

# *MOOC Réseaux Locaux*

## *Le réseau local Wi-Fi*

### **La sécurité dans Wi-Fi**

#### Objectifs

Cette leçon a pour but de présenter les mécanismes de base de sécurisation du réseau local Wi-Fi.

#### Prérequis

Bonne connaissance des réseaux locaux.

#### Connaissances

Principaux enjeux et principales méthodes de sécurisation des réseaux locaux sans fils.

#### Compétences








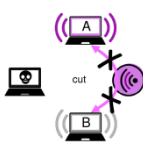

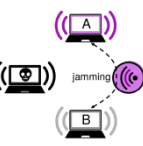


Analyser la sécurité d'un réseau local sans fil.


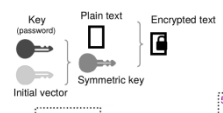

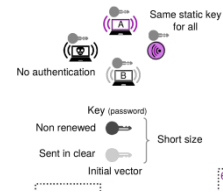

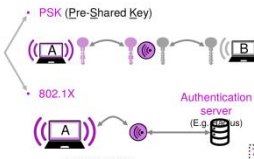
#### Évaluation des connaissances

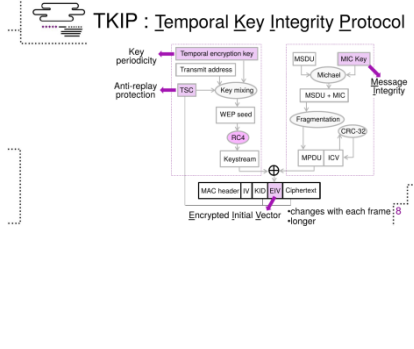
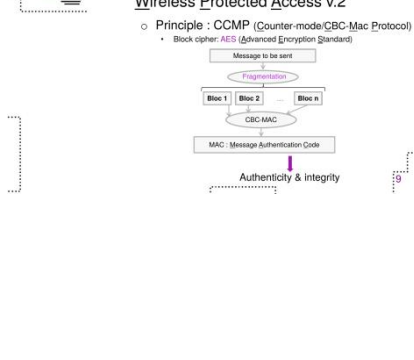
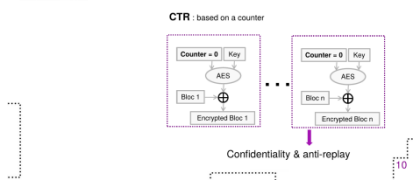
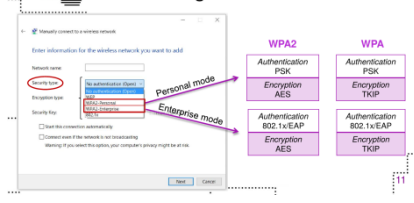
Décrire les principes de la sécurisation de Wi-Fi.


#### Évaluation des compétences

Donner les principaux éléments de sécurité de Wi-Fi.

|   |   |
|---|---|
|  <p><b>Wi-Fi</b><br/>Wi-Fi security</p> <p>Samiha Ayed</p>   | <p>Dans cette vidéo, j'aborde avec vous la sécurité des réseaux Wi-Fi : quelles sont les vulnérabilités associées à ces réseaux, les solutions proposées ainsi que leurs limites ?</p>  |
|  <p><b>Objectives</b></p> <ul style="list-style-type: none"> <li>What <b>vulnerabilities</b>?</li> <li>What <b>solutions</b>?</li> <li>Within what <b>limits</b>?</li> </ul>   | <p>En plus des problèmes de sécurité des réseaux filaires, les réseaux sans fils rajoutent encore des vulnérabilités à cause de leur utilisation des ondes radios qui peuvent être captées par tout le monde. Il suffit juste qu'une machine entre dans la portée d'un point d'accès.</p>   |
|  <p><b>Vulnerabilities of Wi-Fi</b></p>   | <p>Si une machine malveillante entre dans la zone de propagation, elle peut présenter plusieurs risques si le réseau n'est pas sécurisé.</p> <p>Le premier risque est l'interception de données, consistant à écouter passivement les transmissions.</p>  |
|  <p><b>Vulnerabilities of Wi-Fi</b></p>    | <ul style="list-style-type: none"> <li>L'attaquant peut même détourner les connexions pour que toutes les communications passent par lui.</li> </ul>  |
|  <p><b>Vulnerabilities of Wi-Fi</b></p>   | <p>Une attaque de déni de service peut également rendre le réseau inutilisable en envoyant des commandes factices et en coupant les communications entre les différentes machines.</p>  |
|  <p><b>Vulnerabilities of Wi-Fi</b></p>   | <p>Un dernier exemple de ces risques est le brouillage des transmissions consistant à émettre des signaux radio pour produire des interférences et ainsi perturber le fonctionnement du réseau.</p>   |
|  <p><b>Security in Wi-Fi networks</b></p> <p>Authentication<br/>authorised users only</p> <p>Encryption<br/>secure communication</p>  | <p>Pour remédier à ces risques, et assurer la sécurité des réseaux Wi-Fi, plusieurs travaux ont eu lieu. Ces travaux se basent sur</p> <ul style="list-style-type: none"> <li>des mécanismes d'authentification pour limiter les accès au réseau Wi-Fi ;</li> <li>des mécanismes de chiffrement pour crypter les communications.</li> </ul> |

