



# Évaluation des vulnérabilités de Bluetooth

***PUBLICATION TECHNIQUE***

***ITSPSR-17A***

**Juin 2008**



---

**Évaluation des vulnérabilités de Bluetooth (ITSPSR-17A)**

---

Page intentionnellement laissée en blanc.



## Avant-propos

L'*Évaluation des vulnérabilités de Bluetooth (ITSPSR-17A)* est un document NON CLASSIFIÉ, publié avec l'autorisation du chef du Centre de la sécurité des télécommunications Canada (CSTC).

Cet examen de produit a été préparé pour le CSTC à l'intention du gouvernement fédéral. Cet examen est officieux et de portée limitée. Il ne s'agit pas d'une évaluation exhaustive, et ne constitue pas une homologation du produit par le CSTC. Son contenu reflète le meilleur jugement du CSTC, compte tenu de l'information disponible au moment de la préparation du rapport. Toute utilisation de ce rapport par une tierce partie ou toute référence ou décision basée sur celui-ci est la seule responsabilité de ladite partie. Le CSTC se dégage de toute responsabilité à l'égard des dommages encourus par toute tierce partie à la suite de décisions ou d'actions prises sur la base du présent rapport.

Veillez communiquer avec le chef des Services à la clientèle, Sécurité des TI, CSTC, par téléphone, au 613-991-7654, ou par courriel, à l'adresse [itsclientservices@cse-cst.gc.ca](mailto:itsclientservices@cse-cst.gc.ca), pour obtenir des copies supplémentaires ou pour faire modifier la liste de diffusion.

## Date d'entrée en vigueur

La présente publication entre en vigueur en juin 2008.

---

Gwen Beauchemin  
Directrice, Gestion de la mission de la Sécurité des TI

© 2008 Gouvernement du Canada, Centre de la sécurité des télécommunications Canada

La présente publication peut être reproduite textuellement et dans son intégralité, sans frais à des fins personnelles seulement. Toutefois, pour utiliser ce document avec des modifications, sous forme partielle ou à des fins commerciales, il faut obtenir au préalable la permission écrite du CSTC.



---

**Évaluation des vulnérabilités de Bluetooth (ITSPSR-17A)**

---

*Page intentionnellement laissée en blanc.*





---

**Évaluation des vulnérabilités de Bluetooth (ITSPSR-17A)**

---

*Page intentionnellement laissée en blanc.*



## Table des matières

<b>1</b>	<b>Introduction .....</b>	<b>1</b>
1.1	Objet.....	1
1.2	Portée.....	1
1.3	Contexte .....	1
1.4	Applicabilité .....	2
1.5	Structure du document.....	2
<b>2</b>	<b>Analyse des vulnérabilités .....</b>	<b>3</b>
2.1	Couche physique.....	3
2.1.1	Généralités .....	3
2.1.2	Faible puissance.....	3
2.1.3	Réglage de puissance adaptatif.....	4
2.1.4	Saut de fréquence .....	5
2.1.5	Autres caractéristiques .....	5
2.1.6	Résumé .....	6
2.2	Cryptographie.....	6
2.2.1	Généralités .....	6
2.2.2	Éléments cryptographiques Bluetooth patrimoniaux.....	7
2.2.3	Couplage simple sécurisé.....	10
2.2.4	Résumé .....	11
2.3	Autres vulnérabilités .....	11
2.3.1	Généralités .....	11
2.3.2	Authentification des utilisateurs .....	12
2.3.3	Génération de nombres aléatoires.....	12
2.3.4	Erreurs de mise en oeuvre/faiblesses.....	12
<b>3</b>	<b>Au-delà de la technologie.....</b>	<b>15</b>
3.1	Généralités.....	15
3.2	Communications par radiofréquences (RF).....	15
3.3	Politiques de connectivité .....	15
3.4	Caractéristiques techniques .....	16
3.4.1	Généralités .....	16
3.4.2	Fonctions d'économie de pile .....	16
3.4.3	Claviers Bluetooth.....	17
3.4.4	Débits améliorés .....	17
3.5	Sensibilisation des utilisateurs aux questions de sécurité .....	17
<b>4</b>	<b>Solutions.....</b>	<b>19</b>
4.1	Généralités.....	19
4.2	Non-usage.....	19
4.3	Enceintes blindées contre les radiofréquences .....	19
4.4	Applications cryptographiques.....	19



---

**Évaluation des vulnérabilités de Bluetooth (ITSPSR-17A)**

---

4.5	Choix des produits Bluetooth commerciaux .....	20
4.6	Politique de sécurité .....	20
4.7	Résumé .....	21
<b>5</b>	<b>Travaux futurs .....</b>	<b>23</b>
<b>6</b>	<b>Références .....</b>	<b>25</b>



## Liste des figures

Figure 1: Portées des périphériques Bluetooth à l'aide d'une antenne standard ..... 4

Figure 2 : Suite cryptographique Bluetooth ..... 7

## Liste des tableaux

Tableau 1 – Cryptographie Bluetooth..... 6



---

**Évaluation des vulnérabilités de Bluetooth (ITSPSR-17A)**

---

*Page intentionnellement laissée en blanc.*



## Liste des abréviations et des acronymes

BD_ADDR	Adresse des périphériques Bluetooth
CSTC	Centre de la sécurité des télécommunications Canada
dB	Décibel
dBm	Décibel-milliwatt
ECDH	Courbe elliptique Diffie-Hellman
EDR	Débit amélioré
FHS	Séquence de sauts de fréquence
GC	Gouvernement du Canada
GIS	Groupe d'intérêt spécial
GIS Bluetooth	Groupe d'intérêt spécial Bluetooth
ICP	Infrastructure à clé publique
mW	milliwatt
NIP	Numéro d'identification personnel
NIST	National Institute of Standards and Technology
PDA	Assistant numérique personnel
Pmax	Puissance maximale
Pmin	Puissance minimale
PSK	Modulation par déplacement de phase
RAND	Nombre aléatoire
RF	Radiofréquence
STI	Sécurité des technologies de l'information
TI	Technologies de l'information
UWB	Bande ultra-large
WEP	Confidentialité équivalente aux transmissions par fil



---

**Évaluation des vulnérabilités de Bluetooth (ITSPSR-17A)**

---

*Page intentionnellement laissée en blanc.*



# 1 Introduction

## 1.1 Objet

La technologie Bluetooth est grandement répandue dans les ministères et organismes du gouvernement du Canada (GC) et est utilisée par les employés du GC. Par conséquent, les utilisateurs devraient en savoir plus sur les fonctions et les lacunes de sécurité associées à ces produits.

## 1.2 Portée

Le présent rapport examine les vulnérabilités de la technologie Bluetooth en matière de sécurité, plus particulièrement en ce qui concerne la couche physique et sa cryptographie et d'autres éléments touchant la sécurité de cette technologie. Une attention spéciale est accordée à la façon dont les produits Bluetooth sont introduits par les fournisseurs et les options que ces derniers peuvent choisir ou non de mettre en oeuvre.

La spécification Bluetooth faisant l'objet du présent rapport est la version 2.1+EDR, ratifiée par le Groupe d'intérêt spécial Bluetooth (GIS Bluetooth) en août 2007. Elle offre une procédure de couplage (ou jumelage) plus sécurisée entre les périphériques conformes à la version Bluetooth 2.1. La version Bluetooth 2.1 est la toute dernière version publique de la norme Bluetooth; **les utilisateurs devraient toutefois être conscients que la majorité des périphériques sur le marché sont compatibles uniquement avec la version 1.1. ou 1.2 de Bluetooth.** Au moment de la rédaction du présent rapport, très peu de périphériques étaient conformes à la version 2.1 et même **les périphériques Bluetooth 2.1 fonctionneront dans le mode sécurisé réduit original lorsqu'ils seront couplés à des périphériques Bluetooth patrimoniaux (c.-à-d, versions 1.0 à 2.0).** Par conséquent, quoique le présent rapport fasse un survol des fonctions de sécurité de la nouvelle version 2.1, il continuera de mettre l'accent sur les vulnérabilités présentes dans les versions précédentes de Bluetooth.

