par:**
  - Des protocoles spécifiques avec chiffrement,
  - L'infrastructure radio: 4G LTE, 5G NB-IoT, LoRa Wan, Wifi …
  - Le chiffrement des données par les applications (certificat),
  - Le niveau de sécurité n'est pas le même dans toutes les technologies.
- **La zone entreprise (core network) est sécurisée par:**
  - Le chiffrement des données par les applications, les protocoles,
  - L'infrastructure IP: VPN, VLAN …
- Le passage d'une zone radio au core IP est assuré par la sécurité d'une zone puis l'autre. **La sécurité est ainsi assurée de bout en bout**.

Sécurité au niveau du cloud

Sécurité du transport de données / Architecture commune

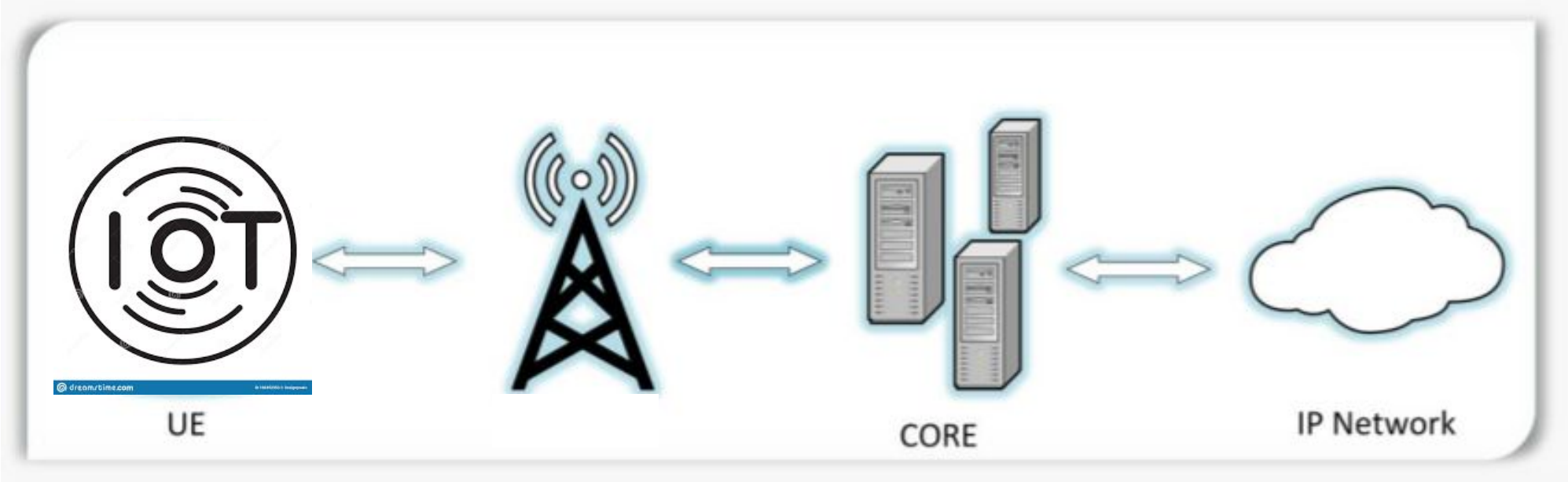
Zone multi-technologique

- Le cloud ne s'occupe **pas de la sécurité des données, c'est juste une zone de transit**,
- Les routeurs et protocoles de routage sont protégés (en principe),
- **Les données en transit sont sécurisées par**:
  - Des protocoles spécifiques avec chiffrement (SSL, CoAp over SSL …),
  - Les équipements de sécurité: firewall, routeur …
  - La sécurité des machines (Linux, Windows …),
  - Le niveau de sécurité n'est pas homogène d'un fournisseur à un autre,

Sécurité au niveau du cloud

https://csrc.nist.gov/CSRC/media/Presentations/LTE-Security-How-Good-is-it/images-media/day2_research_200-250.pdf
https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=1341

Sécurité du transport de données / Architecture radio et sécurité



SÉCURITÉ SPÉCIFIQUE

Sécurité définie par :
LoRA
LTE-M
NB-IoT
Chiffrement des applications

SÉCURITÉ IP

Sécurité définie par les infrastructures IP :
- Firewall, routeur
- VPN,
- IPSec
- Chiffrement des applications avec certificat (HTTPS, CoAP SSL …)

Sécurité au niveau du cloud

https://csrc.nist.gov/CSRC/media/Presentations/LTE-Security-How-Good-is-it/images-media/day2_research_200-250.pdf

Sécurité du transport de données / Architecture radio et sécurité

Communication UE / EUTRAN (Evolved Universal Terrestrial Radio Access Network)

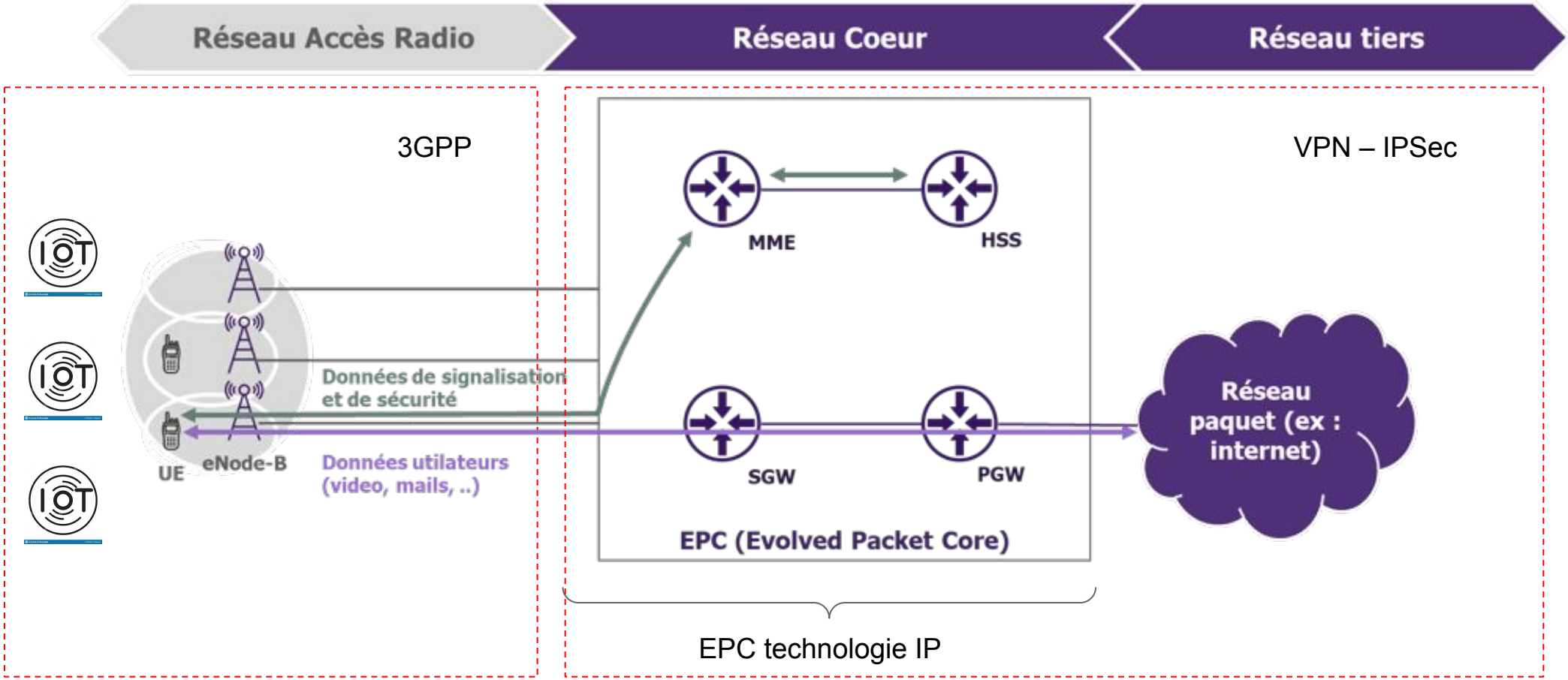
- **Authentification** . L'appareil qui envoie des données vers le cloud est autorisé et personne ne l'a remplacé par un autre
- **Confidentialité:** avec le chiffrement , un observateur des communications ne peut pas comprendre les messages, seul le cloud avec les clés de déchiffrement peut récupérer les messages.
- **Intégrité**: Les données sont vérifiées par les algorithmes de chiffrement.

Sécurité au niveau du cloud

https://www.digitalcorner-wavestone.com/2020/01/de-la-2g-a-la-4g/

Sécurité du transport de données / Architecture 4G/5G

Le cœur de réseau 5G présente beaucoup d'analogies fonctionnelles avec le cœur de réseau 4G, l'évolution majeure consiste en un découpage de fonctions réseau.



