Introduction à la sécurité des objets connectés

DISCLAIMER

Ceci n’est pas un objet connecté: c’est un ordinateur muni d’une caméra, il se protège comme tous système informatique connecté à l’Internet.

Une attaque en 3 mots

QUOI ?

- Cible de l'attaque : l'objet, le réseau, le cœur de réseau, le backend, l'utilisateur …
- Chaque point du système doit être étudié de façon spécifique. Surinvestir sur un point particulier se fait à perte.

COMMENT ?

- Par une intervention directe sur le vecteur
- A distance, quelques km à plusieurs milliers de km
- Ecoute, brouillage, modification, usurpation d'identité
- …

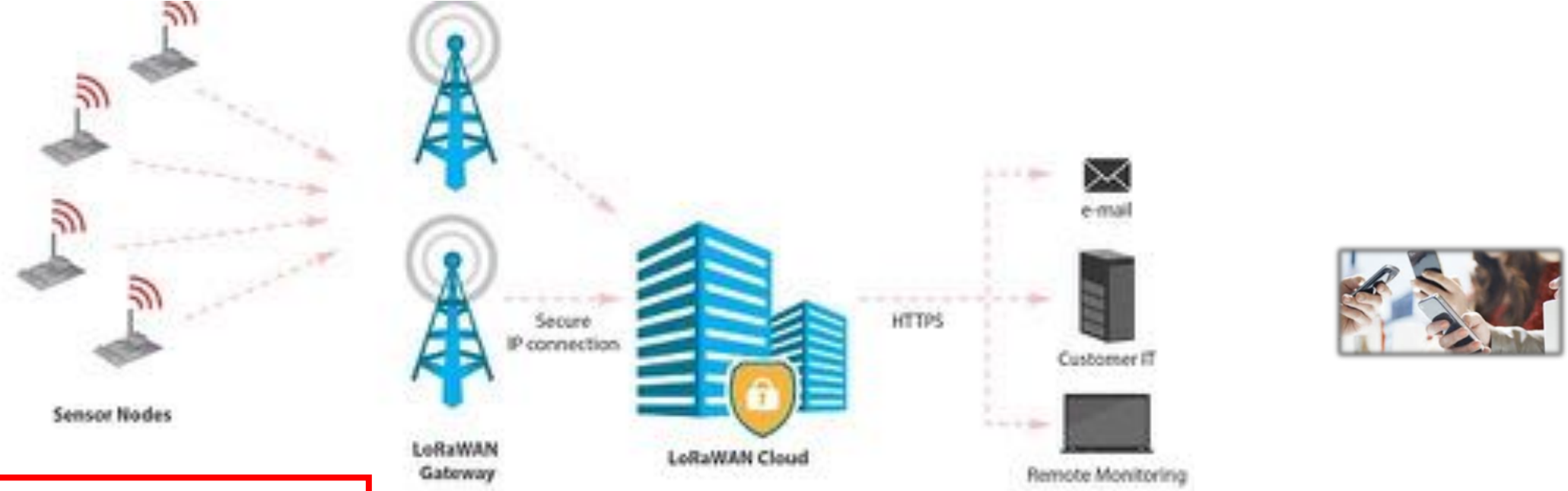
POURQUOI ?

- Pour l'argent, pour nuire, pour la gloire, pour le fun ?
- En fonction les moyens et les risques sont variés.

Objets → Réseau LPWAn → Réseau Opérateur → Cœur de réseau → Back-end solution → Réseau Opérateur → Front-end application

La surface d'attaque des objets connectés (LPWAn)

L'objet est souvent mis en avant comme le principal élément attaqué. C'est à la mode et un certain laxisme existe. Mais la sécurité touche tout autant le protocole radio, le cœur de réseau qui stocke l'ensemble des données, et surtout les application en backend/front-end qui stockent l'ensemble des données traduites. Ce dernier point n'est pas spécifique aux objets connectés mais reste la plus grande surface d'attaque et la plus facile d'accès pour un pirate qui peut agir à distance avec des outils classiques, sur des failles déjà connus.



