



(In)sécurité Bluetooth

Pour plus de sécurité, adoptez les réflexes CASES !

Dans les années à venir, le système Bluetooth équipera de plus en plus de périphériques de communication, augmentant par là-même l'ergonomie des équipements, mais facilitant en contrepartie l'accès des attaquants à une masse toujours croissante de données personnelles.

S'il peut s'avérer difficile, voire aléatoire de contrôler les agissements de certaines personnes malhonnêtes, il n'en reste pas moins qu'il est tout à fait possible et même fortement conseillé, d'assurer soi-même, et ce très simplement, la sécurité de son matériel. (Entre autres, ne pas divulguer ses mots de passe, ne coupler son périphérique qu'avec des appareils connus, le placer en mode non détectable, utiliser les patchs de mise à jour du système d'exploitation de l'équipement, etc.).

En conséquence, ce dossier a pour mission de favoriser une prise de conscience collective quant aux dangers liés aux techniques d'attaques (cracking) et d'attirer l'attention de chacun sur certaines astuces facilitant la mise en place d'une politique de sécurité « personnalisée », permettant de faire fonctionner en toute confiance les appareils dotés de la technologie Bluetooth.

Qui est concerné ?

Pour tous les détenteurs d'appareils de communication de proximité, qui souhaitent se libérer des contraintes que représentent les câbles de connexion entre les divers périphériques et se constituer ainsi un réseau de communication personnel sans fil, la technologie de communication radio Bluetooth représente un formidable progrès.

De ce fait, si à ses débuts cette technologie a été plus particulièrement élaborée pour équiper des appareils de type assistants personnels et téléphones portables, aujourd'hui, les périphériques tels que :

- Les laptops,
- Les imprimantes,
- Les claviers,
- Les souris,
- Les lecteurs MP3,
- Les micros,
- Les casques,
- Les oreillettes kit main libre,
- Les enceintes audio,
- Etc,

peuvent en être très facilement dotés ; d'où le nombre toujours croissant d'acquéreurs de matériel compatible Bluetooth.

Comment fonctionne la sécurité Bluetooth ?

La technologie de communication sans fil Bluetooth a pour vocation de transmettre, en toute sécurité, des données numériques et vocales véhiculées par ondes radio calées sur la bande de fréquence 2,4 à 2,4835 Ghz.

« Frequency hopping »

Grâce à cette méthode il est quasiment impossible pour un tiers, de pouvoir écouter la communication en mode Bluetooth, engagée par 2 personnes. Ainsi, la fiabilité et la confidentialité des échanges restent assurés.

Note technique

La bande de fréquence associée au protocole Bluetooth permet l'établissement de 79 communications en parallèle, ce qui, via le système de frequency hopping dans lequel la fréquence change de canal toutes les quelques nano-secondes, rend l'écoute des communications quasi impossible.

Cependant, des sociétés spécialisées ont développé des outils spécifiques pour suivre le « hopping » et pouvoir écouter ainsi les communications ; néanmoins, leur prix élevé (~10000\$), ne prédispose pas ces techniques à être à la portée de tout un chacun).

Distances de connexion

A l'origine, la norme Bluetooth a été développée pour équi- per principalement des périphériques d'utilisation courante que l'on souhaite connecter entre eux, tels que claviers, souris, PDA, GSM, etc.

Le fait que la technologie ait été pensée pour ce type de matériel explique une distance maximale de connexion rela- tivement courte.

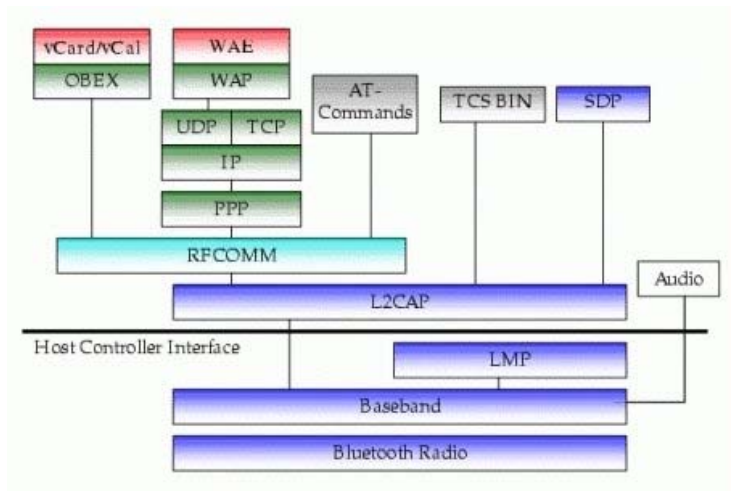
A ce jour, 3 classes spécifiques définissent les distances des zones de réception du signal émis par un périphérique doté de Bluetooth.