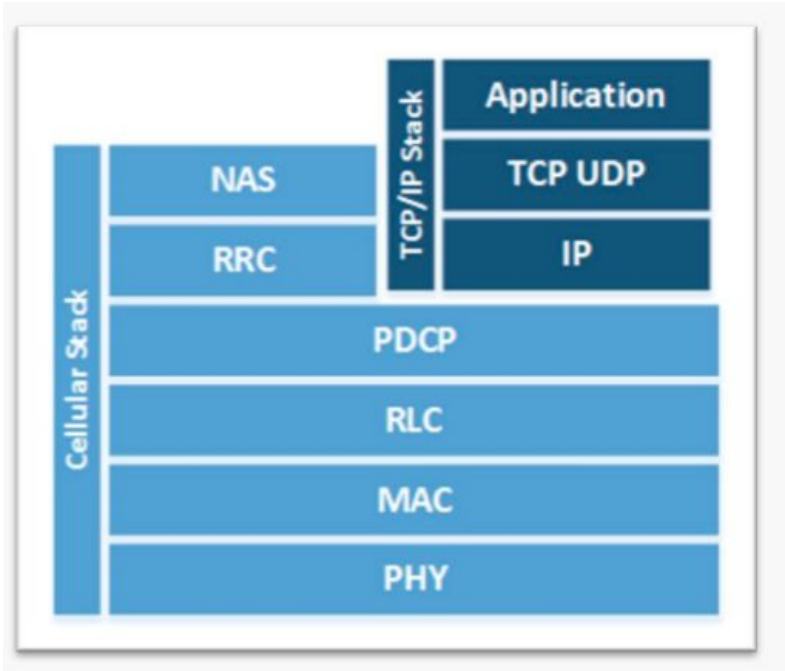
Sécurité au niveau du cloud

https://csrc.nist.gov/CSRC/media/Presentations/LTE-Security-How-Good-is-it/images-media/day2_research_200-250.pdf
https://www.artizanetworks.com/resources/tutorials/pro_sta.html
https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=1341

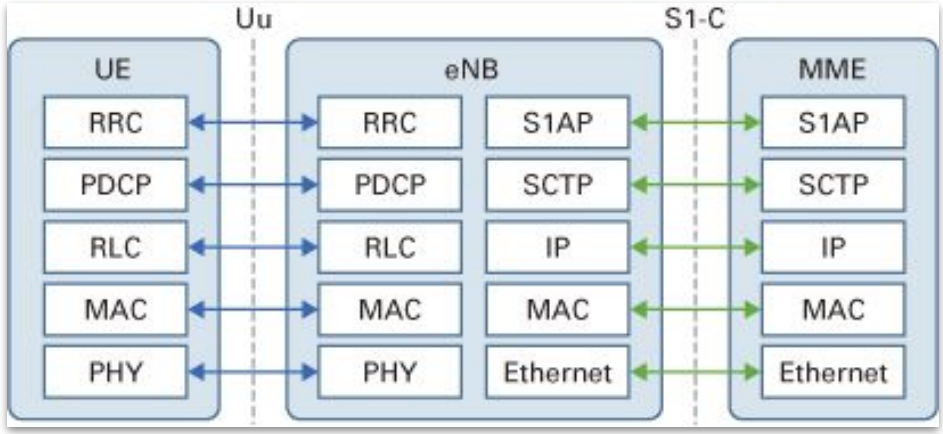
Sécurité du transport de données / Architecture 4G/5G / Pile protocoles LTE

La norme 3GPP définie la pile de protocole, déclinée ensuite pour les interfaces des sous-systèmes:

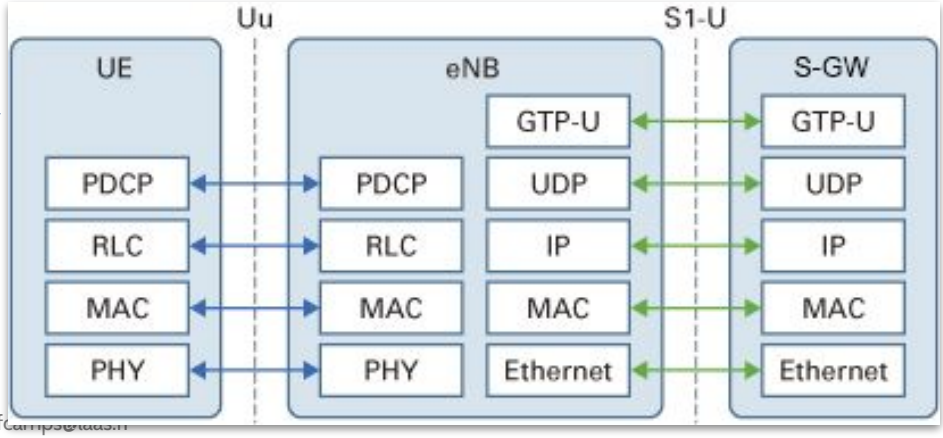
Pile de protocoles



Protocol Stack: Uu (UE/eNB) and S1-C (eNB/MME)



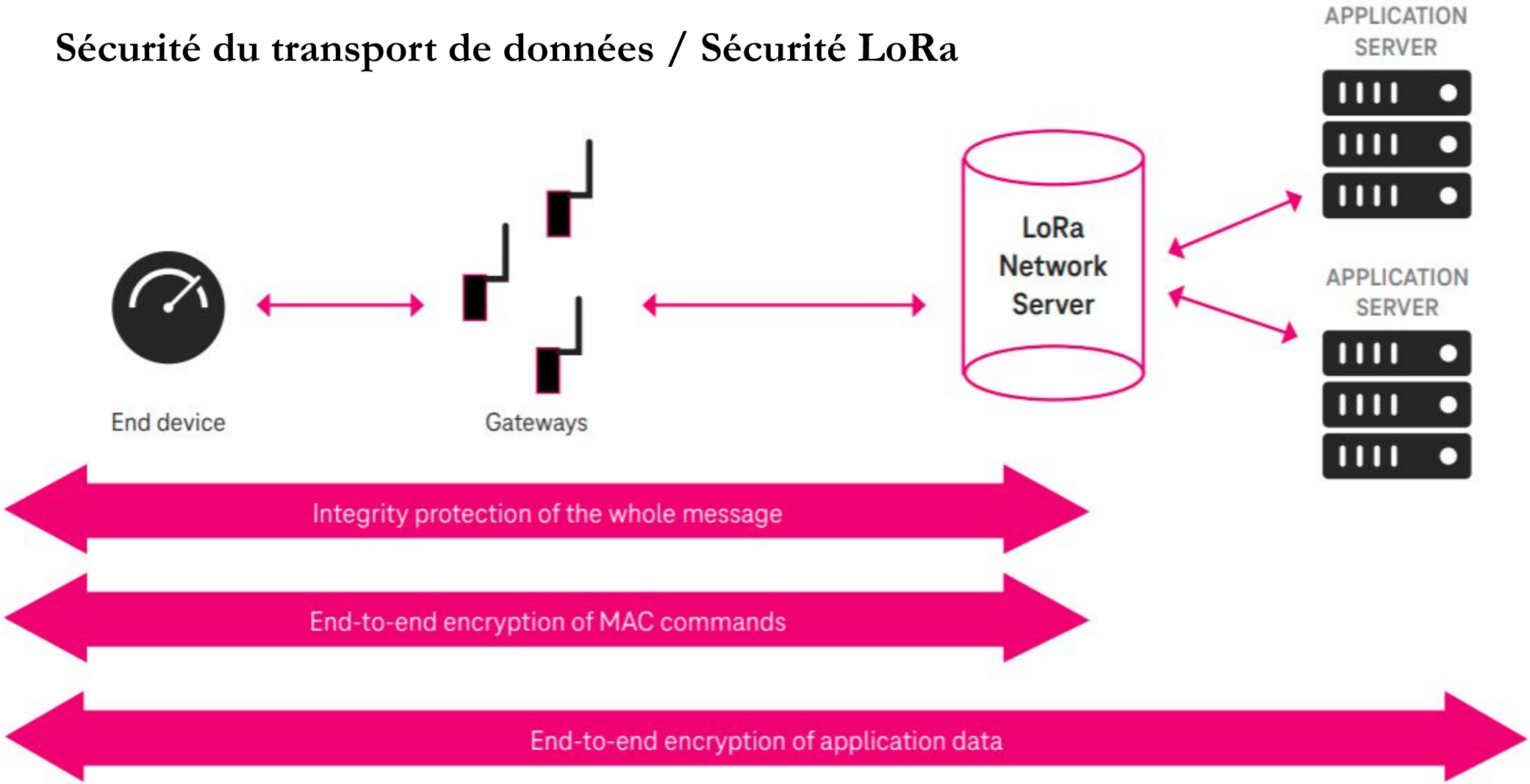
Protocol Stack: Uu (UE/eNB) and S1-U (eNB/S-GW)



Sécurité au niveau du cloud

https://iot.telekom.com/resource/blob/data/489050/f9fb87f65ada3528c8c08a1cb0364a1d/security-aspects-lorawan-nb-iot.pdf
https://lora-alliance.org/wp-content/uploads/2020/11/lorawan_security_whitepaper.pdf

Sécurité du transport de données / Sécurité LoRa



authentification + chiffrement

Sécurité au niveau du cloud

https://fr.wikipedia.org/wiki/CLOUD_Act

Risques des plateformes IoT industrielles USA

- **Le Cloud Act (acronyme de "Clarifying Lawful Overseas Use of Data Act") chapitre 121 du Titre 18 du United States Code, loi fédérale américaine promulguée le 23 mars 2018:**
  - Les forces de l'ordre ou aux agences de renseignement américaines peuvent obtenir des informations sur les données stockées sur les serveurs, sans que la personne "ciblée" ou que le pays où sont stockées ces données n'en soient informés.
  - Les serveurs peuvent être soient située aux États-Unis ou à l'étranger,
  - Des accords bilatéraux peuvent être également signés !: les autorités respectives des pays signataires peuvent alors obtenir des informations,
- Le Cloud Act est en contradiction avec l'article 48 du Règlement européen sur la protection des données (RGPD).

Synthèse

https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

Comment assurer une sécurité fiable ?

