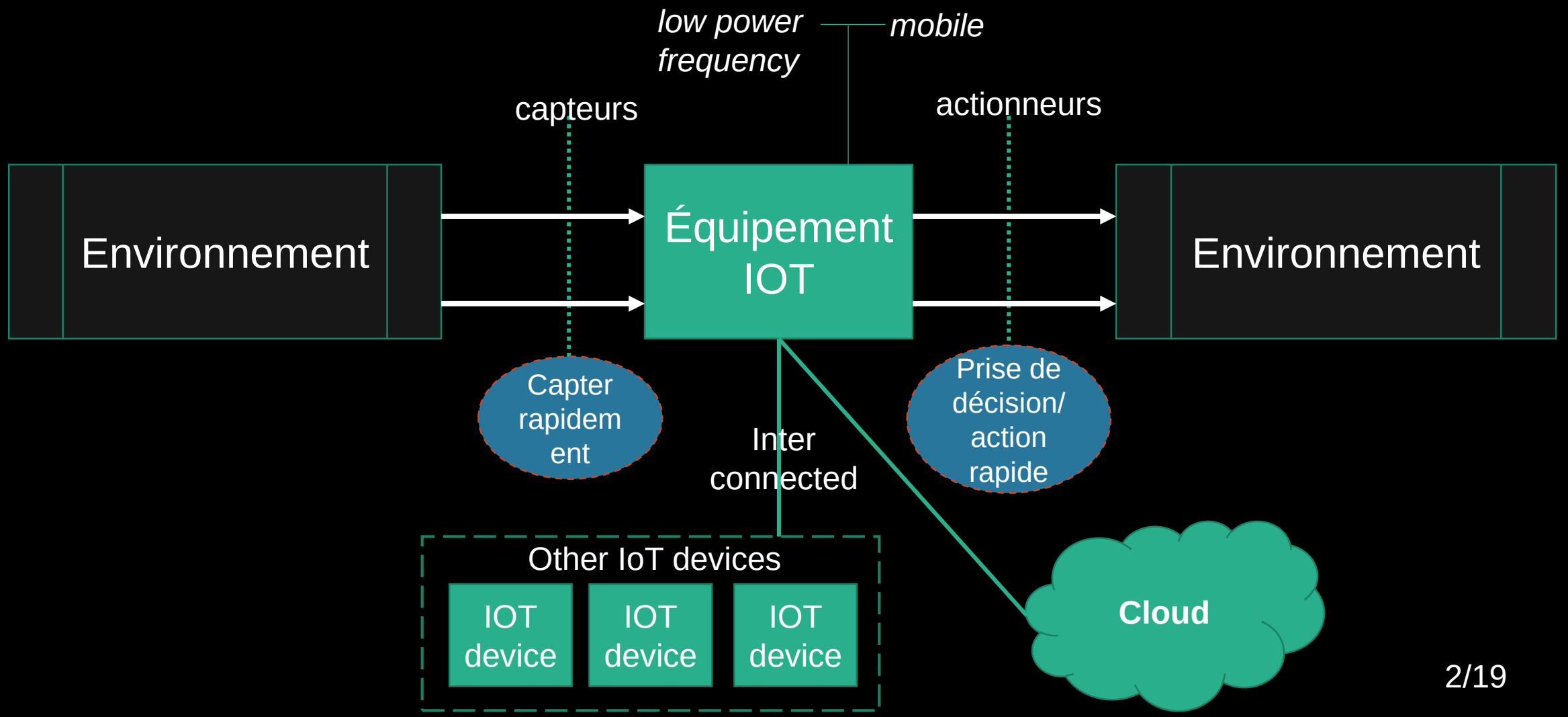
Attention à la communication

ESIR – SRIO

Djob Mvondo

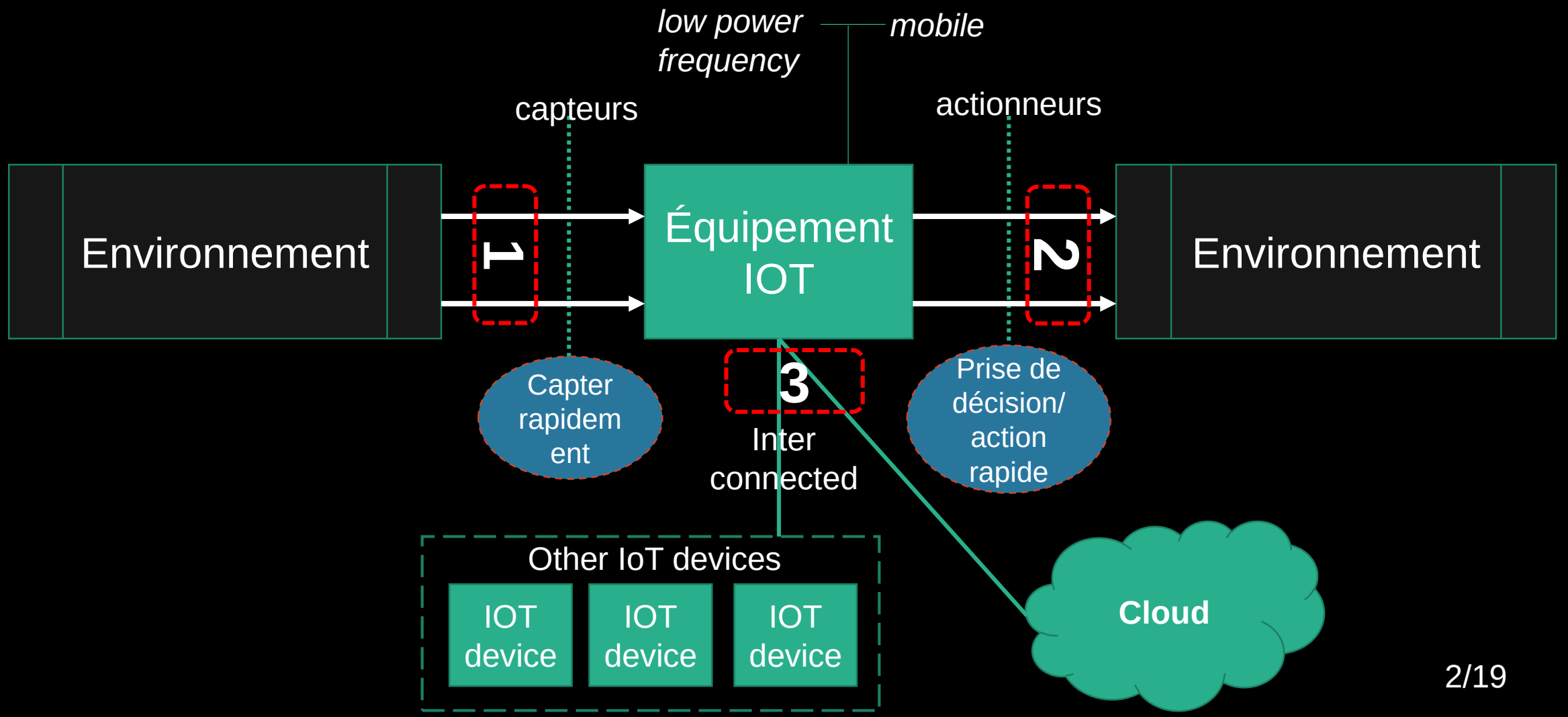
IOT: Internet of Things

- L'interconnexion engendre des failles



IOT: Internet of Things

- L'interconnexion engendre des failles – pourquoi ?