Classe - Portée du signal

- Classe 3 : jusqu'à 10 mètres,
- Classe 2 : entre 20 et 30 mètres,
- Classe 1 : jusqu'à 100 mètres.

En effet, afin d'assurer une meilleure sécurité à l'utilisateur, le protocole limite volontairement (et en fonction du périphé- rique utilisé), la distance maximale de portée du signal ; néanmoins, la vigilance reste de mise puisque les tests réa- lisés en ce sens ont révélé qu'avec des antennes adaptées, des connexions ont pu être établies jusqu'à quelques kilo- mètres de l'émetteur. Bluetooth étant une technologie de communication sans fil, il est indéniable qu'un dépassement de la distance officiellement indiquée est toujours possible.

Note technique



Architecture des protocoles Bluetooth

- *Bleu et rfcmm* : spécifique à Bluetooth
- *Vert* : adopté (existant -> adopté dans la technologie Bluetooth)
- *Gris* : lié à la téléphonie (fax, etc.)
- *Rouge* : applicatif (adopté)

Quelques détails préalables

LMP

"Link Manager Protocol", responsable de la liaison entre équipe- ments Bluetooth, des mécanismes de sécurité, comme l'authenti- fication et l'encryption sont implémentés dès ce bas niveau.

L2CAP

"Logical Link Control and Adaptation Protocol", fait le lien avec les couches plus hautes.

RFCOMM

"Cable Replacement Protocol", fournit le canal de transport pour la communication, nécessaire à la plupart des applications.

SDP

"Service Discovery Protocol", sous-jacente à la plupart des com- munications, se charge de fournir les informations sur les services disponibles et leurs caractéristiques (de sécurité par exemple).

AT commands

Commandes pour l'utilisation des fonctions modem et fax d'un équipement Bluetooth.

OBEX

"Object Exchange Protocol", repris de l'assoc IrDA (infra rouge), permet des échanges simples d'objets (fichiers, etc.) similaires au HTTP sur Internet.

vCard/vCal

Des formats de données ouverts pour des cartes de visite (busi- ness cards) et des agendas personnels, respectivement utilisés dans les applications Contact et Calendrier.

Modes de sécurité

Dans la technologie Bluetooth, la sécurité est incluse dès le plus bas niveau et supporte l'authentification (unidirectionnelle ou mutuelle) et le chiffrement (encryption). L'implémentation de la sécurité passe par ce que l'on appelle le profil d'accès générique, qui définit 3 modes de sécurité :

Mode de sécurité 1 (pas de sécurité) :

Aucune procédure de sécurité n'est initiée.

Mode de sécurité 2 (sécurité au niveau services) :

Procédure de sécurité au niveau des différents services, flexible et adaptable par service (transfert fichiers, contact, synchronisation, accès Internet, etc.).

Dans ce mode, 3 niveaux sont possibles :

- Authentification et autorisation des équipements vis-a-vis des services,
- Uniquement authentification,
- Ouvert à tous.

Mode de sécurité 3 (sécurité au niveau équipement) :

Toutes les procédures de sécurité sont utilisées dès le niveau le plus bas (via LMP),

3 niveaux de confiance sont définis pour les équipements :

- Equipement "trusted", une authentification ainsi qu'une autorisation sont préalablement demandées,
- Equipement non-"trusted", seule une authentification est valide,
- Equipement inconnu.