- **La sécurité de l'IoT est un sujet complexe qui demande**:
  - Une sensibilisation à la sécurité,
  - Une analyse des besoins de sécurité,
  - Des compétences techniques parfois élevées,
- **Une politique de sécurité:**
  - Système (IoT, serveur, Internet, mail, outils de sécurité …)
  - Projets et produits,
  - L'application des normes du domaine,
  - Une veille technologique,
- **Utiliser les normes**: La norme ETSI définit 13 exigences de cybersécurité

Synthèse

https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

Les 13 points de sécurité ETSI EN 303 645

Des règles de bon sens !:

- No universal default passwords
- Implement a means to manage reports of vulnerabilities
- Keep software updated
- Securely store sensitive security parameters 5.5 Communicate securely
- Minimize exposed attack surfaces
- Ensure software integrity
- Ensure that personal data is secure
- Make systems resilient to outages
- Examine system telemetry data
- Make it easy for users to delete user data
- Make installation and maintenance of devices easy
- Validate input data

Synthèse

https://www.etsi.org/technologies/consumer-iot-security
https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf
https://ec.europa.eu/commission/presscorner/detail/fr/ip_21_5634
https://fr.wikipedia.org/wiki/Directive_RED

Normes de sécurité IoT - (documents payants/gratuits)

- IEC 62443 une série internationale de normes sur la cybersécurité
- ETSI EN 303 645 une norme européenne (Cyber Security for Consumer Internet of Things: Baseline Requirements. European Standard)
- La directive RED (directive européenne 2014/53/UE1)
- ISO/IEC 29181-5:2014 (Future Network -- Problem statement and requirements)
- X.1362 (Simple encryption procedure for IoT environments)
- Y.4102/Y.2074 (Requirements for IoT devices and operation of IoT applications during disasters)
- Y.4455 (Reference architecture for IoT network service capability exposure)
- Y.4118 (IoT requirements and technical capabilities for support of accounting and charging)
- Q.3952 (The architecture and facilities of a model network for IoT testing)
- Y.4702 (Common requirements and capabilities of device management in the IoT)
- Q.3913 (Set of parameters for monitoring IoT devices)

Synthèse

Quelles sont les principales mesures à prendre en compte pour l'IoT ?

- Vous assurer que vos systèmes sont protégés:
  - **Réseau**: Firewall, DMZ, segmentation + filtrage
  - **Serveurs**: service, logiciel, mise à jour
  - **IoT**: zone radio + cloud → protocol de chiffrement + authentification
  - **Cloud**: accès, firewall, DMZ virtuelle,

Comment ?

- Audit de sécurité de vos systèmes: formation de hacking,
- Mise à jour des systèmes,
- Veille technologique : CERT, NIST ..

Comment maintenir un niveau de sécurité ?

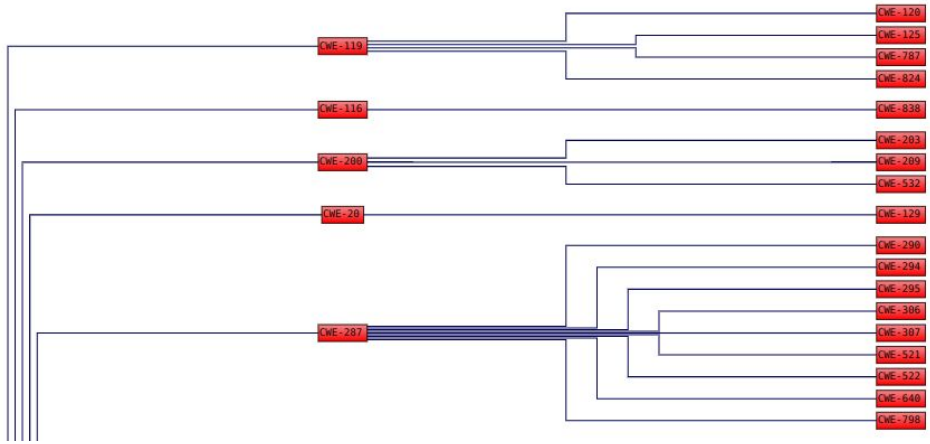
- Audit de sécurité de vos systèmes,
- Respects des normes,
- Politique de sécurité globale.

Les attaques

https://nvd.nist.gov/vuln/categories https://www.redscan.com/media/Redscan_NIST-Vulnerability-Analysis-2020_v1.0.pdf

Introduction

- Il existe des milliers d'attaques possibles en fonction des systèmes,
- Il est possible classifier les attaques:
  - Mémoire,
  - Réseau,
  - OS,
  - Logiciel tiers …
- Le NIST propose une classification: https://nvd.nist.gov/vuln/categories/cwe-layout



Notion d'exploit

- Un exploit informatique, ou exploit, est une attaque contre un système informatique,
- Une attaque qui tire parti d'une vulnérabilité particulière que le système offre aux intrus,
- Utilisation détournée et non prévu par les développeurs,
- Utilisé comme verbe, exploiter fait référence à l'acte de réussir une telle attaque,
- Il existe plusieurs types d'exploits informatiques:
  - DDOS
  - Dépassement de buffer
  - Injection SQL …

https://nvd.nist.gov/vuln/categories https://www.redscan.com/media/Redscan_NIST-Vulnerability-Analysis-2020_v1.0.pdf

Base de données Exploit

Base de données:

- https://www.exploit-db.com/
- https://github.com/offensive-security/exploitdb
- https://www.rapid7.com/db/
- https://cxsecurity.com/exploit/
- https://www.vulnerability-lab.com/
- https://0day.today/
- https://securitytrails.com/blog/google-hacking-techniques

Alertes:

- https://nvd.nist.gov/
- https://www.cisa.gov/uscert/ncas/alerts
- https://www.securityfocus.com/vulnerabilities
- https://packetstormsecurity.com/files/tags/exploit/

https://thehackernews.com/search/label/hardware%20hacking

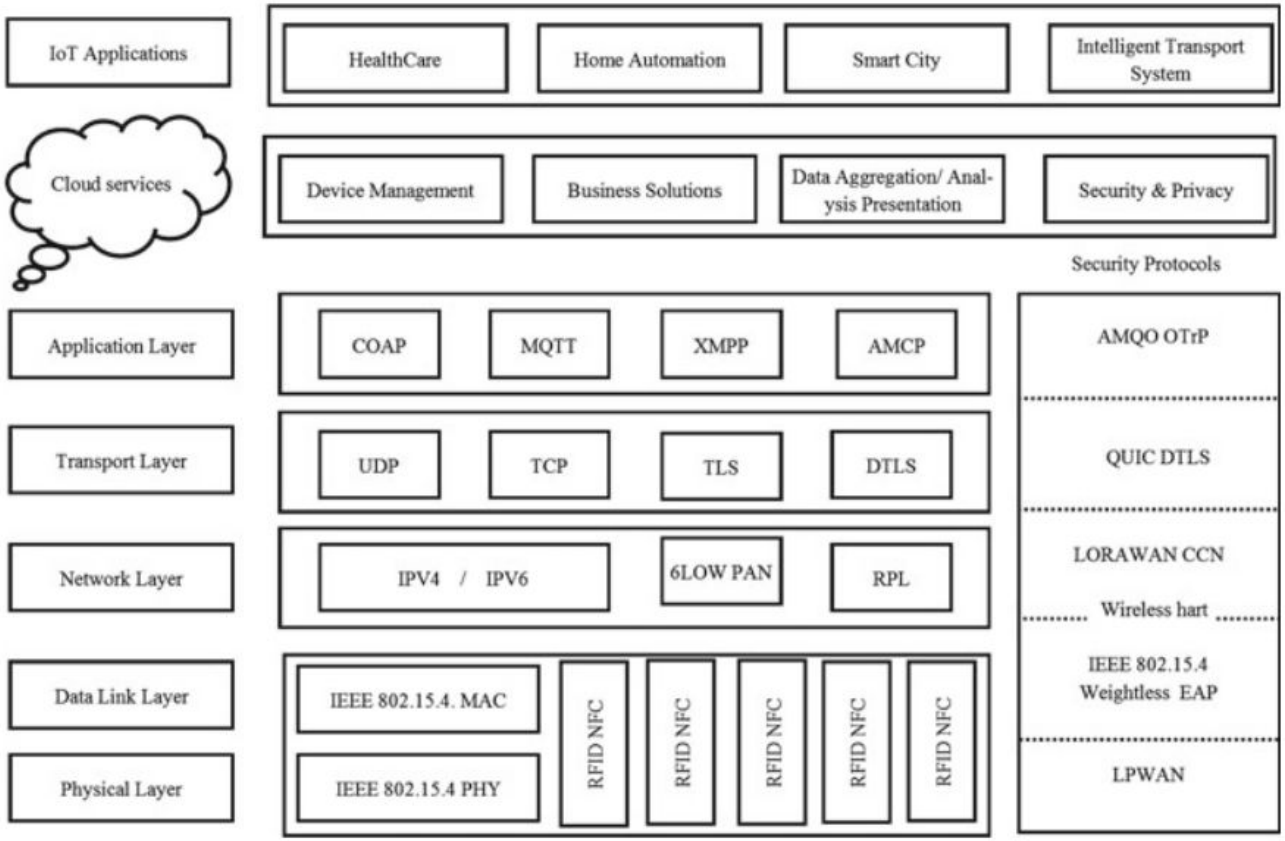
IoT

- L'Internet des objets comprend une variété de capteurs, d'appareils portables, de téléphones portables et d'appareils électroménagers,
- Un IoT peut utiliser ou pas le protocole TCP/IP,
- **Si TCP/IP est utilisé alors l'équipement peut subir les mêmes attaques qu'un équipement standard**,
- Chiffrement: certains IoT ne possèdent aucune possibilité de chiffrement.
- L'IoT utilise de nombreux supports:
  - Wifi,
  - ZigBee,
  - Lora
  - BLE,
  - ZWave
  - 6LoWPAN, GSM, Ethernet …

