Wlan Protection - IT-Sicherheits-Referat

IEEE-Standard 802.11

Das IEEE (Institute of Electrical and Electronics Engineers) ist eine internationale Organisation von Fachleuten und Experten aus der Elektrotechnik und dem Ingenieurwesen. Es ist die weltweit führende Organisation für die Standardisierung im Bereich der Elektronik und Elektrotechnik. Die Nummer 802 steht für eine Projektgruppe des IEEE. Der Name ist aus dem Startdatum des Projekts abgeleitet, Februar 1980. Der Unterpunkt 802.11 steht für den Standard für Wireless LAN (WLAN) bzw. Drahtlose Netze. IEEE 802.11 definiert die Bitübertragungsschicht des OSI-Schichtenmodells für ein Wireless LAN. Der IEEE 802.11 ist ein Standard für eine technische Lösung, die den Aufbau eines Wireless LAN ermöglicht. Es hat sich im allgemeinen Sprachgebrauch durchgesetzt, ein Wireless LAN auch IEEE 802.11 zu nennen.

Wired Equvalent Privacy (WEP)

WEP ist das mittlerweile veraltete Standard-Verschlüsselungsprotokoll für WLAN. Die Aufgabe war den Zugang zum Netz sowie die Vertraulichkeit und Integrität der Daten sicherzustellen und zu regeln. Wegen verschiedenen Schwachstellen gilt das Verfahren als unsicher worauf wir später noch genauer eingehen werden. WEP benutzt die sogennante Open System Authentication. Dies ist eine Standard Authentifizierung, wo der Accesspoint zwei Zustände haben kann. Erstens es ist keine Verschlüsselung konfiguriert. Somit muss keine praktische Authentifizierung stattfinden und jeder Client kann sich mit dem WLAN verbinden. Es gibt noch eine Verschlüsselung. Hier gibt es wieder zwei verschiedene Arten: Einmal logisch und technisch. Bei der logischen Verschlüsselung ist der WEP-Schlüssel gleichzeitig die Authentifizierung, was wiederum heist, dass jeder Client mit korrektem WEP-Schlüssel Zugang zum Netz hat. Bei der technischen Verschlüsselung findet ein Autausch von Authentifizierungsnachrichten statt und der Client wird authentifiziert. Stimmen WEP-Key auf Accespoint und Client überein, ist die Kommunikation möglich. Stimmen diese nicht überein, ist der Client zwar authentifiziert aber, kann aber keine Daten mit den Netzwerk autauschen. Es gibt noch die Shared Key Authentication. Sie scheint sicherer zu sein als die anderen Authentications. Dies stimmt jedoch nicht. Genauers sagen wir Ihnen im nächsten Abschnitt. Die Authentifizierung erfolgt über die Challenge-Response Authentifizierung mit einem geheimen Schlüssel. Man muss sagen, dass die Challenge-Response Authentifizierung die selben Schwächen wie WEP aufweist. Durch den Einsatz der Shared-Key Authentication wird der geheime Schlüssel offengelegt. Deswegen ist es ratsam auf die Shared-Key Authentication zu verzichten und die Open Authentication zu benutzen. Es gilt Allerdings: Besser ist irgendeine Verschlüsselung als keine!

WEP Attacke (Challenge-Response Authentifizierung)

Die Shared-Key-Authentification gilt als nicht sicher und gibt Informationen preis. Da wir es mit einer Challenge-Response Authentifizierung zu tun haben, spielt sich das ganze folgendermaßen ab: Der Server schickt als erstes dem Client die Challenge1, beziehungsweise eine Zufallszahl. Danach versucht der Client diese Zahl zu verschlüsseln und schickt das WEP-Paket(IV1+ Cipherntext1) zurück an den Server. Danach kann der Angreifer die Informationen erlangen und zwar die IV1+ Cipherntext1 und Challenge1. Der Angreifer kann dann mittels XOR den Keystream1 errechnen. Hat der Angreifer nun den Keystream1 und IV1 kann er sich

selber versuchen zu authentifizieren. Eine Challenge2 wird nun vom Server geschickt. Beantwortet wird sie mit einem WEP-Paket bestehend aus IV1 und Ciphertext2. Ciphertext2 besteht aus Challenge2 und dem Keystream1. Dies wird dann an den Server geschickt und wird nun erfolgreich authentifiziert.