Objets	Réseau LPWAn	Réseau Opérateur	Cœur de réseau	Back-end solution	Front-end application
Contact physique ou proximité requise pour agir. Difficile à mettre à jour. Des failles spécifiques à chaque objet	Accessible à une distance de quelques mètres à des dizaines de km. Repose en partie sur un standard partagé: des failles communes	3GPP, Internet, largement utilisé, aussi beaucoup attaqué et surveillé par de nombreux états.	Accessible depuis Internet, concentre toutes les données. Repose sur des technos standards.	Accessible depuis Internet, concentre toutes les données. Repose sur des technos standards.	Fonctionne sur un Smartphone ou un ordinateurs classique et sujet aux failles habituelles de ce type d'environnement

Des risques et approches différentes en chaque point

Attaque sur l'objet

Demande un accès physique ou de proximité à l'objet en utilisant ses interfaces : BLE, Serial port ou autre protocole utilisé par l'objets. Excluons le réseau LPWAn qui sera traité plus tard.

Comment ?

En utilisant les mécanismes de mise à jour, en effectuant une manipulation physique, en modifiant le hardware, ou en ajoutant une extension.

Pourquoi ?

Pour vous demander un rançon débloquant vos capteurs.
Pour voler vos données.
Pour détruire ce que l'objet contrôle.

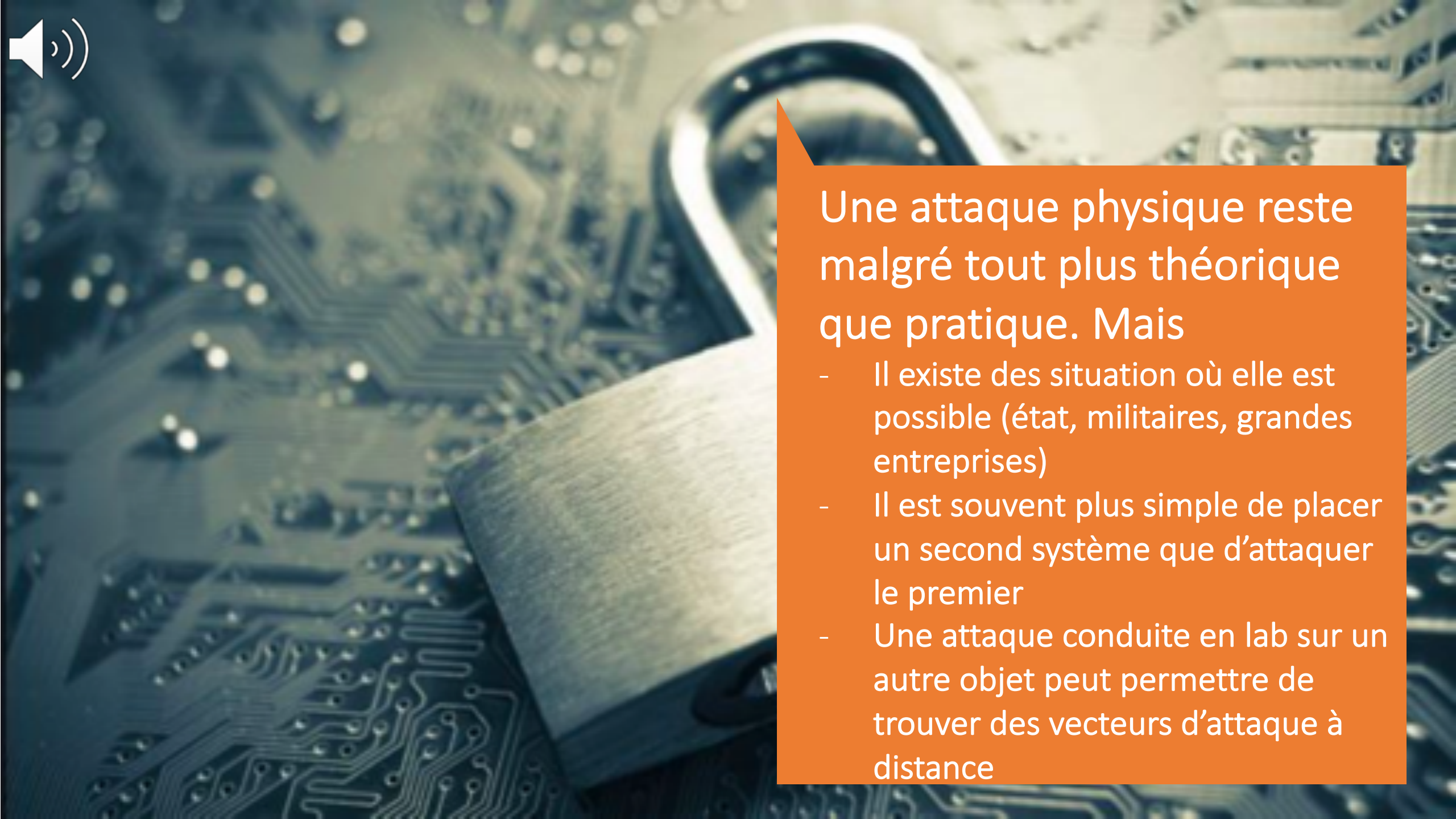
Un thermostat connecté hacké qui élève la température à 37°C si vous ne payez pas …

