



# CASES articles

La sécurité de l'information au Luxembourg sur le banc d'essai

## Êtes-vous repérable par Bluetooth ?

**Pour plus de sécurité, adoptez les réflexes CASES !**

**Plus de 4000 visiteurs du stand d'exposition CASES se sont révélés être « repérables ».**

De nombreux adultes ignorent que leur téléphone mobile dispose d'une interface Bluetooth et que l'activation de cette fonction peut constituer une faille de sécurité. Il suffit pourtant de jeter un œil dans les classes des écoles luxembourgeoises pour s'en rendre compte : enfants et adolescents savent en effet comment accéder à des téléphones mobiles étrangers grâce à Bluetooth. Ces agissements sont bien sûr illégaux.

C'est à l'automne 2007, lors d'un cours sur la sécurité de l'information, que les collaborateurs de CASES ont appris l'existence de « Super-Bluetooth ». Il s'agit d'un petit programme écrit par des crackers auquel les enfants luxembourgeois ont donné ce sobriquet plutôt pertinent. À l'aide de ce programme, il est en effet possible de prendre le contrôle de téléphones mobiles de tiers, par le biais de Bluetooth.

Ce programme permet de téléphoner aux frais d'autrui et également d'espionner le numéro du téléphone en question, de visualiser les photos et autres données qui s'y trouvent, de les transmettre, de les modifier, et même de les effacer. Il peut être obtenu gratuitement sur l'Internet et une notice d'utilisation peut être consultée sur le portail vidéo YouTube. Au cours de l'année scolaire 2007-2008, Super-Bluetooth a été observé de plus en plus souvent dans les écoles luxembourgeoises, et ce, dans diverses régions du pays.

Les enfants ignorent majoritairement que ces agissements sont contraires à la loi. Bien souvent ce sont également des phrases telles que « C'est de leur faute, ils n'ont qu'à pas laisser Bluetooth activé », qui fusent lorsqu'on les interroge à ce sujet.



CASES et le Service National de la Jeunesse voulaient en savoir plus et ont donc mis au point une expérience : à l'aide de deux antennes, de deux ordinateurs, de deux écrans géants et d'un programme « fait maison », le stand CASES a été transformé en laboratoire d'essais lors de la Foire d'automne 2008. Les visiteurs ont alors fait office de sujets et les infrastructures mises en place devaient scruter passivement les environs du stand d'exposition à la recherche d'appareils dont la fonction Bluetooth était activée. Les noms des appareils ainsi détectés étaient ensuite communiqués aux visiteurs à l'aide des deux écrans géants. Le but de l'opération était de déterminer si les visiteurs du stand connaissaient la fonction Bluetooth de leur téléphone mobile et s'ils l'avaient activée délibérément. Il s'agissait également d'établir si les utilisateurs avaient connaissance des possibles failles de sécurité et dangers émanant de Bluetooth.

### Titre intermédiaire : Résultats du test luxembourgeois relatif à Bluetooth

Plus de 4000 appareils, dont la fonction Bluetooth était activée, ont été répertoriés. Dans la plupart des cas, il s'agissait de téléphones mobiles, mais quelques ordinateurs portables et PDA ont également été détectés.

« En fait, nous disposons désormais d'une analyse de marché pour les téléphones mobiles : nous connaissons les modèles les plus utilisés à Luxembourg et dans sa région. De telles données peuvent se révéler très intéressantes, et pas seulement pour l'industrie. Les criminels peuvent exploiter ce genre d'information afin de mettre au point des attaques avec un maximum d'efficacité. Mais ce n'était pas le but de ce test. Il apparaît par contre que de nombreux adultes ignorent tout de Bluetooth, alors que les enfants l'utilisent aussi naturellement qu'un interrupteur pour l'éclairage, explique Pascal Steichen, responsable du dispositif de test pour CASES.

