



Affaire suivie par :  
CERTA

## NOTE D'INFORMATION DU CERTA

### Objet : Sécurité des réseaux sans fil Bluetooth

---

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>  
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-003>

---

### Gestion du document

Référence	CERTA-2007-INF-003
Titre	Sécurité des réseaux sans fil Bluetooth
Date de la première version	01 août 2007
Date de la dernière version	–
Source(s)	
Pièce(s) jointe(s)	Aucune

TAB. 1 – Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

### Table des matières

<b>1</b>	<b>Introduction</b>	<b>2</b>
<b>2</b>	<b>Présentation de la technologie Bluetooth</b>	<b>2</b>
2.1	Réseau personnel sans fil de courte portée . . . . .	2
2.2	Bluetooth 1.2 et Bluetooth 2.0 . . . . .	3
2.3	Distance et puissance . . . . .	3
2.4	Profils Bluetooth . . . . .	3
<b>3</b>	<b>Sécurité et technologie Bluetooth</b>	<b>4</b>
3.1	Mode de sécurité . . . . .	4
3.2	Jumelage ou couplage . . . . .	4
3.3	Mode découverte . . . . .	5
<b>4</b>	<b>Risque associé à l'utilisation de la technologie Bluetooth</b>	<b>5</b>
4.1	Attaques et vulnérabilités . . . . .	5
4.2	Distance de réception d'un signal Bluetooth . . . . .	6
4.3	Protection du sésame . . . . .	6
4.4	(In)sécurité liée au mode découverte . . . . .	6
<b>5</b>	<b>Recommandations</b>	<b>6</b>
<b>6</b>	<b>Documentation</b>	<b>7</b>

# 1 Introduction

La technologie Bluetooth est un système de communication radio à courte portée destinée au réseau personnel (WPAN — *Wireless Personal Area Network*). Créée dans le but de remplacer les connexions filaires entre toutes sortes d'équipements, cette technologie est peu coûteuse ( $\leq 3$  euros) et peu consommatrice d'énergie. Ces deux atouts lui ont permis d'être rapidement et largement mise en œuvre dans de nombreux équipements (500 millions d'appareils équipés de la technologie Bluetooth en 2005)<sup>1</sup>

À ce jour, les dispositifs utilisant la technologie Bluetooth peuvent être des téléphones portables, ordinateurs portables, imprimantes, périphériques de saisies mais également des équipements tels que les récepteurs GPS (*Global Positioning System*), les appareils photos, les assistants personnels numériques (PDA — *Personal Digital Assistant*), certains équipements médicaux et systèmes embarqués (système audio, kit main-libre, etc.) dans les véhicules automobiles. La liste et le nombre de ces appareils continue de s'accroître.

## 2 Présentation de la technologie Bluetooth

La technologie Bluetooth est normalisée par le Bluetooth *Special Interest Group* (SIG). Il s'agit d'une association créée en 1998, elle compte aujourd'hui plus de 8000 membres et a pour mission de promouvoir le développement de cette technologie sans pour autant être partie prenante dans sa conception.

La technologie sans fil Bluetooth fonctionne sur la bande de fréquence des 2,4GHz identique à celle utilisée par certaines normes IEEE 802.11. La fonction «saut de fréquence» définie dans la spécification Bluetooth permet de limiter les interférences et d'améliorer la qualité de service.

### 2.1 Réseau personnel sans fil de courte portée

Les appareils équipés de la technologie Bluetooth communiquent entre eux en formant des réseaux ad-hoc (maître-esclave) de faible portée nommés *picoréseaux*. Un périphérique esclave peut avoir plusieurs maîtres, mais ne sera pas en mesure de communiquer directement avec un autre esclave.

Ces *picoréseaux* permettent à 8 périphériques (1 maître et 7 esclaves) de communiquer de façon simultanée. La limitation des *picoréseaux* à 8 périphériques actifs est due à l'utilisation de trois 3 bits<sup>2</sup>. Cependant ces *picoréseaux* peuvent contenir jusqu'à 255 équipements Bluetooth en mode *parked*.

Un équipement Bluetooth appartenant à un *picoréseau* qui ne nécessite plus de communiquer peut rester synchronisé à celui-ci pour, à terme, communiquer à nouveau. Un équipement Bluetooth en mode *parked* est identifiable par son adresse *Parked Member*<sup>3</sup>. Si cette adresse est nulle, l'équipement en mode *parked* reste identifiable via son adresse MAC<sup>4</sup>.

