TELECOM DESIGN

ZATAZ ITrust CYBERSECURITY AS A SERVICE

TELECOM DESIGN

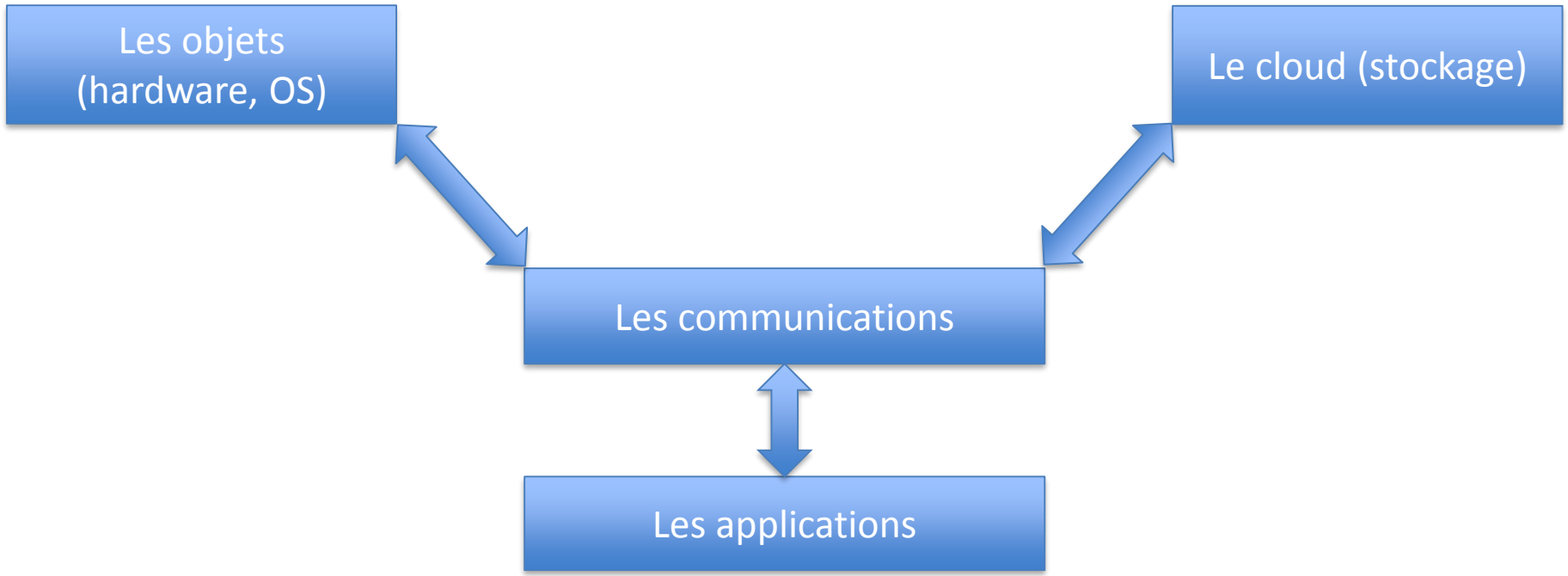
Sécurisation de l'IoT : où en est-on ?

Source : Webinar ITrust & Zataz du 28/03/2019

Les challenges liés à la sécurisation des objets

Les challenges liés à la sécurisation des objets

Plusieurs éléments composent l'environnement de l'objet connecté.
Ceux-ci peuvent être attaqués indépendamment.



Problématique 1 : surface d'attaque

Les objets (hardware, OS)

Accès physique à l'objet

Le cloud (stockage)

Le backend de stockage peut être accédé publiquement

Les communications

Elles peuvent être interrompues / brouillées / interceptées (MITM) / ...

Les applications

Elles peuvent être vérolées pour prendre le contrôle du smartphone par exemple

Problématique 2 : la diversité des utilisations

Objets liés à la mesure de soi

Objets liés à la domotique

Véhicules connectés

Objets liés à l'industrie

Objets liés à la santé

Jouets pour enfants

Etc …

Problématique 3 : les ressources

Pour gagner en coût & temps, on limite :

- Les CPUs
- La mémoire
- La taille de l'objet

…

Problématique 3 : les ressources

Cela impacte directement la sécurisation de l'objet :

- CPU faible : les calculs cryptographiques seront plus faibles ou plus long, ...