## 1.3 Contexte

La sécurité inhérente de Bluetooth fait l'objet d'une importante controverse. Selon le site Web du GIS Bluetooth, « la technologie sans fil Bluetooth offre des fonctionnalités intégrées de chiffrement et d'authentification suffisantes, et elle est donc très sûre dans tout environnement » (traduction libre). Ce groupe soutient également qu'il est très difficile de faire de l'écoute clandestine contre les dispositifs Bluetooth et ce, pour deux raisons : Bluetooth utilise d'une part un mécanisme de saut de fréquence de 1 600 sauts par seconde, et d'autre part un mode d'adaptation automatique de la puissance de sortie qui réduit la portée exactement selon les besoins. Il y a lieu de noter que ces assertions ne figurent plus sur le site Web du GIS Bluetooth.



---

## Évaluation des vulnérabilités de Bluetooth (ITSPSR-17A)

---

Le présent rapport explore la validité des affirmations courantes du GIS Bluetooth et examine de plus près les vulnérabilités de sécurité associées à Bluetooth. Il présuppose que le lecteur a déjà une certaine connaissance de Bluetooth. Les lecteurs qui ne connaissent pas cette technologie ou qui désirent une bonne initiation à celle-ci devraient lire le document *Bluetooth Revealed* [2].

Le Centre de formation en sécurité des TI du CSTC présente des détails et des démonstrations pratiques des vulnérabilités communes associées à Bluetooth et à d'autres technologies sans fil dans son cours *La sécurité du sans-fil*. Toute personne intéressée à suivre ce cours ou d'autres cours en STI offerts par le CSTC peut communiquer par courriel avec le Centre de formation en sécurité des TI à l'adresse suivante : [learningcentre@cse-cst.gc.ca](mailto:learningcentre@cse-cst.gc.ca).

Le présent rapport remplace le document *ITSPSR-17* produit par le CSTC en octobre 2002 [4].

### 1.4 Applicabilité

À l'origine, la technologie Bluetooth avait été conçue uniquement pour des applications commerciales et n'était pas destinée à protéger des renseignements classifiés ou protégés. De plus, la technologie Bluetooth avait été développée pour être mise en oeuvre sur une puce coûtant 3 \$US ou moins. Quoique la spécification Bluetooth permette une sécurité au niveau des applications, peu de solutions techniques ont été développées comme couches supplémentaires pour accroître la sécurité de Bluetooth afin de protéger adéquatement l'information très sensible. De telles solutions coûtent beaucoup plus que la puce de 3 \$ pour laquelle l'application fondamentale avait été conçue. La technologie Bluetooth offre toutefois une certaine sécurité intrinsèque qui peut être suffisante pour protéger des applications peu sensibles. Dans le présent rapport, nous tenterons de présenter une analyse objective de la technologie Bluetooth, indépendamment de son utilisation.

### 1.5 Structure du document

Quoique la pile de protocoles de communication de Bluetooth soit très complexe et s'étende de la couche physique (suivant le modèle OSI des protocoles réseau en couches) jusqu'à la couche application, le présent document porte principalement sur les couches inférieures. Nous abordons d'abord la couche physique, en accordant une attention spéciale à l'adaptation de puissance et au saut de fréquence. Ensuite, nous traitons des fonctions cryptographiques incluses dans la couche liaison, puis décrivons, dans la section subséquente, quelques vulnérabilités de Bluetooth. Suit une analyse plus poussée de la façon dont les produits Bluetooth seront mis à la disposition des consommateurs et des diverses options de sécurité retenues par les fabricants pour mettre en oeuvre Bluetooth dans leurs produits. Enfin, nous suggérons quelques solutions permettant de protéger les applications peu sensibles contre la plupart des vulnérabilités constatées dans les sections précédentes.



## 2 Analyse des vulnérabilités

### 2.1 Couche physique

#### 2.1.1 Généralités

Bluetooth présente bon nombre des vulnérabilités inhérentes aux systèmes sans fil en général. Un émetteur Bluetooth envoie un signal dans l'espace libre vers tout récepteur, légitime ou non, situé à portée. Par ailleurs, Bluetooth fonctionne dans la bande de 2,4 GHz, laquelle ne nécessite pas de licence, et aucune restriction n'est appliquée à la vente des dispositifs émettant et recevant dans cette bande. Par conséquent, un dispositif de surveillance non autorisé qui n'est pas en contact physique avec l'émetteur Bluetooth peut capter ses transmissions. Un tel dispositif de surveillance est facile à cacher, est indétectable durant son utilisation et peut être déployé beaucoup plus rapidement qu'un dispositif d'écoute clandestine sur fil.

Or, Bluetooth utilise trois mécanismes qui réduisent (sans toutefois l'éliminer) la probabilité d'interception, à savoir :

- une faible puissance;
- un contrôle de puissance adaptatif (facultatif);
- le saut de fréquence.

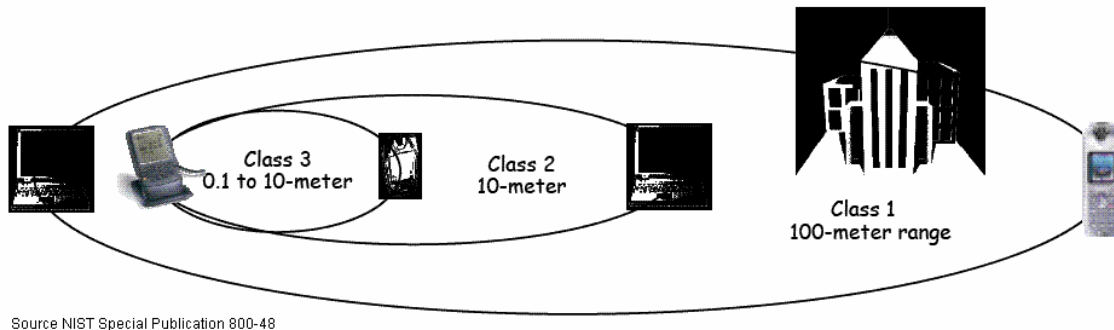
#### 2.1.2 Faible puissance

Les périphériques Bluetooth sont classés en fonction de la puissance de sortie maximale de leur émetteur. La plupart des périphériques Bluetooth tels les oreillettes, les souris et les claviers appartiennent à la classe 3, avec une puissance d'émission effective maximale de 1 milliwatt (1 mW). Il existe également des périphériques de classes 2 et 1, dont la puissance d'émission effective maximale est de 2,5 mW et de 100 mW respectivement, mais ces produits sont généralement limités à l'équipement industriel et peu d'entre eux sont offerts commercialement.

La puissance de sortie standard de classe 3, soit 1 mW, se traduit par une portée effective d'environ 10 mètres entre deux périphériques pourvus chacun d'une antenne isotrope quart d'onde standard. Il est possible d'atteindre une portée allant jusqu'à 100 mètres environ, toujours à l'aide d'antennes standard, avec des périphériques de classe 1 de plus grande puissance. Les utilisateurs devraient toutefois être conscients que l'utilisation d'amplificateurs ou d'antennes à gain élevé au niveau de l'émetteur OU du récepteur peut augmenter de manière considérable la portée des périphériques de classe 3 (il a été démontré qu'on pouvait obtenir une réception Bluetooth sur plusieurs kilomètres à l'aide d'une antenne à gain élevé commerciale au niveau du récepteur seulement).