Communication

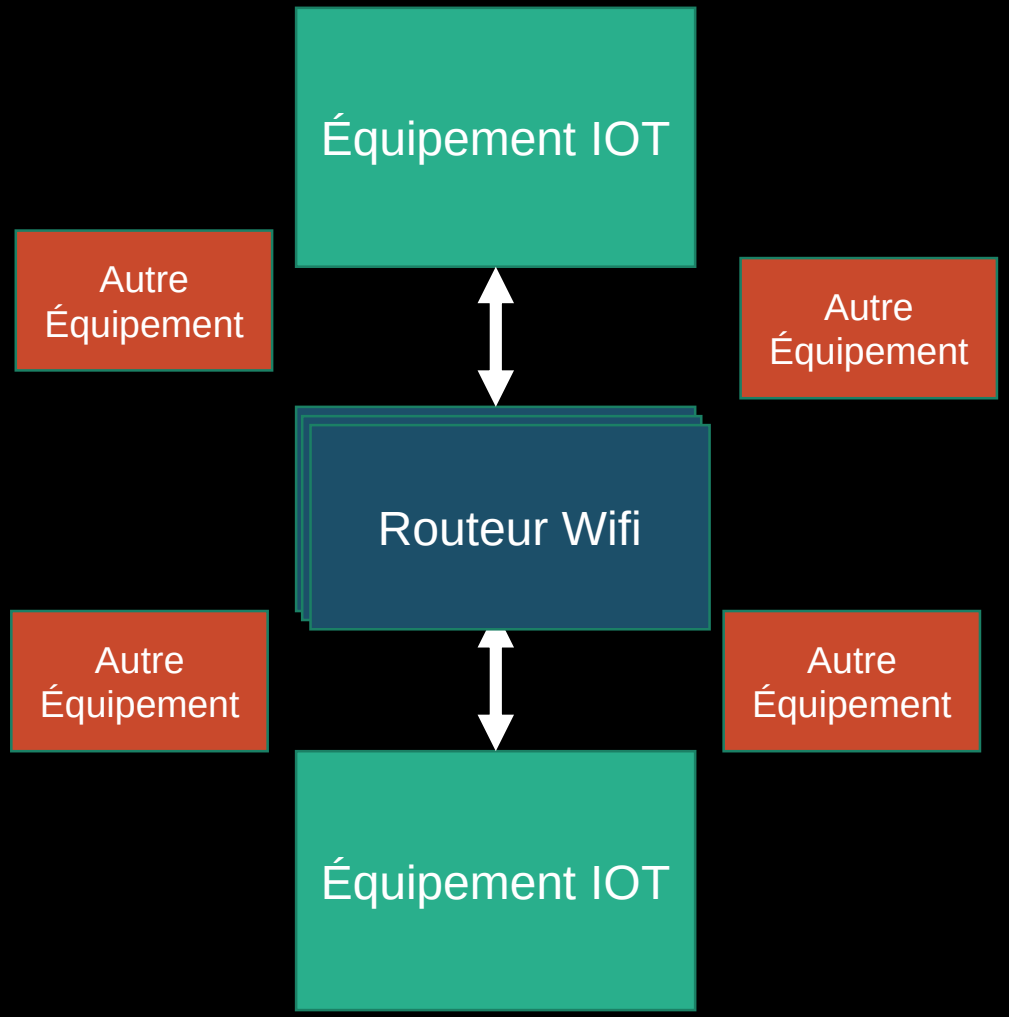
- Analogie avec une soirée/fête
- Vous ne connaissez pas tout le monde …
- Comment faîtes vous pour communiquer ?

Quelles sont les problématiques ?

Communication

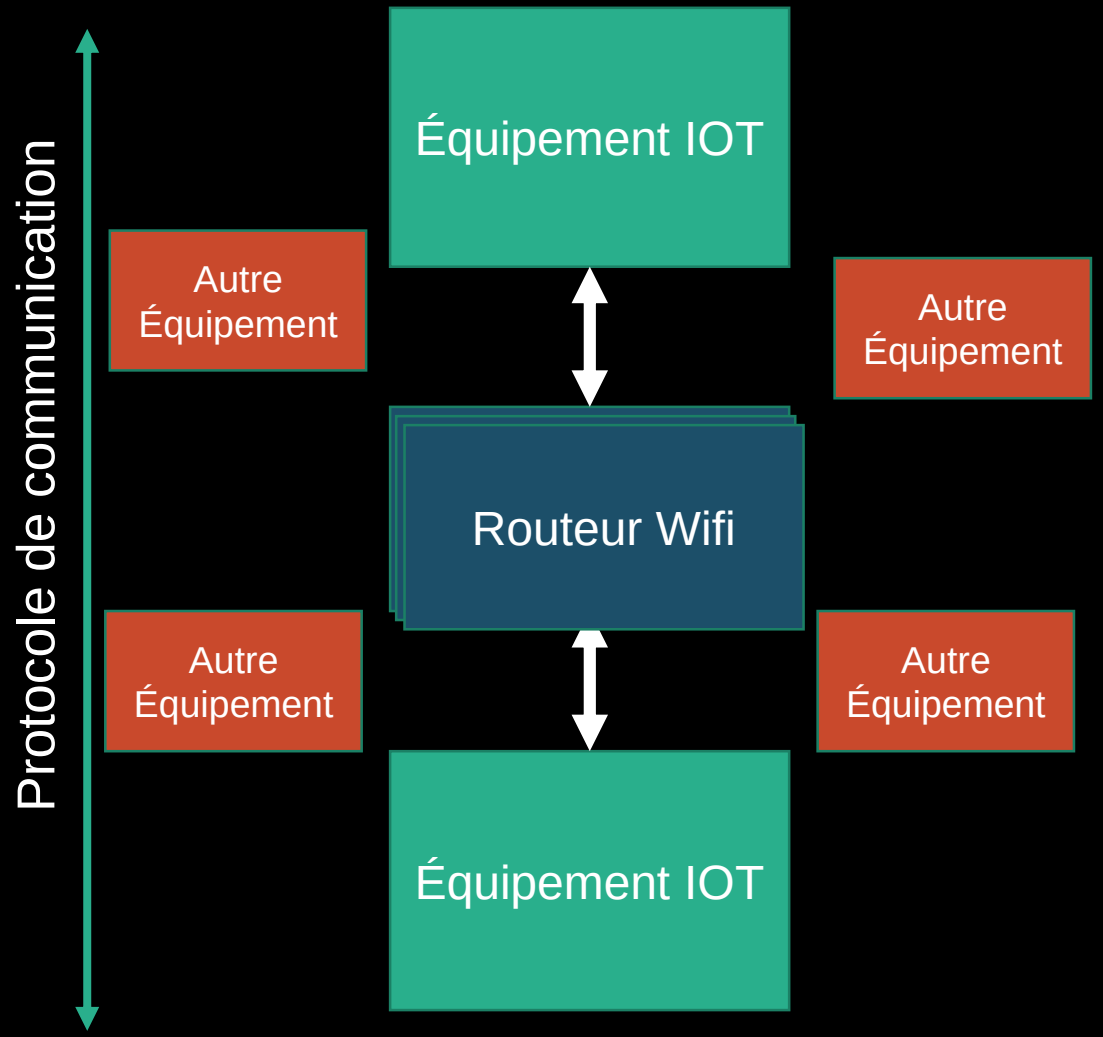
- La langue …
- Echange codifiée ?
- Les espions/espionnes