Un thermostat connecté hacké qui élève la température à 37°C si vous ne payez pas …

Everything in the thermostat runs with **root** privileges. "**We got command injection by the SD card**, so it was a local attack," Tierney explained. "With root, you can set off alarm (and set the frequency very high) and can heat and cool at the same time."
While this was a local attack, it also isn't impossible to pull this off without gaining physical access to the device. The thermostat owner can use the SD card to load custom settings or wallpaper

Il n’y a pas de limite dans le possible d’une attaque physique sur le Hardware!

Mais il est toujours possible d’éviter les bêtises de base…



Une attaque physique reste malgré tout plus théorique que pratique. Mais

- Il existe des situation où elle est possible (état, militaires, grandes entreprises)
- Il est souvent plus simple de placer un second système que d'attaquer le premier
- Une attaque conduite en lab sur un autre objet peut permettre de trouver des vecteurs d'attaque à distance

To do or not to do …

Les choses à faire:

- Utiliser des clefs qui soient uniques par objet.
- Une clef calculée est déjà mieux qu'une clef en dur.
- Protéger les clefs stockées en flash par un simple XOR est déjà mieux que rien.
- Nettoyer les variables qui ont stockées des clefs après usage.
- Bloquer les accès JTAG et Série en production.
- Assurer pas plusieurs moyens l'authenticité d'un firmware avant chargement.
- Réfléchir comme un hacker et au besoin soumettre l'objet à des hacker avant d'aller en production.

Les choses à ne pas faire:

- Croire que personne n'accédera à votre code source (lire Ghost in the wires K. Mitnick)
- Croire que vous pourrez corriger les problèmes une fois en production. (cf shodan.io)
- Croire que parce qu'il n'y a aucun enjeu personne ne va casser votre solution.
- Croire que parce qu'il n'y a aucun enjeu vous arriverez à convaincre que la sécurité n'est pas un point d'importance.
- Croire que votre solution est fiable parce que vous avez beaucoup investi dans sa sécurisation.

Attaque sur le réseau

Une attaque qui peut se faire à une certaine distance et donc facilite la procédure en limitant les risques pour l'attaquant. Accessible donc à des enjeux moins importants.

Comment ?