En plus de ces différentes possibilités pour l'accès aux services et/ou équipements, il est possible d'activer l'encryption au plus bas niveau, dans les modes 2 et 3. Pour toute une série de services le chiffrement est activé par défaut, on peut donc considérer que très peu d'informations sont envoyées "en clair".

Système de couplage (« pairing procedure »)

L'existence d'un mécanisme nommé l'échange de clés, (encore appelée couplage) est à souligner. En effet, il est important pour le propriétaire de 2 appareils compatibles Bluetooth de pouvoir établir une connexion sécurisée entre eux. Il est alors possible d'accéder, à partir de l'un des appareils, aux services partagés situés sur l'autre appareil. Cependant, gardez à l'esprit qu'il peut s'avérer dangereux de coupler son périphérique avec des appareils inconnus, car ceux-ci auraient alors accès à tous les services dont vous bénéficiez.

Pour effectuer un couplage il suffit de créer un code PIN lors de la première connexion du périphérique, (code à ne partager qu'avec des individus et des équipements de confiance). Ce code peut en théorie occuper 16 positions à caractères alphanumériques ; sachant toutefois que dans la pratique, l'on a tendance à opter pour 4 positions numériques, il est conseillé aux utilisateurs d'en choisir un à 8 caractères alphanumériques minimum ; ce qui va créer une clé de session permettant la connexion. Par la suite, les autres connexions pourront automatiquement être réalisées par la réutilisation directe de cette clé, il ne sera donc pas nécessaire de réencoder le PIN.

Néanmoins, afin de limiter les risques, après un certain laps de temps il est fortement conseillé de renouveler cette clé, ce qui peut être facilement effectué en changeant uniquement le code PIN.

Mesures de protection

La plupart des appareils bénéficiant de Bluetooth (PDA, GSM, etc.) permettent d'être placés, à loisir, en mode non détectable par leur propriétaire. Cette fonction permet à celui-ci, s'il le souhaite, de passer inaperçu en cas de recherche par un autre utilisateur de cette technologie dans son champ d'action. (Tout l'intérêt de cette précaution résidant dans le fait qu'elle

n'a pas d'impact sur les fonctionnalités des appareils couplés). Cependant si une personne connaît l'adresse spécifique de l'équipement, elle pourra tout de même se connecter, et ce, même si ladite fonction est inactivée...

Il est également conseillé de protéger ses données sensibles :

- En évitant de coupler son périphérique avec un appareil inconnu,
- En refusant une invitation à coupler son téléphone avec un autre équipement,
- En ne saisissant pas son code PIN, si l'on n'est pas sûr de l'identité de l'émetteur,
- En mettant à jour le système d'exploitation de son équipement avec les derniers patchs (il en existe également pour GSM, imprimantes, PDA, etc.),
- Etc.

Enfin, la possibilité de désactiver le système Bluetooth représente la manière la plus simple et la plus efficace de se protéger d'une attaque potentielle !

Conclusion

Au vu de ces diverses possibilités, il est indéniable que le système autorise une grande souplesse d'utilisation et qu'un usager, averti et conscient des enjeux, peut aisément se prémunir contre la plupart des risques de cracking.

Enfin, grâce à une utilisation de plus en plus répandue et intensive des appareils équipés du système Bluetooth, quelques vulnérabilités portant sur la sécurité du protocole ont pu être détectées et des failles ont été précisément isolées au niveau des mécanismes d'authentification et de transfert de données.

De ce fait, les concepteurs se sont attachés à renforcer le volet sécurité du système qui, depuis lors, a évolué dans le sens d'une protection accrue dans ses diverses utilisations. Néanmoins, et bien que Bluetooth con-

tienne toute une série de mécanismes de sécurité, tout propriétaire d'un appareil compatible avec cette technologie doit pouvoir assurer la sécurité de ses équipements. Il est ainsi conseillé de s'informer sur les différents types d'attaques dont peuvent être victimes les périphériques dotés de cette technologie.