Les attaques

https://thehackernews.com/search/label/hardware%20hacking

IoT / Architecture et protocoles (rappel)



Les attaques

https://www.picotech.com/library/oscilloscopes/serial-bus-decoding-protocol-analysis

Attaque physique

- Les attaques matériels sont sous conditions d'un accès physique à la cible,
- **Deux types d'attaques:**
  - Attaques sur un équipement opérationnel (en cours de fonctionnement),
  - Attaque pour réaliser un reverse engineering d'un système,
- **Les attaques sont réalisées avec des équipements électroniques:**
  - Analyseur numérique
  - Oscilloscope
- **Analyse des composants électroniques:**
  - Référence composant sur les boîtiers
  - Rayon X pour connaître la structure des processeurs

Les attaques

https://book.hacktricks.xyz/hardware-physical-access/physical-attacks

Attaque physique

Une liste non exhaustive des attaques matérielles possibles:

- **BIOS password**
  - **battery**
  - **jumper CMOS**
- **UEFI**
- **USB**
- **Clavier** (https://www.youtube.com/watch?v=58iGT0jfVUs)
- **Boot sur un disque externe**
- **Bus: JTAG, UART, SPI, I2C …**

Les attaques

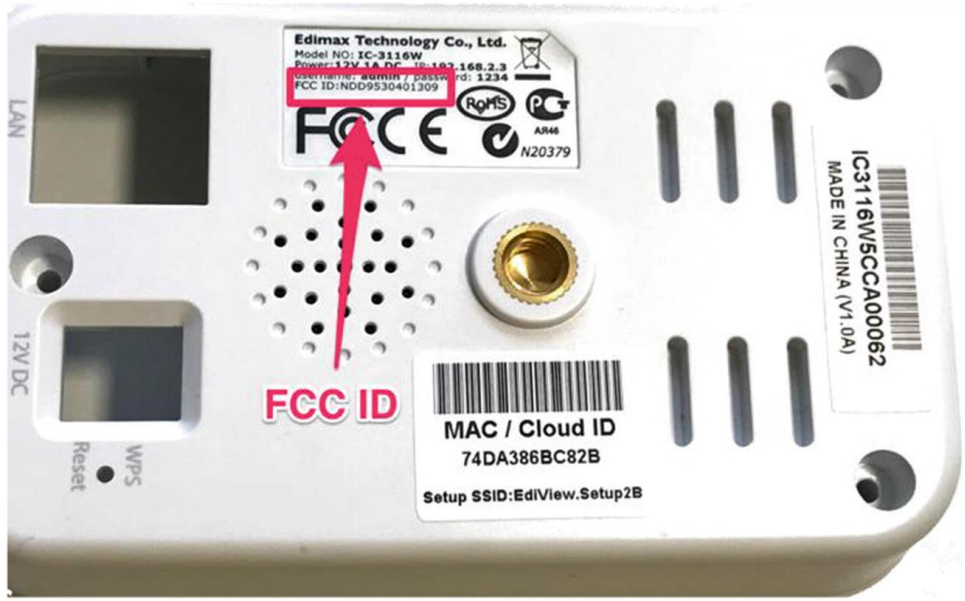
https://thehackernews.com/search/label/hardware%20hacking

Attaque physique / FCC ID

Information FCC ID : Federal Communication Commission (FCC)

https://apps.fcc.gov/oetcf/eas/reports/GenericSearch.cfm

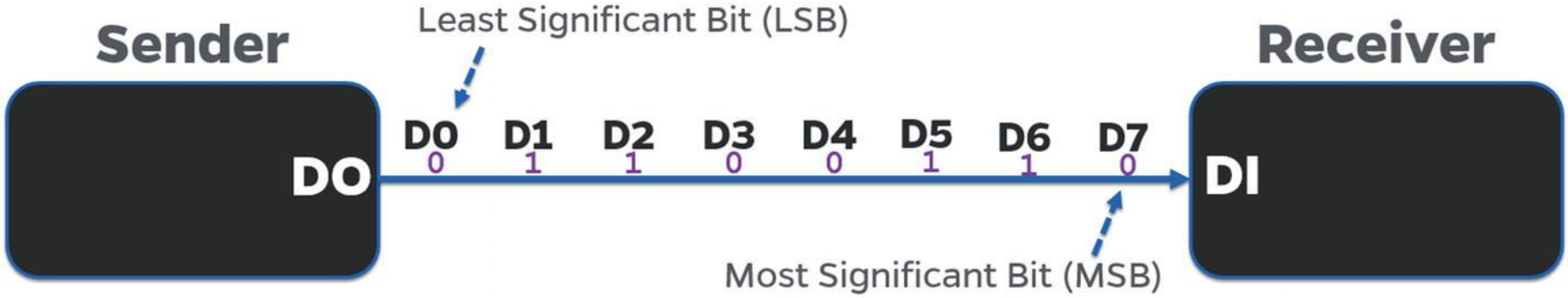
https://fccid.io → tester avec NDD9530401309

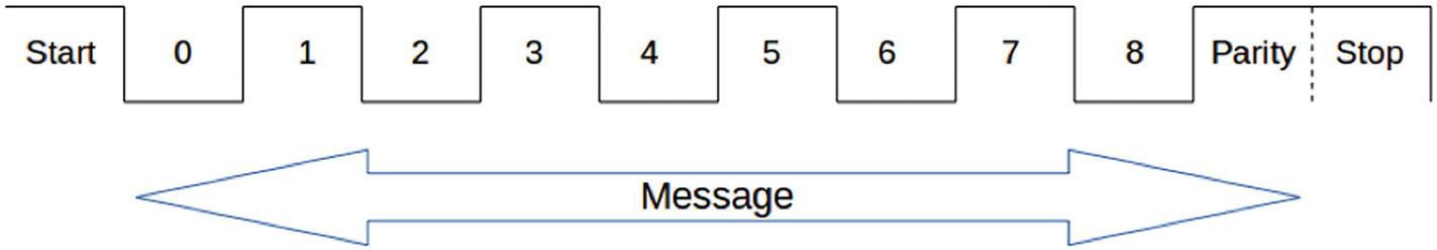


https://thehackernews.com/search/label/hardware%20hacking

Attaque physique / UART

La communication série et la communication parallèle sont les deux façons dont les composants d'un appareil échangent des données. Il est très facile de se connecter sur un port UART.

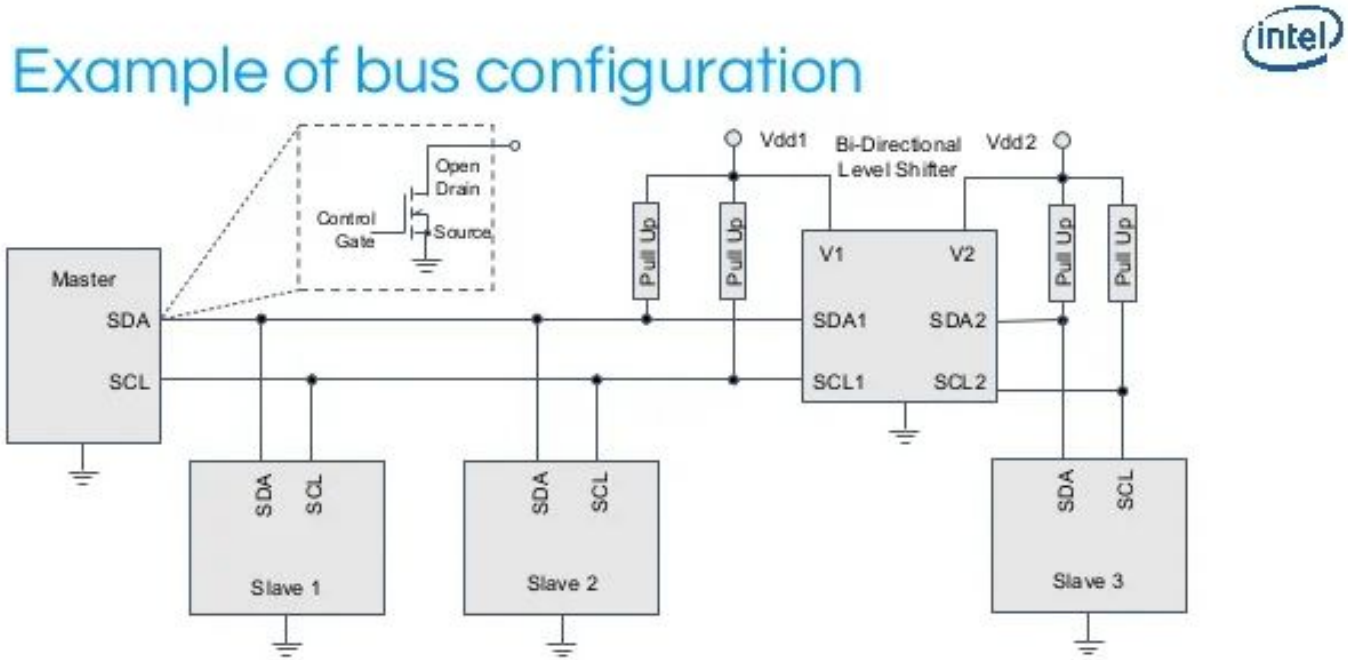




https://thehackernews.com/search/label/hardware%20hacking

Attaque physique / I2C (Inter-Integrated Circuit)