Communication



Problématique similaire avec un réseau wifi public utilisé par des équipements IoT

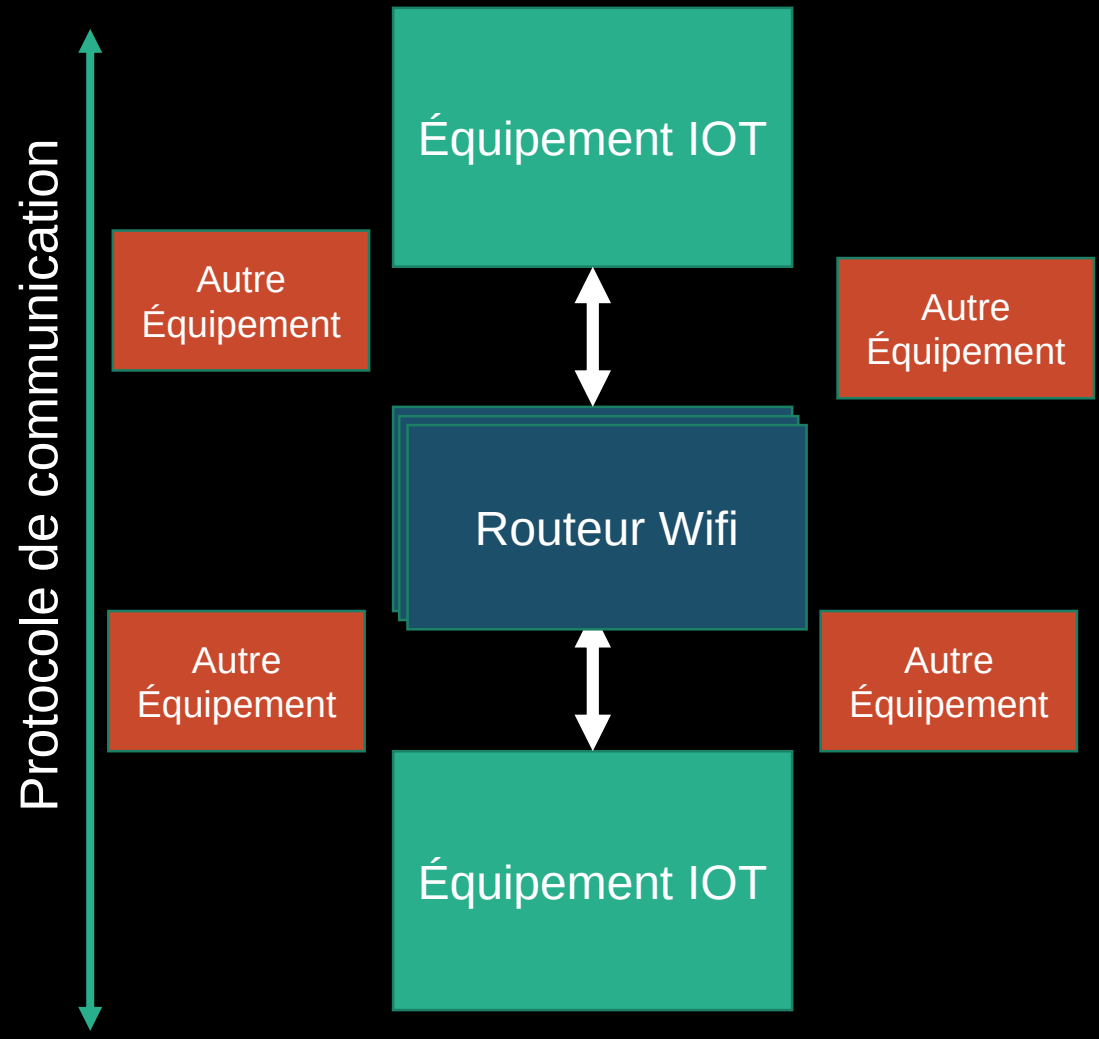
Communication



Un début de solution avec le **protocole de communication**

Le protocole de communication

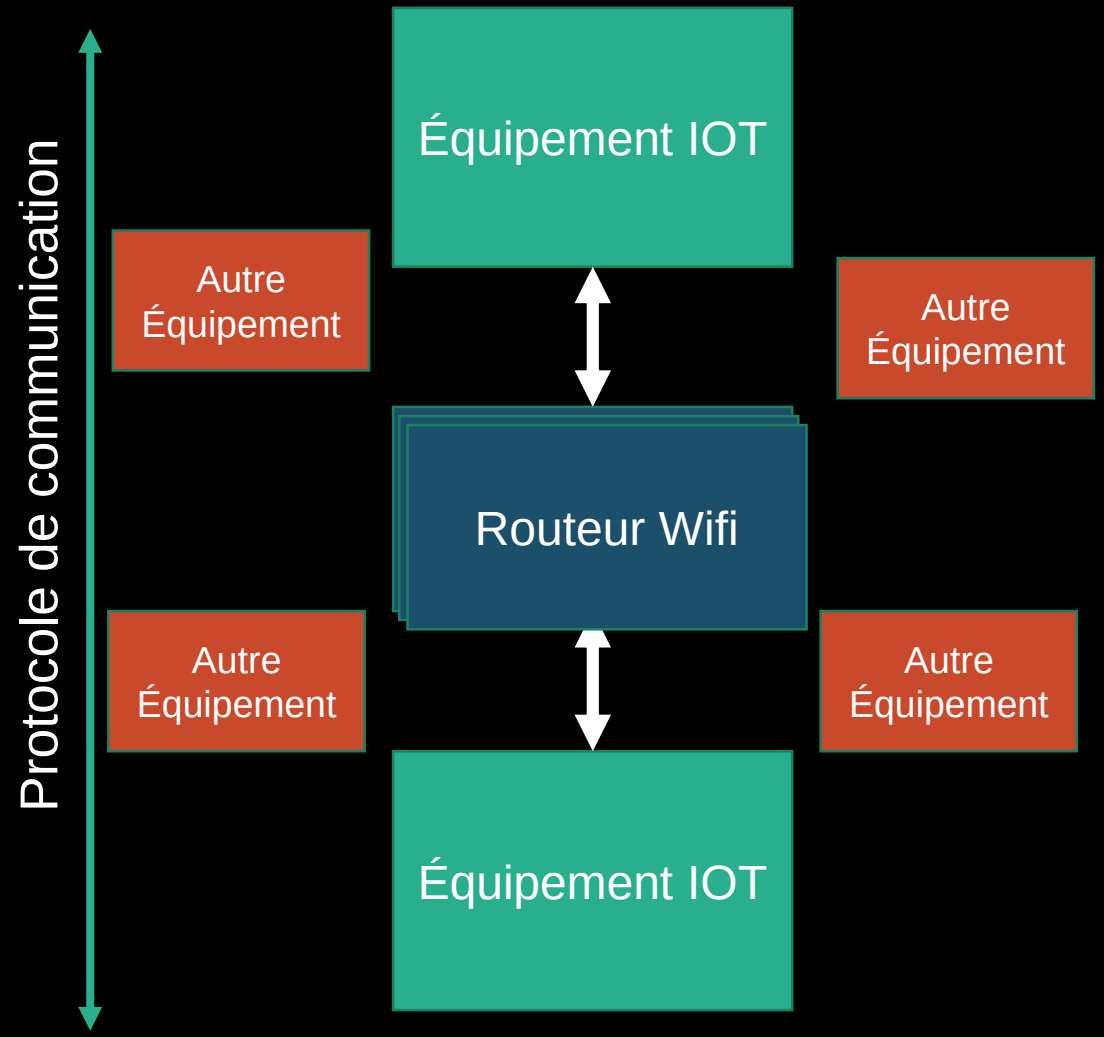
Permet un socle commun afin d'initialiser les échanges (même format)



