Panoptinet

Gardez un oeil sur votre réseau

Le Bluetooth ? Pas vraiment sécurisé...

admin · Thursday, September 29th, 2011

Des test récents ont percé à jour les failles d'un système que l'on utilise au quotidien et dont on pense naïvement qu'il est parfaitement sécurisé : le Bluetooth. Quels sont les risques ?

C'est une entreprise finlandaise, Codenomicon Defensics, qui vient de révéler les menaces qui se cachent derrière le Bluetooth, technologie apparemment sécurisée. Les tests qu'elle a effectués étant particulièrement poussés, nous allons simplement présenter ici les principaux **défauts de sécurité**. Ceux qui veulent en savoir plus sur les aspects techniques peuvent consulter le détail des expériences (ENG).

La technologie Bluetooth équipe la plupart de **nos appareils mobiles** : smartphones, téléphones, tablettes, PDA, netbooks, laptops, etc. Les **failles Bluetooth** pointées par les chercheurs finlandais sont cruciales, parce qu'en les exploitant, un pirate peut facilement **obtenir les données personnelles** stockées sur un appareil mobile (smartphone, netbook, etc.). Le premier écueil concernant cette technologie est de croire aux idées reçues, comme par exemple la confiance absolue dans le **procédé d'appareillage** : "*un appareil reçoit une demande de connexion d'une autre machine, que l'utilisateur doit accepter pour permettre l'appareillage. La plupart du temps, cette autorisation doit être confirmée avec un code PIN*". Or cette soit-disante sécurité n'est pas si fiable que ça, puisque facilement contournable :

- Le code PIN n'est composé que de 4 caractères
- Il correspond très souvent à *1234* ou *0000*
- Sur certains appareils, le code *0000* est même implémenté en amont et ne peut être changé
- Les méthodes d'ingénierie sociale actuelles permettent d'obtenir ces codes des utilisateurs eux-mêmes

Par ailleurs, la plupart des utilisateurs sous-estiment largement **le nombre et la valeur des données personnelles stockées** sur leurs appareils mobiles. Ils s'en servent énormément, notamment pour se connecter à Internet via leurs différents

comptes : **Facebook, Twitter, mails, sites commerciaux, banques en ligne, etc.** Or, pour faciliter chaque authentification, les informations de connexion (**identifiants**) sont bien souvent **stockées sur le smartphone** (ou autre) : ainsi, nul besoin de les saisir à chaque utilisation ! Ces informations personnelles représentent une **mine d'or pour tous les hackers** – même débutants – qui peuvent les réutiliser (**usurpation d'identité**) ou les **revendre sur des marchés** spécialisés, généralement fréquentés par des personnes peu scrupuleuses…

Les failles de la technologie Bluetooth sont réelles et sont probablement **déjà exploitées**. La plupart des protocoles utilisés par le Bluetooth ont été testés par les chercheurs finlandais, et à leur grande surprise, les tests se sont révélés négatifs dans **80% des cas**. Même les protocoles considérés jusqu'alors comme les plus robustes (SDP, L2CAP, etc.) ont échoué. L'étude complète est consultable en ligne pour plus de détails.

Toujours est-il que les constructeurs ont négligé depuis un certain temps les critères de sécurité dans l'implémentation de la technologie Bluetooth sur nos appareils mobiles. Peut-être suivaient-ils eux aussi les mêmes idées reçues que nous, usagers ?

Si vous souhaitez vous protéger au maximum contre ce risque d'intrusion, vous pouvez déjà commencer par désactiver le Bluetooth sur vos différents appareils mobiles lorsque vous n'en avez pas l'utilité : non seulement vous annulez tous les risques, mais vous verrez également que vous économiserez votre batterie ! Ah, quand sécurité et écologie se rencontrent… 😉

Source : news.softpedia.com

This entry was posted on Thursday, September 29th, 2011 at 2:40 pm and is filed under Autres actualités
You can follow any responses to this entry through the Comments (RSS) feed. You can leave a response, or trackback from your own site.