

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche
Scientifique

Centre de Recherche sur l'Information Scientifique et Technique



Mémoire de fin d'études

Pour l'obtention du diplôme de post graduation spécialisée en
sécurité informatique

Promotion 2005-2006

Thème :

La Sécurité et les Réseaux Bluetooth

Présenté par : - Mr YAKOUB Ali
- Mr BELHOUL Ferhat Nabil

Encadré par:
Mr DJENNOURI Djamel

Devant le jury

Mr	Omar	NOUALI	Président
Mme	Souad	BENMEZIANE	Examinatrice
Mr	Abdelouahid	DERHAB	Examineur

Juin 2007

Sommaire

Sommaire

Introduction Générale	01
Chapitre I : Etude générale sur bluetooth	02
1. Introduction	02
2. Introduction aux réseaux sans fil	03
2.1 Réseaux personnels sans fil (WPAN)	04
2.2 Réseaux locaux sans fil (WLAN)	05
2.3 Réseaux métropolitains sans fil (WMAN)	05
2.4 Réseaux étendus sans fil (WWAN)	06
2.5 Pourquoi Bluetooth plutôt que Wifi ?	06
3. Caractéristiques de la technologie Bluetooth	06
3.1 Normes Bluetooth	06
3.2 Spectre de fréquences	07
3.3 Portée	07
3.4 Puissance	08
3.5 Débit de données	08
3.6 Domaine d'utilisation	08
4. Principe de communication	08
5. Etablissement des connexions	10
6. Pile du protocole Bluetooth	11
a- Couche Radio (RF).....	11
b- Couche BaseBand	12
✓ Lien SCO (Synchronous, Connection Oriented)	13
✓ Lien ACL (Asynchronous, Connection Less)	13
c- Le contrôleur de liaisons LC (Link Controller).....	15
d- Couche LMP (Link Manager Protocol).....	15
e- L'interface de contrôle de l'hôte (HCI).....	17
f- Couche L2CAP (Logical Link Control and Adaptation layer Protocol).....	17
g- Couche RFCOMM.....	18
h- Profiles.....	19
i- Applications	21
7. Connexion de deux périphériques Bluetooth	21
8. Connexion d'un périphérique à un piconet existant	22
9. Utilisation d'IP au dessus de Bluetooth	22
Conclusion	23
Chapitre II : Les services de sécurité dans les réseaux Bluetooth	24
1. Introduction	24
2. Sécurité de Bluetooth	24
2.1 Représentation des Paramètres Bluetooth	24
2.2 Architecture de sécurité	24

3. Caractéristiques de sécurité bluetooth selon les spécifications	26
3.1 Modes de sécurité	26
3.2 Intérêt pour la cryptographie	28
3.3 Génération de la clé de liaison – Couplage Bluetooth (pairing).....	28
3.4 Authentification	29
3.5 Confidentialité (Cryptage)	31
4. Niveaux de confiance, niveaux de service, et autorisation	33
Conclusion	34
Chapitre III : Vulnérabilités des réseaux Bluetooth	35
1. Introduction	35
2. Problèmes associés à la sécurité standard bluetooth	35
2.1 Les PINs courts sont permises	35
2.2 La longueur des clés de cryptage est négociable	36
2.3 La clé d'unité est réutilisable et devenant ainsi publique	36
2.4 Absence de l'authentification de l'utilisateur	36
2.5 Répétition des tentatives d'authentification	36
2.6 L'algorithme de cryptage E0 (stream cipher algorithm) est faible	36
2.7 Le partage de la clé d'unité peut conduire à l'écoute clandestine	36
2.8 L'authentification de l'appareil est basée sur simple défi de clé partagée	37
2.9 La sécurité de bout en bout n'est pas assurée	37
2.10 Les services de sécurité sont limités	37
2.11 Faible protection de l'intégrité	37
3. Analyse des vulnérabilités Bluetooth	37
3.1 Vulnérabilités liées à la couche physique	37
3.1.1 Communications par radiofréquences (RF).....	38
3.1.2 Contrôle de puissance adaptatif	38
3.1.3 Saut de fréquence	39
3.2 Vulnérabilités liées aux fonctionnalités cryptographiques	40
3.2.1 Authentification des utilisateurs.....	40
3.2.2 La fonction de cryptage n'est pas obligatoire	40
3.2.3 Les paramètres par défaut (non sécurisés) ne sont pas éliminés	40
3.2.4 Les PINs faibles peuvent être devinées	40
3.2.5 Les clés d'unité ne sont pas sécurisées	40
3.2.6 Qualité du générateur du nombre aléatoire	41
3.3 Autres vulnérabilités	41
3.3.1 Vol et perte	41
3.3.2 Vulnérabilité de la liaison clavier/PC	41
4. Types d'attaques	42
4.1 Écoute clandestine et usurpation d'identité	42
4.2 Attaque "Man in the Middle".....	42
4.3 Attaque par déni de service	43

5. Techniques d'attaques et vulnérabilités associées	44
5.1 BlueJacking	44
5.2 BlueSnarf	44
5.3 BlueSnarf ++	44
5.4 BlueBug	44
5.5 Helomoto	45
5.6 BlueSmack	45
5.7 BlueStab	46
5.8 BlueBump	46
5.9 BlueSpooof	46
5.10 BlueDump	46
5.11 BlueTooone	46
Conclusion	47
Chapitre IV: Solutions aux vulnérabilités des réseaux Bluetooth	48
1. Introduction	48
2. Minimisation des risques	48
2.1 Contre-mesures administratives	48
2.2 Contre-mesures opérationnelles	48
2.3 Contre-mesures techniques	49
2.3.1 Solutions softwares	49
2.3.2 Solutions hardwares	50
3. Mesures de protection	51
3.1 Protection des appareils Bluetooth	51
3.1.1 Configuration du fabricant	51
3.1.2 Equipements de bureau (fixes)	52
3.1.3 Equipements mobiles	52
3.2 Conseils sur le choix des PINs	53
3.3 Autres Mesures de protection	53
3.3.1 Cage de Faraday	53
3.3.2 Applications cryptographiques	54
3.3.3 Choix de produits commerciaux	54
4. Politique de sécurité et risques résiduels	54
Conclusion	55
Conclusion générale	56
Bibliographie	57
Glossaire	59