## Évaluation des vulnérabilités de Bluetooth (ITSPSR-17A)



Source NIST Special Publication 800-48

Figure 1: Portées des périphériques Bluetooth à l'aide d'une antenne standard

## 2.1.3 Réglage de puissance adaptatif

Pour pouvoir intercepter des communications Bluetooth, un dispositif de surveillance passive doit normalement se trouver à portée effective des périphériques ciblés. Bluetooth comprend un réglage de puissance adaptatif qui tente de limiter la puissance de sortie au niveau minimum nécessaire pour maintenir la communication. Cette fonction aide à conserver l'énergie de la pile de même qu'à réguler la portée effective de la transmission. Or, il faudrait toutefois prendre note des points suivants concernant le réglage de la puissance :

- La portée de 10 mètres d'un périphérique type de classe 3 est en réalité uniquement une approximation. Le canal de la radio mobile terrestre est un milieu difficile où les obstacles (mobiles ou fixes) dans la ligne de visée radio absorbent le signal et les surfaces réfléchissantes créent un brouillage intersymbole additif ou destructif. De plus, la proximité d'autres émetteurs peut provoquer des interférences mutuelles. Ces obstacles nuisent grandement à la portée réelle de toute liaison. Par ailleurs, cette portée varie considérablement dans le temps à cause de plusieurs facteurs. Une liaison de communication conçue pour une application mobile présente toujours des interruptions de service. La nécessité d'accroître la puissance et la portée de l'émetteur afin de réduire les interruptions de service contrebalance toujours la nécessité de réduire au minimum la portée pour des raisons de sécurité;
- Un dispositif de surveillance équipé d'un mécanisme d'amplification de puissance (y compris les antennes directionnelles à gain élevé) peut capter des signaux venant de beaucoup plus loin que la portée nominale de 10 mètres, même lorsque le réglage de puissance est utilisé);
- La technologie Bluetooth vise les applications sur monopuce coûtant 3 \$US ou moins. Par conséquent, il est fort probable que des dispositifs d'écoute clandestine de taille semblable puissent être construits à un coût similaire et être placés à portée de réception sans qu'il soit facile de les détecter;



## Évaluation des vulnérabilités de Bluetooth (ITSPSR-17A)

- Un écouteur clandestin n'a pas besoin de surveiller continuellement une station pour obtenir des renseignements utiles. De même, il peut obtenir suffisamment d'information sur un picoréseau complet en surveillant seulement quelques stations de ce réseau;
- La fonction de réglage de puissance adaptatif est facultative seulement. De plus, le pas maximal du réglage de puissance est de 8 dB, alors que le pas minimal est de 2 dB. Par conséquent, la puissance utilisée par un émetteur pourrait probablement être près de 8 dB plus élevée que ce qu'il faut pour atteindre une station particulière;
- La spécification ne stipule aucun taux d'adaptation de puissance dans le temps. Par conséquent, il est possible qu'une liaison doive augmenter rapidement la puissance émise à cause d'une perturbation instantanée dans le canal radio, et qu'elle demeure à ce niveau élevé longtemps après que la qualité du canal est revenue à la normale.

### 2.1.4 Saut de fréquence

Les sauts de fréquence utilisés par un émetteur Bluetooth ne présentent pas un défi de taille pour un écouteur clandestin, car toute puce Bluetooth peut facilement suivre les sauts, qu'il s'agisse de la puce du périphérique destinataire ou non. La seule information requise pour bien recevoir le signal est la séquence de sauts de fréquence (FHS), qui est émise en clair par le périphérique maître au moment de l'établissement de la liaison. Si le dispositif d'écoute est à portée à ce moment-là, il peut saisir la FHS et se synchroniser au reste des communications.

Si le dispositif de surveillance est à portée du ou des émetteurs après l'établissement de la liaison, il peut toujours tenter une attaque de déni de service (par brouillage, par exemple), afin de perturber le picoréseau et forcer le périphérique maître à tenter de rétablir la connectivité. En obligeant le périphérique maître à réémettre la FHS, l'écouteur clandestin a la possibilité de se synchroniser avec le picoréseau une fois que celui-ci est rétabli. Cette procédure peut s'exécuter en quelques secondes. Si le service est rétabli rapidement, il est possible que les utilisateurs légitimes ne soient pas alarmés par l'interruption de service momentanée.

### 2.1.5 Autres caractéristiques

Dans les couches supérieures à la couche physique, d'autres mécanismes d'adaptation optimisent la liaison entre l'émetteur et le destinataire prévu, notamment le codage de correction des erreurs, la demande de répétition automatique, etc. Comme ces fonctions adaptatives réagissent aux signaux émis par le destinataire vers le périphérique initiateur, elles aident habituellement la liaison initialement prévue, et non la liaison vers l'écouteur clandestin. Par conséquent, ces fonctions accroissent la protection contre l'écoute clandestine, ne serait-ce que légèrement.

Bluetooth 2.1 apporte également deux schémas de modulation différents reposant sur la technologie de modulation par déplacement de phase (PSK pour *phase-shift-keying*) pour prendre en charge la fonction de débit amélioré (EDR pour *Enhanced Data Rate*). Ces schémas de modulation additionnels augmentent la complexité des circuits et des systèmes de contrôle RF, mais n'ont aucune incidence sur la sécurité ou sur la facilité d'intercepter les signaux.



## Évaluation des vulnérabilités de Bluetooth (ITSPSR-17A)

### 2.1.6 Résumé

L'importance relative de ces vulnérabilités au niveau de la couche physique dépend de l'application et de l'environnement d'exploitation. Dans la plupart des situations, l'absence d'un mécanisme obligatoire de réglage de puissance adaptatif et d'une granularité fine dans les paramètres du réglage de puissance constitue la vulnérabilité la plus grave, puisqu'il en résulte que le périphérique transmet à une puissance beaucoup plus élevée que ce qui est requis, ce qui contribue à étendre inutilement la portée à laquelle il peut être intercepté.

## 2.2 Cryptographie

### 2.2.1 Généralités

La cryptographie dans Bluetooth sert à assurer les services d'authentification, de confidentialité et d'autorisation. Le Tableau 1 décrit les fonctions cryptographiques de la technologie Bluetooth.

**Tableau 1 – Cryptographie Bluetooth**

Routine interrogation-réponse	Authentification pour empêcher la mystification des identités et l'accès non autorisé aux données et fonctions essentielles.
Chiffrement de flux ou chiffrement par flot	Chiffrement visant à empêcher l'écoute clandestine et à assurer la confidentialité des liaisons individuelles.
Génération de clé de session	Les clés de session peuvent être changées à tout moment pendant une connexion. [5]
Échange de clés reposant sur l'infrastructure à clé publique	Utilisé dans Bluetooth 2.1, le protocole <i>Secure Simple Pairing</i> remplace la routine interrogation-réponse et permet le couplage sécurisé de périphériques sans NIP.

Au niveau des couches application et liaison, Bluetooth fait appel à la cryptographie pour assurer la confidentialité et l'authentification. Bluetooth utilise deux algorithmes de chiffrement, désignés par  $E_0$  et  $E_1$  dans la norme Bluetooth.  $E_0$  est un simple algorithme de chiffrement de flux OU exclusif (XOR), tandis que  $E_1$  repose sur l'algorithme de chiffrement bien connu SAFER+ et est utilisé pour l'authentification Bluetooth. Aucun de ces algorithmes n'est approuvé par le gouvernement du Canada :  $E_0$  a été cassé [7] et SAFER+ a été rejeté comme candidat AES (Advanced Encryption Standard) du NIST à cause de sa lenteur et de sa vulnérabilité aux attaques par canaux cachés (*side-channel attacks*) [8]. La spécification Bluetooth version 2.1 ajoute la courbe elliptique Diffie-Hellman pour améliorer la sécurité du processus d'échange de clés seulement; une fois le couplage réalisé, les chiffres existants continuent d'être utilisés pour la confidentialité des données.

