Une architecture standard pour sécuriser la mobilité des équipements

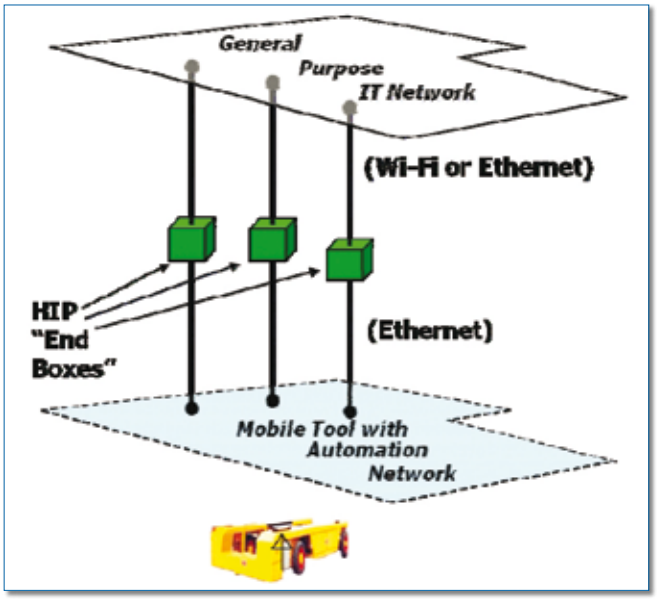
par ***Harry Forbes***

Boeing a adopté une architecture standard afin de fournir un service de mobilité sécurisé à ses équipements implantés sur ses lignes de fabrication. Le constructeur d'avions négocie avec les fournisseurs et fabricants pour faire émerger un nouveau standard, dans un contexte habituellement en proie à des solutions propriétaires.

IP, le principal protocole de l'Internet n'assure pas fondamentalement la mobilité des équipements. A mesure que les utilisateurs et les équipements sont devenus mobiles, le besoin de services Internet sécurisés s'est fait ressentir dans l'industrie manufacturière. Objectif : accéder à Internet d'où que l'on soit. Il y a cependant des obstacles pour atteindre ce but. Les adresses IP sont utilisées pour deux principales raisons très différentes. Tout d'abord, les adresses numériques sont employées comme indicateurs de topologie réseau pour router les trames de données à un équipement précis. Ensuite, le système de noms de domaine (DNS) cartographie les identités logiques par rapport aux adresses IP. Les difficultés surviennent du fait que les protocoles de transport (TCP et UDP) sont limités aux adresses IP des équipements. Les services en liaison avec les équipements sont alors déconnectés lorsqu'une adresse IP change du fait de la mobilité même du composant.

Il existe d'autres difficultés comme : le déploiement d'applications de pare-feu de réseau utilisant la translation d'adresse (NAT), la configuration automatique des paramètres IP (dynamic host configuration – DHCP)… Le même phénomène est observé avec la cartographie DNS (pour l'instant, l'identité DNS www.google.com ne représente pas une interface physique unique). Le système de noms de domaine n'a pas été conçu pour une mobilité rapide des adresses.

Ces propriétés de l'Internet sont critiques pour la mobilité, car le routage de réseau nécessite des changements au même titre qu'un équipement se déplace d'un endroit à un autre.



Outils et actifs mobiles de Boeing.

En outre, rien dans l'actuel réseau ou dans les protocoles de transport, adresse la sécurité fondamentale d'authentification des équipements mobiles. Alors comment procéder à l'identification, avec la certitude que les équipements clients soient ceux qu'ils prétendent être ?

Cependant, les réseaux d'entreprise intègrent différentes possibilités d'accompagner la mobilité. Cela est particulièrement vrai avec les réseaux d'entreprise WLAN. Dans le cas de telles architectures, le réseau est doté de contrôleurs d'équipements WLAN capables de fournir un numéro de points d'accès sans fil (APs). Le contrôleur WLAN établit une cartographie d'adresses IP vis-à vis des équipements clients et gère la mobilité de ces équipements dans le cadre d'une zone relative au réseau d'entreprise. Le contrôleur communique avec les équipements clients au niveau d'une couche de liaison de données (data link layer – L2) et doit router toutes les trames de données IP vers le point d'accès courant (acces point – AP) desservant le client mobile à mesure qu'il se déplace dans la zone.

Mobilité sécurisée chez Boeing

Chez Boeing, certaines opérations de fabrication ont nécessité la mise en place de solutions pérennes pour assurer la mobilité sécurisée. Boeing appelle cela Architecture Mobile Sécurisée (Secure mobile architecture – SMA). Boeing a décidé de poursuivre une stratégie de services de localisation, au cœur de son réseau standard avec une couverture de zone WLAN, selon une localisation temps réel.

A terme, Boeing souhaite étendre sa stratégie SMA à une plus grande part de ses opérations manufacturières. Initialement, l'utilisation de ces services de mobilité était prévue pour deux principales applications.