En écoutant ou communiquant sur les ondes radio utilisées par l'objet.
En se faisant passer pour l'objet ou le réseau, en perturbant les communications…

Pourquoi ?

Pour connaitre des secrets industriels, suivre des personnes ou matériels.
Pour détruire une machine, cambrioler une maison.
Pour atteindre l'image du fabriquant des objets.

Plusieurs approches

Ecouter le réseau

- Pour voler les données qui circulent
- Toute RF peut être écoutée à distance, ici plusieurs dizaines de km.

Emettre sur le réseau

- Pour donner un ordre à un objet
- Pour se faire passer pour un autre objet

Perturber le réseau (jamming)

- Pour empêcher un objet de communiquer
- Pour empêcher la réception d'une commande

Ecouter le réseau

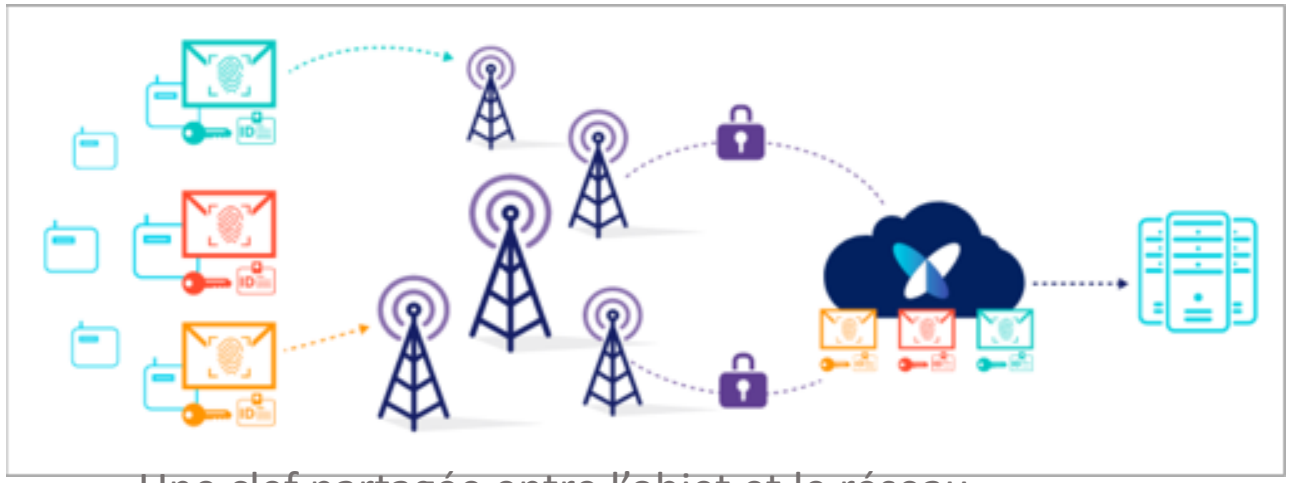
sigfox

- Réseau asymétrique
- La réception à distance demande une technologie SDR qui n'est pas à ce jour facilement accessible au quidam.
- Ceci n'a rien d'impossible et sera possible dans un temps très proche (6 mois à 5 ans)
- Par défaut les données sont transmises en clair.
- Une couche de chiffrement peut être ajoutée soit au niveau réseau, soit au niveau applicatif.

LoRaWAN™

- Réseau symétrique
- La réception demande le même matériel que l'émission et est donc accessible à tous.
- Une couche de chiffrement est ajoutée lors des échanges de données.