Problématique 3 : les ressources

Cela impacte directement la sécurisation de l'objet :

- CPU faible : les calculs cryptographiques seront plus faibles ou plus long, ...
- surface silicium plus petite : on met moins de composants, moins de ressources, ...

Problématique 3 : les ressources

Cela impacte directement la sécurisation de l'objet :

- CPU faible : les calculs cryptographiques seront plus faibles ou plus long, ...
- surface silicium plus petite : on met moins de composants, moins de ressources, ...
- mémoire limitée : on fera tourner des applications moins complexes, moins sécurisées ...

Problématique 4 : les standards de communication

En fonction des cas d'utilisation, chaque fournisseur va utiliser un standard :

LoRa™ sigfox Wi Fi™ ®

Aucun de ces standards n'est officiellement reconnu comme plus sûrs que les autres.

Ni le NIST, ni l'ENISA ne recommande l'utilisation d'un standard plutôt qu'un autre.

NIST National Institute of Standards and Technology U.S. Department of Commerce

enisa European Union Agency for Network and Information Security

Problématique 5 : les nouveaux acteurs

Les nouveaux acteurs du marché de l'IoT sont rarement sensibilisés à la sécurisation des objets et cherchent à faire du business.

Le RGPD a apporté un réel élan de sécurité en Europe.

Problématique 6 : les enjeux techniques

- Complexité des compétences : pour réaliser un projet IoT, il faut des profils très différents : dev hardware / software / backend, sécuriser les communication, ...
  ➔ augmente le coût de développement de l'objet.

Problématique 6 : les enjeux techniques

- Complexité des compétences : pour réaliser un projet IoT, il faut des profils très différents : dev hardware / software / backend, sécuriser les communication, ...
  ➔ augmente le coût de développement de l'objet.

- Des enjeux vitaux : plus ou moins importants suivant les objets.

Problématique 6 : les enjeux techniques

- Complexité des compétences : pour réaliser un projet IoT, il faut des profils très différents : dev hardware / software / backend, sécuriser les communication, ...
  ➔ augmente le coût de développement de l'objet.

- Des enjeux vitaux : plus ou moins importants suivant les objets.

- Pouvoir mettre à jour / contrôler un objet une fois déployé : il faut pouvoir revenir à un état stable si celui-ci est compromis.

Sécuriser les objets connectés, en bref

Bonnes pratiques au niveau hardware

- signer le code

- avoir une résistance aux altérations hardware : à la première modification hardware tout l'objet est détruit par exemple

- limiter les interfaces d'administration hardware (JTAG, série, ...) : il faut désactiver ces interfaces une fois l'objet déployé pour éviter qu'un attaquant se branche dessus

Bonnes pratiques au niveau OS

- les services d'administration doivent être sécurisés & chiffrés

- ne pas utiliser un mot de passe par défaut. Avoir un mot de passe différent par objet

- mettre à jour l'OS et les composants 'On The Air' depuis des sources sûres

- permettre le monitoring de l'OS

Bonnes pratiques au niveau des communications

- ajouter une couche cryptographique souvent non proposée par le standard choisi

- limiter les distances si possible : statistiquement plus on est loin de l'objet et plus la communication pourra être interférée et manipulée par un attaquant

- attente de standards approuvés : aucun n'est reconnu et approuvé aujourd'hui

Bonnes pratiques au niveau applicatif

- security by design : prendre la sécurité de l'objet dès la conception

- faire du développement sécurisé :
  = former les développeurs
  = authentification
  = contrôle des paramètres utilisateurs

- utiliser des briques logicielles sûres, à jour et avec une communauté active

Bonnes pratiques au niveau des données

- limiter les données recueillies (privacy by design) dès la conception

- anonymiser les données

- chiffrer les données

- sauvegarder les données (chiffrées et anonymisées)

Bonnes pratiques au niveau des moyens de détection

- mettre en place un SOC au niveau de l'infrastructure d'administration de l'objet

- la verbosité des objets est trop variée

- faire une analyse comportementale sur un réseau d'objets pour détecter une attaque

Merci pour votre attention.
Téléchargez-moi ici