Techniques d'attaques et vulnérabilités associées

BlueJacking

Historiquement, la raison d'être du BlueJacking était de permettre aux possesseurs de GSM utilisant la technologie sans fil Bluetooth, d'envoyer leur carte de visite sous couvert de l'anonymat. Cette fonction première ayant été quelque peu « contournée », une des tendances actuelles est de créer un contact dans le répertoire et d'entrer, dans le champ « nom », des messages très divers, du type « Vous avez été « blueJacké », « J'aime bien tes chaussures », « Votre cravate est mal nouée », etc. et de profiter du spectacle que cette entrée en matière provoque ! Ce type de mise en relation peut paraître surprenant mais pourrait être le point de départ de situations, voire de rencontres, plutôt amusantes... d'autant plus que cette « intrusion » ne permet ni l'altération, ni la suppression de données et qu'il suffit de se mettre en mode invisible pour ne pas y être exposé.

A ce titre, le BlueJacking n'est pas réellement considéré à ce jour comme une attaque sérieuse.

Note technique

Le bluejacking utilise OBEX pour échanger des vCards personnalisées.

BlueSnarf

L'attaque BlueSnarf, identifiée en septembre 2003, a été le premier gros problème de sécurité répertorié, en ce qui concerne les GSM dotés de la technologie Bluetooth. Elle permet au pirate d'extraire des données confidentielles d'un téléphone mobile, sans que son propriétaire en soit alerté (ré-

cupération du calendrier, consultation du carnet d'adresses, d'images enregistrées, du répertoire des codes PINs, écoutes sauvages, etc.).

Note technique

L'attaque BlueSnarf se connecte à la cible OBEX PUSH (qui permet le transfert de petits fichiers entre des périphériques) et exécute une requête OBEX GET pour des noms de fichiers connus tels que « telecom/pb.vcf » contenus dans un répertoire téléphonique et « telecom/cal.vcs » contenus dans l'agenda. (les noms de fichiers sortent des specs IrMC).

BlueSnarf ++

BlueSnarf ++ est en quelque sorte un prolongement de l'attaque BlueSnarf. L'attaquant a un plein accès en lecture et écriture au système de fichiers du périphérique. Il a l'opportunité de voir tous les fichiers contenus dans le système, (même ceux éventuellement stockés sur des mémoires de type « memory sticks » ou cartes SD) mais aussi le pouvoir de les effacer.

Note technique

Plutôt qu'un fonctionnement moins performant d'OBEX PUSH, ces périphériques utilisent le serveur FTP OBEX interne, et ce, sans couplage.

BlueBug

BlueBug est le nom d'une vulnérabilité détectée en 2004 affectant la sécurité de certains téléphones cellulaires utilisant Bluetooth.

Exploiter cette faille, qui revient à se faire passer pour une oreillette, permet à l'attaquant de pirater un téléphone en :

- Passant un appel téléphonique,
- Envoyant des SMS vers n'importe quel numéro,
- Lisant les SMS reçus,
- Lisant le répertoire téléphonique,
- Entrant des données dans le répertoire,
- Faisant suivre des appels,
- Interceptant des communications,
- Se connectant à Internet,
- Forçant le téléphone à recourir aux services de certains fournisseurs d'accès en particulier,

- Etc.

Il faut savoir que dans des conditions « idéales » d'utilisation, une attaque BlueBug ne prend que quelques secondes et que le propriétaire n'en est aucunement alerté.

Le pirate détient ainsi un contrôle quasi total du périphérique de sa victime (GSM) et peut bien évidemment causer d'énormes torts, comme vous pouvez l'imaginer !

Note technique

La faille permet d'utiliser les commandes AT du téléphone vulnérable **et autorise ainsi un contrôle quasi-total du mobile.**

Helomoto

Cette attaque, appelée ainsi depuis sa découverte sur un téléphone Motorola est, en quelque sorte, une combinaison des attaques BlueSnarf et BlueBug. Elle s'explique par une mauvaise implémentation de certains composants installés sur des appareils Motorola.

L'attaquant initie l'envoi d'une carte de visite et interrompt le processus avant la fin, son périphérique sera ainsi répertorié dans la liste des « périphériques de confiance » du téléphone de la victime. Une fois intégré dans cette liste, l'attaquant est capable de se connecter quand il le souhaite et ce, sans authentification préalable puisqu'il sera automatiquement reconnu.