Chiffrement sur les réseaux LPWAn



Une clef partagée entre l'objet et le réseau pour sécuriser les communications

Unique pour chaque objet; échangée ou dérivée

Sigfox

La clef utilisée s'appuie sur la clef privée utilisée pour le calcul HMAC

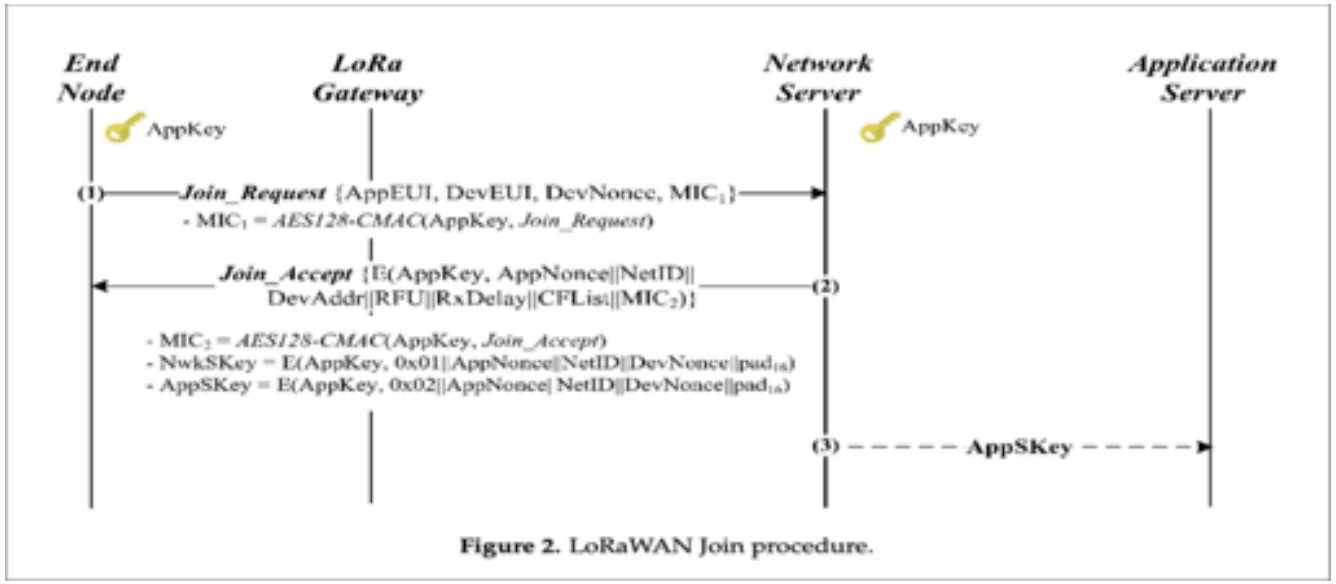
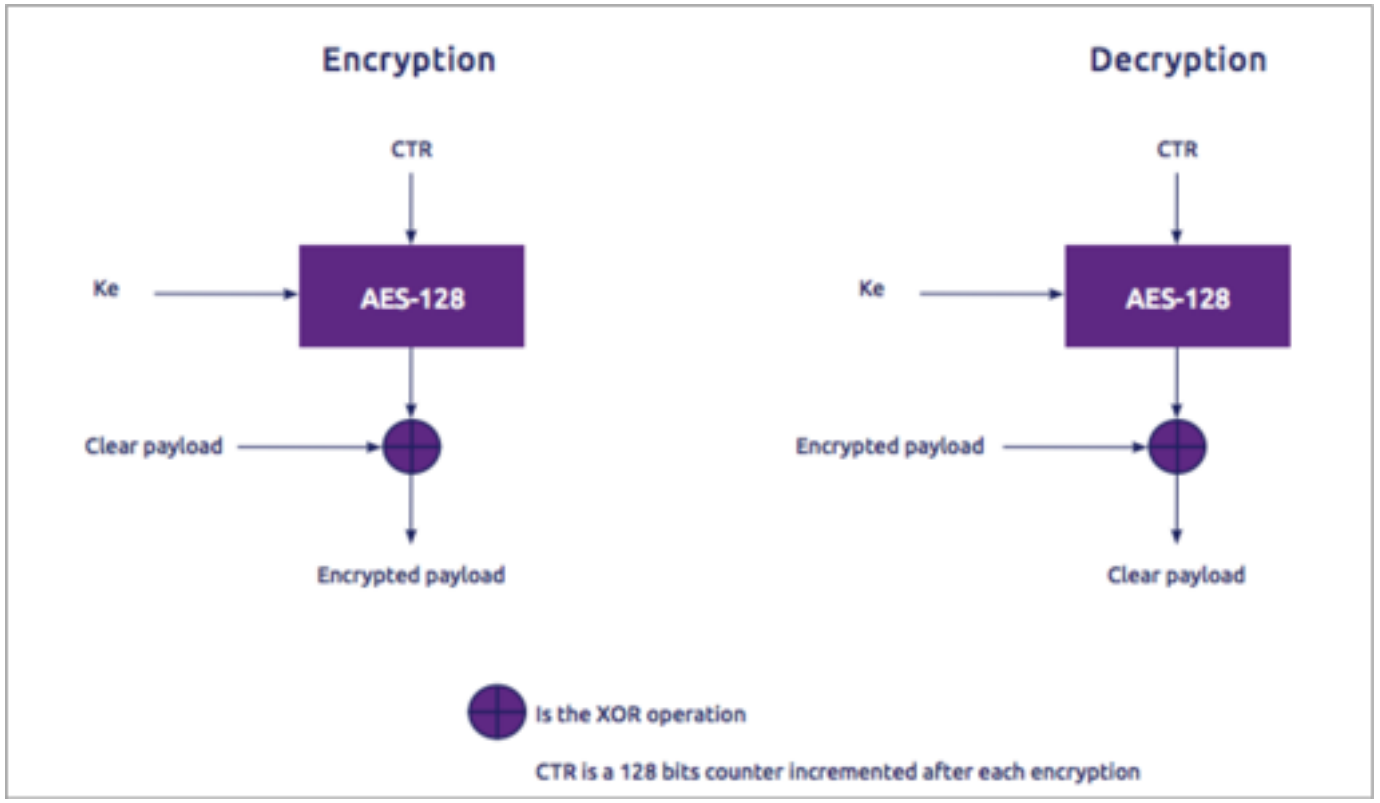