WLAN Protection - WPA

WPA steht für "WiFi Protected Access". Dies ist eine Verschlüsselungsmethode für Drahtlosnetzwerke. WPA ist der 2003 verabschiedete Nachfolgestandard von WEP, der zur Verschlüsselung und Authentifizierung in WLAN-Netzwerken verwendet wurde. WPA sollte die bekannt gewordenen Sicherheitslücken sowie Schwachstellen von WEP beseitigen. Außerdem sollte damit Schaden und Imageverlust der WLAN-Technik verhindert, sowie der entstehende Markt für kabellose Netzwerke nicht gefährdet werden.

Der ehemalige IEEE-Standard 802.11 (WEP) stellte sich als unsicher heraus, und die Verabschiedung des bereits geplanten, neuen Sicherheitsstandards IEEE 802.11i (heute WPA2) verzögerte sich. Da man aber dringend eine Zwischenlösung benötigte, nutze die WiFi Alliance eine Teilmenge des zukünftigen, bereits vorhandenen IEEE-Standards 802.11i in Kombination mit IEEE 802.11 und etablierte dies unter dem Namen „WPA" als Pseudostandard.

WPA enthält zwar die Architektur von WEP, doch durch dynamische Schlüssel die auf TKIP (Temporal Key Integrity Protocol) basieren, wird zusätzlicher Schutz gewährleistet. Aufgrund dessen, dass WPA auf WEP-Hardware basiert, konnte durch ein Software Update auf das neue WPA aktualisiert werden, anstatt komplett neue Geräte mit dem neuen Standard produzieren zu müssen. Es bietet zur Authentifizierung von Clients PSK (Pre-shared key) oder EAP (Extensible Authentification Protocol) über IEEE 802.1X an. EAP wird meist nur in großen Wireless-LAN-Installationen verwendet, da hierfür eine Authentifizierungsinstanz in Form eines Servers benötigt wird. PSK wird in kleineren Netzwerken verwendet, zum Beispiel in einer kleinen Firma oder beim Home Office. Damit der Sitzungsschlüssel generiert werden kann, muss der PSK also den Nutzern des WLAN bekannt sein. Im Gegensatz zu WEP wird zusätzlich zu dem 48 Bit langen Initialisierungsvektor für jedes Datenpaket ein neuer Schlüssel sowie ein MIC (Message Integrity Check / Prüfsumme) verwendet.

WPA Schwachstellen

WPA bietet ähnliche Schwachstellen und somit Angriffsmöglichkeiten wie auch WEP. Da das Temporal Key Integrity Protocol auf RC4 basiert, ist es anfällig für Known-Plaintext-Angriffe (Der Angreifer besitzt neben dem Chiffre/Geheimtext auch den dazu gehörenden Klartext und versucht daraus den Schlüssel zu ermitteln). Diese Schwachstelle bessert WPA2 aus, da dort AES (Advanced Encryption Standard) anstelle von TKIP verwendet wird.

Auch ARP-Spoofing ist möglich. Mit dieser Attacke kann der Angreifer den gesamten Datenverkehr mitschneiden und ggf. manipulieren. Auch kann das Passwort des WLANs mithilfe einer Dictionary Attack erraten werden. Aus diesem Grund sind simple, kurze Passwörter mit wenigen unterschiedlichen Zeichen nicht empfohlen. Es gibt zahlreiche Listen mit den meistbenutzen Passwörtern, mithilfe solch einer Wordlist und der Aufzeichnung eines Four-Way Handshakes zwischen Access Point und WLAN-Client kommt man bereits in das entsprechende Netzwerk. Aus diesem Grund haben z.B. Router ein kompliziertes, zusammenhangloses Passwort.

