


Tests Intrusifs

- Cours Wi-Fi -

Damien GITTER

Senior Ethical Hacker | Cybersecurity Department

damien.gitter@telindus.lu

 @S_Team_Approved

WIFI

Sécurité des réseaux WiFi



Menaces sur les réseaux WiFi



Vulnérabilités

- LAN accessible de tous (Ondes)
- Chiffrement peu robuste (suivant le protocole)

Menaces associés

- Perte de confidentialité (écoute du support)
- Perte d'intégrité (intrusion)
- Dénis de service

Sécurité de base



SSID (Service Set Identifier)

- Identificateur de réseau (son nom)
- Le point d'accès et le client doivent utiliser le même SSID lors de l'association
- SSID non chiffré et diffusé la plupart du temps
- Possibilité de supprimer la diffusion du SSID (trames de balisage)
 - > Souvent une mauvaise idée car c'est les clients qui le diffuse après

Sécurité de base



Filtrage des adresses MAC (Ethernet)

- Identifier et autoriser certaines adresses à se connecter
- Administration lourde
- Niveau de sécurité faible, substitution @mac possible

Sécurité de base

Réseau OPEN



- Comme son nom l'indique aucune Protection ou chiffrement.
- Librement accessible
- Tout le trafic est en texte claire -> pas besoin de se connecter pour sniffer

Cryptage WEP (Wired Equivalent Privacy)

- Les données qui circulent sur le WLAN sont cryptées (algorithme RC4, clés de 64 ou 128 bits)
- Assure l'authentification et le chiffrement (cryptage)
- Clé secrète partagée par les stations et le(s) point(s) d'accès
- Clef de chiffrement statique - niveau de sécurité très faible (possibilité d'appliquer plusieurs clefs et de tourner)
- Identification possible de la clé par observation de trames vulnérables

Sécurité de base

WPA (Wifi Protected Access)



- Le 802.11i a été ratifié le 24 juin 2004 - Amélioration du WEP (WEP +TKIP)
- Solution de transition compatible avec les matériels existants. WPA est une version allégée de 802.11i créée par Wifi Alliance en 2003
- Basé sur TKIP (Temporary Key Integrity) qui construit des clés temporaires
- Utilise encore l'algorithme RC-4
- Sécurisation des réseaux de type infrastructure
- Clef de chiffrement:
 - WPA-Personal / WPA PSK
 - WPA-Enterprise / WPA-802.1x

Sécurité de base

WPA2 (Wifi Protected Access)



- Version définitive de la 802.11i - Amélioration du WPA
- Obligatoire depuis 2006 les équipements WiFi
- Remplace TKIP (Temporary Key Integrity) par de CCMP (*Counter-Mode/CBC-Mac protocol*) pour plus de sécurité
- CCMP s'appuie sur le chiffrement AES
- Sécurisation des réseaux de type infrastructure et de type Ad-Hoc
- Clef de chiffrement:
 - WPA-Personal / WPA PSK
 - WPA-Enterprise / WPA-802.1x

Sécurité de base



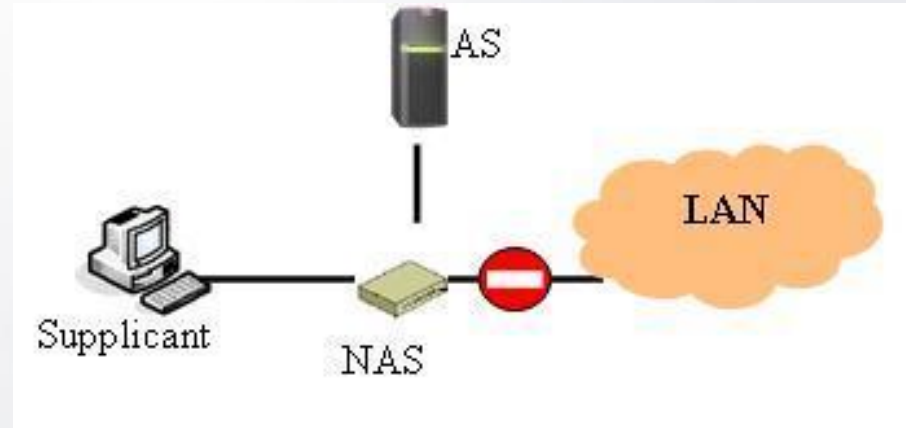
Deux façons de mise en œuvre des protocoles WPA et WPA2

- WPA Entreprise :
Nécessite un serveur d'authentification de type RADIUS (WPA+802.1x+EAP)
Différentes façons d'utiliser EAP -> EAP-TLS, EAP-TTLS et EAP-SIM)
- WPA Personnel :
Utilise une même clé de chiffrement sur l'ensemble des matériels (WPA+PSK pour Pre-Shared Key)