Figure 2. LoRaWAN Join procedure.

LoRaWAN

La clef est calculée à partir d'une clef partagée APPKEY lors de la procédure de JOIN. Cette clef est changée lors de chaque connexion.

Chiffrement sur les réseaux LPWAn



LoRaWAN CTR format / 2 - pour uplink et downlink

					D										
1	0	0	0	0	0/1	DEV ID				COUNTER				0	0

Sigfox et LoRaWAN

Le problème : chiffrer un bloc de données variable et de petite taille.
La solution : réaliser un XOR (permuter des bits) avec un masque donnant une répartition non prédictible. Ceci ne mélange pas les bits.
Pour cela, constituer le masque avec la clef précédemment calculée (Ke) et l'utiliser pour chiffrer, à l'aide de AES-128, une donnée variable CTR. Ke et CTR sont connus de l'objet et du cœur de réseau. Ainsi le masque sera connu des deux et chiffrement/déchiffrement sont possibles.

Au final peu d'inconnues

CTR									
1	0	0	0	0	0/1	DEV ID	COUNTER	0	0

Aucune inconnue ici : COUNTER est égal à FCNT ou presque.

Payload déchiffrée									
XX	??	??	YY	??	??	ZZZZZZZ	??????	??	??

Une partie des informations (entête, flags…) peuvent être connus

- Combien de temps et trames faut il pour trouver Ke avec tous ces éléments ?
- Donc de temps en temps il est préférable de renouveler Ke.
- Ce qui nous protège : un faible nombre d'échanges

Recommandation : Ajouter son propre chiffrement

La question n'est pas de savoir si ces solution seront cassés où si des outils vont exister pour les casser mais seulement de quand ils seront disponibles.