Outre la désignation de l'appareil proprement dit, de nombreux téléphones mobiles détectés lors de la Foire d'automne s'identifiaient par les noms et prénoms de leurs propriétaires, ou encore par des créations telles que « Souris Mignone », « Fan de Porsche », « Meilleur Steph du monde » ou « Superman ».

De nombreux visiteurs étaient très surpris de retrouver le nom de leur téléphone mobile sur les écrans géants et ignoraient pour la plupart que leur GSM possédait une fonction Bluetooth, que celle-ci était activée et que cela rendait leur appareil repérable pour des tiers.

Seules quelques personnes étaient au courant des failles de sécurité et des dangers liés à Bluetooth.

« Certains utilisateurs activent délibérément la fonction Bluetooth et agissent ainsi de façon imprudente. Mais notre test démontre que de nombreuses personnes ignorent tout simplement que leur téléphone mobile dispose d'une telle fonction et que celle-ci peut être activée. Ils ignorent également qu'une fonction Bluetooth activée est repérable par des tiers. De nombreux visiteurs de la foire ne savaient pas à quoi cette interface pouvait bien servir, ou comment la désactiver. Ils ignoraient également tout des dangers potentiels liés à une fonction Bluetooth activée. Les utilisateurs s'exposent donc à des risques sans même en avoir conscience. Le test démontre que la sensibilisation des utilisateurs dans ce domaine de la sécurité de l'information est absolument nécessaire...Il appartient à tout un chacun de prendre ses responsabilités », précise François Thill, responsable du portail de la sécurité de l'information luxembourgeois CASES.

Il est recommandé d'étudier attentivement la notice d'utilisation lors de l'achat d'un ordinateur ou d'un téléphone mobile. Les fonctionnalités décrites devraient être vérifiées soigneusement, car des données très personnelles sont bien souvent confiées à un téléphone mobile. Chaque utilisateur devrait de plus s'informer régulièrement des dangers et des mesures de protection éventuelles liés au monde numérique. Ceci n'est d'ailleurs guère plus compliqué que de s'informer sur les conditions météo en hiver, telles que le verglas ou la neige.

## **Présentation de Bluetooth**

De nos jours, quasiment tous les téléphones mobiles et tous les ordinateurs sont dotés d'une fonction Bluetooth.

### **Qu'est-ce que Bluetooth ?**

Bluetooth est un standard industriel. Initialement développé par Ericsson au cours des années 90, il était destiné à la liaison sans fil d'appareils sur de courtes distances. Bluetooth permet la communication entre petits appareils mobiles et entre ordinateurs et équipements périphériques. Des exemples d'application sont par exemple la liaison entre une souris et un ordinateur ou encore celle entre un micro-casque et le kit mains libres d'un téléphone mobile dans une voiture.

### **Comment fonctionne Bluetooth ?**

Bluetooth est une technologie de transmission reposant sur les ondes radio dans une gamme de fréquences de 2,4 à 2,4835 GHz. Ce système radio permet la transmission de la voix et de données. Le rayon de la zone de réception se situe entre un et trente mètres. La propagation des signaux est toutefois rapidement perturbée par des obstacles, tels que des murs ou des cloisons.

En fonction de leur puissance d'émission, les interfaces Bluetooth sont classées dans trois catégories : classe 3 pour une puissance d'émission couvrant jusqu'à dix mètres, classe 2 pour une couverture jusqu'à 30 mètres et classe 1 pour une couverture jusqu'à 100 mètres. Les téléphones mobiles sont généralement équipés d'interfaces Bluetooth de classe 2 et disposent ainsi d'une puissance d'émission couvrant jusqu'à 30 mètres.

À l'aide d'antennes spéciales, il est toutefois possible de recevoir des signaux émis par des appareils Bluetooth distants jusqu'à deux kilomètres. Les personnes laissant la fonction Bluetooth activée sur leur téléphone mobile ou sur leur ordinateur augmentent considérablement le risque de devenir victimes d'une attaque Bluetooth.

