Cybersécurité pour l'IdO

CYBERSÉCURITÉ DE L'IOT À TOUS LES NIVEAUX

Un système IoT se compose de divers appareils connectés - qui comprennent à leur tour un certain nombre de composants intégrés - ainsi que d'une infrastructure de gestion, de contrôle et de traitement.

Applus+ Laboratories dispose d'une équipe d'ingénieurs expérimentés dans l'évaluation de la sécurité du matériel, des logiciels et des protocoles de communication et capables d'évaluer la cybersécurité des composants IoT, des appareils IoT et, de fait, des systèmes IoT entiers.

ÉVALUATIONS DE LA CYBERSÉCURITÉ DES COMPOSANTS IOT

Chaque appareil IoT est constitué d'un certain nombre de composants, qui sont eux-mêmes responsables des principales fonctionnalités de sécurité de l'appareil. D'où l'importance d'utiliser des composants certifiés ou dont la sécurité a été évaluée.

Évaluations de la sécurité dans le cadre de programmes de certification reconnus :
Applus+ est un laboratoire de sécurité accrédité pour évaluer les composants matériels et logiciels intégrés dans les appareils IoT conformément à une série de schémas de certification reconnus au niveau international :

- Common Criteria (laboratoire accrédité pour les schémas américains, canadiens et espagnols).
- Sesip (laboratoire accrédité)
- PSA Certified (Laboratoire accrédité)
- Fido (solutions d'authentification)
- GlobalPlatform (TEE - Trusted Execution Environments)

Évaluations personnalisées et indépendantes :

Dans les cas où la certification n'est pas obligatoire mais où un fabricant a besoin d'évaluer la sécurité d'un produit particulier, Applus+ peut fournir des évaluations indépendantes et personnalisées adaptées à tous les types de composants et à toutes

les applications. Ces évaluations peuvent être entièrement adaptées pour répondre aux besoins du client : boîte blanche/grise/noire, examen du code source, analyse de la vulnérabilité, examen de la conception, etc.

ÉVALUATIONS DE LA CYBERSÉCURITÉ DES DISPOSITIFS IOT

Évaluations de la sécurité dans le cadre de systèmes de certification reconnus :
Applus+ peut évaluer la sécurité des solutions IoT dans le cadre des Common Criteria. Il existe également un certain nombre d'autres schémas de certification IoT actuellement en cours de développement. Contactez-nous pour en savoir plus sur ces nouveaux schémas.

Évaluations indépendantes de la cybersécurité :
Bien conscients de la grande variété d'applications qui existent dans le domaine de l'IoT, nos experts peuvent créer une évaluation adaptée aux particularités du produit en question, en tenant compte de la nature du produit, du type de solution IoT dont il est

destiné à faire partie et du type de données qu'il traitera. Une ampoule intelligente, une passerelle qui gère le système d'éclairage d'un hôtel et le compteur intelligent d'une compagnie d'électricité ne présentent pas tous la même criticité. Nos évaluations portent sur les aspects suivants, mais sont toujours adaptées aux besoins du client :

- **Protection des données :** Les appareils IoT sont capables de stocker et de partager des informations sensibles telles que des clés cryptographiques et des données personnelles qui doivent être protégées. À ce titre, nous évaluons la sécurité des communications pour tous les types de protocoles (BLE, Zigbee, Wi-Fi, LTE, etc.), ainsi que la sécurité des mécanismes de stockage (protection des actifs).
- **Sécurité de l'interface :** Toutes les interfaces d'accès d'un appareil IoT doivent être identifiées et leurs niveaux de protection évalués, ainsi que leurs mécanismes d'authentification/identification : interfaces web, interfaces réseau (ports ouverts non sécurisés), interfaces physiques (JTAG, UART, etc.), API Cloud et API Mobile.
- **Mises à jour sécurisées :** Quel est le mécanisme permettant d'effectuer des mises à jour de manière sécurisée ? Existe-t-il un protocole pour valider l'intégrité et l'authenticité d'un nouveau binaire ? Nos experts évaluent les systèmes de mise à jour et les protocoles de correctifs de l'appareil.
- **Démarrage sécurisé :** Quel est le mécanisme du système d'amorçage/redémarrage de l'appareil ? Nous évaluons le protocole de démarrage de l'équipement pour nous assurer qu'il est sécurisé et fiable.

Méthodologies et guides de bonnes pratiques : La plupart des pays sont encore en train d'élaborer leurs réglementations/normes IoT. En attendant, il existe plusieurs méthodologies et guides de bonnes pratiques sur lesquels les évaluations peuvent se baser, notamment :

- GSMA IoT Security Guidelines and Assessment (Lignes directrices et évaluation de la sécurité de l'IoT).
- OWASP IoT Top 10
- Code de pratique pour la sécurité de l'IdO des consommateurs
- Recommandations de base de l'ENISA en matière de sécurité pour l'IoT.

N'hésitez pas à prendre contact avec Applus+ Laboratories pour une évaluation conforme à l'une de ces méthodologies/guides.

ÉVALUATIONS DE LA CYBERSÉCURITÉ DES SYSTÈMES IOT

La sécurité d'un système IoT va au-delà de la protection de chacun des appareils qui le composent. Bien que ceux-ci puissent être sécurisés individuellement, une fois qu'ils sont déployés et connectés, de nouvelles menaces systémiques peuvent faire surface. De même, la gestion de la chaîne d'approvisionnement est cruciale, car la sécurité d'un système repose en grande partie sur le fait de pouvoir faire confiance à ses différents composants.

Évaluations de la sécurité de la chaîne d'approvisionnement :
Un seul appareil vulnérable peut compromettre tout un système. Les fabricants doivent avoir confiance dans les appareils et les solutions qui composent leurs systèmes et pour cela, ils ont besoin de chaînes d'approvisionnement fiables. Comment Applus+ peut-il les aider à atteindre cet objectif ?

- En évaluant les risques et les menaces inhérents à une chaîne d'approvisionnement donnée.
- En réalisant des audits de sécurité sur les plans de développement et de production
- En essayant les solutions de sécurité qui ne détiennent pas de certificat de sécurité reconnu.

- En évaluant les risques et les menaces inhérents à un système
- En évaluant les différentes couches (nuage, brouillard, contrôleurs mobiles à distance) et leurs interfaces.

Remarque : parce que Applus+ Laboratories est accrédité en tant que laboratoire tiers par plusieurs schémas d'évaluation et de certification, et afin de garantir son impartialité, les ingénieurs d'Applus+ ne sont jamais impliqués dans le développement réel des produits ou la mise en œuvre des solutions.