Note technique

L'envoi partiel de la vCard se fait comme toujours via OBEX PUSH. L'attaquant pourra, par la suite, prendre le contrôle du périphérique par le biais des commandes AT (comme dans l'attaque BlueBug).

BlueSmack

Avec BlueSmack, il s'agit de solliciter une demande de réponse continue depuis l'équipement compatible Bluetooth du pirate, auprès de l'appareil victime. Le pirate occupe le lien Bluetooth avec des demandes de communication non valides, ce qui produit ainsi un déni de service sur l'appareil.

Note technique

L'attaque *BlueSmack*, similaire à celle du « ping of death », permet de causer un DoS (*Denial of Service*) (déni de service) sur des équipements Bluetooth via la couche L2CAP (sans nécessiter un canal L2CAP ouvert) et peut faire planter les périphériques.

Beaucoup d'iPaqs sont particulièrement vulnérables à cette attaque.

BlueStab

Autre attaque de déni de service qui utilise simplement le nom du périphérique attaquant. En ajoutant des caractères de tabulation et/ou des points dans le nom de ce dernier, il est possible de planter certains périphériques mobiles.

Note technique

Ceci est dû à une mauvaise conversion unicode des caractères « tab » et/ou « dot ».

BlueBump

Cette attaque nécessite l'intervention de « social engineering » (ingénierie sociale). Le scénario suivant explique son fonctionnement :

L'attaquant établit une connexion de confiance avec un autre périphérique. Ceci peut être concrétisé par l'envoi d'une carte de visite en forçant le receveur à s'authentifier. L'attaquant garde la connexion ouverte et demande à la victime d'effacer la clé de lien. Puis l'attaquant demande la réactivation d'une clé de lien. En faisant cela, le périphérique de l'attaquant obtient une nouvelle entrée dans la liste « des périphériques de confiance ». L'attaquant sera donc capable de se connecter au périphérique à n'importe quel moment et tant que la clé de lien ne sera pas effacée.

BlueSpoon

Dans l'attaque *BlueSpoon*, un périphérique doté du Bluetooth peut être cloné par simulation de son adresse, de son profil, de ses services, etc.

L'attaquant peut ainsi se connecter à tous les appareils auxquels le périphérique cloné a été connecté au

moins une fois, et si ce dernier figure toujours dans la liste des « périphériques de confiance ».

BlueDump

Cette attaque permet de retrouver le code PIN et de ce fait, la clé de liaison d'une communication Bluetooth, en observant le processus de couplage (pairing).

Cependant pour exécuter cette attaque, des équipements spécifiques sont nécessaires, permettant de suivre le frequency hopping et ainsi d'écouter la communication et plus spécifiquement le processus de couplage (pairing).

BlueTooone

Technique consistant, grâce à une certaine manipulation d'un dongle Bluetooth, à augmenter la distance des attaques grâce à l'amélioration des antennes. Des distances de connexion de plusieurs kilomètres ont été réalisées à ce jour.

BlueChop

Cette attaque permet en quelque sorte de couper la communication de tout un réseau de périphériques Bluetooth (ce que l'on appelle un « piconet »).

Outils et malware

BluePrinting

La technique de *BluePrinting* consiste en l'élaboration de statistiques sur les équipements Bluetooth, permettant d'identifier ainsi les appareils ne remplissant pas l'ensemble des garanties en matière de sécurité. Ceci en vue de créer un répertoire des équipements vulnérables.

Note technique

Pour le *blueprinting* on utilise les informations sur les services fournis par le protocole SDP.

RedFang

Logiciel capable de détecter des périphériques dont la fonction « non détectable » a été activée. Pour entrer en contact avec un périphérique, *RedFang* passe en revue toutes les adresses possibles dans le but de trouver celle qui lui a été attribuée au moment de sa fabrication par le constructeur.

Note technique

RedFang est une attaque classique du type « brute force » sur l'adresse Bluetooth d'un équipement.