Le protocole de communication

Permet un socle commun afin d'initialiser les échanges (même format)

Définit les standards pour authentifier un équipement au réseau

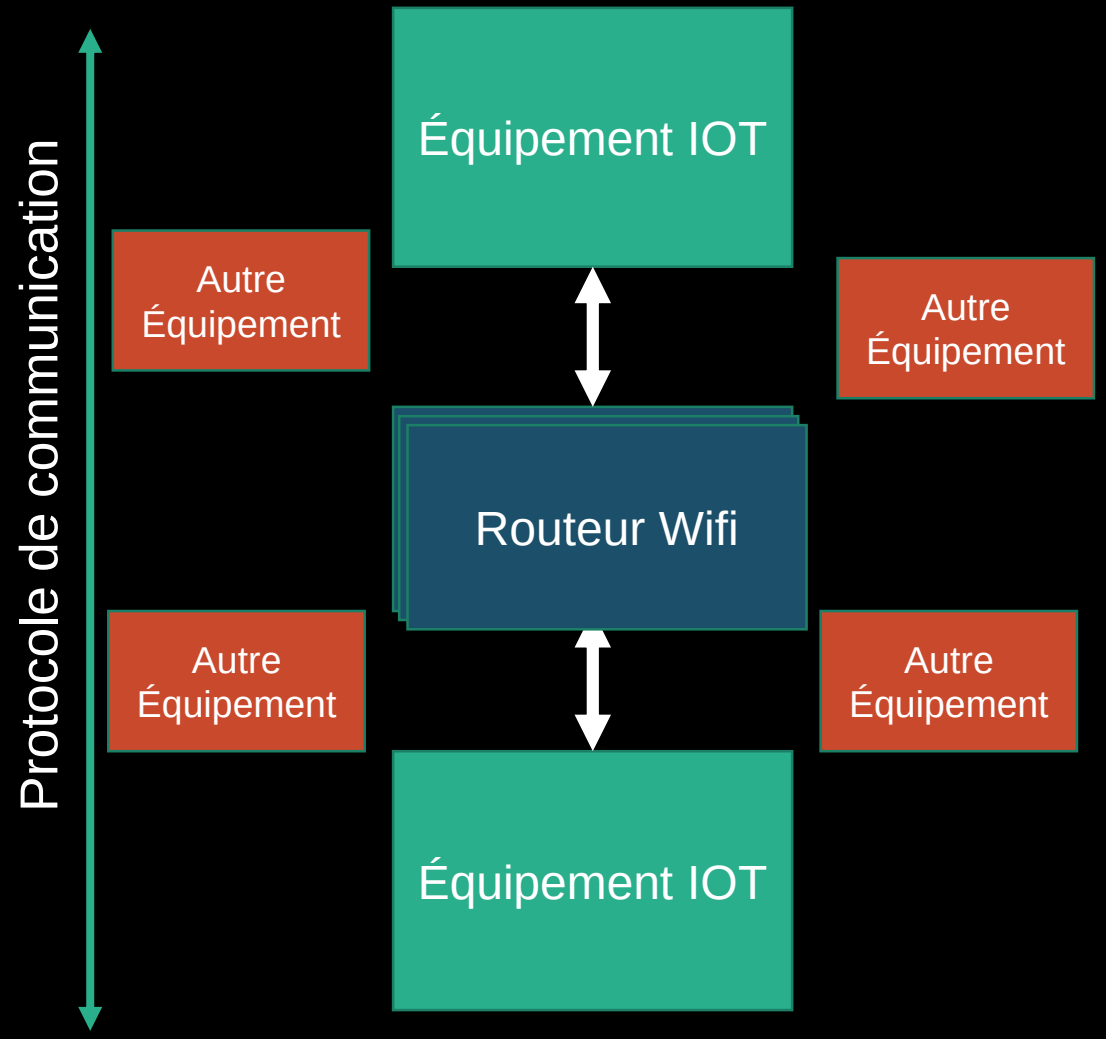


Le protocole de communication

Permet un socle commun afin d'initialiser les échanges (même format)