Toutefois, un périphérique peut appartenir à plusieurs *picoréseaux* ce qui constitue alors un *scatternet* (réseau chaîné). Les *scatternet* et *picoréseaux* se font et se défont de façon dynamique au fil des connexions et des déconnexions des périphériques Bluetooth.

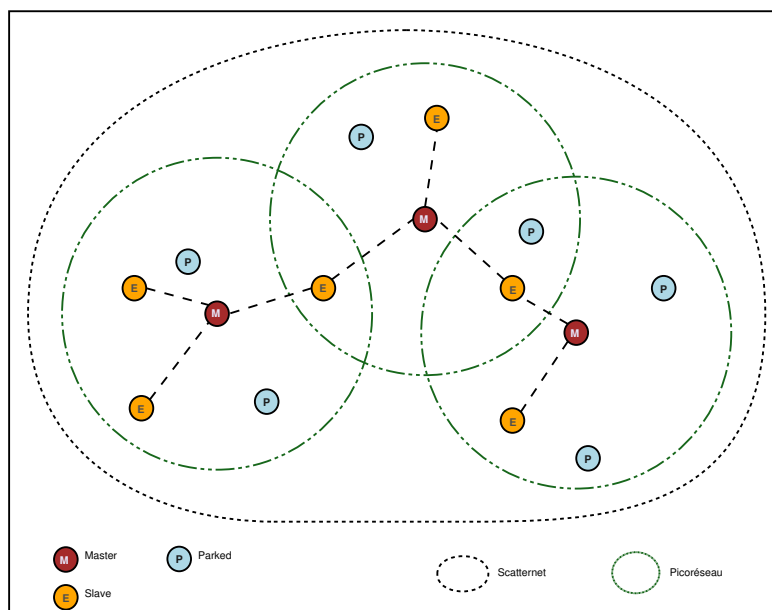
---

1. Source : Site officiel [www.bluetooth.com](http://www.bluetooth.com),  
<http://www.bluetooth.com/Bluetooth/Learn/Benefits/>

2. LT\_ADDR : Logical Transport Address

3. PM\_ADDR : Parked Member Address

4. Medium Access Control : est un identifiant unique stocké sur l'interface réseau.



## 2.2 Bluetooth 1.2 et Bluetooth 2.0

Les équipements Bluetooth connectés à un *picoréseau* peuvent se transmettre simultanément des informations de type voix et données (comme défini dans la spécification du protocole Bluetooth). (cf. Section 6)

En novembre 2003, la version 1.2 de la spécification Bluetooth a été adoptée. Cette version permet des taux de transfert de l'ordre de 1Mbits/s, en pratique cela se traduit par un débit de 720kbits/s. Un an plus tard, c'est la version 2.0 qui est adoptée à son tour. Cette nouvelle version permet des transferts plus rapides, le taux de transfert peut aller jusqu'à 3Mbits/s théorique.

## 2.3 Distance et puissance

La technologie sans fil Bluetooth est destinée à des réseaux personnels de courte portée. La distance maximum spécifiée entre les équipements peut varier de quelques mètres à une centaine de mètres pour les appareils les plus puissants. La distance est directement liée à la puissance d'émission et à la sensibilité de réception des dispositifs Bluetooth (cf. Section 4.2).

La technologie Bluetooth, à l'inverse de la technologie infrarouge, ne requiert pas des appareils communicants qu'ils soient sur ligne directe et dégagée, en effet, cette technologie est omnidirectionnelle et les ondes radio sont capables de traverser des objets massifs tels que des murs.

Les appareils Bluetooth sont divisés en trois catégories définies par leur puissance d'émission et donc par leur portée. Les équipements dont la puissance est la plus faible sont appelés Classe 3 tandis que ceux dont la puissance est la plus importante sont appelés Classe 1.

Classe	Puissance (Atténuation en dBm)	Portée
Classe 3	1 mW (0dBm)	≤ 10 mètres
Classe 2	2,5 mW (4dBm)	10 à 20 mètres
Classe 1	100 mW (20dBm)	100 mètres

TAB. 2 – Bluetooth: classe, puissance et portée.

Ces données sont théoriques et le matériel peut être modifié de manière à étendre la portée en réception (cf. Section 4.2).