## **Quels sont les domaines d'application de Bluetooth ?**

La technologie Bluetooth permet la détection et la configuration automatiques ainsi que l'établissement automatique de liaisons entre appareils. Ordinateurs, téléphones mobiles ou lecteurs MP3, tous les appareils peuvent être synchronisés et reliés entre eux sans fil, automatiquement. Bluetooth permet aux enfants par exemple d'échanger des sonneries, des photos ou de la musique. Les adultes ne devraient d'ailleurs pas hésiter à demander une sonnerie pour leur téléphone mobile à leurs enfants. Ceux-ci seront alors certainement ravis d'expliquer comment fonctionne la transmission d'une sonnerie par Bluetooth et les parents peuvent ainsi faire rapidement et simplement connaissance avec les applications de cette technologie.

### **Les dangers liés à Bluetooth**

**Bluejacking**: il s'agit de la réception par le propriétaire d'un téléphone mobile de messages qu'il n'a pas sollicités. Étant donné que la personne ayant reçu un tel message ignore comment celui-ci lui est parvenu, il est possible qu'elle pense qu'une défaillance du téléphone mobile en soit responsable. Les téléphones mobiles modernes permettent également la transmission de photos ou de musique. Des attaques à l'aide de malwares, pouvant se traduire par une prise de contrôle de l'appareil concerné, ne peuvent désormais plus être exclues. Depuis quelques années, Bluetooth est également utilisé pour la propagation de vers à destination des téléphones mobiles.

**Bluesnarfing**: découverte en novembre 2003, cette attaque exploite une faille de sécurité à l'aide de programmes de crackers spécifiques. À l'insu de l'utilisateur, le bluesnarfing obtient accès à l'agenda, au carnet d'adresses, aux e-mails et à d'autres données. Quiconque ayant activé une liaison Bluetooth peut ainsi être attaqué, et cela même lorsque l'appareil a été configuré de manière à rendre la liaison invisible à des tiers. La seule protection contre le bluesnarfing consiste à désactiver la fonction Bluetooth.

Le **bluebugging** permet à des utilisateurs de téléphones mobiles d'accéder à d'autres GSM. L'attaquant a ensuite par exemple la possibilité d'émettre et de recevoir des appels par le biais de ce téléphone, d'écouter des conversations ou encore d'activer la connexion à Internet.

Bluesnarfing et bluebugging diffèrent l'un de l'autre : ils exploitent des points faibles différents, dont certains sont humains. Afin de remédier à ces points faibles, certains fabricants proposent des programmes de mise à jour du firmware de l'appareil.

### **Mesures de protection**

Les utilisateurs devraient vérifier la présence d'une fonction Bluetooth sur leur appareil, par exemple ordinateur, ordinateur portable ou téléphone mobile.

Sur un téléphone mobile, la fonction Bluetooth peut par exemple être activée ou désactivée. Lorsque cette fonction est activée, l'utilisateur peut choisir si l'appareil doit être « visible » pour les autres ou non.

Si la fonction Bluetooth est activée, l'utilisateur devrait opter pour le réglage « non visible ». La meilleure protection reste toutefois de désactiver la fonction Bluetooth dès qu'elle n'est plus nécessaire.

Les utilisateurs devraient en outre régulièrement se tenir informés des points faibles et dangers éventuels et procéder à la mise à jour du firmware de leur appareil. Ceci permet de remédier aux points faibles identifiés et pour lesquels le fabricant propose des solutions.

Les ordinateurs, et même les téléphones mobiles, doivent être dotés d'un programme anti-virus mis à jour régulièrement et d'un pare-feu correctement paramétré.

Un récapitulatif détaillé des dangers, points faibles et mesures de protection est disponible sur le site [www.cases.public.lu](http://www.cases.public.lu), sous la rubrique Dossier dans « (in)sécurité Bluetooth ».

Retrouvez les dossiers, fiches thématiques alertes et actualités sur:

[www.cases.lu](http://www.cases.lu)