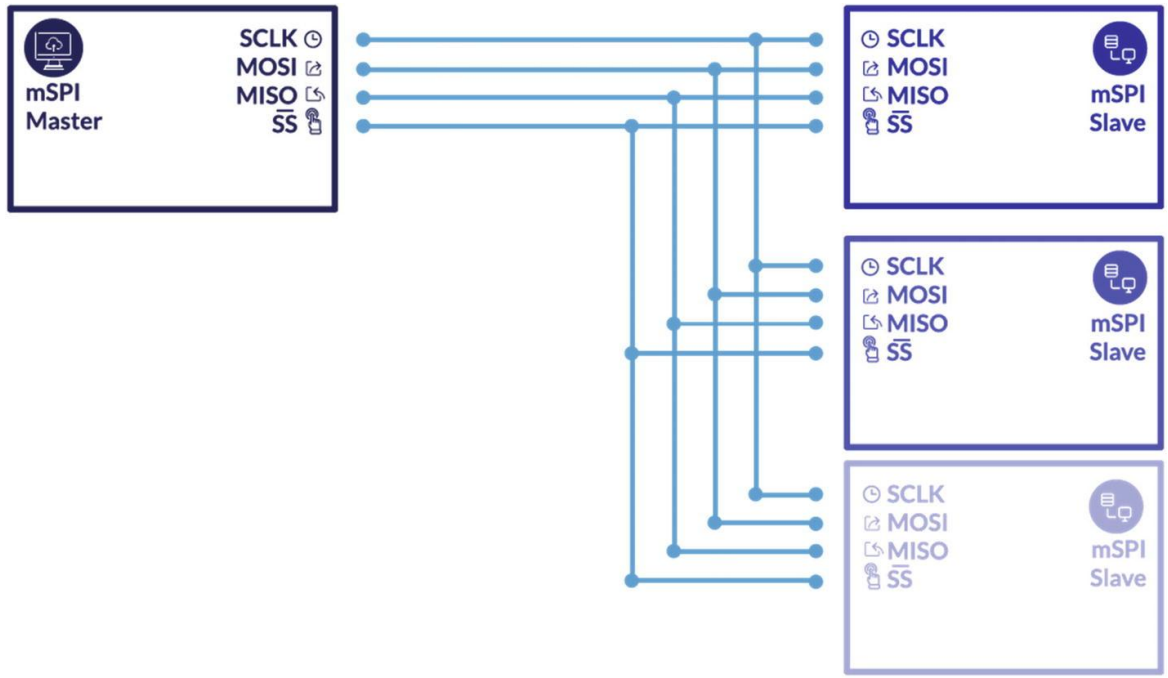
I2C a été développé en 1982, par Philips, pour permettre à leurs puces de communiquer et d'échanger des données avec d'autres composants. C'est aussi une communication série.



https://thehackernews.com/search/label/hardware%20hacking

Attaque physique / SPI

SPI (interface périphérique série) est une spécification d'interface de communication série synchrone. L'interface a été développée par Motorola au milieu des années 1980 et est devenue un standard de facto . Les appareils SPI communiquent en mode duplex intégral en utilisant une architecture maître-esclave



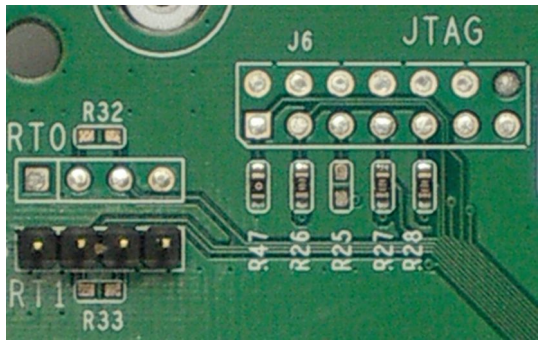
https://thehackernews.com/search/label/hardware%20hacking

Attaque physique / JTAG

JTAG (Joint Test Action Group) est une norme industrielle pour vérifier les conceptions et tester les cartes électroniques.

Le but est de se connecter directement au processeur pour accéder au programme, on peut lancer un debug, faire une mise à jour du firmware, lire des données. Il est possible d'extraire le logiciel et faire un reverse engineering du code.

Contre-mesure: Il est possible de rendre le bus inaccessible lors de la programmation de la puce (fusible).



http://www.man-linux-magique.net/man8/hping3.html

DOS (Denial-of-Service) / Flooding ICMP

Commande: `sudo hping3 –icmp --flood <cible>`

C'est le DOS le plus classique. Normalement on attend la réponse ICMP avant d'envoyer un autre paquet, ici on ne pas attendre pour augmenter le débit.

```
$ sudo hping3 --icmp --flood –data 40 192.168.0.29
HPING 192.168.0.29 (eth0 192.168.0.29): icmp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Contre-mesures:

- Désactiver la fonctionnalité ICMP du routeur, de l'ordinateur ou du périphérique ciblé.
- Limitation du trafic par rapport au flux ICMP (10 paquets /s par exemple), la configuration dépend du firewall ou du routeur.

http://www.man-linux-magique.net/man8/hping3.html

DOS (Denial-of-Service) / SMURF Attack

Commande: `sudo hping3 –icmp –flood <@ip cible> -a <@ip src spoof>`

Il s'agit d'une sorte d'attaque DDoS dans laquelle l'adresse source usurpée envoie une grande quantité de paquets ICMP à l'adresse cible. Il utilise une adresse victime comme adresse source pour envoyer/diffuser la requête ping ICMP multiple.

```
$ sudo hping3 --icmp --flood 192.168.0.29 -a 192.168.0.80
HPING 192.168.0.29 (eth0 192.168.0.29): icmp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Contre-mesures:

- Désactiver la fonctionnalité ICMP du routeur, de l'ordinateur ou du périphérique ciblé.
- Filtre IP pour autoriser des machines en ICMP.

http://www.man-linux-magique.net/man8/hping3.html

DOS (Denial-of-Service) / LAND Attack

Commande: `sudo hping3 -S -p <port cible> <@ip cible> -a <spoof @src>`

Attaque ICMP avec un spoof sur l'adresse source et port destination.

```
$ sudo hping3 -S --flood -p 80 192.168.0.29 -a 192.168.0.60
HPING 192.168.0.29 (eth0 192.168.0.29): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Contre-mesures:

- Désactiver la fonctionnalité ICMP du routeur, de l'ordinateur ou du périphérique ciblé.
- Filtre IP pour autoriser des machines en ICMP.

http://www.man-linux-magique.net/man8/hping3.html

DOS (Denial-of-Service) / SYN/FIN/RST/PUSH Flood

Commande: `hping3 -<FLAG> -p 80 <Target> –flood`

Il est possible d'utiliser un mixte de tous les flood !