|  |   |
|--|---|
|  | <p>Le résultat de ces travaux a donné naissance à trois mécanismes de sécurité</p> <ul style="list-style-type: none"> <li>le WEP, apparu en 1999, est la première tentative qui a essayé de sécuriser la norme 802.11. Ce protocole n'a pas beaucoup résisté et a été rapidement craqué. Des outils open source existent sur internet pour casser l'algorithme en quelques secondes.</li> <li>Vues ses failles, le WEP a été remplacé par le WPA qui respecte la majorité de la norme IEEE 802.11i et a été prévu comme une solution intermédiaire en attendant que la norme IEEE 802.11i soit terminée.</li> <li>En 2004, il y a eu la sortie officielle de la norme IEEE 802.11i dédiée à la sécurité du Wi-Fi et présentant le WPA2.</li> </ul>  |
| <p> <b>WEP : Wired Equivalent Privacy</b></p> <p>o Principe :</p> <ul style="list-style-type: none"> <li>RC4 encryption <math>\Rightarrow</math> privacy</li> <li>CRC (Cyclic Redundancy Check) <math>\Rightarrow</math> message integrity</li> </ul>  | <p>Le WPA et le WPA2 ont bénéficié de l'apparition de la norme d'authentification 802.1x. Si on regarde un peu plus en détail les spécificités de ces trois mécanismes, on trouve que le WEP se base principalement sur l'algorithme de chiffrement par flot RC4, connu pour sa simplicité, pour crypter les communications et assurer leur confidentialité. Il se base également sur le CRC, qui est le champ de contrôle de redondance cyclique pour assurer l'intégrité des messages.</p> <p>Le WEP utilise une clef de chiffrement (qui est votre mot de passe) à laquelle est concaténé un vecteur d'initialisation formant ainsi la clef symétrique WEP. Une opération logique XOR est, par la suite, appliquée entre la clef WEP générée et le message à chiffrer pour produire le message crypté.</p> |
| <p> <b>WEP : limits</b></p>    | <p>La grande faiblesse du protocole WEP provient de la taille et de la gestion de ces clefs. En fait, la même clef WEP est utilisée par le point d'accès et toutes les stations se connectant à ce point d'accès. De plus, le WEP n'assure aucune authentification : il considère qu'il suffit à un utilisateur qui rejoint le réseau de prouver sa possession de la clef partagée, même s'il l'a obtenue frauduleusement pour qu'il soit authentifié.</p> <p>En outre, lors de la création de la clef WEP, la clef de chiffrement n'est pas renouvelée. Le vecteur d'initialisation est envoyé en clair et leurs tailles respectives sont considérées petites.</p>   |
| <p> <b>WPA / WPA2 authentication methods</b></p>   | <p>Pour remédier à ces failles, WPA et WPA2 ont introduit l'utilisation de deux méthodes d'authentification</p> <ul style="list-style-type: none"> <li>La première est l'authentification par la clef symétrique, qui est un secret partagé entre la station et le point d'accès.</li> <li>La deuxième méthode, c'est l'authentification 802.1x. Dans ce cas, le point d'accès sert de relai entre la station</li> </ul>  |