## 2.2.2 Éléments cryptographiques Bluetooth patrimoniaux

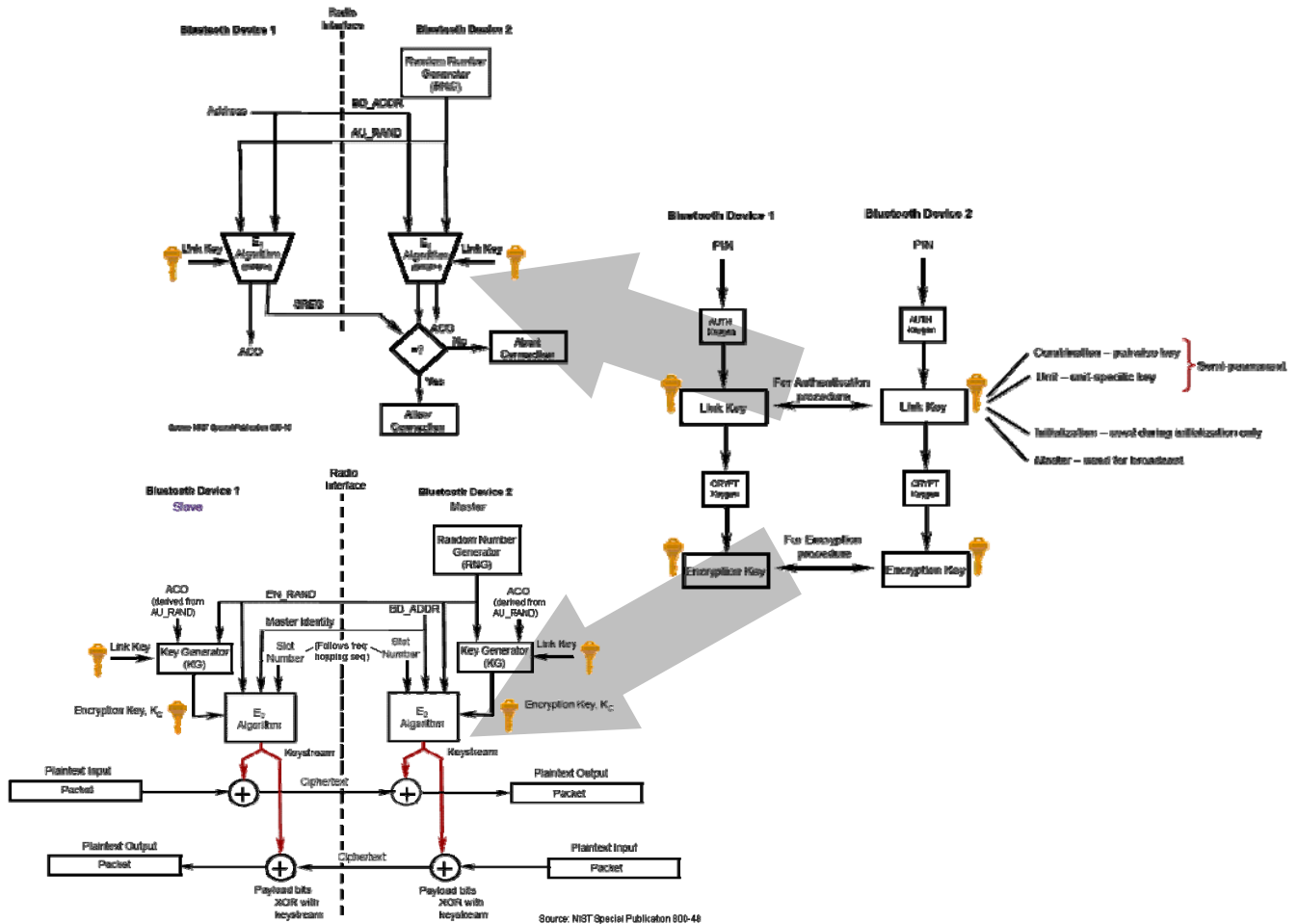


Figure 2 : Suite cryptographique Bluetooth

La suite cryptographique Bluetooth patrimoniale (Figure 2) est utilisée comme suit : la première fois que deux stations Bluetooth communiquent entre elles, une procédure d'initialisation, appelée couplage (ou jumelage), crée une clé de liaison commune. Une clé d'initialisation est utilisée comme clé d'authentification temporaire pour protéger le transfert des paramètres d'initialisation, puis est supprimée. Les entités participant au maintien de la sécurité au niveau de la couche liaison sont les suivantes :

- nombres aléatoires (RAND);
- adresse de périphérique Bluetooth (BD\_ADDR);
- numéro d'identification personnel (NIP);



## Évaluation des vulnérabilités de Bluetooth (ITSPSR-17A)

- clés d'authentification;
- clé de chiffrement.

### 2.2.2.1 Nombre aléatoire (RAND)

La technologie Bluetooth utilise des nombres aléatoires (appelés également *nonces* en cryptographie) pour tenter de rendre les sessions uniques et résistantes aux attaques par réinsertion (*replay attacks*). Des nombres aléatoires sont échangés à plusieurs occasions : deux durant l'initialisation de la liaison de communication (*in\_rand* et *lk\_rand*), un autre durant l'authentification (*au\_rand*) et un autre pour générer la clé de chiffrement (*en\_rand*). Dans tous les cas, le nombre aléatoire est un nombre de 128 bits obtenu au moyen d'un processus pseudo-aléatoire dans chaque périphérique Bluetooth. Comme l'indique la spécification Bluetooth, on entend par « aléatoire » qu'il n'est pas possible de prévoir la valeur du nombre avec un coefficient de probabilité bien supérieur à  $1/2^L$ , pour une longueur de clé de  $L$  bits. Il s'agit d'une spécification très vague, qui donne beaucoup de latitude aux fabricants de dispositifs dans la mise en oeuvre d'un générateur de nombres pseudo-aléatoires. Le caractère aléatoire d'un générateur de nombres aléatoires est essentiel à la sécurité de Bluetooth, parce qu'un attaquant capable de prédire la séquence des nombres aléatoires pourrait facilement calculer les clés de liaison et de chiffrement utilisées.

### 2.2.2.2 Adresse de périphérique Bluetooth (BD\_ADDR)

L'adresse BD\_ADDR est une adresse IEEE 48 bits, qui est propre à chaque périphérique Bluetooth. L'adresse est publique et peut être obtenue au moyen d'une interaction homme-machine ou automatiquement par la procédure de demande de renseignements. L'adresse BD\_ADDR sert également à générer une clé d'unité semi-permanente pour le périphérique la première fois qu'il est mis en service. Cette clé d'unité est enregistrée dans une mémoire non volatile et peut être utilisée comme clé de liaison dans l'authentification Bluetooth et, en fait, peut également être utilisée pour authentifier des connexions subséquentes entre les périphériques Bluetooth qui se partagent cette clé. Une fois créée, une clé d'unité ne change (presque) jamais. En fait, selon la spécification, « une clé de liaison basée sur une clé d'unité peut être modifiée, mais pas très facilement » (traduction libre). De telles clés d'unité fixes constituent une vulnérabilité importante de Bluetooth parce qu'elles ne sont pas régénérées à chaque session mais existent pendant de longues périodes de temps (peut-être même pour toute la durée de vie du périphérique). Par ailleurs, si une clé d'unité est découverte, tout périphérique qui s'en sert aux fins de sécurité peut être compromis. Compte tenu de ce qui précède, les clés d'unité ne sont plus guère utilisées (leur utilisation n'est plus recommandée quoiqu'elles continuent d'être prises en charge) depuis la version 1.2 de Bluetooth.



### 2.2.2.3 Numéro d'identification personnel (NIP)

Le NIP peut être défini par l'utilisateur, et a une longueur de 1 à 16 octets. Le NIP est généré au niveau de la couche application par divers moyens, allant de la programmation manuelle du numéro à un échange de clés Diffie-Hellman (nota : cela n'a aucun rapport avec la courbe elliptique Diffie-Hellman [ECDH] utilisée dans le mode de couplage simple sécurisé [*Secure Simple Pairing*] de Bluetooth 2.1). Certains périphériques Bluetooth peuvent avoir une mémoire limitée, tandis que d'autres peuvent ne pas avoir l'interface requise pour la saisie d'un NIP. En pareil cas, ces périphériques peuvent utiliser un NIP fixe ou le NIP par défaut (0x0000) avec une sécurité plus faible correspondante.

