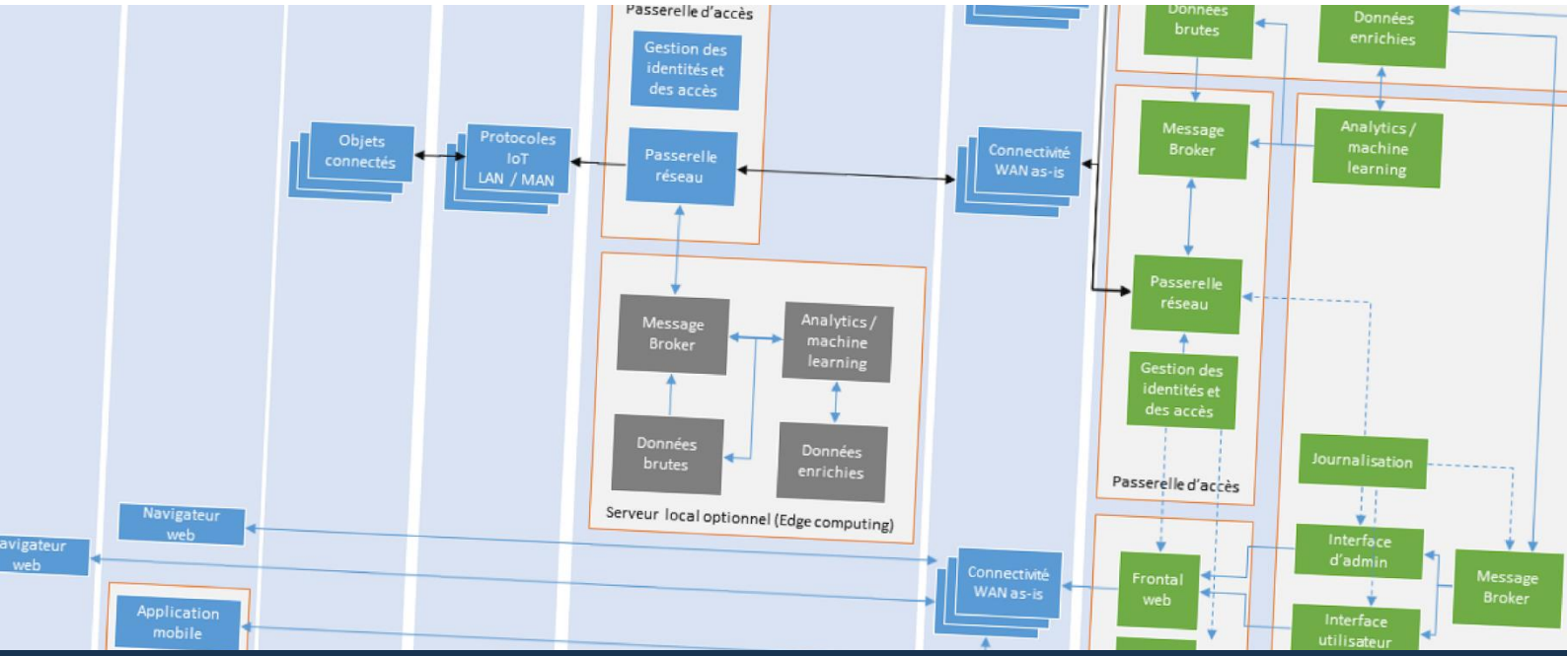
LES FICHES PRATIQUES du CLUSIF - IoT



QUELS PRINCIPES DE CYBERSÉCURITÉ ENVISAGER ET EXPLORER LORS DE LA CONCEPTION D'UN OBJET CONNECTÉ ?

Version 1.0

1. LA NÉCESSITÉ D'INTÉGRER LA SÉCURITÉ DÈS LA CONCEPTION DES OBJETS CONNECTÉS

L'essor des objets connectés amène de nombreuses opportunités pour les acteurs malveillants. Prenons pour exemple un assistant domestique moderne, qui dispose de capacités d'enregistrement audio, vidéo et de reconnaissance vocale. Il permet d'assurer la surveillance des locaux, d'alerter à distance en cas d'intrusion et de piloter d'autres objets connectés. Par ailleurs, il aide son propriétaire en lui permettant d'effectuer des achats en ligne par simple commande vocale, de gérer ses comptes bancaires, de demander un diagnostic médical et d'obtenir des conseils pour l'automédication. Il est aisé d'imaginer l'intérêt potentiel que peut trouver un attaquant pour ce type d'objet et les risques que cela comporte pour son usager :

1. Atteinte à la vie privée (interception, vol & revente de données à caractère personnel) ;
2. Désactivation de systèmes de sécurité physique ;
3. Multiples scénarios de fraude (plateformes bancaires, achats en ligne, assurance…) ;
4. Altération des prescriptions médicales ;
5. Détournement du système en plateforme malveillante (dénis de service répartis, minage de cryptomonnaie).