Utiliser une solution maison en plus de la solution réseau offre un second niveau de sécurité qui est moins diffusé et donc potentiellement avec moins d'outillage disponible.

Illustration : WEP n'est plus fiable mais HTTPs ou IPSec sur WEP l'est en grande partie.

Solution de type Sigfox/LoRaWan

La première option est d'appliquer sa propre méthode basée sur AES comme le font les LPWAn, il est tout a fait possible d'empiler les couches de chiffrement. En utilisant ses propres règles pour générer Ke et CTR.

Solution de type SPECK

SPECK est une solution de chiffrement adaptée à des blocs pouvant être de 32bits qui a l'avantage de mélanger des bits au sein d'un bloc. Par contre un bloc source donnera toujours le même résultat chiffré sauf à changer la clef. Elle est adapté à l'embarqué.

Une difficulté commune: partager et mettre à jour la clé dans un réseau qui perd les paquets, sans risquer de désynchroniser l'émetteur du récepteur.

Emettre sur le réseau

sigfox

- Les messages sont authentifiés par signature HMAC basée sur une clef connue seulement de l'objet et du réseau.
- Les messages inclus un numéro de séquence qui empêche le rejeu immédiat. Il faut attendre un tour complet (4096 – en général 6 mois à 1 an) pour un rejeu et ne pas rater le slot.
- Le chiffrement protège du rejeu avec l'usage d'un compteur plus grand que le seqID.
- Les messages descendants sont eux aussi signés

LoRaWAN™

- Les messages sont authentifiés à l'aide de la NTWSKey qui est négociée à chaque session.
- Le rejeu est bloqué par les même principes que ceux vus coté Sigfox.
- Le chiffrement par défaut empêche le rejeu même après dépassement de FCNT
- Le seul problème est que **si vous connaissez** les données DEVEUI, APPKEY, NTWKEY alors vous pouvez usurper l'identité de l'objet en créant une nouvelle connexion.
- Vous pouvez par là même aussi simplement couper sa connexion et le rendre muet.

Perturber le réseau

sigfox

- Les objets n'ont pas besoin d'écouter pour communiquer ils ont donc une très grande résistance aux perturbations.
- La largeur de bande du signal et sa concentration de puissance rendent compliqué les perturbations, d'autant plus que le nombre des antennes réceptrices est grand et disséminé dans l'espace.
- Changement « aléatoire » de fréquence à chaque communication.
- Downlink sur une fréquence prédéterminée facile à brouiller.

LoRaWAN™

- La connexion au réseau demande une communication bidirectionnelle qui peut être perturbée. Une fois la communication établie la situation est comparable à Sigfox.
- Le nombre de canaux de communication est faible et les 3 premiers sont connus et partagés, globalement la fréquence de communication est prédictible.
- La communication peut être rapide (5.4Kbs) rendant un brouillage ciblé complexe.
- Downlink sur « plusieurs » fréquences mais plutôt facile à brouiller.

To do or not to do …

Les choses à faire:

- Protéger l'ensemble des clefs de l'objet
- Vous assurer que ces clefs ne puissent pas être déduites de celles d'un autre objet.
- Ne pas rendre les clefs visibles sur l'objet ou sur son packaging (genre box Internet/Wifi)
- Ne pas avoir à se connecter pour remonter une information critique (LoRaWan)
- Implémenter sa propre couche de chiffrement.

Les choses à ne pas faire:

- Penser que la solution de chiffrement utilisée par le réseau est fiable dans le temps (10 ans ou plus).
- Penser que la solution de chiffrement utilisée par le réseau est fiable concernant votre objet, y compris à 6 mois.
- Penser que le réseau est fiable lorsque vous implémentez votre propre solution de chiffrement : des paquets seront perdus, il faut le gérer.
- Penser que l'on pourra recevoir un downlink au moment où l'on en aura besoin.

Merci de votre attention
Questions ?