## 2.4 Profils Bluetooth

Les services et/ou applications d'un équipement Bluetooth sont déterminés par les profils Bluetooth (*Bluetooth Profiles*) de façon à permettre l'interopérabilité entre les appareils Bluetooth disposant des mêmes profils.

Dans la spécification Bluetooth, au moment de la rédaction de ce document, il existe 33 profils Bluetooth qui offrent des fonctionnalités variées. Parmi ces profils Bluetooth, on retrouve des services permettant :

- de transporter des données audio de qualité stéréo (casque audio, haut-parleurs, baladeur audio, ...);
- de contrôler un système d'imagerie afin d'envoyer ou de récupérer des images ou même d'utiliser la fonction de capture et d'affichage à distance (appareil photo, caméscope, ...);
- de transmettre des données vidéos en continu;
- d'imprimer à distance;
- d'accéder aux données, signalisation et services fournies par le réseau RNIS;
- d'accéder à l'Internet au moyen d'un modem;
- d'accéder ou d'offrir un service FTP (*File Transfer Protocol*);
- ...

Cette liste de profils Bluetooth on peut expliquer l'engouement des industriels pour cette technologie aux multiples possibilités. Pour les utilisateurs, cette technologie permet d'échanger, de partager, d'accéder à un grand nombre d'informations et de données à tout moment avec une facilité poussée. Cependant, ces informations qui transitent dans l'atmosphère doivent être protégées afin d'assurer un niveau minimum de sécurité (confidentialité et intégrité).

### 3 Sécurité et technologie Bluetooth

Le fait d'intégrer la technologie Bluetooth et toutes les fonctionnalités associées dans de plus en plus d'équipements a contribué à transformer ces mêmes équipements en systèmes d'information communicants. Avec leur capacité de stockage, leurs services et leurs connectivités, il est primordial de prendre en considération la sécurité des équipements Bluetooth.

#### 3.1 Mode de sécurité

La spécification Bluetooth propose 3 modes de sécurité. Il est à noter que ces modes de sécurité sont déployés ou non dans les équipements Bluetooth selon la décision prise par les fabricants. Les modes de sécurité sont les suivants :

- mode de sécurité 1 : non sécurisé;
- mode de sécurité 2 : sécurisé au niveau applicatif;
- mode de sécurité 3 : sécurisé au niveau de la liaison.

Le mode de sécurité 3 intervient sur la couche de liaison du modèle OSI, il permet d'établir une connexion avec authentification et chiffrement au moyen d'une clé.

Le mode de sécurité 2 permet de sécuriser de façon logicielle<sup>5</sup> le dispositif Bluetooth en paramétrant les profils Bluetooth.

Le mode de sécurité 1 permet à un appareil Bluetooth d'offrir ses services à tous dispositifs Bluetooth à portée.

#### 3.2 Jumelage ou couplage

Deux dispositifs Bluetooth destinés à communiquer ensemble fréquemment devront être couplé<sup>6</sup> au moyen d'une clé symétrique. Cette étape permet aux deux appareils de partager une clé secrète utilisée pour chiffrer et déchiffrer les données. Cette clé secrète est conçue au moyen d'un algorithme mettant en œuvre l'adresse physique des dispositifs jumelés, de nombres aléatoires mais surtout d'un sésame fourni par l'utilisateur (code PIN<sup>7</sup>, mot de passe, etc...).

Le sésame symétrique requis lors de l'opération de jumelage est directement subordonné au périphérique utilisé :

- certains équipements ne disposant pas d'interface de saisie (tel qu'un clavier), mettent en œuvre un sésame stocké définitivement dans le matériel (micrologiciel). Les dispositifs les plus élaborés mettent en place une

---

5. Couche applicative du modèle OSI

6. Jumelage et couplage sont synonymes.

7. Ce code PIN (*Personal Identification Number*) est différent de celui de la carte SIM fourni par les opérateurs téléphoniques

série de sésames prédéfinis. Ce qui laisse à l'utilisateur l'opportunité de choisir un sésame (parmi l'un de ceux disponibles) afin de remplacer celui par défaut ;

- dans le cas d'un téléphone portable avec la technologie Bluetooth, le sésame nécessaire pour coupler deux dispositifs Bluetooth sera de type numérique ou également appelé code PIN ;
- d'autres équipements, disposant d'une interface de communication avec une méthode de saisie évoluée, permettent de saisir un sésame plus robuste qu'un code numérique. Uniquement si ce sésame est composé de caractères alphanumériques (majuscule et minuscule) et de caractères spéciaux (tels que . , , : etc...).