Bloover, Bloover II

Jusqu'à présent, les attaquants avaient recours à un ordinateur portable pour soutirer les informations des périphériques Bluetooth. *Bloover* est une application qui s'installe sur un téléphone mobile Bluetooth et qui permet d'exploiter les failles *BlueBug* sur tous les autres mobiles se trouvant à proximité. *Bloover II* inclut de nouvelles possibilités, notamment des attaques basées sur: *BlueSnarf*, *HelloMoto*, *BlueSmack*, *BlueStab* et d'autres.

Note technique

Bloover et Bloover II, étant des applications Java, elles nécessitent un téléphone implémentant la norme J2ME MIDP2.0 ainsi que l'API Bluetooth JSR-82.

Bloonix

Nom du projet destiné à créer un CD incluant les pratiques et outils discutés ici. (Sachant que ce CD n'existe pas encore).

Note technique

C'est en fait un « liveCD » (basé sur un système Knoppix), contenant toute une panoplie d'outils Bluetooth.

BluePot

Logiciel que l'on peut installer sur son GSM et qui a pour fonction d'imiter les vulnérabilités déjà répertoriées (BlueBug, BlueSnarf, etc.); le but étant d'enregistrer les comportements d'attaques sur son périphérique.

Note technique

C'est en fait un « honeypot » bluetooth, ayant aussi des fonctions de réponse sur attaques.

Car Whisperer

Logiciel destiné à tester à distance la sécurité des systèmes Bluetooth installés dans les automobiles (kits main libres, etc.). Il permet d'envoyer et de recevoir des signaux audio, pour en quelque sorte « converser » avec le chauffeur du véhicule.

Note technique

L'outil « car whisperer », utilise simplement les codes PIN par défaut des systèmes Bluetooth automobiles (qui d'ailleurs ne peuvent pas toujours être changés), pour se connecter. L'envoi et la réception audio se font par le biais de fichiers « wav ».

Blueworms

Cabir : Premier ver se propageant (à l'insu des utilisateurs) via la technologie Bluetooth sur des smartphones (GSM ou PDA) dotés de cette technologie.

Il a pour but d'infecter automatiquement d'autres smartphones via les connexions Bluetooth présentes dans son environnement. Bien qu'il ne cause pas de dommages importants, sa présence dans la mémoire et le fait qu'il soit constamment à la recherche d'appareils actifs Bluetooth, peut perturber le fonctionnement normal du téléphone infecté. De plus, c'est un gros consommateur de batterie. Sachez enfin que le ver maintient l'interface Bluetooth activée même si vous essayez de l'éteindre.

Mabir : Mutation du ver Cabir proliférant par l'envoi de MMS, ce qui peut entraîner d'importants problèmes de coûts.

Présentation d'un programme de démonstration

Afin de proposer aux utilisateurs une aide efficace en matière de protection contre certains types d'attaques, les ingénieurs de CASES ont reconstitué 3 attaques Bluetooth classiques.

Les screenshots suivants présentent le résultat des attaques BlueSnarf et BlueBug.

```
*****
*          CASES & Telindus PSF bluetooth demo crack          *
*          -----                                           *
*                                                                 *
*          Idea & Code by Thierry Zoller, Pascal Steichen     *
*          based upon Bluesnarfer and Redfang.                *
*                                                                 *
*****
Menu:
-----
1. Standard scan for devices
2. Brute search hidden devices
3. Read private information
4. Read Phonebook entry N
5. Search name in Phonebook
6. Delete Phonebook entry N
7. Dial number
8. Take call
9. Denial of Service (hinder calling)
10. Denial of Service (crash)

0. Reset device or exit demo
-----

Enter Command: █
```

Ci-dessous la présentation (visuellement différente) des informations soutirées selon l'attaque utilisée :