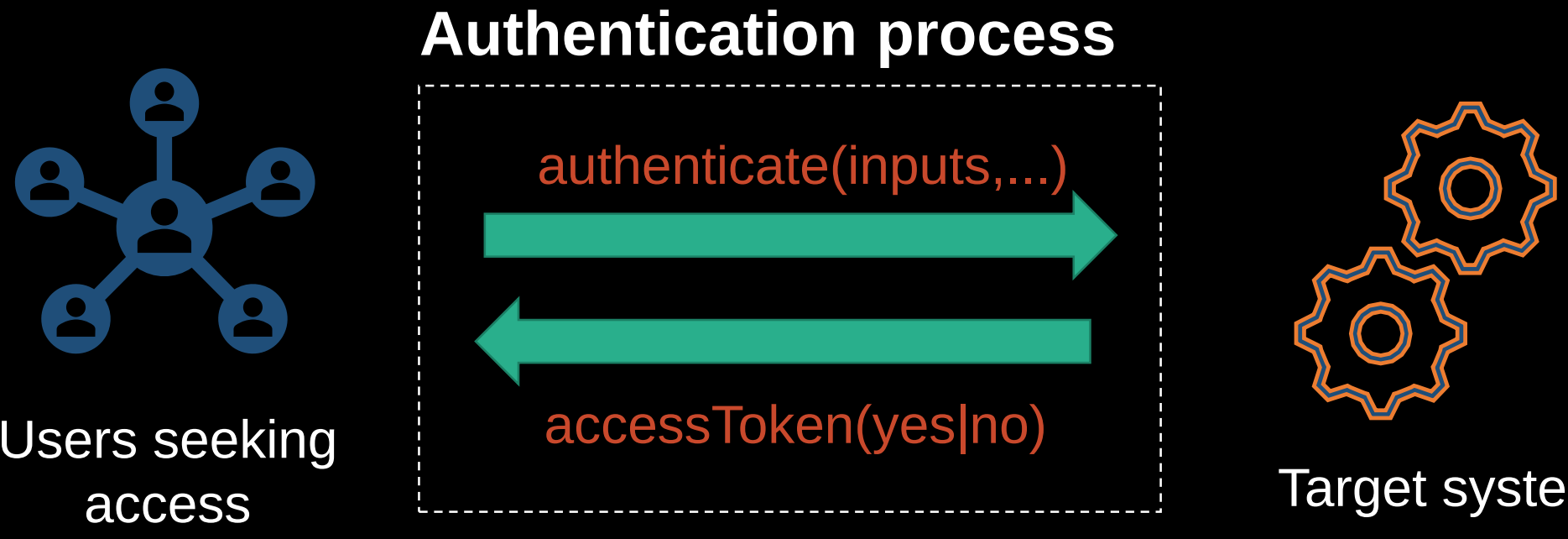
Définit les standards pour authentifier un équipement au réseau

Impose une politique afin de sécuriser et protéger l'intégrité des échanges



Le protocole de communication

L'authentification est le mécanisme qui permet à une entité de donner un **niveau d'accès** à un système.



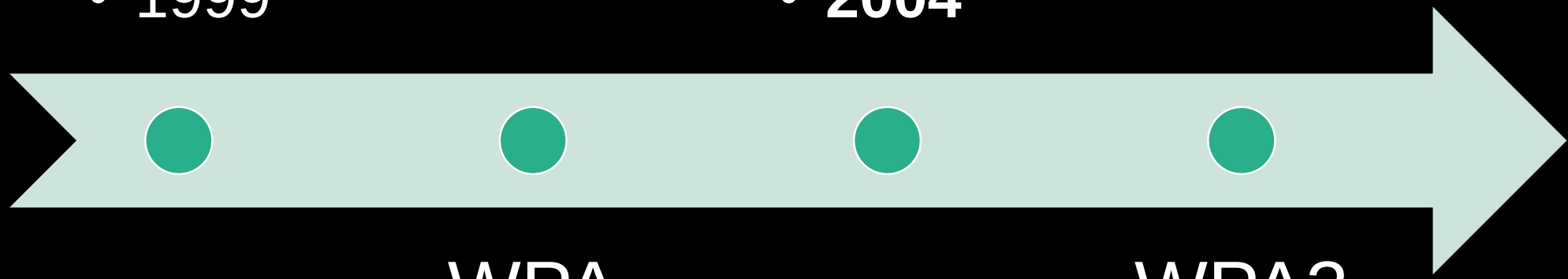
Le protocole de communication

Un protocole de communication WIFI est plus complexe à élaborer et à maintenir qu'un protocole de communication filaire.

Les ondes électromagnétiques appartiennent à tout le monde

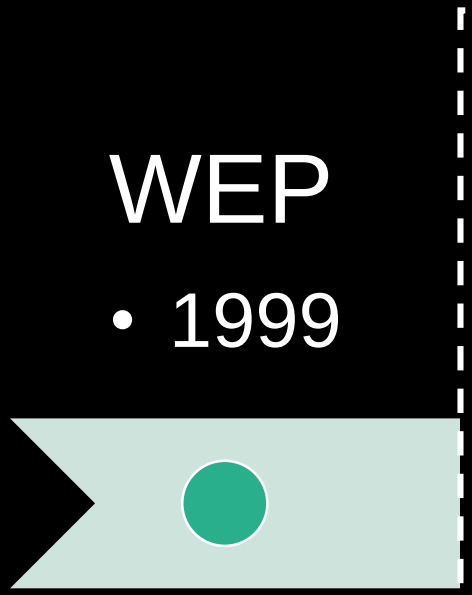
Authentification dans un réseau WiFi

Les protocoles sont ratifies par un consortium qui définis les standards technologiques des équipements reseau. L'une des plus connues – **IEEE** avec le consortium **IEEE 802.11**