Ähnlich ist es bei der Bruteforce Attacke. Bei dieser Attacke wird allerdings keine Liste mit möglichen

Passwörtern benötigt, da hier solange alle möglichen Zeichenkombinationen durchprobiert werden, bis die richtige Kombination gefunden wird.

Dictionary Attack

Ein Dictionary Attack wird unter anderem beim Pentesting verwendet, oder aber auch um sich tatsächlich böswillig in ein Netzwerk zu hacken.

Die Voraussetzung, damit der Wörterbuchangriff auch erfolgreich ist, dass der Betreiber des WLANs ein simples Passwort gewählt hat, welches auch in einer Wordlist steht.

Der Ablauf eines WPA WLAN-Hacks per Dictionary Attack ist folgender:

1. „Material" beschaffen
    - Wordlist
    - WLAN-Adapter
    - Zielnetzwerk
    - WLAN identifizieren
2. Four-Way Handshake aufzeichnen
    - Deauthentication Attack
3. Passwort mit Hilfe von Wordlist herausfinden

Schritt 1: „Material" beschaffen

Zuerst einmal wird ein Zielnetzwerk benötigt, dafür kann man eine virtuelle Instanz in Kombination mit dem Router nutzen. Man muss im Wireless-Setup WPA mit einem Passwort einrichten. Außerdem muss sich in diesem WLAN ein aktiver WLAN Client befinden, da man den Handshake zwischen einem Client und dem Access Point aufzeichnen möchte. Außerdem wird eine Wordlist benötigt, mit Hilfe derer findet man im letzten Schritt das Passwort heraus. Dies ist eine Textdatei in der sich in jeder Zeile ein Passwort in Klartext befindet. In einer Worldlist stehen häufig verwendete Passwörter, unter denen sich im Idealfall auch das gesuchte Passwort befindet. Man kann diese selbst schreiben, wobei dies ziemlich aufwendig ist, oder man lädt eine beliebige Datei aus dem Internet herunter. Ohne eine Wordlist funktioniert diese Attacke nicht!

Schritt 2: Four-Way Handshake aufzeichnen

Als nächstes muss man den Handshake zwischen Client und Access Point aufzeichnen. Ein Handshake findet dann statt, wenn sich ein Client mit dem Passwort im WLAN anmelden möchte. Unter Umständen dauert es eine Weile, bis ein Client eine Authentifizierung vornimmt. Für diesen Fall kann man eine Deauthentifizierung vornehmen, damit der Client gezwungen ist, sich neu zu Authentifizieren. Den Handshake nimmt man am besten mehrfach auf, denn wenn der Client versucht sich mit einem falschen Passwort anzumelden, ist der Handshake ebenfalls fehlerhaft. Wenn man einen erfolgreichen Handshake aufgezeichnet hat, kann man zu Schritt 3 übergehen.

Schritt 3: Passwort mit Hilfe einer Wordlist herausfinden

Mit Hilfe des aufgezeichneten Handshakes und einer Wordlist kann man nun das WLAN-Passwort herausfinden. Nun werden der Reihe nach alle Passwörter aus dem Textdokument ausprobiert, bis eines der Wörter mit dem richtigen Passwort übereinstimmt. Dies geschieht automatisch.

WPA2 (Wi-Fi protected access 2)

Dient zum Schutz der übertragenen Daten in einem WLAN und der teilnehmenden Clients, wurde der Sicherheitsstandard WEP oder auch Wired Equvalent Privacy eingeführt. Schon nach relativ kurzer Zeit stellte sich dieser Standard als anfällig für Angriffe heraus. Durch Aufzeichnung und Analyse größerer Datenmengen kann der Netzwerkschlüssel ermittelt werden. Auch die im WEP integrierte Authentifizierung stellt kein nennenswertes Hindernis für Angreifer dar.