BlueSnarf

La lecture de toutes les informations contenues dans le GSM peut se faire par le biais de cette attaque classique. Ainsi, l'attaquant peut télécharger les informations trouvées telles que des noms de contact, des coordonnées, prendre connaissance du calendrier, etc.

```
BEGIN:VCARD
VERSION:2.1
N:-Claude;Jean
TEL;PREF:+352508636
END:VCARD
BEGIN:VCARD
VERSION:2.1
N:Lolly
TEL;PREF;VOICE:00352044000035
END:VCARD
BEGIN:VCARD
VERSION:2.1
N:
FN:
TEL:
END:VCARD
BEGIN:VCARD
VERSION:2.1
N:
FN:
TEL:
END:VCARD
BEGIN:VCARD
VERSION:2.1
N:Georges
TEL;PREF;VOICE:00352044000035
END:VCARD
BEGIN:VCARD
VERSION:2.1
N:
FN:
TEL:
END:VCARD
BEGIN:VCARD
VERSION:2.1
N:Charles
TEL;PREF;VOICE:0213000000
END:VCARD
BEGIN:VCARD
VERSION:2.1
N:Home;Charles
TEL;PREF;VOICE:7200000
END:VCARD
```

BlueBug

En plus des informations générales du GSM (adresse unique donnée par le constructeur, le nom que vous lui avez personnellement attribué, etc.), l'attaquant récupère, via la commande AT, et en se faisant « passer » pour l'oreillette Bluetooth du GSM, les informations contenues dans le carnet d'adresses, le journal, etc. Il peut prendre connaissance de la mémoire du GSM, des informations de la carte SIM, des SMS lus ou pas, passer un appel, effacer des entrées etc. Cette attaque est une porte ouverte aux exactions les plus graves car le GSM obéit strictement aux ordres de son oreillette.

```
-----
"00:02:EE:4E:F1:B8" "Nebucadnezar"
-----
Constructeur: Nokia
Modèle: Nokia 6310i
Version: V 5.50 03-03-03 NPL-1 (c) NNP.
Numéro IMEI: 350780208"
-----
Contacts: "ME" "500"
Entry #3:
Name: R Vinck
Number: 003215
-----
Contacts: "DC" "20"
Entry #1:
Name: Juliane H
Number: 00491
-----
Contacts: "MC" "10"
Entry #1:
Name: CFB
Number: +3525
-----
Contacts: "RC" "10"
Entry #1:
Name:
Number: +4968
-----
Contacts: "SM" "250"
Entry #1:
Name: Marco Mowson
Number: +352091
-----
SMS Container: "ME"
-----
SMS Container: "SM"
SMS Message: "REC READ", "+3520", "05/05/02,09:20:32+08" Hast du die od vergessen?
SMS Message: "REC READ", "+3520", "05/05/02,09:39:28+08" Dann eben heut abend. :)
```

Conclusion

Il faut savoir que quel que soit le modèle de GSM que vous possédez, celui-ci est potentiellement vulnérable à une de ces attaques, voire à plusieurs d'entre elles. En effet, certains sont plus sensibles au protocole Obex, d'autres au protocole de commandes AT et d'autres,...aux deux ! L'attaquant doit donc tester les différentes techniques pour trouver celle qui réussira à atteindre votre appareil. Sachant encore que le protocole Obex (via l'attaque BlueSnarf) pourra « seulement » lui permettre de lire les informations contenues dans votre

périphérique alors que le protocole de commandes AT (via l'attaque BlueBug) lui permettra d'en prendre le contrôle total, ce qui rend cette attaque extrêmement dangereuse.

Enfin, la combinaison de diverses attaques est toujours possible et engendre de réels scénarios catastrophes ! Ainsi un attaquant muni des équipements nécessaires a, par exemple, la possibilité d'écouter des conversations privées ou « d'assister » de manière virtuelle à une réunion confidentielle.

Il peut réussir à envoyer un SMS en lieu et place du propriétaire du GSM ; etc.

Sachez toutefois que même si les outils permettant de perpétrer ces attaques sont librement disponibles sur Internet, celles-ci ne sont possibles qu'à partir de PC tournant sous système d'exploitation Linux.

De plus, si vous restez vigilant et appliquez les mesures de sécurité présentées dans ce dossier, il y a peu de risques que vous deveniez à l'avenir, victime de manœuvres indécrites et que vous figuriez sur le tableau de chasse des crackers !

Sources

- bluetooth.com
- bluejackq.com
- bluestumber.org
- trifinite.org
- [Bluesniper Rifle](#)
- secuobs.com

Retrouvez les dossiers, fiches thématiques alertes et actualités sur:

www.cases.lu