Authentification dans un réseau WiFi

WEP: Wired Equivalent Privacy



WEP

- 1999

10, 26, 32, or 58 hexadecimal digit keys

Rivest Cipher 4 (RC4) stream cipher

Officially abandoned in 2004

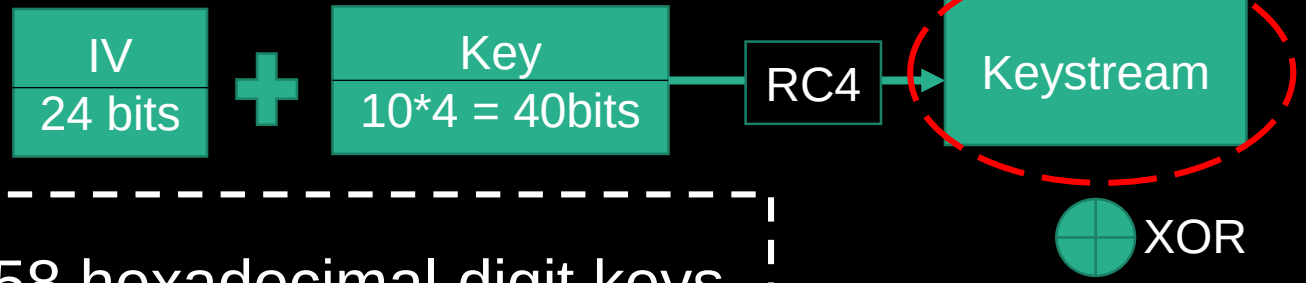
Several exploits known

Shared key is the same per device

Authentification dans un réseau WiFi

La cible principale des attaques …

WEP: Wired Equivalent Privacy



WEP

- 1999

10, 26, 32, or 58 hexadecimal digit keys

Rivest Cipher 4 (RC4) stream cipher

Officially abandoned in 2004

Several exploits known

Shared key is the same per device

Authentification dans un réseau WiFi

WAP2/3: Wifi Protection Access

WiFi Protection Access

256 hexadecimal **dynamic** digit keys

TKIP (Temporal Key Identification protocol) algorithm

Still widely supported by adaptaters

Several exploits known

WPA2

- **2004**

WPA3

- 2018

Authentification dans un réseau WiFi

Le chiffrement a un cout

Pour chaque phrase, je dois:

- Choisir un dialecte spécial - **clé**
- Valider avec l'interlocuteur (l'ensemble des interlocuteur) – **transmission de la clé**
- Traduire chaque phrase et l'exprimez – **chiffrement + transmission**
- L'interlocuteur doit décoder avant de vous répondre – **chiffrement + transmission**

Chiffrement

Authentification dans un réseau WiFi

Le chiffrement a un cout

Pour chaque phrase, je dois:

- Choisir un dialecte spécial - **clé**
- Valider avec l'interlocuteur (l'ensemble des interlocuteur) – **transmission de la clé**
- Traduire chaque phrase et l'exprimez – **chiffrement + transmission**
- L'interlocuteur doit décoder avant de vous répondre – **chiffrement + transmission**

Chiffrement

Pas de chiffrement

Pour chaque phrase, je dois:

- Parler ☺ - transmission

Authentification dans un réseau WiFi

Le chiffrement a un coût

Pour chaque phrase, je dois:

- Choisir un dialecte spécial - **clé**
- Valider avec l'interlocuteur (l'ensemble des interlocuteur) – **transmission de la clé**
- Traduire chaque phrase et l'exprimez – **chiffrement + transmission**
- L'interlocuteur doit décoder avant de vous répondre – **chiffrement + transmission**

Le chiffrement impacte le temps de transmission
→ **algorithmes optimisés**

Plus la clé est longue, plus elle mettra du temps à être casser mais plus de contraintes physiques
→ **espace de stockage et puissance de calcul**