```
$ sudo hping3 --xmas --flood  --data 40  192.168.0.29
HPING 192.168.0.29 (eth0 192.168.0.29): X set, 40 headers + 40 data bytes
hping in flood mode, no replies will be show
```

Contre-mesures:

- Différenciation du trafic, canaliser le flux par adresse IP
- Supprimer le protocole ICMP avec un filtre

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst_pon/software/configuration_guide/sec/b-gpon-config-security/preventing_arf_spoofing_and_flood_attack.html

DOS (Denial-of-Service) / Flooding HTTP

- **Slowloris** est un type d' outil d'attaque par déni de service qui permet à une seule machine de désactiver le serveur Web d'une autre machine avec une bande passante minimale et des effets secondaires sur des services et des ports non liés.

- **Contre-mesures**:
  - Créer une route vers un trou noir avec les @IP pour canaliser le trafic,
  - Détection d'augmentation de trafic,
  - Utiliser un pare-feu d'application Web (WAF),
  - Augmenter le nombre maximum de client sur serveur,
  - Limiter le nombre de connexions qu'une seule adresse IP est autorisée à établir,
  - Restreindre la durée à laquelle un client est autorisé à rester connecté.
  - Les modules Apache mod_limitipconn, mod_qos , mod_evasive, mod security , mod_noloris et mod_antiloris ont tous été suggérés comme moyen de réduire la probabilité d'une attaque Slowloris réussie.

Brut force

- **Protocol avec mot de passe:** AFP, Cisco AAA, authentification Cisco, activation Cisco, CVS, Firebird, FTP, HTTP-FORM-GET, HTTP-FORM-POST, HTTP-GET, HTTP-HEAD, HTTP-POST, HTTP-PROXY, HTTPS-FORM -GET, HTTPS-FORM-POST, HTTPS-GET, HTTPS-HEAD, HTTPS-POST, proxy HTTP, ICQ, IMAP, IRC, LDAP, MS-SQL, MYSQL, NCP, NNTP, auditeur Oracle, Oracle SID, Oracle , PC-Anywhere, PCNFS, POP3, POSTGRES, RDP, Rexec, Rlogin, Rsh, RTSP, SAP / R3, SIP, SMB, SMTP, Enum SMTP, SNMP v1 + v2 + v3, SOCKS5, SSH (v1 et v2), SSHKEY, Subversion, Teamspeak (TS2), Telnet, VMware-Auth, VNC et XMPP …
- **Le brut force**: Une attaque par force brute utilise des mots de passe d'un dictionnaire pour tenter de se connecter à un système. Le terme brut force est utilisé car il faut des moyens élevés pour réaliser les tentatives, parfois plusieurs millions de test !
- Il s'agit d'une ancienne méthode d'attaque, mais elle est toujours efficace et populaire auprès des pirates.

Les attaques

Brut force

- **Attaques par force brute simples**: les pirates tentent de deviner logiquement vos informations d'identification, sans l'aide d'outils logiciels ou d'autres moyens. Ceux-ci peuvent révéler des mots de passe et des codes PIN extrêmement simples. Par exemple, un mot de passe défini comme "pass12345".
- **Attaques par dictionnaire** : dans une attaque standard, un pirate choisit une cible et exécute des mots de passe possibles contre ce nom d'utilisateur. Celles-ci sont connues sous le nom d'attaques par dictionnaire. Les attaques par dictionnaire sont l'outil le plus basique des attaques par force brute.
- **Attaques par force brute hybrides** : ces pirates mélangent des moyens extérieurs avec leurs suppositions logiques pour tenter une effraction. Une attaque hybride mélange généralement des attaques par dictionnaire et par force brute. Ces attaques sont utilisées pour trouver des mots de passe combinés qui mélangent des mots courants avec des caractères aléatoires.

0day.today

0 Day exploit

- Une vulnérabilité logicielle récemment découverte avec aucune solution immédiate !
- Exploitation par les pirates,
- Difficile à interpréter,
- Demande une prise de décision immédiate,
- Le 0-Day peut aussi venir d'une faille créée sans intention par les administrateurs / développeur d'un système …

Contre-mesures:

- Consulter https://www.ssi.gouv.fr/agence/cybersecurite/ssi-en-france/les-cert-francais/
- Avis des fournisseurs
- Test de vulnérabilité régulier et surtout après modification !

https://askubuntu.com/questions/118273/what-are-icmp-redirects-and-should-they-be-blocked

ICMP REDIRECT

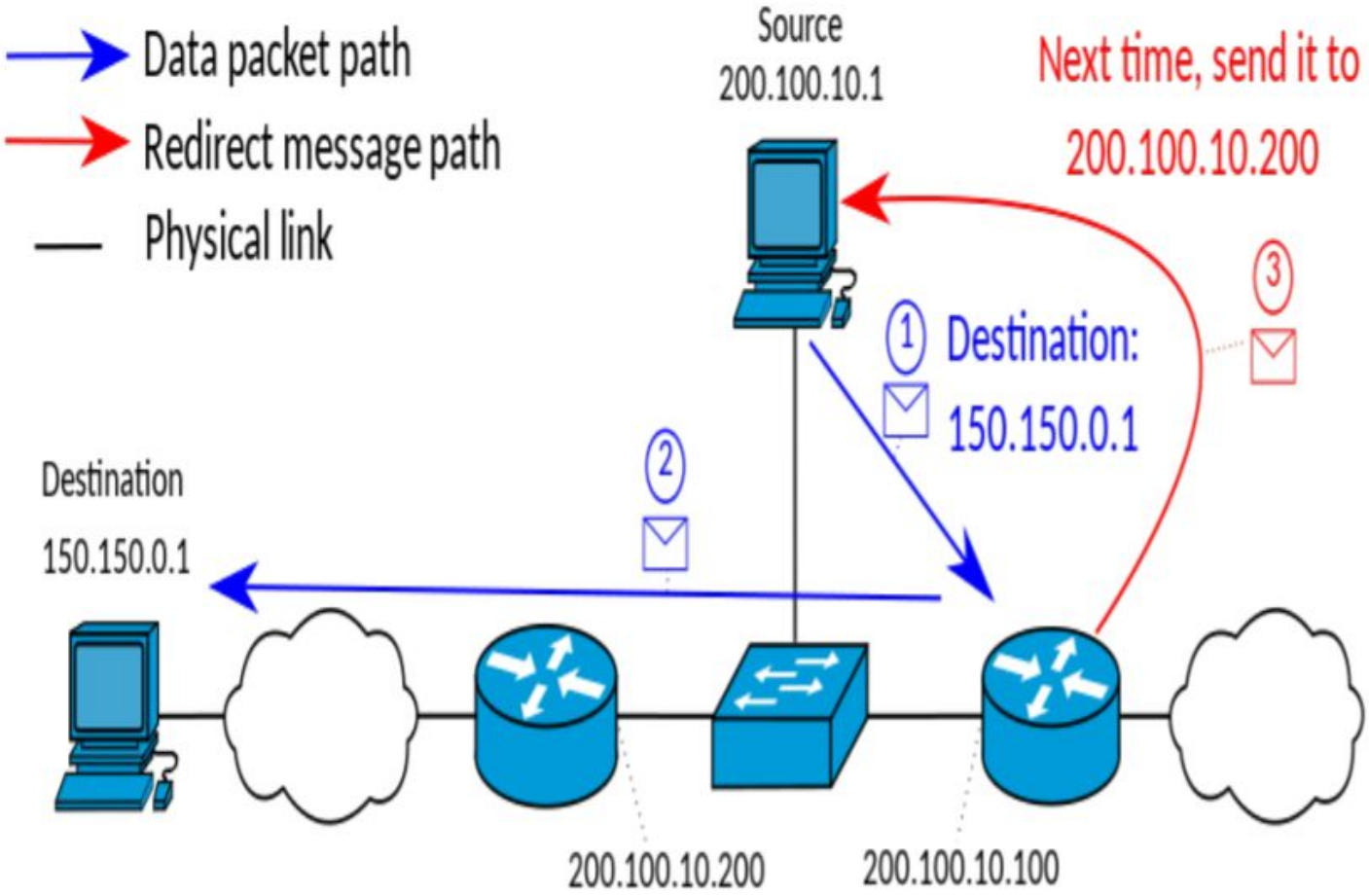
- Le protocole ICMP permet de rediriger les trafic en cas de problème sur le réseau (panne, congestion …),
- Il est possible de rediriger le trafic d'une machine de façon mal intentionné avec un paquet de type ICMP REDIRECT,

Contre-mesures:

- Les routeurs ne doivent pas accepter les paquets ICMP redirect,
- Les machines ne doivent pas accepter de paquets ICMP redirect, sous Linux désactiver IP FORWADING (par défaut sous Linux).

https://blog.securityevaluators.com/icmp-the-good-the-bad-and-the-ugly-130413e56030

ICMP REDIRECT

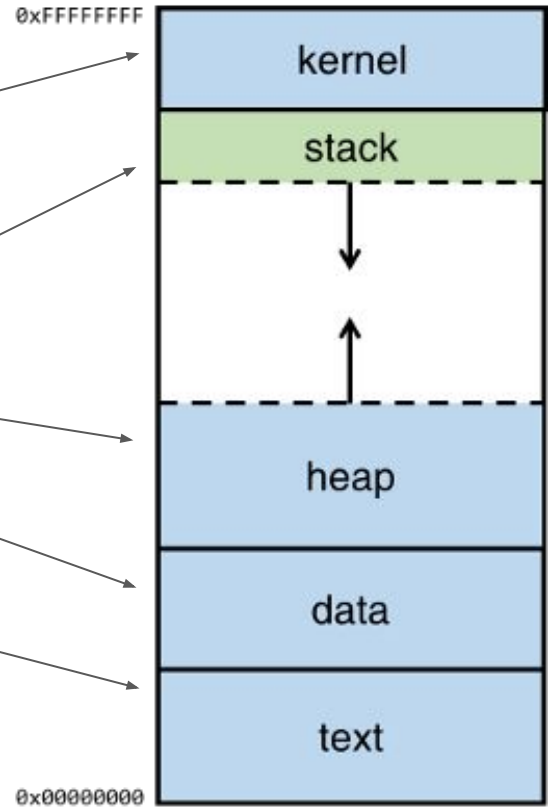


https://stackoverflow.com/questions/17775186/buffer-overflow-works-in-gdb-but-not-without-it

Buffer overflow

- **Principe**: Un débordement de tampon se produit lorsqu'un programme ou un processus tente d'écrire plus de données dans un bloc de mémoire de longueur fixe (un tampon) que le tampon n'est alloué pour en contenir.
- Un attaquant peut amener l'application à exécuter du code arbitraire, prenant éventuellement le contrôle de la machine.

- La partie supérieure de la mémoire est la zone du ***noyau*** , qui contient les paramètres de ligne de commande transmis au programme et les variables d'environnement.
- la pile contient les variables locales pour chacune des fonctions. Lorsqu'une nouvelle fonction est appelée, celles-ci sont poussées à la fin de la pile
- Au-dessus de la zone de données, se trouve le ***tas*** . Il s'agit d'une grande zone de mémoire où de gros objets sont alloués (comme des images, des fichiers, etc.)
- Les données , où les variables non initialisées et initialisées sont stockées.
- La zone inférieure de la mémoire est appelée **texte et contient le code réel**, les instructions machine compilées, du programme. Il s'agit d'une zone en lecture seule, car celles-ci ne doivent pas pouvoir être modifiées.



IP sourcing

- Un expéditeur d'un paquet IP peut forcer le chemin au lieu de prendre le meilleur routage possible,
- Les options d'en-tête Strict Source Route (SSR) et Loose Source Route (LSR) rarement utilisées sautorise le mécanisme de routage à la source,
- Dans l'IPv4, une liste partielle ou complète des nœuds sur le réseau peut être déterminée en utilisant respectivement les champs LSR et SSR.
- Dans ce cas, la liste d'adresses de nœud ne peut pas dépasser 40 octets de long, c'est-à-dire la taille maximale de la partie d'option IPv4 de l'en-tête. Cela permet de définir au maximum 9 nœuds de routage pour les réseaux IPv4.
- Le routage source n'est pas considéré comme sécurisé et, comme suggéré par l'IETF, il doit être désactivé par défaut sur les périphériques réseau et sur les systèmes d'exploitation.

https://www.kali.org/tools/sqlmap/

SQL Injection

- L'injection SQL est devenue un problème courant avec les sites Web basés sur des bases de données,
- L'attaque consiste à exécuter une requête SQL dans la base de données via les données d'entrée du client au serveur,
- Un exploit d'injection SQL réussi peut lire des données sensibles de la base de données, modifier (insérer, mettre à jour ou supprimer) des données de base de données, exécuter des opérations d'administration,
- Exemple:
  - "SELECT * FROM utilisateurs WHERE account = '" + userProvidedAccountNumber +"' ;"
  - "SELECT * FROM users WHERE account = '' or '1' = '1';"

https://www.cisco.com/c/en/us/products/wireless/what-is-wi-fi-security.html#~q-a

WIFI (Wireless Fidelity) / Méthodes de sécurisation

- Autre cryptage, le Wi-Fi Protected Access (WPA) utilise TKIP . WPA a été spécialement conçu pour fonctionner avec des équipements plus anciens,
- Le WPA2 plus sécurisé utilisant Advanced Encryption Standard,
- Une faille dans une fonctionnalité ajoutée au Wi-Fi en 2007, appelée Wi-Fi Protected Setup (WPS), permet de contourner la sécurité WPA et WPA2,
- Le cryptage Wi-Fi Protected Access (WPA2) est considéré comme sécurisé, à condition qu'une phrase de passe forte soit utilisée,
- En 2018, WPA3 a été annoncé en remplacement de WPA2.
- Il est possible aussi d'utiliser un VPN pour créer des tunnels sécurisés et protégés par l'identité entre les réseaux Wi-Fi non protégés et Internet.

WIFI (Wireless Fidelity)

- Les attaques du Wifi sont en partie identiques aux machines standards,
- Attaques DOS :
  - ‹ ‹ - Deauthentication
  - ‹ ‹ - Disassociation
  - ‹ ‹ - CTS-RTS attack
  - ‹ ‹ - Signal interference or spectrum jamming attack
- Obtenir un SSID secret : réaliser une écoute BEACON, car le SSID est donné lors de la connexion sur le point d'accès,
- Sniffer le réseau pour obtenir les adresses MAC.

https://www.kali.org/tools/skipfish/

Website crawler software (robot d'exploration de site Web)

- Le spidering comporte plusieurs facettes : chercher et trouver l'information, construire des mots clés par site pour une attaque de mot de passe …
- Un site web est parfois très complexe:
  - Liens externes,
  - Liens intranet,
  - Liens directes,
  - http / https,
  - code: HTML, CSS, Javascript, Flash … → analyse du code JS
  - robots
  - structure …

https://www.kali.org/tools/skipfish/

Website crawler (robot d'exploration de site Web)

- Il faut comprendre les liaisons entre les sites pour pouvoir mener des attaques plus performantes:
  - Les mots clés pour constituer plus tard un dictionnaire d'attaque de mot de passe,
  - La logique des liens entre les sites,
  - Les possibles rebonds d'un site à un autre,
  - Les liens entre Internet et intranet …

https://www.kali.org/tools/skipfish/

Analyse d'un site Web / Command skipfish