Le NIP est utilisé avec un nombre aléatoire et une adresse BD\_ADDR pour créer une clé d'initialisation. Si aucun des périphériques ne possède de NIP fixe, l'adresse BD\_ADDR du périphérique demandeur est utilisée. Si un seul des périphériques a un NIP fixe, l'adresse BD\_ADDR utilisée est celle du périphérique sans NIP fixe. Si les deux périphériques ont des NIP fixes, il est impossible d'établir une liaison authentifiée entre eux [6]. Afin d'empêcher les recherches exhaustives de NIP, la spécification indique qu'« il faut attendre un certain temps avant que le vérificateur n'amorce une nouvelle tentative d'authentification [...] Pour chaque échec subséquent, le temps d'attente augmente de façon exponentielle » (traduction libre) [1]. Les tests ont permis d'indiquer que très peu de périphériques commerciaux imposent des durées d'attente croissantes; la plupart permettent un nombre illimité de tentatives d'authentification sans pénalité.

Étant donné que les valeurs aléatoires utilisées pour le calcul des clés doivent être échangées, un attaquant capable d'intercepter la procédure de couplage Bluetooth peut utiliser ces valeurs interceptées et les diverses réponses échangées entre les deux périphériques Bluetooth pour inverser le protocole et calculer le NIP de l'utilisateur. Ce type d'attaque est extrêmement rapide et efficace : un attaquant peut calculer un NIP de 4 chiffres en moins d'une seconde sur un PC standard, et un NIP de 8 chiffres en 10 minutes environ.

### 2.2.2.4 Clés d'authentification

Deux clés d'authentification distinctes sont utilisées dans Bluetooth : la clé d'initialisation et la clé de liaison. Ces deux clés sont des entités de 128 bits qui sont partagées entre deux ou plusieurs parties, mais qui ne sont pas disponibles au public. La première clé d'authentification établie pendant l'initialisation d'une liaison entre des périphériques Bluetooth est appelée la clé d'initialisation et, comme il a été décrit plus haut, dépend en partie du NIP de l'utilisateur. L'étape suivante consiste à générer la clé de liaison. Comme il est décrit plus haut, une clé d'unité articulée sur l'adresse BD-ADDR peut servir de clé de liaison; or, compte tenu raison des vulnérabilités associées à une clé fixe, une biclé temporaire appelée « clé de combinaison » est la forme privilégiée de la clé de liaison. Dans le processus de génération de la clé de combinaison, la clé d'initialisation protège un second échange de nombres aléatoires entre les périphériques, qui servent à créer une nouvelle clé. Par comparaison à la clé d'unité semi-permanente, la durée de vie d'une clé de combinaison temporaire est limitée à une seule session entre deux ou



## Évaluation des vulnérabilités de Bluetooth (ITSPSR-17A)

plusieurs périphériques Bluetooth. Lorsque la liaison est rompue, la clé de combinaison temporaire ne peut plus être réutilisée. Selon la spécification, le processus de création d'une clé de liaison dépend de la nature et des restrictions de mémoire des périphériques en cause. La clé d'initialisation est toujours créée avant la clé de liaison.

Une fois les clés d'authentification générées, un mécanisme d'interrogation-réponse entre les deux périphériques sert à vérifier si chacun connaît les clés : le nombre aléatoire *au-rand*, l'adresse BD\_ADDR et la clé de liaison sont chiffrés sur chaque périphérique à l'aide de l'algorithme SAFER+ à l'intérieur de  $E_1$  et les résultats sont comparés. S'ils concordent, cela signifie que les deux périphériques ont la même clé.

### 2.2.2.5 Clé de chiffrement

La clé de chiffrement  $K_C$  est établie à partir d'un autre algorithme appelé  $E_3$ , lequel combine la clé de liaison précédemment calculée, un nombre de décalage de chiffrement de 96 bits et un nombre aléatoire généré par l'une des deux stations. La taille de cette clé de chiffrement  $K_C$  est un multiple de 8 bits, et va de 8 à 128 bits (en théorie 128 bits, quoique Bluetooth permette la négociation d'une taille de clé pouvant être aussi petite que 8 bits).

Une fois générée à chaque extrémité, la clé de chiffrement est utilisée par l'algorithme de chiffrement de flux avec l'adresse BD\_ADDR de l'une des stations et l'horloge du saut de fréquence de la même station. À noter que si la taille de la clé est inférieure à 128 bits, l'algorithme  $E_0$  l'élève à 128 bits (par remplissage) pendant le processus de chiffrement.

### 2.2.3 Couplage simple sécurisé

Pour simplifier le processus de couplage et pour améliorer la sécurité, on a introduit dans Bluetooth version 2.1 le mode de couplage simple sécurisé (*Secure Simple Pairing*). Ce mode ne fait pas appel aux NIP mais à la courbe elliptique Diffie-Hellman (ECDH) pour échanger les clés entre périphériques de manière sécurisée.

Dans ce mode, un système cryptographique à clé publique reposant sur les courbes elliptiques vient remplacer l'algorithme SAFER+ qui était utilisé dans le mode de couplage patrimonial. Grâce au couplage simple sécurisé, le couplage est amorcé par un échange de clés publiques qui sont utilisées avec la clé secrète de chaque périphérique pour calculer une clé Diffie-Hellman partagée. Par la suite, des échanges de nonces aléatoires qui sont uniques à chaque session (afin d'empêcher les attaques par réinsertion [*replay attack*]) sont utilisés pour faciliter l'authentification mutuelle des clés publiques.

Le mode de couplage simple sécurisé fonctionne normalement en mode sans NIP mais il permet en option les échanges d'authentification hors bande (p. ex., authentification de personne à personne), de même que les échanges de clés passe-partout. L'échange de clés passe-partout est semblable à l'échange de NIP, à la différence que les passe-partout ne servent pas au calcul des clés de liaisons ou de chiffrement, de sorte que la connaissance du passe-partout ne permettra pas à l'attaquant de déterminer les clés dont il a besoin pour déchiffrer la session. Les fonctions de contrôle de vérification utilisées pour l'authentification dans le mode de couplage simple



## Évaluation des vulnérabilités de Bluetooth (ITSPSR-17A)

sécurisé reposent sur le code HMAC-SHA-256, avec une clé de 128 bits. En mode sans NIP, pour réduire le risque de couplage automatique (mais sécurisé) de périphériques non autorisés, ceux-ci peuvent afficher les valeurs de contrôle calculées aux fins de comparaison et demander à l'utilisateur d'autoriser ou non (par un simple oui ou non) le couplage. Les périphériques Bluetooth comme les oreillettes, qui n'ont généralement pas d'écran ou de clavier, ne mettraient probablement pas en oeuvre cette étape de validation de l'utilisateur, ce qui pourrait permettre à des périphériques non autorisés de se connecter en silence à un picoréseau.

Une fois l'authentification terminée, les deux périphériques calculent une clé de liaison en fonction de l'information publique précédemment échangée, et de la clé Diffie-Hellman calculée. Vient ensuite l'étape finale du couplage simple sécurisé, qui est la génération des clés de chiffrement, laquelle s'effectue exactement de la même manière que dans le couplage patrimonial (voir [2.2.2.5](#)).

### 2.2.4 Résumé

Les vulnérabilités associées à la cryptographie des périphériques Bluetooth patrimoniaux sont connues depuis longtemps. Elles comprennent notamment l'utilisation des clés permanentes (clés d'unité), l'utilisation de NIP courts pour créer les clés et l'utilisation de NIP par défaut codés en dur (normalement 0x0000) et la capacité de négocier des clés de chiffrement courtes (aussi courtes que 8 bits). L'utilisation de clés d'unité permanentes ou semi-permanentes est probablement le maillon le plus faible de la cryptographie Bluetooth et, heureusement, leur emploi a été abandonné depuis Bluetooth version 1.2. Comme un périphérique Bluetooth est conçu pour établir rapidement une connexion avec d'autres périphériques, le partage de la même clé sur plusieurs liaisons, connexes ou non, constitue une faiblesse que peuvent exploiter des attaquants. Cette faiblesse est probablement plus grave que celle qui est associée au protocole WEP (*Wired Equivalent Privacy*) des réseaux sans fil 802.11, qui a fait l'objet d'une couverture médiatique intense en 2001 [3].