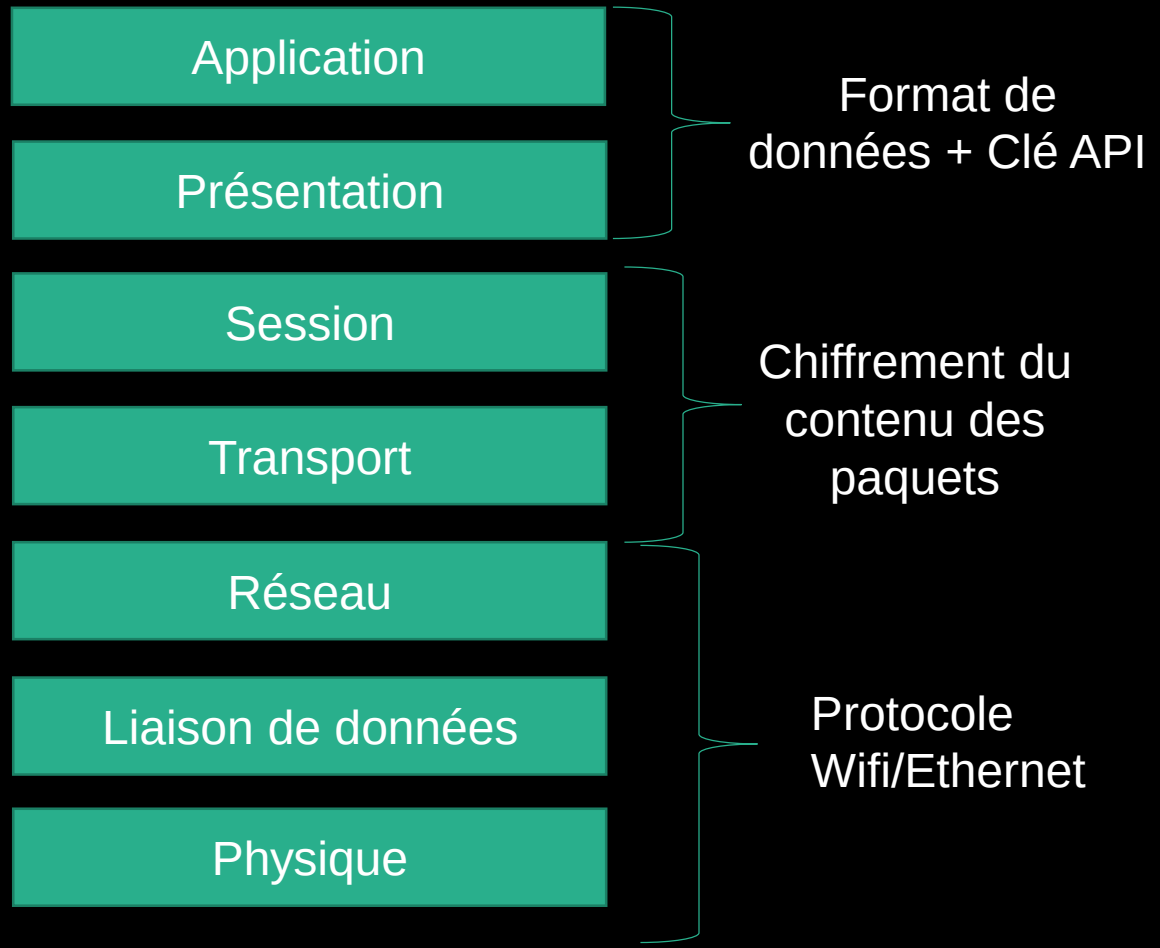
Authentification dans un réseau WiFi

Le chiffrement a un cout quelque soit la couche concernée

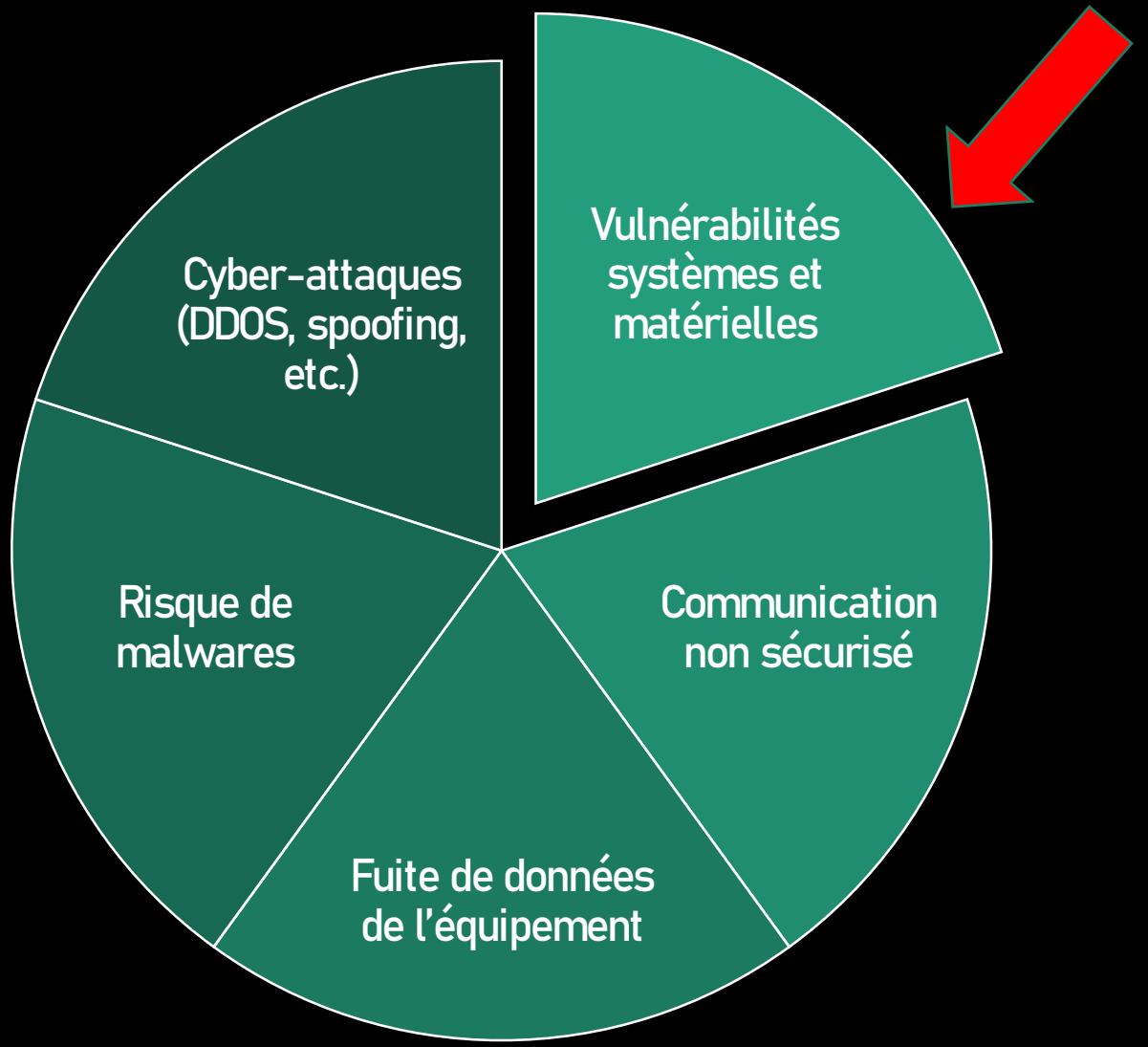
Très souvent, la force brute est couteuse et incertaine.

Nombre de combinaisons pour des clés de 64 et 256 charactères ?

Des alternatives qui exploitent le fonctionnement du protocole



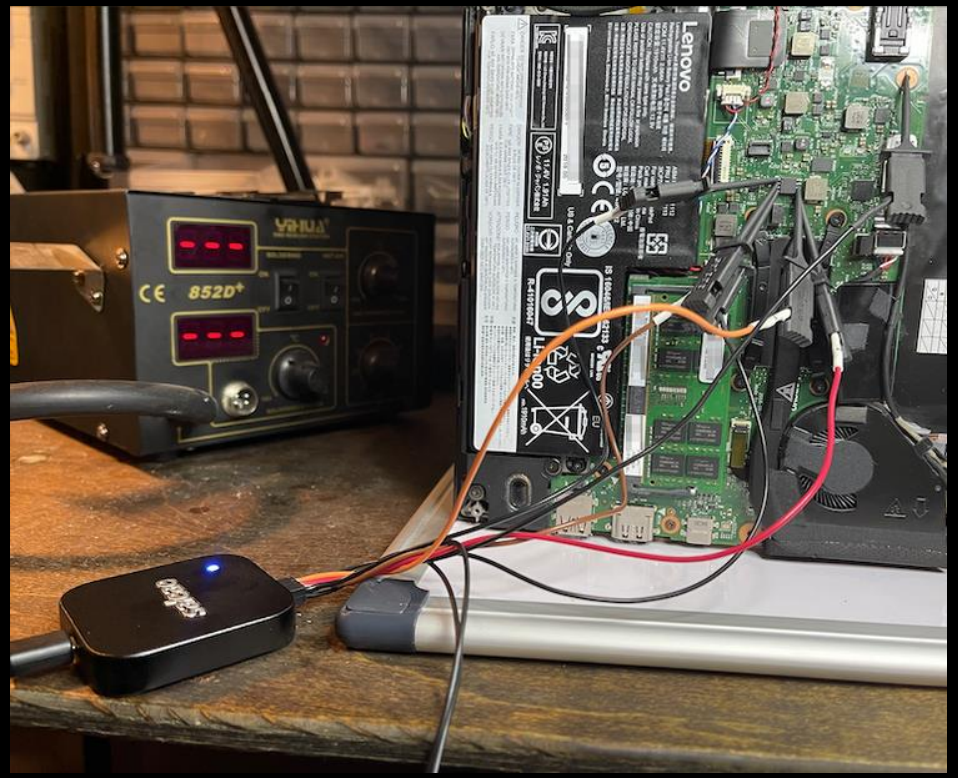
Exploiter les protocoles de communication



