Panoptinet

Gardez un oeil sur votre réseau

Les téléphones cryptés de la Défense française

admin · Friday, November 4th, 2011

Depuis peu La DGA fournit aux hautes autorités de l'Etat et aux forces armées un nouveau téléphone portable capable de chiffrer les conversations : Theorem.

Intercepter des conversations téléphoniques mobiles n'est pas bien sorcier. ça l'est encore moins pour les **agences de renseignement**, qu'elles soient gouvernementales ou privées. C'est pourquoi la DGA (**Direction générale de l'armement**) a développé un téléphone portable, conçu par **Thales**, capable de **protéger les conversations téléphoniques en les cryptant** : les échanges d'informations stratégiques par téléphone sont désormais beaucoup **plus difficiles à intercepter**.

Les communications qui passent par le téléphone mobile **Theorem** (Téléphone Cryptographique pour Réseau Etatique et Militaire) sont soumises à des a**lgorithmes et composants cryptographiques** gouvernementaux, et régies par un **système d'authentification** des correspondants basé sur des **certificats numériques**.

14 000 appareils doivent être mis en service. Ils sont compatibles avec tous les réseaux fixes, mobiles, civils, militaires et interministériels (interopérabilité).

C'est quoi une conversation cryptée ?

On le voit souvent dans les fictions anglo-saxonnes, les protagonistes d'une intrigue politique ou militaire demandent l'**accès à une ligne sécurisée**. Il s'agit en fait d'utiliser un téléphone, fixe ou mobile, qui permet de **chiffrer (crypter) la conversation**. Cela signifie que **le téléphone émetteur "brouille"** complètement le message à l'aide d'un code, le plus complexe possible, pour qu'il se soit pas cracké ou piraté facilement. De l'autre côté, l**e téléphone récepteur dispose déjà du code de chiffrement**. Il l'applique alors à la conversation, pour que celle-ci soit "dé-brouillée". Ainsi, si jamais un hacker a réussi à intercepter le signal d'appel, il ne pourra pas être en mesure de comprendre la conversation.

Les particuliers utilisent également des dispositifs de cryptage, sur leur réseau Wi-Fi par exemple : **chiffrements WEP, WPA, WPA2**, etc. Ils sont composés d'algorithmes plus ou difficiles à percer. Pour plus d'informations sur ces cryptages domestiques, vous pouvez lire ces **fiches Panoptinet** :

- Fiche théorique : les réseaux sans fil (Wi-Fi)
- Fiche pratique : la clé de cryptage (WEP, WPA, WPA2)

Et les américains, ils ont quoi comme super téléphone ?

La **NSA** (National Security Agency), qui collecte et analyse toutes sortes de communications, aura prochainement son propre **smartphone**. Son développement a été confiée à Troy Lange, responsable de la mission Mobilité. Le futur smartphone devra être suffisamment **sécurisé** pour permettre aux agents gouvernementaux qui utilisent des **informations hautement sensibles** de pouvoir **travailler en déplacement**.

La NSA prend très au sérieux les **menaces d'intrusion** via les appareils mobiles. C'est d'ailleurs pourquoi, jusqu'à présent, les agents devaient nécessairement se connecter sur leur poste fixe, connecté au serveur par un câble (pas de Wi-Fi), ne serait-ce que pour consulter leurs e-mails. Le but de Troy Lange est de **favoriser la mobilité sans entraver la sécurité**. Pas simple...

En résumé, le smartphone de la NSA sera basé sur un téléphone commercial existant, fonctionnant avec un système d'exploitation grand public. De nombreuses modifications particulières seront néanmoins apportées pour répondre au cahier des charges. Des **applications spécialisées** seront également développées pour améliorer l'efficacité à travers une meilleure mobilité.

A l'heure actuelle, les téléphones gouvernementaux sont sécurisés (cryptés), mais uniquement connecté au réseau d'Etat (Secret Internet Protocol Router Network). Comme le Theorem, le futur smartphone de la NSA pourra se connecter à l'ensemble des réseaux (interopérabilité), tout en préservant l'intégrité des informations confidentielles transmises. Car selon Lange, "*ce sont les informations qui sont confidentielles*", pas les appareils ou infrastructures.

Développé pour la NSA, le futur smartphone pourrait dépasser les frontières de l'Agence, et équiper "*chaque employé du Département de la Défense (DoD), de la communauté du renseignement, et du gouvernement*".

Sources : pro.01net.com / uberreview.com

This entry was posted on Friday, November 4th, 2011 at 2:57 pm and is filed under Actualités décryptées par Panoptinet
You can follow any responses to this entry through the Comments (RSS) feed. You can leave a response, or trackback from your own site.