```
$ skipfish -o sni http://192.168.0.29


skipfish version 2.10b by lcamtuf@google.com

  - 192.168.0.29 -

Scan statistics:

      Scan time : 0:00:01.694
  HTTP requests : 2578 (1522.5/s), 1302 kB in, 485 kB out (1055.0 kB/s)
    Compression : 6 kB in, 21 kB out (55.3% gain)
    HTTP faults : 0 net errors, 0 proto errors, 0 retried, 0 drops
 TCP handshakes : 43 total (60.4 req/conn)
     TCP faults : 0 failures, 0 timeouts, 5 purged
 External links : 4 skipped
   Reqs pending : 20

Database statistics:

         Pivots : 10 total, 9 done (90.00%)
    In progress : 0 pending, 0 init, 1 attacks, 0 dict
  Missing nodes : 1 spotted
     Node types : 1 serv, 2 dir, 6 file, 0 pinfo, 1 unkn, 0 par, 0 val
   Issues found : 2 info, 0 warn, 0 low, 0 medium, 0 high impact
      Dict size : 13 words (13 new), 1 extensions, 256 candidates
     Signatures : 77 total

[+] Copying static resources...
[+] Sorting and annotating crawl nodes: 10
[+] Looking for duplicate entries: 10
[+] Counting unique nodes: 7
[+] Saving pivot data for third-party tools...
[+] Writing scan description...
[+] Writing crawl tree: 10
[+] Generating summary views...
[+] Report saved to 'sni/index.html' [0xef0e73cd].
[+] This was a great day for science!
```

https://securitytrails.com/blog/google-hacking-techniques

WEB engineering / Google

Manipulation de la base de données :

– "Welcome to phpMyAdmin" AND "Create new database"

– "Select a database to view" intitle: "filemaker pro"

– "# Dumping data for table (username|user|users|password)" -site: mysql.com -cvs

– "# Dumping data for table (username|user|users|password)" –site: mysql.com -cvs

Rapport de sécurité du réseau :

– "Network Host Assessment Report" "Internet Scanner"

– "Host Vulnerability Summary Report"

– "This file was generated by Nessus" || intitle:"Nessus Scan Report" -site:nessus.org

https://securitytrails.com/blog/google-hacking-techniques

WEB engineering / Google / Caméra

Manipulation de caméra :

inurl:indexFrame.shtml Axis

intitle:”Live View / - AXIS”

intitle:”Live View / - AXIS” | inurl:view/view.sht

intitle:liveapplet inurl:LvAppl

intitle:”The AXIS 200 Home Page”

intext:”MOBOTIX M1” intext:”Open Menu”

intitle:”WJ-NT104 Main Page”

inurl:”ViewerFrame?Mode=”

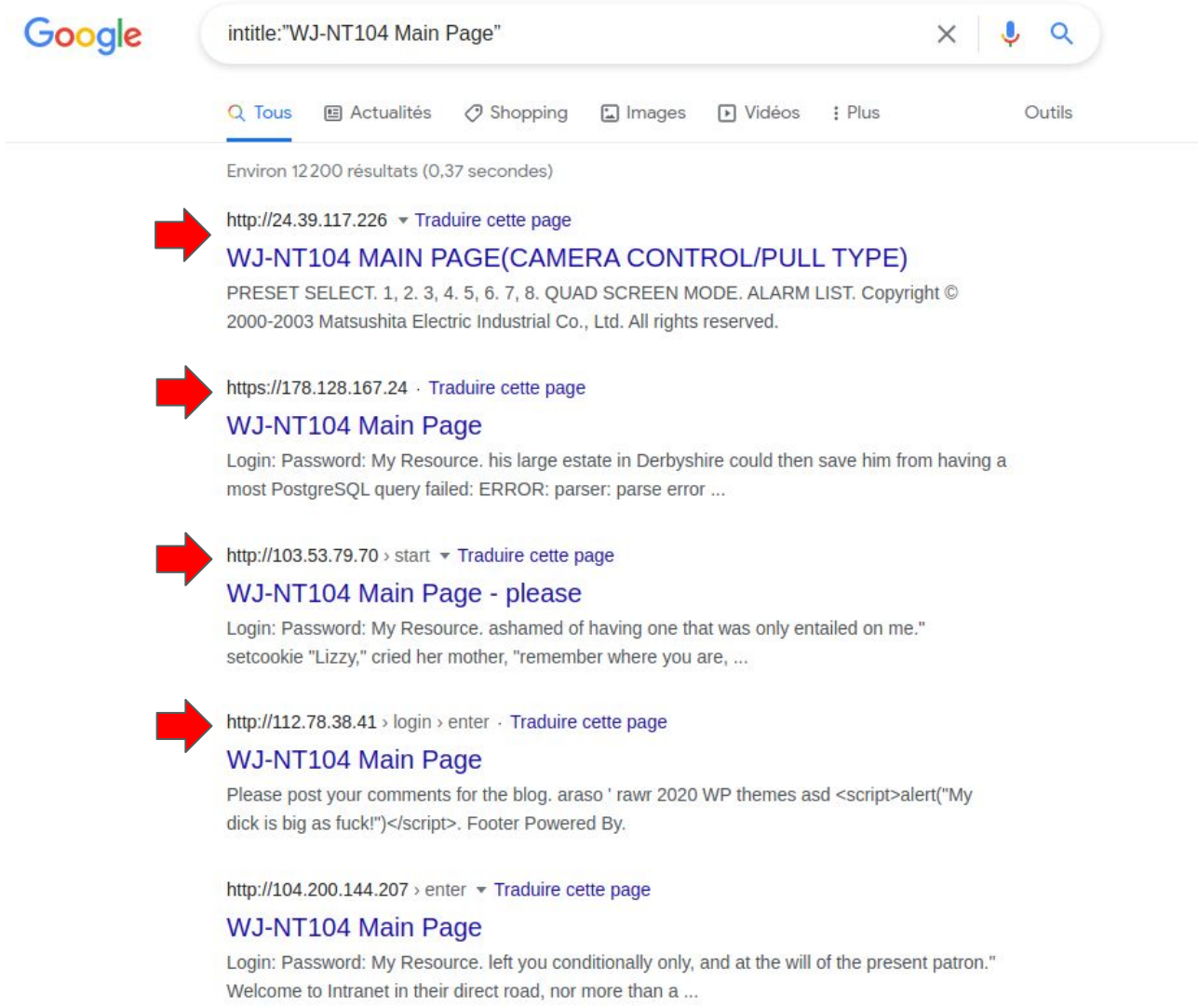
SNC-RZ30 HOME

intitle:flexwatch intext:”Home page ver”

intitle:snc-z20 inurl:home/

“powered by webcamXP” “Pro|Broadcast”

intitle:”remote ui:top page”

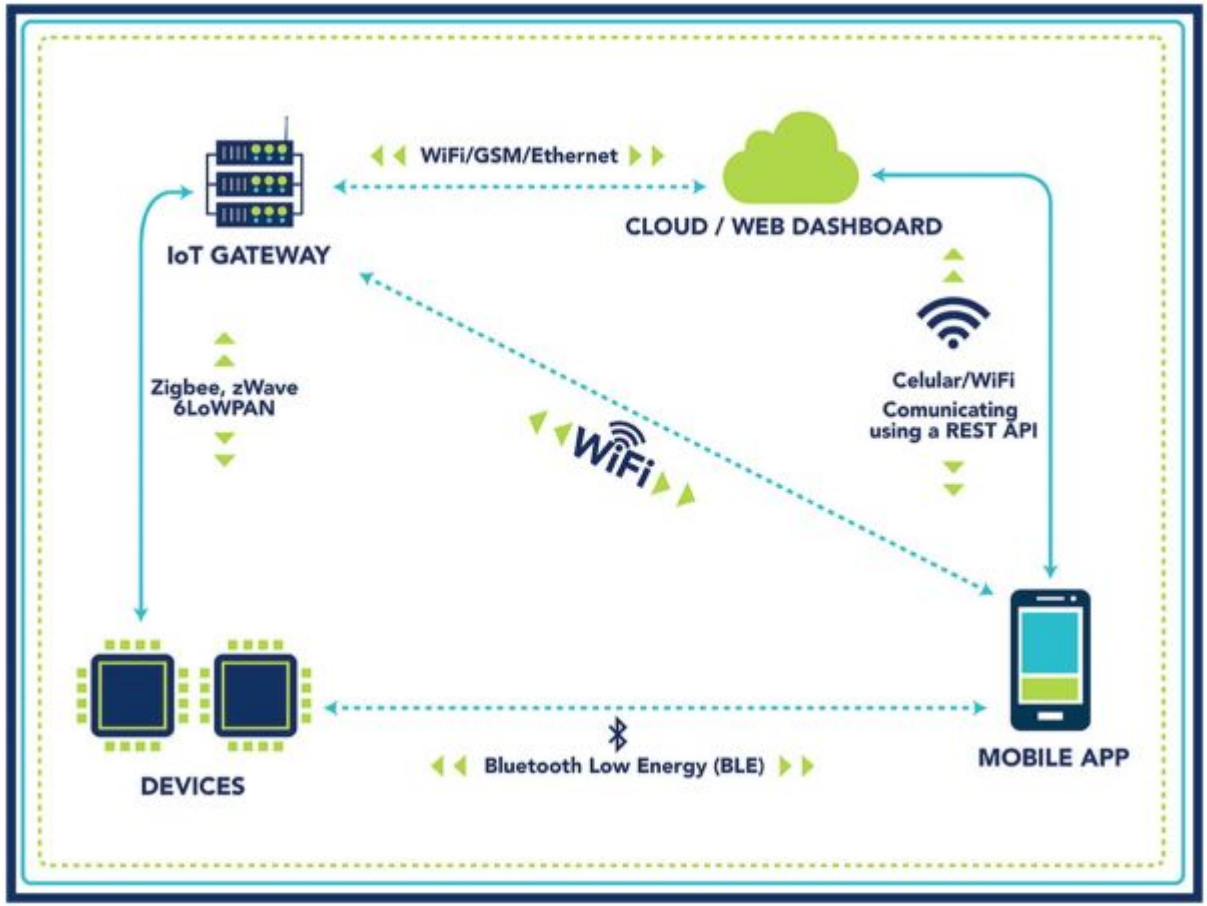


https://thehackernews.com/search/label/hardware%20hacking

IoT / Architecture et protocoles

Utilisation d'une architecture spécifique avec une gateway

Vecteur d'attaque: Gateway



Outils de piratage et éthique

https://techlog360.com/top-ethical-hacking-operating-systems/
https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_tools.htm

Outils éthiques / Open Source

- Kali Linux,
- Parrot Security OS,
- BackBox,
- BlackArch,