Exploiter les protocoles de communication

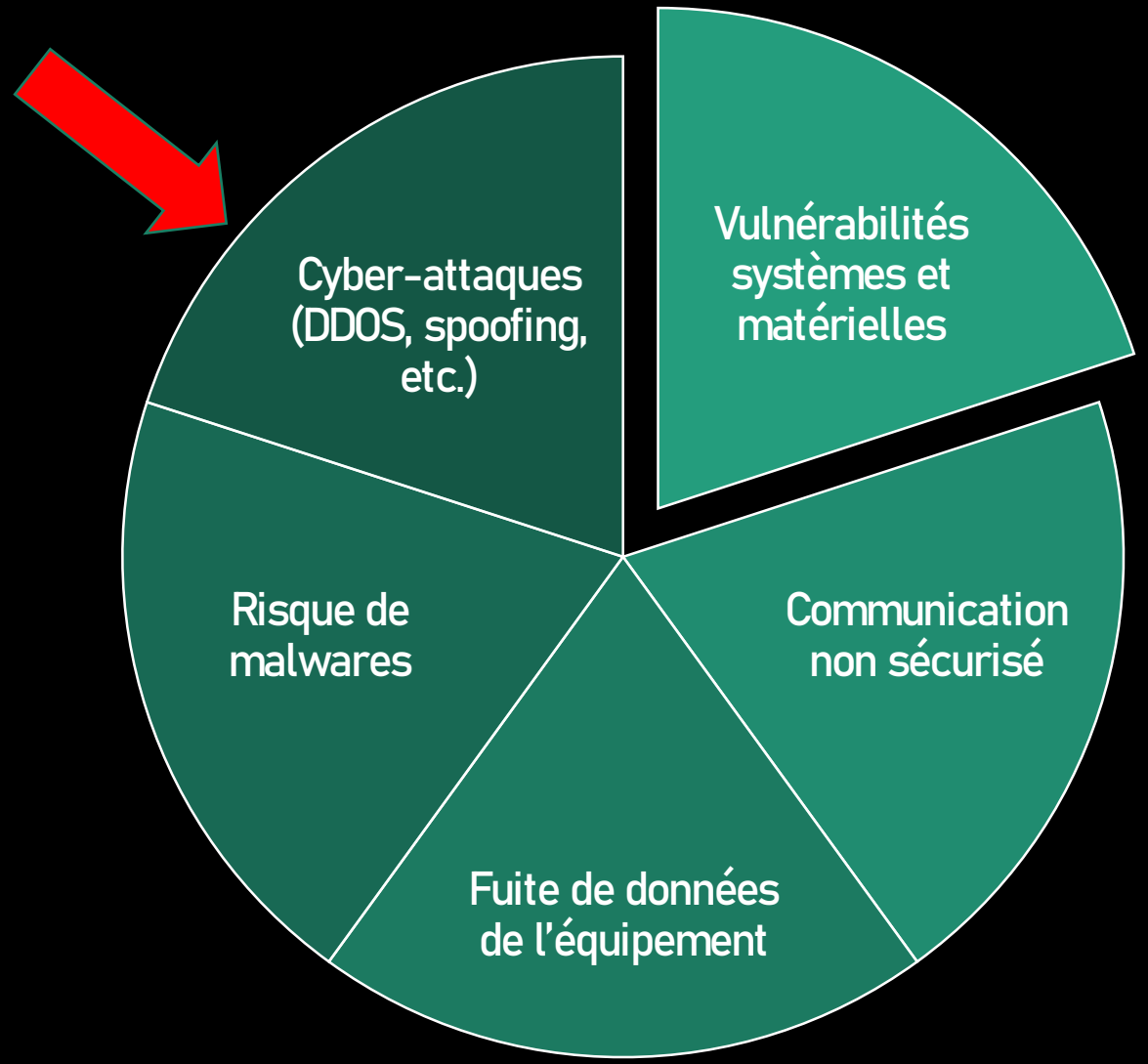
Extraire les clés en ayant un **accès physique** aux équipement du réseau

SPI is a communication protocol for embedded systems and is extremely common amongst virtually all hardware. Due to its simplicity, there is no encryption option for SPI. Any encryption must be handled by the devices themselves. At the time of this writing BitLocker does not utilize any encrypted communication features of the TPM 2.0 standard, which means any data coming out of the TPM is coming out in plaintext, including the decryption key for Windows. If we can grab that key, we should be able to decrypt the drive, get access to the VPN client config, and maybe get access to the internal network.



https://twitter.com/0xdea/status/1568897268136431616?s=20&t=AZGungLlyX_t4YPjzAsC_A

Exploiter les protocoles de communication



Exploiter les protocoles de communication

Accéder à l'interface d'administration des équipements réseau.

Ces pages sont généralement protéger par une page d'authentification, les utilisateurs laissent par mégarde les logins standards fournies par le constructeur

Exploiter les protocoles de communication

Accéder à l'interface d'administration des équipements réseau.

Ces pages sont généralement protéger par une page d'authentification, les utilisateurs laissent par mégarde les logins standards fournies par le constructeur

Login: admin Password: admin	Login: default Password: 12345	Login: admin Password: 0000	Login: root Password: root

Exploiter les protocoles de communication

Accéder à l'interface d'administration des équipements réseau.

Ces pages sont généralement protéger par une page d'authentification, les utilisateurs laissent par mégarde les logins standards fournies par le constructeur

Login: admin Password: admin	Login: default Password: 12345	Login: admin Password: 0000	Login: root Password: root

15% of network + IOT devices operate with default settings --- companies and individuals

Exploiter les protocoles de communication

La prochaine fois → DDOS + SPOOFING + MOTM