



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



Université des Sciences et de la Technologie HOUARI BOUMEDIENE  
Faculté d'Electronique et Informatique  
Département Informatique

Mémoire de Projet de Fin d'Etudes  
Pour l'obtention du Diplôme d'Ingénieur d'Etat en  
Informatique

Option : Systèmes et Réseaux.

Sujet :

*Implémentation de protocole  
de sécurité pour WiFi*

*Proposé par :*

**Mr K. ZERAOULIA**

*Présenté par :*

**Mr BEGGAS AMINE**

**Mr KACIOUSSALAH BELHADJ**

*Soutenu le :* 20/11/2006

**Présenté devant le jury composé de:**

**Mr. KEHMISA HAMID**

Président

**Mme. ZAUCHE DJAOUIDA**

Membre

**Mlle. ZEBBANE BAHIA**

Membre

N° 30/06

Année universitaire 2005/2006

## TABLES DES MATIERES

<b>Introduction générale</b>	<b>6</b>
<b>Chapitre I : Généralité sur les réseaux sans fil 802.11</b>	<b>8</b>
<b>I.1. Introduction</b>	<b>9</b>
<b>I.2. la norme 802.11</b>	<b>9</b>
<b>I.2.1. Architecture de la norme 802.11</b>	<b>10</b>
La notion de cellule	10
<b>I.2.1.1. Mode avec infrastructure</b>	<b>10</b>
<b>I.2.1.2. Mode Ad-hoc</b>	<b>10</b>
<b>I.2.2. Description des couches de la norme 802.11</b>	<b>12</b>
<b>I.2.2.1. Couche physique</b>	<b>13</b>
<b>I.2.2.2. Couche liaison de données</b>	<b>14</b>
<b>I.2.3. Méthodes D'accès au médium</b>	<b>14</b>
<b>I.2.3.1. Espace inter trames IFS (<i>Inter Frame Spacing</i>)</b>	<b>14</b>
<b>I.2.3.2. Algorithme de <i>backoff</i></b>	<b>14</b>
<b>I.2.3.3. La méthode d'accès DCF</b>	<b>15</b>
<b>I.2.3.4. La méthode d'accès PCF</b>	<b>18</b>
<b>I.2.4. Extension de IEEE 802.11</b>	<b>18</b>
<b>I.2.4.1. IEEE 802.11b</b>	<b>18</b>
<b>I.2.4.2. IEEE 802.11e</b>	<b>18</b>
<b>I.2.4.3. IEEE 802.11g</b>	<b>18</b>
<b>I.2.4.4. IEEE802.11i</b>	<b>19</b>
<b>I.3. Conclusion</b>	<b>19</b>
<b>Chapitre II : Sécurité dans les réseaux WiFi</b>	<b>20</b>
<b>II.1. Introduction</b>	<b>21</b>
<b>II.2. Les risques liés aux réseaux sans fil WiFi</b>	<b>22</b>
<b>II.2.1. Le manque de sécurité</b>	<b>22</b>
<b>II.2.2. Les risques en matière de sécurité</b>	<b>22</b>
<b>II.2.2.1. L'interception de données</b>	<b>22</b>
<b>II.2.2.2. L'intrusion réseau (<i>Le détournement de connexion</i>)</b>	<b>22</b>
<b>II.2.2.3. Le brouillage des transmissions</b>	<b>23</b>
<b>II.2.2.4. Les dénis de service</b>	<b>23</b>
<b>II.3. Principales technologies de défense</b>	<b>23</b>
<b>II.3.1. Les réseaux VPN</b>	<b>23</b>
<b>II.3.2. Contrôles des adresses MAC</b>	<b>24</b>
<b>II.3.3. Détection des intrusions</b>	<b>25</b>