|   |  |
|---|--|
|  <p><b>TKIP : Temporal Key Integrity Protocol</b></p> <p>Key periodicity<br/>Anti-replay protection<br/>TSC<br/>Transmit address<br/>Key mixing<br/>WEP seed<br/>RC4<br/>Keystream<br/>MIC Key<br/>MSDU<br/>MIC<br/>Message Integrity<br/>Fragmentation<br/>CRC-32<br/>MPDU<br/>IV<br/>MAC header<br/>KID<br/>EN<br/>Encrypted Initial Vector<br/>changes with each frame<br/>longer</p> | <p>et un serveur d'authentification comme RADIUS.</p> <p>Concernant les méthodes de chiffrement, le WPA utilise le protocole TKIP qui se base, comme le WEP, sur l'algorithme RC4. Le WPA élimine les failles du WEP en changeant périodiquement la clef. Il renforce l'intégrité des messages en ajoutant un code d'intégrité de message. Il assure une protection contre les attaques par rejeu en définissant un compteur de séquence sur les paquets. Finalement, il agit sur le vecteur d'initialisation qui change avec chaque trame, a une taille plus importante, et il est envoyé crypté.</p>   |
|  <p><b>WPA2 Wireless Protected Access v.2</b></p> <p>Principe : CCMP (Counter-mode/CBC-Mac Protocol)<br/>Block cipher: AES (Advanced Encryption Standard)</p> <p>Message to be sent<br/>Fragmentation<br/>Bloc 1<br/>Bloc 2<br/>Bloc n<br/>CBC-MAC<br/>MAC: Message Authentication Code<br/>Authenticity &amp; integrity</p>   | <p>Le WPA2 peut également implanter le protocole TKIP pour rester compatible avec les anciens équipements. Il implante essentiellement le protocole CCMP. Avec ce protocole, WPA2 a ramené une grande innovation en se basant sur le chiffrement symétrique par bloc au lieu du chiffrement par flot. Il a donc remplacé le RC4 par l'AES qui est beaucoup plus robuste. Tous les équipements conçus à partir de 2006 supportent le WPA2/AES. L'algorithme CBC-Mac est appliqué sur les différents blocs d'un message pour générer un code d'authenticité qui assure l'intégrité des messages.</p>   |
|  <p><b>WPA2 Wireless Protected Access v.2</b></p> <p>CTR: based on a counter</p> <p>Counter = 0<br/>Key<br/>AES<br/>Bloc 1<br/>Encrypted Bloc 1<br/>Counter = 0<br/>Key<br/>AES<br/>Bloc n<br/>Encrypted Bloc n<br/>Confidentiality &amp; anti-replay</p>  | <p>L'algorithme CTR est utilisé pour crypter ces différents blocs. La protection anti rejeu est assurée par l'utilisation d'un compteur.</p>   |
|  <p><b>Configuration modes</b></p> <p>Personal mode<br/>Enterprise mode<br/>WPA2<br/>Authentication PSK<br/>Encryption AES<br/>WPA2<br/>Authentication 802.1x/EAP<br/>Encryption AES<br/>WPA<br/>Authentication PSK<br/>Encryption TKIP</p>  | <p>La combinaison de ces mécanismes d'authentification et de chiffrement a donné lieu aux deux modes de configuration que vous pouvez rencontrer lors de la configuration d'un réseau Wi-Fi.</p> <p>Je prends ici l'exemple de configuration en utilisant Windows. Comme vous pouvez le voir, vous avez l'option WPA2 personnel et WPA2 entreprise. Il est conseillé de choisir le mode personnel si vous configurez un réseau domestique. Cette configuration se base sur le TKIP et l'authentification par clef partagée. Le mode entreprise, conseillé pour les utilisations professionnelles, assure un chiffrement AES et une authentification 802.1x.</p> <p>Le WPA propose également ces deux modes de configuration.</p> |

|   |  |
|---|--|
|  <p>Conclusion</p> <p>✗ WEP</p> <p>✓ WPA2 with AES = The more secure</p> <p>Recommendations:<br/>Use IPSec<br/>Use VPN</p> <p>12</p> | <p>Pour conclure, vous devez retenir que le</p> <ul style="list-style-type: none"><li>• WEP est à éviter, même s'il est encore proposé dans les configurations des réseaux ;</li><li>• le WPA2 avec l'algorithme AES reste le protocole le plus sûr ;</li><li>• si jamais vous avez des besoins critiques en sécurité, sachez que vous pouvez accompagner le protocole WPA2 par l'utilisation de IPSec ou encore l'utilisation de VPN (réseaux privés virtuels).</li></ul> |
|---|--|