Bluetooth 2.1 offre le nouveau mode de couplage simple sécurisé qui vient remplacer la procédure de couplage Bluetooth patrimonial avec une procédure reposant sur la courbe elliptique Diffie-Hellman. La cryptographie de ce nouveau mode est certes beaucoup plus forte, mais elle s'applique uniquement à la procédure de couplage elle-même, le chiffrement des données de session étant effectué de la même manière qu'auparavant. Par ailleurs, le fait que le développeur a l'option de se dispenser de la validation utilisateur dans le processus de couplage peut donner lieu à des instances où un périphérique non autorisé peut se connecter silencieusement (et de manière sécurisée) à un picoréseau.

## 2.3 Autres vulnérabilités

### 2.3.1 Généralités

Outre la couche physique et la cryptographie, la technologie Bluetooth présente quelques vulnérabilités qui sont communes à de nombreuses autres technologies de télécommunications.



## Évaluation des vulnérabilités de Bluetooth (ITSPSR-17A)

### 2.3.2 Authentification des utilisateurs

Comme pour la plupart des dispositifs TI, l'utilisateur n'est pas authentifié, seul le périphérique l'est. Un utilisateur qui ne protège pas son mécanisme d'authentification (p. ex., s'il utilise un NIP faible ou un mot de passe facile à deviner) ou qui égare ou perd un périphérique authentifié risque d'être victime d'une attaque d'usurpation d'identité, où l'attaquant peut voler le périphérique et assumer l'identité de l'utilisateur légitime. Dans de telles situations, la victime n'est pas seulement l'utilisateur légitime du périphérique volé, mais aussi possiblement toute autre personne qui communique avec le périphérique volé.

### 2.3.3 Génération de nombres aléatoires

Comme il a été mentionné plus haut, les spécifications de Bluetooth sur la génération de nombres aléatoires sont relativement faibles. Par conséquent, on peut s'attendre à de nombreuses mises en oeuvre différentes de Bluetooth, offrant divers degrés de caractère aléatoire mais satisfaisant toutes à la définition du terme « aléatoire » dans la spécification.

### 2.3.4 Erreurs de mise en oeuvre/faiblesses

De nombreuses attaques contre les erreurs de mise en oeuvre ou les faiblesses de Bluetooth en matière de sécurité sont documentées dans la littérature publique et se sont vu donner des noms hauts en couleur comme, par exemple :

- *Bluedumping* – Cette attaque mentionnée plus haut consiste à faire le calcul inverse du NIP de l'utilisateur à partir des échanges de couplage interceptés.
- *Bluesnarfing* – Permet à l'attaquant d'accéder au répertoire téléphonique et au calendrier des périphériques ciblés en raison d'une erreur de mise en oeuvre dans le protocole OBEX Push.
- *Bluebugging* – Utilise les canaux RFCOMM de Bluetooth et permet à l'attaquant de commander le téléphone à distance, y compris faire des appels non autorisés et allumer le microphone pour transformer l'appareil en dispositif d'écoute.
- *Bluejacking* – La faible sécurité du profil OBEX sur certains périphériques permet à l'attaquant d'ajouter des entrées dans le répertoire d'un périphérique ciblé.
- *Bluestabbing* – Permet à l'attaquant d'exploiter le périphérique Bluetooth en y définissant un nom de périphérique mal formaté; lorsque le périphérique ciblé essaie de localiser d'autres périphériques se trouvant à proximité, il lit le nom mal formaté et cesse de fonctionner.
- *Bluebumping* – Attaque d'ingénierie sociale qui exploite le fait qu'un couplage ne disparaît pas totalement tant que **les deux** périphériques n'ont pas supprimé la connexion. L'attaquant utilisera l'ingénierie sociale pour convaincre la cible de coupler avec son périphérique. La cible supprimera le couplage de son appareil par la suite, mais



---

## Évaluation des vulnérabilités de Bluetooth (ITSPSR-17A)

---

l'attaquant ne le fera pas, ce qui lui permettra de garder une « porte dérobée » sur le périphérique de la cible.

- *Bluesmacking* – Consiste à envoyer une requête d'informations mal formatée, ce qui a l'effet d'un « ping de la mort » et fait planter tout périphérique qui la reçoit.

D'autres vulnérabilités, comme « l'attaque par recouplage » (*re-pairing attack*) découverte par Wool et Shaked [9], permettent à l'attaquant d'exploiter des erreurs de mise en oeuvre du traitement des exceptions dans Bluetooth durant l'établissement de la connexion, ce qui force les périphériques à rejeter les clés de liaison et à effectuer un nouveau couplage. L'attaque a une valeur limitée en soi, mais si elle est bien exécutée, elle permet de réaliser d'autres types d'attaque, comme le *bluedump* (pour récupérer le NIP de l'utilisateur).



---

**Évaluation des vulnérabilités de Bluetooth (ITSPSR-17A)**

---

*Page intentionnellement laissée en blanc.*



## **3 Au-delà de la technologie**

### **3.1 Généralités**

Les sections précédentes traitent de la technologie Bluetooth, telle qu'elle figure dans la spécification, sans tenir compte de mises en oeuvre particulières de produits ou de fournisseurs. Comme la spécification Bluetooth offre de nombreuses options qui influent sur le degré de sécurité, on peut supposer qu'un large éventail de ces options est offert aux utilisateurs. Toutefois, dans les faits, les utilisateurs ont très peu de latitude quant à la possibilité de modifier les configurations de sécurité que les fournisseurs mettent à leur disposition dans les produits commerciaux, et doivent généralement se contenter d'un compromis entre la facilité de connexion du périphérique et la sécurité.

### **3.2 Communications par radiofréquences (RF)**

Il faut examiner de très près les particularités de l'environnement RF. Une des incertitudes majeures au sujet de Bluetooth est due au fait que cette technologie a été conçue pour établir des réseaux ad hoc le plus rapidement possible, sur le canal radio mobile terrestre. Comme ce canal est utilisé dans un milieu difficile où abondent les interférences, les évanouissements et les occultations des signaux, il arrive souvent que les liaisons soient momentanément interrompues. Les tests en laboratoire ont démontré que les liaisons Bluetooth sont peu stables dans de nombreux produits commerciaux. Par conséquent, les utilisateurs doivent passer beaucoup de temps à rétablir les réseaux, car les liaisons ont été rompues et que les pannes de liaison fréquentes sont acceptées comme un inconvénient normal des communications RF. Par conséquent, l'utilisateur peut penser, à tort, qu'un attaquant aura également des difficultés à mettre en échec la sécurité d'une liaison.

À mesure que la technologie évolue, les fournisseurs conçoivent leurs produits de telle sorte que le rétablissement de la liaison se fait automatiquement et de manière transparente pour l'utilisateur, ce qui augmente leur vulnérabilité aux attaques. Par exemple, une attaque de déni de service instantané suivie du rétablissement du picoréseau peut passer inaperçue. De plus, si un périphérique fait l'objet de tentatives constantes d'attaques de type découverte de périphérique et/ou de service, il est possible qu'il n'alerte pas automatiquement l'utilisateur (à moins qu'il ne soit en mode non-découverte), mais qu'il gère les tentatives de découverte en arrière-plan, sans éveiller les soupçons de l'utilisateur.