<b>II.4. Les services du sécurité.....</b>	<b>25</b>
<b>II.4.1. Le chiffrement.....</b>	<b>25</b>
<b>II.4.2. L'authentification.....</b>	<b>27</b>
<b>II.4.3. L'intégrité.....</b>	<b>27</b>
<b>II.5. Les protocoles de sécurité.....</b>	<b>27</b>
<b>II.5.1. Le protocole WEP.....</b>	<b>27</b>
<b>II.5.2. Le protocole TKIP.....</b>	<b>29</b>
<b>II.5.3. Le protocole AES.....</b>	<b>30</b>
<b>II.5.4. Le protocole 802.1x.....</b>	<b>31</b>
<b>II.5.4.1. Les méthodes d'authentification de 802.1X.....</b>	<b>31</b>
<b>II.5.4.1.1. La méthode EAP .....</b>	<b>31</b>
<b>II.5.4.1.1.1. la méthode EAP-MD5.....</b>	<b>33</b>
<b>II.5.4.1.1.2. La méthode EAP-TLS (<i>Transport Layer Security</i>).....</b>	<b>33</b>
<b>II.5.4.1.1.3. EAP-TTLS et EAP-PEAP.....</b>	<b>33</b>
<b>II.5.4.2. Protocole RADIUS.....</b>	<b>34</b>
<b>II.5.4.3. Les évolutions de 802.1X.....</b>	<b>34</b>
<b>II.5.5. Le protocole WPA, WPA2 (<i>WiFi Protected Access</i>).....</b>	<b>34</b>
<b>II.6. Le choix des protocoles à implémenter.....</b>	<b>36</b>
<b>II.7. Conclusion.....</b>	<b>36</b>
<b>Chapitre III : Etude des protocoles WEP et 802.1x</b>	<b>37</b>
<b>III.1. Introduction.....</b>	<b>38</b>
<b>III.2. Etude du protocole WEP.....</b>	<b>38</b>
<b>III.2.1. Algorithme RC4.....</b>	<b>39</b>
<b>III.2.1.1. Fonctionnement de l'algorithme RC4.....</b>	<b>39</b>
<b>III.2.1.2. Initialisation de RC4.....</b>	<b>39</b>
<b>III.2.1.3. Génération des octets pseudo aléatoire.....</b>	<b>40</b>
<b>III.2.2. Calcule d'ICV.....</b>	<b>40</b>
<b>III.2.2.1. Fonction polynomial.....</b>	<b>41</b>
<b>III.2.3. Le processus de fonctionnement du WEP.....</b>	<b>42</b>
<b>III.3. Etude du protocole 802.1x.....</b>	<b>45</b>
<b>III.3.1. Les protocoles d'encapsulations.....</b>	<b>46</b>
<b>III.3.1.1 Le protocole EAPOL : EAP Over Lan.....</b>	<b>46</b>
<b>III.3.1.2 Le protocole RADIUS ou EAP Over Radius.....</b>	<b>47</b>
<b>III.3.2. Le protocole EAP : (<i>Extensible Authentication Protocol</i>).....</b>	<b>49</b>
<b>III.3.2.1 Description du paquet EAP.....</b>	<b>49</b>
a) Les différents types de paquet EAP.....	49
b) La trame EAP.....	50
<b>III.3.2.2. Méthodes d'authentification EAP.....</b>	<b>51</b>
a) EAP-MD5 ( <i>Message Digest 5</i> ).....	51

