Sécurité à la Mobilegov

Philosophie

Avec le Scénario Industriel, Mobilegov propose de développer et de tester une approche qui simplifie la vie du fontainier, au lieu de la compliquer comme c'est souvent le cas lorsque la sécurité doit être améliorée.

Dans son activité quotidienne, que ce soit pour procéder au téléchargement d'informations potentiellement sensibles ou à la mise à jour de données de terrain, Maurice était jusqu'à présent authentifié par la saisie d'un identifiant et d'un mot de passe.

L'arrivée de l'informatique ambiante avec ses dispositifs pas toujours adaptés à la saisie d'un mot de passe et l'utilisation du réseau public avec les risques de logiciels espions capables d'intercepter un mot de passe obligent à revoir cette technique de contrôle d'accès.

Le plus souvent, une solution de type « authentification forte », combinant le contrôle de la présence d'une carte à puce et la saisie d'un code PIN est préconisée. Si cette solution, banalisée par la carte bancaire, est bien adaptée aux distributeurs de billets de banque, elle n'est pas utilisable sur des postes de travail qui n'intègrent pas de lecteur. Les solutions d'authentification par boitier OTP sont malcommodes sur le terrain d'un fontainier, et les solutions par token logiciel (PKI) mal adaptées à la grande diversité de terminaux utilisés par notre fontainier.

Nous proposons donc de nous appuyer sur l'identification de matériels que Maurice possède déjà pour l'authentifier dans toutes ses connexions au réseau, tout en intégrant la sécurité dans la séquence des activités de Maurice plutôt que dans chaque tâche prise isolément. Ainsi, une nouvelle tâche effectuée sur un système différent du système utilisé pour effectuer la tâche précédente hérite de crédentiels du système précédent. Cette approche permet une authentification allégée pour le fontainier à chaque nouvelle tâche, le niveau de sécurité nécessaire étant atteint autant que possible par des opérations effectuées sur le serveur.

Maurice dispose toujours d'un smartphone et peut disposer aussi d'un dispositif de stockage USB (clé USB, baladeur USB, appareil photo, etc.). Ces appareils lui sont personnels et Maurice pourra choisir librement celui ou ceux qui lui serviront aussi d'identifiants matériels via l'application MON-COMPTE décrite plus loin.

En effet, selon Mobilegov, chacun de ces appareils est unique et peut être identifié de façon difficilement falsifiable. Ces appareils sont banalisés : si Maurice perd ou se fait dérober son smartphone, il s'en apercevra rapidement, on peut espérer avant que le voleur n'ait pu l'utiliser pour usurper l'identité de Maurice sur le réseau, d'autant plus qu'un appareil seul ne permet pas d'accéder au réseau.

Scénario

Dans ce contexte, les opérations successives que Maurice effectue sur divers systèmes (PC, Voiture, PDA) sont reliées entre elles par une chaîne de sécurité. Le scénario est le suivant :

1. Maurice commence sa journée de travail en se connectant, via un PC (ou un smartphone ?) au système central
2. Puis il quitte le PC pour continuer à échanger des données depuis sa Voiture
3. Puis il quitte sa Voiture et continue à échanger des données via son PDA
4. Puis il revient à sa Voiture et continue à échanger des données soit depuis sa Voiture soit depuis son PDA. Les étapes 3 et 4 sont répétés un certain nombre de fois
5. Enfin il termine sa journée, Voiture et PDA sont éteints.

La chaîne de sécurité est la suivante :

1. PC (domicile ou autre) : Maurice dispose d'un accès sécurisé (par exemple VPN) aux données de l'entreprise protégé par un matériel d'authentification (smartphone ou dispositif USB) et code PIN. Pour se connecter au réseau de l'entreprise depuis n'importe quel PC, Maurice connecte au PC son matériel d'authentification et invoque l'application VPN. Le serveur de contrôle d'accès récupère l'ADN numérique des composants du poste de travail. Si l'identifiant matériel de Maurice est reconnu, un miniclavier logiciel aléatoire s'affiche pour lui permettre de saisir son code PIN. Ainsi, pas de risque de key logger qui conserverait un mot de passe. A noter que 2 possibilités sont offertes ici, et il faudra choisir : soit Maurice saisit son identifiant, soit son compte est déterminé par le serveur par la simple reconnaissance de l'identifiant matériel de Maurice. Voir www.id4yoo.com, Modèle n°1 pour une démo (création d'un compte sécurisé par l'ADN du Numérique)