### 3.3 Mode découverte

Un dispositif Bluetooth peut activer ou non le mode découverte. Ce mode de fonctionnement permet à un appareil Bluetooth de manifester sa présence en répondant aux requêtes destinées à découvrir les équipements Bluetooth à portée.

La désactivation de ce mode peut s'avérer très utile lorsque l'on souhaite établir une communication entre deux appareils Bluetooth sans pour autant révéler leur présence aux autres équipements Bluetooth à portée. Le mode découverte est de plus en plus souvent désactivé par défaut sur les équipements Bluetooth tels que les oreillettes Bluetooth.

## 4 Risque associé à l'utilisation de la technologie Bluetooth

L'utilisation de cette technologie, avec tous les services qu'elle propose, est assortie à des risques bien réels de voir des informations dérobées par des individus qu'il sera très difficile d'identifier, car les équipements en question sont conçus pour être petits, légers et mobiles. Rares sont les équipements qui journalisent les connexions et les activités Bluetooth.

### 4.1 Attaques et vulnérabilités

De nombreuses vulnérabilités liées aux dispositifs Bluetooth ont été découvertes depuis la création et l'utilisation des équipements Bluetooth. Ces vulnérabilités ont d'ailleurs été suivies par l'apparition d'attaques à l'intitulé accrocheur. Les principales attaques sont détaillées ci-dessous :

**Bluejacking** : Cette première attaque, qui s'apparente à du pourriel, consiste à détourner l'utilisation principale liée au profil OBEX Object Push Service (cf. Section 2.4).

Ce profil Bluetooth permet d'envoyer des éléments (contacts, carte de visite, rendez-vous ...) entre périphériques compatibles.

Un utilisateur malintentionné peut remplir arbitrairement les champs de sa carte de visite et faire afficher ce texte sur un appareil Bluetooth choisi.

**Bluesmack** : Cette attaque consiste en l'exploitation d'une vulnérabilité présente dans des piles réseau Bluetooth.

Un utilisateur malintentionné peut fabriquer des paquets spécialement conçus pour réaliser un déni de service de la pile réseau Bluetooth ou sur l'équipement vulnérable.

**Bluebug** : Cette attaque affecte principalement les téléphones portables équipés d'une interface Bluetooth. Un utilisateur ayant accès au profil Bluetooth vulnérable d'un téléphone portable peut exécuter arbitrairement toutes sortes de commandes lui donnant ainsi un contrôle total sur l'équipement ciblé. Les actions auxquelles l'individu pourrait avoir accès sont :

- l'accès en lecture et en écriture au répertoire téléphonique ;
- appel vers n'importe quel numéro (surtaxé ou malveillant) ;
- modification de la configuration de l'appareil (volume sonore, renvoi d'appel, ... ) ;
- lecture et envoi de message SMS ;
- etc.

**Bluesnarfing** : Cette attaque permet à un utilisateur malintentionné de télécharger arbitrairement depuis l'équipement Bluetooth vulnérable un ou plusieurs fichiers.

Ces attaques<sup>8</sup> ont beaucoup perdu en furtivité depuis que les fabricants d'équipements Bluetooth implémentent par défaut le mode sécurité 2. Pour arriver à ses fins un utilisateur malintentionné devra associer à ces attaques de l'ingénierie sociale.

---

8. On peut ajouter aux attaques citées les suivantes : *Blueprinting*, *BlueDump*, *BlueBump*, *BlueChop*

## 4.2 Distance de réception d'un signal Bluetooth

Le savoir-faire permettant de modifier physiquement un dispositif Bluetooth de type clé USB de manière à augmenter considérablement sa portée de réception est disponible sur l'Internet.

Par l'un de ces procédés, il est possible de modifier la portée de réception d'une clé USB Bluetooth de Classe 3 en y apportant quelques modifications visant à augmenter le gain en dB lié à l'antenne. Une clé USB Bluetooth ainsi modifiée peut voir sa portée de réception passer d'une dizaine de mètres à une centaine de mètres, voir au-delà du kilomètre.

Ces expériences mettent en évidence que les ondes radio émises par un équipement Bluetooth peuvent être captées largement au-delà de la portée théorique, l'élément important lors de ces expérimentations est la sensibilité du récepteur Bluetooth.