### **3.3 Politiques de connectivité**

La philosophie Bluetooth est la suivante : « il revient en définitive à la politique définie au niveau de l'utilisateur (ou, de façon plus générale, au niveau de l'application) de décider quand un périphérique entre dans l'un ou l'autre des états (requête d'informations ou requête de connexion). Dans le même ordre d'idées, une politique définie au niveau de l'utilisateur détermine également si les périphériques se coupleront (s'authentifieront) les uns avec les autres. Il s'agit là d'un point important : les décisions prises par l'utilisateur déterminent jusqu'à quel



## Évaluation des vulnérabilités de Bluetooth (ITSPSR-17A)

point un périphérique donné peut être découvert, connecté ou couplé. Une inquiétude souvent formulée au sujet de la technologie Bluetooth est que tous les périphériques Bluetooth communiqueront automatiquement les uns avec les autres à tout moment, mais cette conception est erronée. Les utilisateurs, ou les applications de niveau utilisateur, établissent les politiques de connectivité qui déterminent quels périphériques peuvent communiquer l'un avec l'autre, et quand. Ces politiques pourraient être définies par les fabricants de périphériques Bluetooth, ou être configurables par les utilisateurs. Par conséquent, les fabricants de périphériques pourraient se baser sur les politiques de connectivité afin de différencier leurs produits. » (traduction libre) [2, p. 213]

Malheureusement, peu nombreux sont les fournisseurs de périphériques Bluetooth qui ont adopté cette philosophie. À titre d'exemple, de nombreuses oreillettes Bluetooth mains-libres sont toujours en mode découverte et ne peuvent être désactivées. Des tests ont démontré que certains modèles, plus particulièrement ceux qui peuvent être utilisés avec des stations de base (pour fournir des fonctions sans fil à des téléphones de bureau standard), contiennent des écarts de protocole qui permettent à la station de base et l'oreillette Bluetooth de même marque de se coupler automatiquement ou de se recoupler **sans** directive expresse de l'utilisateur.

### 3.4 Caractéristiques techniques

#### 3.4.1 Généralités

Les périphériques Bluetooth ont pénétré dans le milieu de travail grâce au marketing de masse ciblant les consommateurs aux connaissances techniques limitées. Les utilisateurs se servent de périphériques qui affichent le logo Bluetooth, sans rien savoir de Bluetooth. Dans certains cas, l'administrateur de système fournira ces périphériques aux utilisateurs de son organisme. Cet administrateur peut en savoir plus sur les TI que les utilisateurs, mais il n'a peut-être pas de connaissances approfondies relativement à Bluetooth ou au sans-fil.

#### 3.4.2 Fonctions d'économie de pile

Les efforts déployés par Bluetooth pour prolonger la durée de vie des piles présente une autre vulnérabilité. En effet, les développeurs ont constaté que, parmi toutes les fonctions que les périphériques mobiles offrent aux utilisateurs, ce sont la longue durée des piles et la légèreté du périphérique qui importent le plus. Ces fonctions ont préséance sur la qualité de la liaison, la couverture, la fiabilité, l'apparence et, malheureusement, la sécurité. Comme elles sont souvent contradictoires (en effet, on réussit généralement à prolonger la durée des piles en utilisant des piles plus grosses, ce qui représente un poids supplémentaire), la spécification Bluetooth a incorporé de nombreuses fonctions visant à prolonger la durée des piles. Par exemple, les modes « mise en garde », « attente » et « renflage » visent tous exclusivement à prolonger la durée des piles. De même, lorsque le périphérique est actif, il est à l'écoute des en-têtes de paquet uniquement, et c'est seulement si un en-tête indique que le paquet lui est adressé que celui-ci écoutera l'ensemble du paquet.



## Évaluation des vulnérabilités de Bluetooth (ITSPSR-17A)

Certains fournisseurs tentent de développer davantage les fonctions d'économie de pile en réduisant la longueur des clés de chiffrement ou en sautant les étapes de vérification nécessitant de nombreux calculs cryptographiques. Le chiffrement consomme de la puissance de calcul et épuise les piles. Dans la plupart des algorithmes, plus la clé est longue, plus les fonctions de chiffrement et de déchiffrement consomment de l'énergie. Dans Bluetooth, l'algorithme bourre toujours la clé qui lui est fournie afin d'en faire une clé dont la longueur artificielle est de 128 bits, **sans** ajouter aucune sécurité, avant d'exécuter l'opération de chiffrement/déchiffrement. Il est possible que certains fournisseurs et utilisateurs ne comprennent pas cela et entrent des clés de chiffrement plus courtes pour économiser les piles. D'autres peuvent même désactiver le chiffrement pour des économies additionnelles.

### 3.4.3 Claviers Bluetooth

On doit accorder une attention spéciale à l'utilisation de la technologie Bluetooth dans les claviers. En effet, un clavier qui communique avec son PC par l'intermédiaire d'une liaison Bluetooth présente un risque particulièrement élevé. L'utilisateur d'un poste de travail filaire peut toujours assumer que ses données clavier demeurent confidentielles et que seules les données transmises sur le réseau peuvent être sujettes à interception. Or, les utilisateurs d'un clavier Bluetooth devraient se rendre compte que toutes les données tapées peuvent être exposées sur une portée de plusieurs mètres.

### 3.4.4 Débits améliorés

Bluetooth 2.1 comprend une fonction de débits améliorés (*Enhanced Data Rates*), allant jusqu'à 3 Mbps, et la technologie de bande ultra-large (UWB pour *ultra-wideband*) proposée pour la norme Bluetooth 3.0 de prochaine génération, promet d'accroître davantage les débits. Cela mènera au développement d'un plus grand nombre d'applications de transfert de données Bluetooth (p. ex. remplacements de réseaux filaires). La largeur de bande accrue et la plus grande variété de types de transfert de données (p. ex. contenus vidéo ou gros documents) qui deviendront possibles grâce à cette technologie augmenteront de façon considérable les risques associés à l'utilisation de Bluetooth.

## 3.5 Sensibilisation des utilisateurs aux questions de sécurité

Le fait que les utilisateurs soient peu conscients de l'aspect sécurité représente probablement le plus grand risque dans l'utilisation de Bluetooth. Vu la complexité des technologies de l'information modernes et du peu de temps que les utilisateurs consacrent aux fonctions qui débordent de la simple fonctionnalité de l'appareil (comme la sécurité), ceux-ci sont nombreux à ne pas prendre l'initiative de se familiariser avec les procédures et les politiques de sécurité requises pour protéger l'information qu'ils traitent.



---

**Évaluation des vulnérabilités de Bluetooth (ITSPSR-17A)**

---

*Page intentionnellement laissée en blanc.*



## **4 Solutions**

### **4.1 Généralités**

Des solutions existent pour réduire les risques associés à l'utilisation de Bluetooth, et elles doivent être adaptées au risque en question. Cela est particulièrement important dans le cas de la technologie Bluetooth, car celle-ci a été conçue comme méthode générale de remplacement de la technologie filaire sur de courtes distances sans cibler des applications particulières. Avant de mettre au point une solution, on doit tenir compte de plusieurs facteurs : l'application, l'environnement, la menace, l'utilisateur, etc. Essentiellement, cela revient à imaginer ce que les problèmes et les solutions seraient pour une situation similaire faisant appel à la technologie filaire.

### **4.2 Non-usage**

Il est évident que la meilleure solution pour éliminer tout risque associé à la technologie Bluetooth est simplement de ne pas s'en servir. En pareils cas, une politique claire interdisant l'usage de tels périphériques doit être mise en place et des procédures TI pour retirer ou désactiver cette fonctionnalité sur le matériel TI doivent être élaborées. À titre d'exemple, il est possible que certains modèles d'ordinateurs portatifs emploient un module Bluetooth interne qui puisse être physiquement retiré avant le déploiement aux utilisateurs finals. D'autres peuvent comporter un commutateur mécanique servant à désactiver la fonctionnalité Bluetooth. Sur d'autres modèles encore, on doit passer par le gestionnaire des dispositifs Windows pour désactiver cette fonction dans les logiciels. Dans les dispositifs comme les assistants numériques (PDA) Blackberry, on peut mettre en oeuvre une politique sur le Blackberry Enterprise Server pour désactiver la fonctionnalité Bluetooth.