Comme nous le voyons au travers de ces enjeux de sécurité, si ces menaces sont réelles, chaque typologie d'objet n'y est pas exposée de la même manière. Nous aurions pu également prendre pour exemple une balance connectée ou encore une trottinette électrique connectée. Ces derniers exemples présentent d'autres caractéristiques qui peuvent entraîner d'autres problématiques de sécurité. Ainsi, comme le pratique l'industrie de la cybersécurité depuis de nombreuses années, il est préférable d'adopter une approche par les risques pour identifier les mesures à prendre en compte

dans la conception d'un objet connecté. En effet, une démarche d'analyse de risque traditionnellement employée permet d'identifier les vulnérabilités et les différents scénarios de risques afin d'anticiper tout détournement malveillant de l'usage de l'objet.

On peut considérer quatre principaux facteurs induisant des risques concernant les objets connectés :

1. **La richesse fonctionnelle de l'objet**, qui matérialisera autant d'opportunités de malveillance. En particulier, si l'objet dispose de fonctions sensibles prévoyant le traitement de données à caractère personnel (collecte, stockage, visualisation...) et/ou une interaction sur le monde physique ;
2. **La pénétration de l'objet sur le marché.** Un objet très répandu sera plus intéressant pour un attaquant car il pourra atteindre un maximum de cibles et augmenter son pouvoir de nuisance ;
3. **Les technologies matérielles et logicielles**, porteuses de vulnérabilités qui constitueront la surface d'attaque de l'objet ;
4. **La connectivité réseau.** Elle caractérisera le degré d'exposition aux menaces, qui seront donc locales ou globales.

> ⓘ **Pour aller plus loin**
> *Vous retrouverez plus d'informations sur les cas d'usage et les enjeux qui en découlent dans les fiches « Qu'est-ce qu'un objet connecté ? » et « Quels sont les enjeux de sécurité de l'IoT ? »*

2. LES PROFILS DE PROTECTION

Il faut ensuite prévoir la mise en œuvre de mesures de sécurité adaptées aux risques les plus importants. Pour rendre cette approche plus opérationnelle et aider les fabricants dans son application, nous proposons de se référer à deux profils de protection prévoyant des mesures de sécurité pré-établies en fonction des risques. Le profil de protection avancé est à envisager pour les cas d'usage ci-dessous :

1. Objet intégrant un traitement de données à caractère personnel susceptible d'induire un risque important sur la vie privée (interception, vol & revente de données) ;
2. Objet disposant de capacités d'interaction sur le monde physique, qui permettrait de porter atteinte à la sécurité physique des biens et des personnes (ex : prise de contrôle d'un système moteur, de systèmes de sécurité physique…) ;
3. Objets largement répandus sur le marché, mettant en œuvre des technologies courantes et disposant d'une connectivité élargie avec Internet, susceptibles d'être piratés et détournés en plateforme de malveillance (ex Botnet, minage de cryptomonnaie…).

Pour tout autre cas, le fabricant se doit d'apprécier les risques selon la nature de l'objet et déterminer si le profil élémentaire est suffisant. Le tableau suivant propose quelques cas d'exemples :

Objet	Facteurs de risques	Niveau de risque, conséquences et profil de protection proposé
Assistant domestique évolué	Pilotage d'autres objets connectés, accès aux comptes bancaires, achats en ligne…	Risque élevé, le préjudice est important sur la vie privée et la sécurité de l'utilisateur → Profil avancé
Réfrigérateur connecté	La température est automatiquement régulée en fonction des denrées et pilotable par smartphone.	Risque modéré pour un réfrigérateur domestique voire élevé pour un réfrigérateur industriel. Dans l'exemple d'un réfrigérateur de cantines scolaires, on peut considérer que le préjudice, en cas d'altération des réglages de température, peut-être plus impactant pour la santé des plus jeunes consommateurs → Profil avancé
Thermostat domestique connecté	Pilotage de la température de chauffage à distance	Risque faible, impact limité sur la sécurité physique ou la vie privée de l'usager en cas de compromission → Profil élémentaire
Serrure connectée	Pilotage à distance de la serrure avec un smartphone	Risque élevé, compte-tenu des possibilités d'intrusion physique et d'atteinte à la sécurité des personnes → Profil avancé

