Protection des équipements sans fil

Mars 2007

Livre blanc

Protection des micro-casques DECT™

Les produits sans fil DECT de Plantronics (CS60™, CS70™ et SupraPlus® sans fil) utilisent une technologie numérique et sont conformes aux conditions de sécurité DECT standard, comme souligné dans la norme ETSI EN 300 175-7.

La protection est l'un des points forts des systèmes DECT qui utilisent des ondes radio numériques TDMA/TDD et une sélection de canaux dynamique, en complément d'un système de sécurité à trois niveaux. Ce système à 3 niveaux (*vérification de connexion*, *cryptage* et *authentification*) assure un degré élevé de protection contre les écoutes indiscrètes :

1. Vérification de connexion

La base et les appareils distants sont couplés entre eux de façon à identifier facilement leur base ou leur appareil distant correspondant. Une clé secrète d'authentification est calculée à l'aide de l'algorithme d'authentification DSAA (DECT Standard Authentication Algorithm). Seuls les fabricants de ce type d'équipements ont accès à la définition de cet algorithme dans son intégralité.

2. Cryptage

Un cryptogramme est utilisé pour crypter les données transmises par communication radio.

3. Authentification

Les deux appareils vérifient que la clé d'authentification adéquate est utilisée et calculent également des cryptogrammes (utilisés pour crypter les données envoyées par ondes radio). Le protocole DECT Standard Cipher (DSC) d'encryptage numérique est utilisé ; là aussi, seuls les fabricants de ce type d'équipements ont accès à la définition de cet algorithme.

Protocole RF :

Grâce à l'allocation de canaux dynamique, le protocole RF fournit à lui seul un niveau élevé de protection grâce à des canaux et des horodatages modifiables selon l'environnement, sur 10 fréquences et 12 horodatages par opérateur (pour chaque communication).

Protection des oreillettes et micro-casques Bluetooth®

Malgré de nombreux rapports diffusés dans la presse sur les vulnérabilités de la technologie Bluetooth dans les appareils tels que les téléphones, les assistants numériques personnels, la connexion audio entre un téléphone et une oreillette ou un micro-casque Bluetooth de Plantronics est hautement sécurisée, grâce aux algorithmes d'authentification et de cryptage avancés.

Les micro-casques et oreillettes doivent être « détectables » (visibles par d'autres périphériques) pendant une courte durée uniquement, notamment lors de leur installation en vue d'une utilisation avec un nouveau périphérique (un nouveau téléphone portable, par exemple). Durant cette procédure (communément appelée « couplage »), les deux périphériques échangent des informations visant à établir une connexion « sécurisée ».

Remarque : pour le système Voyager™ 510 de Plantronics, la base qui se connecte au téléphone de bureau, n'est jamais en mode « détection ».

Une fois le couplage effectué, les oreillettes et micro-casques Plantronics ne sont plus visibles pour les autres périphériques et toutes les données transmises sont cryptées.

La procédure de couplage

Pour procéder au couplage, les informations suivantes doivent être échangées :

1. les adresses Bluetooth de chaque périphérique ;
2. un numéro d'identification saisi par l'utilisateur ;
3. un horodatage unique généré par le téléphone mobile.

Ces éléments sont associés pour générer une clé de sécurité à 128 bits utilisée pour les futures connexions entre le micro-casque ou l'oreillette et le téléphone (ou la base Voyager). Si l'adresse et le numéro d'identification peuvent être connus d'un éventuel auditeur indiscret, l'horodatage est extrêmement difficile à deviner ultérieurement.

Parce que toutes les communications entre les périphériques Bluetooth utilisent la technologie de transmission radio Frequency Hopping Spread Spectrum (FHSS), leur interception est particulièrement difficile.

Protection des conversations

Les micro-casques DECT Plantronics utilisent une clé de sécurité à 128 bits pour crypter numériquement les communications audio entre le micro-casque (ou l'oreillette) et le téléphone (ou la base Voyager), tout comme les signaux radio GSM entre le téléphone mobile et la base sont cryptés.

Bon nombre des prétendues vulnérabilités du Bluetooth ne s'appliquent pas aux micro-casques et aux oreillettes. Cependant, certaines procédures permettent d'améliorer la protection d'un téléphone, la plus importante consistant à désactiver le mode « détection » sur le téléphone.

Désactivation du mode « Détection » :

À moins qu'un utilisateur échange fréquemment des cartes de visite via Bluetooth, Plantronics recommande de régler son téléphone en mode masqué ou « non détectable » pour fonctionner avec une oreillette ou un micro-casque Plantronics ; celui-ci étant toujours en mode non détectable, sauf en cours de couplage.

En désactivant le mode « détection » de votre téléphone, vous réduisez le risque de vol de données Bluetooth (vol de vos contacts téléphoniques d'un téléphone ou d'un assistant numérique personnel Bluetooth). Pour rappel, de telles données ne peuvent être volées à partir d'une oreillette ou d'un micro-casque Plantronics, puisque ces derniers ne stockent aucune donnée.

S'ils sont utilisés correctement, les oreillettes et micro-casques Bluetooth et les téléphones auxquels ils sont couplés sont difficiles à attaquer. Néanmoins, les pirates sont extrêmement inventifs dans leurs méthodes, d'où l'impossibilité de garantir la sécurité de chaque appareil.

Toutefois, en raison de la faible puissance du signal Bluetooth (généralement 10 mètres de portée seulement), le piratage de ce type de connexion sécurisée est plus difficile. En réalité, ces pirates auraient plus de chances d'intercepter la communication en tendant simplement l'oreille à la conversation en cours.