### **4.3 Enceintes blindées contre les radiofréquences**

La solution la plus sûre (quoique extrême) pour parer à la plupart des vulnérabilités Bluetooth (et sans fil) possibles est d'entourer le périphérique (p. ex. un ordinateur utilisant un clavier Bluetooth) d'une enceinte ou d'une tente blindée contre les radiofréquences. Si elle est bien conçue et utilisée correctement, une telle enceinte empêche la transmission vers l'extérieur de toute communication sans fil interne. Toutefois, une telle solution est extrêmement coûteuse et peu pratique; elle convient probablement seulement aux applications classifiées ou militaires où la sécurité est primordiale. Le nombre d'applications Bluetooth qui pourraient profiter d'une enceinte blindée est minime.

### **4.4 Applications cryptographiques**

Pour les versions courantes de Bluetooth (versions 1.0 à 2.0), on recommande l'utilisation de mécanismes cryptographiques approuvés additionnels au niveau de la couche application (au-dessus de Bluetooth) pour protéger l'information désignée PROTÉGÉ et pour assurer la confidentialité requise. Une liste d'algorithmes approuvés figure dans le document *Algorithmes*



## Évaluation des vulnérabilités de Bluetooth (ITSPSR-17A)

*cryptographiques approuvés par le CST pour la protection des renseignements désignés et pour les applications d'autorisation et d'authentification électroniques au sein du gouvernement du Canada (ITSA-11C) [5].*

Avec l'introduction de Bluetooth version 2.1 et l'utilisation d'échange de clés par courbe elliptique Diffie-Hellman (ECDH) dans le mode de couplage simple sécurisé (*Secure Simple Pairing*), il est possible que certains mécanismes cryptographiques de niveau application ne soient pas nécessaires, mais cette question fait encore l'objet de discussions. Règle générale, étant donné que des clés plus longues sont nécessaires pour assurer une bonne sécurité cryptographique, la cryptographie à clé publique est habituellement requise pour échanger ces longues clés symétriques en raison de la difficulté que représente leur distribution manuelle (c.-à-d. saisie des clés par l'utilisateur). Les algorithmes de clés publiques comme Diffie-Hellman, IKE et de nombreux autres schémas sont disponibles à cette fin, mais ils ne conviennent pas toujours à l'environnement opérationnel limité qu'on retrouve dans un périphérique Bluetooth mobile. Malheureusement, même si l'ECDH peut convenir comme mécanisme de distribution de clés, comme il a été décrit plus haut dans le présent document, Bluetooth version 2.1 continue d'utiliser SAFER+ et E<sub>0</sub>, lesquels ne sont pas des algorithmes de chiffrement approuvés pour le GC.

Dans certains cas, l'utilisation de l'infrastructure à clé publique (ICP) peut être justifiée lorsqu'un utilisateur ne se trouve pas à proximité du partenaire à l'autre extrémité de la connexion, comme c'est le cas lorsque la liaison sans fil Bluetooth ne représente qu'un segment de la connexion entière.

### 4.5 Choix des produits Bluetooth commerciaux

Le choix d'un produit Bluetooth approprié est également très important si l'on veut réduire les risques au minimum. Il faudrait tenir compte des caractéristiques suivantes lorsqu'on recherche un produit Bluetooth plus sécurisé :

- fonction de couplage simple sécurisé de Bluetooth 2.1,
- possibilité de changements fréquents de la clé d'unité,
- mise en oeuvre de l'option d'adaptation de puissance,
- forte augmentation du temps d'attente entre les tentatives successives d'authentification,
- utilisation de clés de chiffrement ou de NIP longs.

### 4.6 Politique de sécurité

La technologie ne peut à elle seule assurer la sécurité d'une application; elle doit être accompagnée de la définition et de l'utilisation appropriées de politiques de sécurité solides, incluant notamment ce qui suit :

- effectuer le couplage de périphériques Bluetooth uniquement dans un environnement privé et sécurisé, et non pas dans un lieu public,



---

## Évaluation des vulnérabilités de Bluetooth (ITSPSR-17A)

---

- utiliser des NIP longs,
- modifier fréquemment les NIP,
- utiliser des clés de combinaison au lieu des clés d'unité,
- utiliser le paramètre de non-découverte comme paramètre par défaut pour les périphériques et les services,
- s'assurer que le chiffrement est activé,
- protéger les NIP et les mots de passe
- utiliser un NIP différent sur chaque périphérique.

### 4.7 Résumé

Les lecteurs intéressés à une étude plus approfondie des vulnérabilités de Bluetooth et des solutions connexes peuvent également consulter le document intitulé *Special Publication 800-48* [9], disponible sur le site Web du NIST ([www.nist.gov](http://www.nist.gov)). Toutefois, une combinaison de toutes les mesures décrites ci-dessus représente la meilleure solution, et aussi la plus pratique, afin de contrer les vulnérabilités de sécurité associées à la technologie Bluetooth. La combinaison exacte qu'il convient d'utiliser dépend de l'évaluation des menaces et des risques liée à l'application opérationnelle ou gouvernementale envisagée. Règle générale, toutefois, le CSTC **ne recommande pas** à l'heure actuelle l'utilisation de la technologie Bluetooth pour transférer de l'information classifiée ou protégée.



---

**Évaluation des vulnérabilités de Bluetooth (ITSPSR-17A)**

---

*Page intentionnellement laissée en blanc.*



## 5 Travaux futurs

Depuis le développement initial de Bluetooth, une gamme variée de périphériques sans fil sont apparus sur le marché. La version courante de Bluetooth (version 2.1) offre des débits plus élevés et une fonction de sécurité importante désignée sous le nom de mode de couplage simple sécurisé (*Secure Simple Pairing*). Au moment de la rédaction du présent document, peu de produits conformes à la version 2-1 de Bluetooth étaient disponibles sur le marché; toutefois, comme avec les versions précédentes de Bluetooth, on s'attend à voir arriver bientôt un nombre croissant de produits basés sur la nouvelle norme.

On a testé et examiné certains produits Bluetooth par le passé, et on continue de surveiller l'état de cette technologie. Les plans futurs du CSTC comprennent entre autres des tests de produits de la version Bluetooth 2.1. On mettra l'accent sur les produits les plus communément utilisés par le personnel du GC, notamment :

- oreillettes et dispositifs multimedia Bluetooth,
- claviers et souris Bluetooth,
- LAN sans fil Bluetooth,
- périphériques de sécurité pour PC,
- solutions cryptographiques modulaires fonctionnant aux couches supérieures.



---

**Évaluation des vulnérabilités de Bluetooth (ITSPSR-17A)**

---

*Page intentionnellement laissée en blanc.*



## 6 Références

- [1] *Specification of the Bluetooth System*, version 2.1+EDR, 26 juillet 2007.
- [2] Miller, B. et Bisdikian, C., *Bluetooth Revealed*, Prentice Hall PTR, 2001.
- [3] Security of the WEP Algorithm. <http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html>
- [4] ITSPSR-17, *Évaluation des vulnérabilités de Bluetooth*, CST, octobre 2002.
- [5] ITSA-11C - *Algorithmes cryptographiques approuvés par le CSTC pour la protection des renseignements protégés et pour les applications d'autorisation et d'authentification électronique au sein du gouvernement du Canada (GC)*, CST, 18 avril 2006.
- [6] Shaked, Y. et Wool, A., *Cracking the Bluetooth PIN*, MobiSys Conference 2005
- [7] Lu, Y. et Vaudenay, S., *Faster Correlation Attack on Bluetooth Keystream Generator*, E0, Crypto 2004
- [8] Nechvatal, J. et al, *Status Report on the First Round of the Development of the Advanced Encryption Standard*, Journal of the Research of the National Institute of Standards and Technology, Volume 104-435
- [9] Karygiannis, T. et Owens, L., *Wireless Network Security: 802.11, Bluetooth and Handheld Devices*, Special Publication 800-48, National Institute of Standards and Technology