Le tableau ci-dessous synthétise une proposition de mesures de sécurité à mettre en œuvre pour chaque profil de protection. Les mesures de sécurité portent principalement sur la conception de l'objet en lui-même ainsi que sur son interaction avec les autres composants du système. Naturellement, la plupart des objets connectés étant pilotés au travers de plateformes Cloud, il est nécessaire d'envisager la sécurité globalement en intégrant cette composante. Nous vous conseillons de prendre en compte toutes les recommandations émises par le groupe de travail « Cloud & Sécurité » en complément.

Domaine	Mesures de sécurité	Profil de niveau élémentaire	Profil de niveau avancé (comprend en plus du niveau élémentaire les spécificités ci-dessous)
Sécurité du système	Capacité de mise à jour des composants logiciels	La conception de l'objet rend possible la mise à jour de tous les composants logiciels.	Les mises à jour sont signées électroniquement. La version du logiciel est contrôlée et validée.
	Fréquence de mise à jour des composants logiciels	Le fabricant vérifie régulièrement la présence de vulnérabilités sur son produit et propose les correctifs logiciels adaptés dans un délai raisonnable, cela tout au long du cycle de vente du produit.	Mises à jour proposées jusqu'à cinq ans après la fin de sa commercialisation
Contrôle des accès	Sécurité des accès	L'objet utilise des comptes génériques. L'accès aux fonctions sensibles de l'objet se fait par mot de passe.	L'objet permet de créer des comptes utilisateurs disposant d'un mot de passe spécifique. Des niveaux de privilèges sont définis et l'accès à l'ensemble des fonctions se fait a minima par mot de passe.
	Prévention des intrusions	L'accès est bloqué temporairement après plusieurs erreurs de mot de passe et génère une trace.	L'événement peut générer une alerte pouvant être relayée à son propriétaire (ex par courriel).
	Modification des mots de passe	Si les mots de passe sont pré-configurés en usine, ils sont différents pour chaque objet et générés de manière aléatoire mais l'utilisateur se voit proposer la modification des mots de passe lors de la première utilisation de l'objet.	Les mots de passe doivent être modifiés avant la première utilisation de l'objet.
	Sécurité des mots de passe	La complexité des mots de passe est contrôlée lors de toute modification avec des critères forts et conformes à l'état de l'art.	
Protection des données stockées	Protection des mots de passe	Les mots de passe sont stockés de manière sécurisée en utilisant des fonctions de hash correspondant à l'état de l'art.	
	Protection des données	Pas de chiffrement des données stockées	Les informations sensibles stockées de manière persistante en mémoire sont chiffrées selon l'état de l'art.
	Effacement des données	Toutes informations stockées en mémoire sont effaçables, les paramètres usine peuvent être restaurés pour permettre une mise au rebut sécurisée (ex : bouton reset).	
Protection des données transférées	Connexion au réseau local	La connexion au réseau local sans fil supporte les protocoles sécurisés.	La connexion au réseau local sans fil ne peut se faire qu'au travers de protocoles sécurisés.
	Transfert de données	Les informations sensibles sont transmises sur Internet à l'aide des protocoles réseaux sécurisés.	Une authentification mutuelle est réalisée avant le transfert de données
Traçabilité	Traçabilité des événements	Les erreurs d'accès et d'authentification génèrent une trace consultable, contenant l'heure et les détails de l'événement.	En plus des erreurs d'accès et d'authentification, toute action sensible génère une trace consultable, contenant l'heure et les détails de l'événement.

ⓘ Point de vue du RSSI

On constate encore trop souvent que la sécurité de l'IoT n'est pas efficacement intégrée. Ces objets souffrent de vulnérabilités de conception facilement exploitables, ce qui génère autant d'opportunités de malveillance pour une population large d'attaquants. Étant donné leur diffusion massive et rapide - y compris dans le monde de l'entreprise - et leur diversité, l'essor des objets connectés amène de véritables défis en matière de cybersécurité qu'il convient d'adresser sérieusement. L'approche qui est décrite dans cette fiche vise à aider les concepteurs et les fabricants à améliorer la sécurité de leurs objets en proposant des mesures dont le coût d'implémentation doit être proportionné aux risques à couvrir.