2. Avant de fermer sa connexion VPN, d'éteindre son PC et de rejoindre sa voiture, Maurice active via l'application MA-VOITURE le système de communications de son véhicule. Il dispose alors d'un temps limité pour démarrer son véhicule, et pour retrouver, sans aucune procédure de login, toutes les données transférées automatiquement par le système central au système du véhicule.

3. Au plus tard lorsqu'il arrive sur les lieux de l'intervention, Maurice active le PDA. Un dialogue décrit dans l'application ASSOCIATION ci-dessous s'établit entre le système de voiture, le système central et le PDA pour activer la communication entre système central et PDA. Maurice peut alors échanger des données via le PDA comme avec le système de voiture. Il peut éteindre le système de voiture.

La coupure de la communication Bluetooth entre Voiture et PDA peut aussi désactiver le système de voiture.

4. Le système de voiture est alors verrouillé (il ne peut échanger de données avec le système central), tant que Maurice n'est pas revenu avec son PDA à son véhicule. Une solution de secours est possible pour réactiver le système de voiture, grâce à l'application MA-VOITURE invoquée cette fois via le smartphone. Si Maurice a égaré son PDA dans les hautes herbes, il lui reste la poêle à frire pour le retrouver. C'est peu probable si le PDA est cousu dans sa manche.

5. Rentré chez lui, Maurice éteint Voiture et PDA, qui ne peuvent être réactivés sans une authentification forte de Maurice sur le système central via un PC ou smartphone.

Applications à développer

- MON-COMPTE : logiciel de gestion de compte utilisateur, qui permet d'enrôler ou supprimer les matériels d'authentification et de gérer le code PIN. Voir www.id4yoo.com, option « Mon Compte » pour une démo. Il s'agit d'une application web, utilisable aujourd'hui depuis un PC, demain un smartphone, pour sécuriser un serveur web ou un contrôle d'accès corporate à la norme Radius.
- MA-VOITURE : logiciel de gestion du système de voiture. Depuis son PC ou son smartphone, sur lequel il s'est dûment authentifié et relié par VPN au système central, Maurice peut indiquer qu'il va quitter le PC pour prendre sa voiture et son PDA. Pas besoin de mot de passe. L'application permet à Maurice d'identifier la voiture et le PDA qu'il va utiliser. Il suffit de saisir le n° d'immatriculation du véhicule et/ou le n° d'inventaire du PDA. Le PDA étant équipé d'une puce, Maurice peut utiliser sa poêle à frire pour le lire, s'il a été effacé. Maurice dispose alors d'un temps limité pour mettre en route le système qu'il vient d'activer. Ainsi, il faudrait pour usurper son identité lui voler sa voiture ou son PDA pendant ce temps limité. L'activation déclenche automatiquement le transfert vers le système qui vient d'être activé des données nécessaires aux tâches définies dans l'OT de Maurice. Le système de la voiture ne communique avec le système central que s'il a été activé.

- ASSOCIATION : logiciel qui permet d'activer un système lorsqu'il est proche d'un autre système déjà activé. Par exemple, le PDA peut être activé s'il est à proximité d'un système de voiture en service selon le dialogue suivant :
    - Le PDA éteint est allumé
    - Le système de voiture le détecte (liaison Bluetooth ou RFID par exemple)
    - Le système de voiture interroge le PDA pour récupérer son ADN numérique
    - Il communique cet ADN numérique au système central
    - A partir de cet ADN, le système central identifie le PDA et active la communication avec lui, et lui transfère les données dont il a besoin pour accomplir les tâches de l'OT

  L'association est automatique, elle ne nécessite aucune action et aucune saisie de la part de l'opérateur.