- Fedora Security Lab,
- Dracos Linux
- Network Security Toolkit (NST),
- DemonLinux,
- Live Hacking OS,
- DEFT Linux,
- Samurai Web Testing Framework …

Outils de piratage et éthique

https://www.kali.org/
https://www.kali.org/docs/introduction/what-is-kali-linux/

KALI

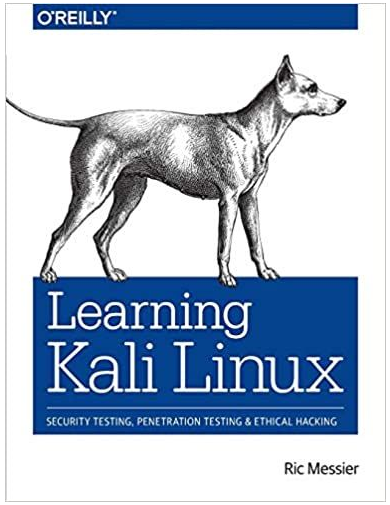
- Kali Linux (anciennement connu sous le nom de BackTrack Linux),
- Distribution Linux open-source basée sur Debian destinée aux tests de pénétration avancés et à l'audit de sécurité,
- Contient plusieurs centaines d'outils destinés à diverses tâches de sécurité de l'information,
- Solution multiplateforme, accessible et disponible gratuitement,
- Il existe de nombreuses solutions d'utilisation: virtuelle, bare metal, cloud, ARM.

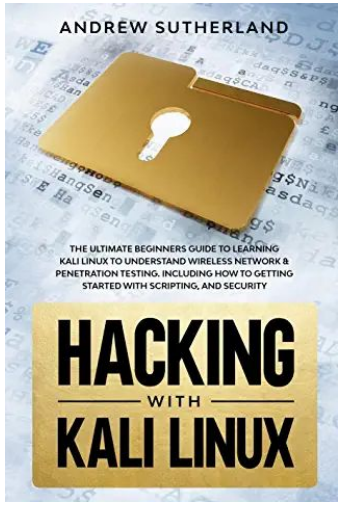
Outils de piratage et éthique

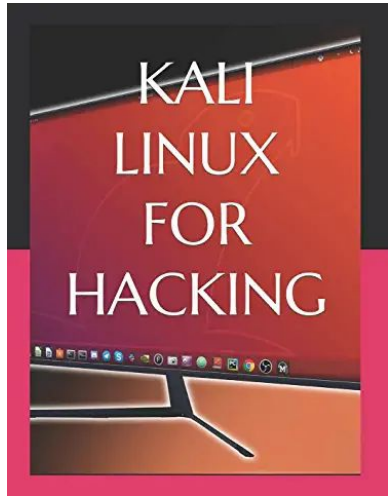
https://www.kali.org/tools/
https://www.kali.org/docs/

KALI / Outils && Docs

- Tous les outils ne sont pas forcément installés,
- Il faut utiliser les commandes Debian pour la mise à jour des packages,
- La documentation en ligne est très riche, avec de nombreux exemples de mise en oeuvre,
- Il existe aussi des ouvrages de référence sur Kali:







Scanner / Définition

- Un scanner est un programme qui balaye une plage de ports TCP ou UDP sur un ensemble de machines,
- Le but est d'établir la liste des couples machine/services ouverts,
- TCP ouvre une session en émettant un SYN et attend la réponse SYN/ACK,
- UDP n'ouvre pas de session mais émet un datagramme et attend une réponse,
- Il existe neuf types de scan de port TCP:
  - Vanilla connect()
  - Half-open SYN flag
  - Inverse TCP flag
  - ACK flag probe
  - TCP fragmentation
  - FTP Bounce
  - Proxy Bounce
  - Sniffer-based spoofed
  - IP ID header

https://nmap.org/book/man-os-detection.html

Scanner / Identification des OS

```
$ sudo nmap -O scanme.nmap.org
[sudo] Mot de passe de fred :
Starting Nmap 7.80 ( https://nmap.org ) at 2022-01-17 17:01 CET
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.18s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    open     http
9929/tcp  open     nping-echo
31337/tcp open     Elite
Device type: general purpose|WAP|storage-misc|webcam|media device
Running (JUST GUESSING): Linux 2.6.X|3.X|4.X (93%), Ubiquiti embedded (93%), HP embedded (89%), Tandberg embedded (89%), Ubiquiti
AirOS 5.X (89%), Infomir embedded (89%)
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:2.6.32 cpe:/h:ubnt:airmax_nanostation
cpe:/o:linux:linux_kernel:4 cpe:/h:hp:p2000_g3 cpe:/o:ubnt:airos:5.2.6 cpe:/h:infomir:mag-250
Aggressive OS guesses: Linux 2.6.32 - 3.13 (93%), Ubiquiti AirMax NanoStation WAP (Linux 2.6.32) (93%), Linux 2.6.22 - 2.6.36
(91%), Linux 3.10 - 4.11 (91%), Linux 3.10 (91%), Linux 2.6.32 (90%), Linux 3.2 - 4.9 (90%), Linux 2.6.32 - 3.10 (90%), Linux
2.6.18 (90%), Linux 3.16 - 4.6 (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 11 hops
```