b) EAP-TLS ( <i>Transport Level Security</i> ).....	51
c) EAP-TTLS ( <i>Tunnelled TLS</i> ).....	51
d) PEAP ( <i>Protected EAP</i> ).....	51
e) LEAP ( <i>Lightweight EAP</i> ).....	51
III.3.2.3. La méthode EAP-TLS ( <i>Transport Level Security</i> ).....	52
III.3.2.3.1. L'algorithme RSA <i>Ron Rivest, Adi Shamir et Len Adleman</i> ).....	53
III.3.2.3.1. Séquence d'authentification.....	55
III.3.2.3.2. Les problèmes liés au protocole EAP-TLS.....	56
III.4. Conclusion.....	56
<b>Chapitre IV : Conception et implémentation</b>	<b>57</b>
IV.1. Introduction.....	58
IV.2. Cadre du Travail.....	58
IV.2.1. Network Simulator (NS2).....	58
IV.2.2. Conception des Agents du protocole 802.1x.....	59
IV.2.2.1. Étude de l'existant.....	59
IV.2.2.2. Définition des modules.....	60
IV.2.2.2.1. Définition de la structure d'un Agent.....	60
IV.2.2.2.2. Les principes méthodes de la classe Agent.....	60
IV.2.2.2.3. Les Agents du protocole 802.1x.....	61
IV.2.2.3. Modélisation du protocole 802.1x.....	61
IV.2.2.3.1 Architecture des classes.....	61
Les méthodes fondamentales.....	61
IV.2.2.3.2 Diagramme de séquence du protocole 802.1x.....	63
IV.2.3. Implémentation du protocole 802.1x dans NS2.....	68
IV.2.3.1 Structures des données des paquets du protocole 802.1x.....	68
IV.2.3.2. Déclaration des paquets du protocole 802.1x dans NS.....	69
IV.2.3.3. La définition des classes du protocole 802.1x.....	71
IV.2.3.3.1 Description des méthodes fondamentales.....	71
a) La méthode <i>void reponse(int *req)</i> .....	71
b) La méthode <i>virtual int command(int argc, const char*const* argv)</i> .....	71
c) La méthode <i>virtual void recv(Packet*, Handler*)</i> .....	72
d) La méthode <i>virtual void send(Packet*, Handler*)</i> .....	72
e) La méthode <i>int Verifier_certificat(char *cle, char *certificat)</i> ...	72
f) La méthode <i>void cle_session(char *cle_session, char *defi_client, char *defi_serveur, char*premaster_secret)</i> ....	72
IV.2.4. Conception du protocole WEP.....	72
IV.2.4.1. Les cas d'utilisation.....	72
Description des cas d'utilisation.....	74
a) Envoi du message.....	74
b) Réception du message.....	74
IV.2.4.2. Le diagramme d'activité.....	74

IV.2.4.3. Le Cheminement du message dans les différentes couches sous l'environnement NS2.....	76
IV.2.5. Implémentation du protocole WEP.....	77
IV.2.5.1. Description de la classe wep.....	77
IV.2.5.1.1. Structure des données de la classe Wep.....	77
IV.2.5.1.2. Les méthodes de la classe wep.....	78
IV.2.5.2. Modification de la classe <i>MessageAgent</i> .....	78
IV.2.5.3. Modification de la classe <i>mac802_11</i> .....	80
IV.3. Conclusion.....	82
<b>Chapitre V : Simulation et résultats</b>	<b>83</b>
V.1. Introduction.....	84
V.2. Métriques de simulations mesurées.....	84
V.3. Modèle de simulation.....	84
V.3.1. Topologie de simulation.....	84
V.3.2. Configuration du réseau.....	85
V.3.3. Le modèle de trafic.....	86
V.4. Simulation et discussion des résultats.....	86
V.4.1. Simulation du protocole 802.1x.....	86
V.4.2. Simulation du protocole WEP.....	88
V.4.2.1. Etude par rapport à la charge du réseau (nombre de noeuds)..	89
V.4.2.2. Etude par rapport à la taille du message à chiffrer.....	91
V.5. Conclusion.....	94
<b>Conclusion générale et perspective</b>	<b>95</b>
<b>Annexe</b>	<b>97</b>
A.1. Présentation de NS2.....	98
A.2. Installation de NS2.....	98
A.2.1. Etapes de l'installation de NS2.....	98
A.3. Les langages utilisés dans NS2.....	98
A.3.1. Le langage Tcl.....	98
A.3.2. Le langage OTcl .....	99
A.3.3. Interaction entre C++ et Tcl .....	99
A.4. Architecture de NS2.....	99
A.4.1. Une simple application de NS2.....	99
A.4.2. La structure de NS2.....	100
A.4.3. Arborescence des classes dans NS2.....	101
A.5. Extraction et traitement des résultats dans NS2.....	102
<b>Bibliographies</b>	<b>102</b>