Partie 1 :
Introduire de nouveaux services sans risques

Une introduction à l'utilisation du cadre d'application Legato ® pour jouer dans la boîte

L'ajout de nouvelles fonctionnalités ou d'applications tierces à un dispositif IoT peut être risqué, car les nouvelles fonctions peuvent rendre plus difficile la prévision des performances sur le terrain, le maintien de la sécurité et la préservation de la confidentialité des données.

Le « Sandboxing » est une technique, soutenue par la plateforme de développement open source Legato, qui rend plus facile et plus sûre la conception, le test et le déploiement de nouvelles fonction IoT (sans risquer l'application principale).

Les mises à jour, les modifications et les nouvelles fonctionnalités sont une réalité dans l'IoT. De nombreux dispositifs IoT commencent comme des systèmes électroniques relativement simples mais qui évoluent rapidement pour prendre en charge de multiples les candidatures. Un dispositif de première génération pour le suivi des véhicules, par exemple, pourrait être mis à jour pour prendre en charge l'assurance basée sur l'utilisation, ou la dernière version d'un compteur de gaz pourrait être configuré avec une application de paiement, pour prendre en charge les nouveaux services de paiement à l'utilisation et de rechargement.

L'ajout de fonctionnalités supplémentaires et la prise en charge de nouvelles applications peuvent créer mais elle ajoute aussi la complexité au système, ce qui peut accroître le risque. Ce n'est pas toujours facile de savoir comment une nouvelle fonctionnalité, développée par un sous-traitant, ou une nouvelle applications, fournie par un partenaire tiers, interagira avec les fonctionnalités existantes. Les nouveaux services peuvent ralentir les performances, produire des résultats imprévus ou, pire encore, introduire des vulnérabilités, compromettent la sécurité ou rendent plus difficile la protection des informations.

Le « Sandboxing » pour la protection de la vie privée

L'un des moyens dont disposent les développeurs pour minimiser les risques liés aux fonctionnalités complexes est le « sandboxing », une technique qui facilite la création, l'évaluation et l'extension des système tout en maintenant la sécurité. Le sandboxing permet d'isoler une application et de contrôler son comportement, afin de garantir les performances et d'accroître la sécurité. Dans le contexte IoT, les points clés du sandboxing sont la confidentialité des données et les privilèges d'accès.

Confidentialité des données

Le « Sandboxing » empêche une application d'accéder aux données d'une autre application d'accéder aux données d'une autre application, si sensibles l'information reste privée. Une application du type « Sandboxing » est limitée aux limites de son et ne peut fonctionner qu'avec des données autorisées. Les données pertinentes peuvent être stockées n'importe où dans le système (dans un système de fichiers non volatil ou dans une mémoire vive volatile) et peut être lié à une ou plusieurs applications bac à sable. Chaque application en bac à sable peut faire ce qu'elle veut et accéder aux données dont il a besoin, sans voir ni perturber le reste du système.

Les privilèges d'accès

Le Sandboxing permet également d'accorder des privilèges d'accès, afin d'accroître la sécurité et gérer les ressources du système de manière plus efficace. Une application « sandboxed » peut être autorisée l'utilisation limitée d'une fonction ou d'une API, de sorte que, par exemple, l'application n'ouvre qu'un pour accéder à un seul serveur ou pour demander le positionnement d'un appareil. Tous les autres actions sont strictement interdites. De même, l'accès à l'unité centrale, à la mémoire ou au réseau la largeur de bande peut être limitée, de sorte que l'application ne puisse pas monopoliser les ressources et donc ralentir performance ou le gaspillage d'énergie. Une application « Sandboxing » ne fonctionne qu'avec les ressources qu'elle a besoin sans pour autant surcharger le système.

Le Sandbox Legato

Le Sandboxing trouve son origine dans les systèmes virtualisés à grande échelle, tels que les serveurs et les PC, mais il s'agit d'une technique qui, lorsqu'elle est mise à l'échelle, apporte des avantages importants aux système embarqués compacts utilisés dans l'IoT.

Le Sandbox Legato peut être utilisé tout au long du cycle de vie d'un appareil pour réduire les risques tout en créant une plus grande différenciation, une fonctionnalité élargie et de nouvelles sources de revenus. Au cours du développement, le sandbox Legato crée un environnement de programmation plus sûr, afin que les concepteurs puissent faire ce qu'ils doivent faire (tester des idées, créer de nouvelles fonctionnalités, intégrer des applications tierces) sans compromettre la sécurité. Une fois que les dispositifs sont déployés sur le terrain, le sandbox Legato permet de mettre à jour plus facilement et plus sûrement les appareils et d'introduire de nouvelles pour une approche plus sûre afin de rester compétitif.

De nouvelles sources de revenus

Le sandbox Legato crée un environnement protégé et restreint pour l'ajout de nouveaux services aux appareils qui sont déjà sur le terrain. De nouvelles fonctionnalités et applications peuvent être ajoutées en mode natif ou à distance, grâce à des mises à jour par voie hertzienne (OTA). La mise à jour peut être chargée directement dans le sandbox, pour une validation rapide et sécurisée, et le sandbox de chaque module peut être géré à partir d'un point central, dans le nuage AirVantage ™. Les nouveaux déploiements peuvent être émis et validés en une seule fois ou par étapes. En permettant l'intégration rapide et sécurisée de nouvelles fonction, le sandbox Legato augmente la flexibilité et la réactivité, pour une différenciation plus rapide.

Lorsqu'il est combiné avec des applications qui suivent les données ou l'utilisation du réseau, le système sandbox Legato peut également être utilisé pour réduire les coûts d'exploitation et augmenter l'efficacité.

- **Exemple de surveillance du trafic sur le réseau :** Le sandbox Legato isole les applications et les rend. Il est possible de surveiller chacun d'entre eux individuellement, de sorte que l'utilisation du réseau pour une application donnée peuvent être suivis et facturés. Les factures sont plus précises et il est possible d'établir des options, telles que la facturation échelonnée et les remises aux membres.
- **Exemple de gestion de la bande passante du réseau :** De la même manière, le sandbox Legato peut être utilisé pour suivre et gérer le trafic de données sur les appareils fonctionnant en Wi-Fi hotspot, pour une meilleure expérience globale du client. Les gros utilisateurs peuvent être facturés en supplément, comme moyen de décourager les comptes de dépasser une limite fixée, et d'empêcher les utilisateurs de prendre plus que leur juste part de la bande passante disponible.

Une ingénierie plus sûre

Le sandbox Legato réduit les inconnues, les surprises et les erreurs intentionnelles qui font partie intégrante du processus de création. Les développeurs peuvent essayer de nouvelles idées et tester différents scénarios, dans un environnement sécurise. Ils peuvent expérimenter en utilisant une approche réglementée et progressive qui facilite la détection des erreurs et la correction des bugs, sans perturber ce qui fonctionne déjà.

Le sandbox Legato offre également un environnement sécurisé pour les essais de conduite par des tiers. Il est donc moins risqué de travailler avec des sous-traitants, des partenaires et d'autres développeurs. Une application tierce peut être exécutée de manière isolée, avec des restrictions d'accès strictes et le reste du système, afin d'identifier tout impact potentiel sur le système et avant d'être accepté pour utilisation