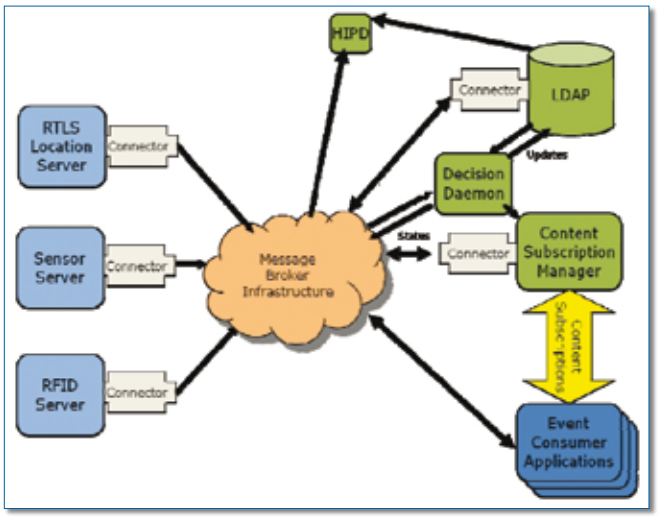
La première était le service de localisation temps réel (RTLS). Boeing souhaitait étendre ce service au-delà des applications typiquement supportées par les fournisseurs de services RTLS. Boeing avait pour objectif initial de suivre ses actifs en temps réel sur plusieurs usines différentes.

Quant au deuxième type d'applications, Boeing avait besoin de sécuriser l'accès à des équipements et outils mobiles utilisés de façon intensive pour certaines opérations de fabrication. De tels outils intègrent souvent des équipements et des systèmes d'automatismes qui doivent rester totalement opérationnels indépendamment de l'infrastructure de communication. Boeing a aussi identifié un certain nombre de futures applications prometteuses.

L'approche « mobilité sécurisée » de l'avionneur est basée sur 4 composants clés :
- PKI (public key infrastructure) : tous les composants clients supportent un encryptage utilisant une infrastructure de clé publique ;
- HIP (host identity protocol) : Il s'agit d'une implémentation d'un futur protocole Internet, capable d'établir des identités sécurisées indépendantes des adresses IP. Applications et protocoles peuvent alors communiquer avec les équipements mobiles, sous de telles identités, sans recourir aux adresses IP ;
- NDS (network directory services) : Boeing a mis à jour plusieurs portions de ses services réseaux afin de prendre en compte les nouvelles identités sécurisées à la place des adresses IP. Cela passe par la modification des infrastructures DNS ;
- LENS (location-enabled network services) : Boeing souhaite faire évoluer ses services sur la base de standards indépendants de fournisseurs. Cette approche favorise un marché d'applications de qualité élevée et évite les recours à l'adaptation. Boeing est entré en relation avec plusieurs fournisseurs pour analyser leurs stratégies face à une telle interface standard. Ces derniers utilisent habituellement des interfaces propriétaires pour le système de localisation, auxquels s'ajoute une part de programmation pour adapter la solution aux besoins du client. Pour sa part, Boeing a défini un « ensemble de service de localisation réseau ». Ces services s'entendent pour des actifs connectés en Wi-Fi et capables de gérer des étiquettes de données RFID.

Les avantages

Boeing a mis en avant de nombreux avantages relatifs à cette architecture. Ceux-ci incluent :
- communication client à client sur la base d'une identité sécurisée : les équipements peuvent évoluer en dehors d'une zone sécurisée tout en maintenant des communications sécurisées ;
- compatibilité : l'architecture mobile sécurisée est valide dans le cadre d'un réseau IP existant ;
- mobilité : l'architecture mobile sécurisée rend disponible les équipements indépendamment des frontières des sous-réseaux ;
- politique en vigueur – la connectivité est basée sur les identités PKI, plus que sur les adresses IP ou MAC. Le tout reste facile à maintenir et à auditer.



Implémentation des services de localisation Boeing.

Objections à l'approche Boeing

ARC a posé la question suivante : pourquoi Boeing a-t-il créé sa propre architecture de mobilité au lieu de recourir aux solutions de mobilité d'un ou plusieurs fournisseurs ? A cela, Boeing répond qu'il utilise de telles offres dans certaines situations. Quoi qu'il en soit, les réseaux doivent s'adapter de façon dynamique pour se connecter avec d'autres nœuds partagés. Les actifs qui se déplacent d'un lieu à un autre (tel que les avions) ont besoin de cette capacité, comme l'exigent des systèmes militaires. A terme, il serait préférable que la connectivité adaptative s'accomplisse au travers de standards ouverts bien plus qu'au travers d'implémentations ou de solutions propriétaires. Cette approche est valable pour les applications commerciales ou militaires, même dans les cas où il est plus rapide et plus facile d'utiliser des solutions propriétaires existantes, à court terme.

En créant SMA, l'avionneur a choisi de définir une « architecture objectif », mais recherche des voies d'implémentation à court terme et définit le cahier des charges. Le contrôle sans fil d'outils mobiles a regroupé les premières applications autour de ce besoin. Boeing espère mobiliser d'autres industriels dans le cadre de son architecture SMA.

Le travail de Boeing est plutôt visionnaire, mais les produits commerciaux et standards prendront au mieux un certain laps de temps pour s'adapter à des changements d'architecture IT aussi fondamentaux. Les industriels qui collaborent avec Boeing au projet SMA devront être capables de supporter eux-mêmes les implémentations, au moins dans les premiers temps.