802.1x et WiFi



Accroître la sécurité avec l'authentification 802.1x



NOM	TRADUCTION	FONCTION
Supplicant	Client	Client identifié comme utilisateur ou machine
NAS = Network Access Server = Authenticator	Serveur d'accès ou Contrôleur d'accès	Ouvre l'accès réseau si accord de l'AS
AS = Authentication Server	Serveur d'authentification	Vérifie l'autorisation d'accès

Choisir son protocole d'authentification



Protocole EAP (Extensible Authentication Protocol)

- EAP est un protocole d'authentification opérant au niveau 2 OSI (avant que le client n'obtienne une adresse IP)
- EAP est utilisé dans une architecture 802.1x et fonctionne avec un serveur d'authentification, généralement RADIUS.
- Basées sur EAP, il existe de nombreuses variantes comme une authentification par mot de passe (PEAP, TTLS), par certificat (TLS), etc.

Choisir son protocole d'authentification



Méthodes d'authentification associées à EAP

- LEAP (Lightweight EAP) : Variante allégée d'EAP développée par CISCO pour la sécurité WIFI intégrant la norme 802.1x. Authentification simple par mot de passe via une encapsulation sécurisée
- PEAP signifie «Protected Extensible Authentication Protocol». PEAP est une des implémentations d'EAP les plus utilisées. Elle utilise le protocole CHAP pour authentifier un client grâce au challenge request/response.
- EAP/MD5 : Repose sur le protocole CHAP (RFC 3748)
- EAP/MS-CHAP V2

Choisir son protocole d'authentification



Méthodes d'authentification associées à EAP #2

- EAP/TLS (Transport Layer Security) : Authentification par certificat des équipements clients et du serveur d'authentification (RFC 2716)
- EAP/PEAP (Protected EAP) : Authentification simple par mot de passe via une encapsulation sécurisée
- EAP/TTLS (Tunneled TLS) : Authentification mixte par certificat et mot de passe grâce à la génération d'un tunnel sécurisé
- EAP/FAST (Flexible Authentication via Secure Tunneling) : EAP protégé dans un tunnel symétrique (CISCO). Il corrige le manque de sécurité qu'on attribue souvent à LEAP
- EAP/SIM Authentification via carte SIM pour smartphone
- EAP/AKA (Authentication and Key Agreement) est une méthode EAP pour les clients des réseaux de téléphonie mobile de 3e génération

Choisir son protocole d'authentification



Recommandations CISCO

- CISCO recommande aux administrateurs du protocole LEAP de mettre en œuvre une politique de sécurité afin de choisir des mots de passe robustes et de changer régulièrement de mot de passe.
 - > CISCO conseille éventuellement de changer de méthode d'authentification afin de choisir un mécanisme qui n'est pas vulnérable aux attaques par dictionnaire (EAP-FAST « CISCO », PEAP ou EAP-TLS).
- TLS n'est vulnérable aux attaques par dictionnaire que s'il y a compromission des clés privées

Menaces sur l'authentification 802.1x



Les failles 802.1x

- Attaque de la méthode d'authentification EAP
- Attaque de la session une fois qu'elle est établie
- Attaque MIM (Man In the Middle)
- EAP dump-down -> vidéo démo



Sécurité des réseaux WiFi



Protocoles de chiffrement



Utilisation « personnelle » Sans authentification 802.1x	Utilisation « entreprise » Avec authentification 802.1x
WEP	WEP
WPA-PSK / TKIP	WPA / TKIP
WPA-PSK / CCMP	WPA-PSK / TKIP
WPA2 / WEP	
WPA2-PSK / TKIP	WPA2 / TKIP
WPA2-PSK / WRAP	
WPA2-PSK / CCMP	WPA2 / CCMP

Choisir son matériel



Maîtrise du champ de porté des antennes

- Ajustement de la puissance en fonction des plans du bâtiment
- Choix des type d'antenne en fonction de l'environnement (directionnelle, omnidirectionnelle etc.)

Maîtrise des liens inter-bâtiment

- Antennes directives ou mieux câble ou fibre

Détection d'EAR pirate

- Authentification des éléments actifs réseaux (EAR)

Choisir son matériel



Centralisation des parties intelligentes des EAP

- Point d'accès maître et esclave

Authentication centralisée des utilisateurs

- Authentication par serveur RADIUS

Authentication forte des utilisateurs

- Authentication par certificat (802.1x)

Best practices



A prendre en compte

- Utiliser des méthodes de type tunnels (EAP/TLS, TTLS ou PEAP)
- Sécuriser le trafic entre le client et le contrôleur d'accès
- Utiliser un chiffrement puissant (WPA2...)
- Il est important d'être conscient qu'aucune méthode d'authentification n'est infaillible
- Adopter des mesures de sécurité organisationnelles peuvent augmenter de façon significative la sécurité des réseaux WiFi

Exercices



THANK
you

Exercice Noté