## 4.3 Protection du sésame

Le savoir-faire, ainsi que les moyens matériels nécessaire pour casser un sésame utilisé par deux périphériques Bluetooth jumelés peuvent être réunis. Avec ces ressources, un utilisateur distant malintentionné peut compromettre la confidentialité d'un sésame. Par ce procédé, un sésame de type code PIN de 4 caractères peut être cassé en moins d'une seconde. Le temps de calcul maximum nécessaire pour casser un code PIN est exponentiel en fonction du nombre de caractères.

Certains dispositifs Bluetooth exigent de l'utilisateur de saisir à chaque connexion le sésame symétrique déjà utilisé lors du jumelage des équipements. Cependant cette méthode introduit des risques supplémentaires qui peuvent être exploités aux moyens d'attaques Bluetooth spécifiques (basées sur une attaque en force brute) visant à casser le sésame.

## 4.4 (In)sécurité liée au mode découverte

Un équipement Bluetooth ayant désactivé le mode « découverte » reste tout de même détectable par un utilisateur malintentionné. Pour un utilisateur non averti, le fait de désactiver le mode découverte donne une fausse impression de sécurité car un périphérique Bluetooth sous tension reste joignable.

Une attaque consiste à envoyer une requête spécifique qui ne peut être ignorée par les périphériques Bluetooth à portée, même avec le mode découverte désactivé. Ainsi, une personne malveillante va tenter de balayer une ou plusieurs plages d'adresses physiques prédéfinies associées aux dispositifs Bluetooth afin de détecter leur présence. Cette attaque de type force brute est coûteuse en temps pour l'attaquant mais reste efficace.

# 5 Recommandations

La technologie Bluetooth est encore récente et reste largement orientée par les considérations de marketing, et ce, au détriment de la sécurité.

- Privilégier les équipements dont l'interface Bluetooth peut être amovible ;
- choisir un dispositif Bluetooth maintenu dans le temps par son fabricant/éditeur. Cet équipement devra faire l'objet d'un suivi et de publication de mises à jour destinées aux micrologiciels, drivers, applications, etc ;
- appliquer les dernières mises à jour de sécurité destinées aux équipements Bluetooth ;
- envisager le remplacement périodique des équipements bluetooth par de plus récents mettant en œuvre de nouvelles fonctionnalités de sécurité ;
- dissocier les données personnelles des données professionnelles sur les appareils et limiter les informations stockées au strict nécessaire ;
- désactiver la connexion Bluetooth ou retirer le composant dès qu'il n'est plus nécessaire, la distance n'est pas une protection ;
- configurer les profils Bluetooth indispensables de façon à ce que toutes connexions mettent en œuvre une authentification et un chiffrement des données ;
- opter pour un sésame aussi fort que possible en fonction de l'interface de saisie présente sur l'équipement Bluetooth :
  - clavier numérique/téléphonique : séquence de chiffres (basée ou non sur les lettres présentes sur le clavier) ;
  - clavier alphanumérique : utiliser les caractères alphanumériques et spéciaux disponibles ;

- activer le mode découverte uniquement lors d'un jumelage avec un autre appareil ;
- désactiver tous services non indispensables et/ou ceux ne nécessitant pas d'authentification ;
- procéder à l'association de deux équipements Bluetooth de confiance dans un environnement sûr :
  - éviter les emplacements très fréquentés tels que les lieux publics (voie publique, transports en commun, centres commerciaux, conférences) pour réaliser l'association. Préférer un endroit calme au bureau, à la maison ;
  - dans le cas d'un appareil dont la confiance est limitée, supprimer les paramètres associés après l'échange.
- suivre l'évolution liée à la technologie Bluetooth.

## 6 Documentation

- «Bluetooth», site officiel :  
<http://www.bluetooth.com/bluetooth/>
- Site Internet du groupe «*Trifinite.org*» :  
<http://trifinite.org/>
- «Sécurité Bluetooth» de Pierre Betouin, SecuObs :  
<http://secuobs.com/news/05022006-bluetooth1.shtml>
- «(In)sécurité des périphériques Bluetooth» de Pierre Betouin :  
[http://www.secuobs.com/pres\\_eurosec06\\_bluetooth\\_pbetouin\\_version\\_slides.pdf](http://www.secuobs.com/pres_eurosec06_bluetooth_pbetouin_version_slides.pdf)
- «Bluetooth», The Bunker :  
<http://www.thebunker.net/resources/bluetooth>

## Gestion détaillée du document

01 août 2007 version initiale.