Ein weiterführender, sehr umfangreicher, Standard für Sicherheit im WLAN IEEE 802.11i war zu diesem Zeitpunkt zwar in Arbeit, aber eine Verabschiedung war nicht in Sicht. Daher wurde ein Zwischenstandard auf Basis mehr oder weniger verabschiedeter Teile geschaffen:WPA. Dieser konnte durch Funktionen wie dynamische Schlüssel, vernünftige Authentifizierung und Unterstützung von Radius-Authentifizierung den Funknetzen ihre Sicherheit zurückgeben. Mit fortschreitender Entwicklung des Standards IEEE 802.11i, der auf dem Verschlüsselungsalgorithmus AES basiert, wurden auch Anstrengungen unternommen, AES in WPA zu integrieren. Daraus entstand der Standard* *WPA2. Die Herstellervereinigung Wi-Fi-Alliance begann zum 1. September 2004 als erste mit der Zertifizierung von WLAN-Geräten mit WPA2.

Für WPA und WPA2 waren lange Zeit nur Passwort-Angriffe bekannt. Aus diesem Grund ist es dringend zu empfehlen, ein ausreichend langes Passwort (mindestens 20 Zeichen lang mit Groß- und Kleinbuchstaben sowie Sonderzeichen und Zahlen) zu verwenden, das möglichst auch nicht vollständig aus sinnvollen Wörtern besteht. (Wörterbuchangriff) Einige Hersteller ermöglichen, durch proprietäre Verfahren den Passwortschlüssel mit einem USB-Stick auf die anzuschließenden Clients zu übertragen. Dieser braucht nach der einmaligen Installation nicht mehr geändert zu werden. Ein, mit ausreichend langem, Passwort geschützter Wireless-Router mit WPA2-Verschlüsselung und CCMP sowie deaktiviertem WPS gilt aus heutiger Sicht im Unterschied zu WEP als relativ sicher.

FourWayHandshake

Im ersten Schritt ist der erste Input der PMK (Primary Master Key). Beide haben diesen und es wird sicher gegangen das der PMK noch nie über das Wireless-Medium übertragen wurde. Der zweite Input sind die Anonce (die Authentifikationsnummern). Der dritte Input sind die Snonce das ist die Clientnummer. Der vierte und fünfte Input sind die MAC-Adressen der teilnehmenden Stationen(Client AA Router SA). Das sind die Schritte um die Encrypthungskeys zu erstellen. Darauf hin antwortet der Client mit dem Snonce , da schon alle vollständigen Inputs vorhanden sind und somit kann es sein, dass die Snonce mit einem Message-Integrity-Code gesichert werden. Jetzt kann der Router die Snonce bestätigen, da Sie mit der MIC gesichert sind und somit sicher gegangen wird, dass sie nicht sabotiert wurden. Jetzt bestätigt der Router den PTK (Pariwaise-Transient-Key). Jetzt sendet der Router den GTK (Group-Temporal-Key) zu den Client. Ebenfalls ist dieser durch MIC geschützt. Jetzt installiert der Client den GTK und sendet dann nochmal eine Nachricht mit der Bestätigung, dass er den bekommen hat und, dass er beide jetzt installiert hat, sowie startbereit für den Encrypted-Data Austausch ist.

Man the Harpoons

Der belgische Forscher Mathy Vanhoef hat im Jahre 2017 den KRACK wieder ins Leben gerufen. Laut seiner Aussage hat er ihn in der Sicherheitsanfälligkeit verbessert. Der sogenannte „Key-Reinstallation Attack“, oder

auch KRACK genannt, funktioniert potentiell gegen alle modernen geschützten Wi-Fi Verbindungen/Netzwerke (Stand 2017). Man kann mit dem KRACK die Daten manipulieren sowie abhören/abfragen. Das ist aber auf die Konfiguration des angegriffenen Zieles abhängig. Die einzige Limitation des Angreifers ist, dass er in Reichweite seines Zieles sein muss. Es betrifft aber nicht nur WPA2 Personal sondern auch Enterprise, egal welche Verschlüsselungs-Chiffren das Netzwerk benutzt. Die anfälligsten Clients sind Linux und Android 6.0. Herr Vanhoef sagt selber, dass nicht die individuellen Produkte oder Implementationen unsicher sind, sondern der Wi-Fi Standard selbst. Zum verhindern der Attacken muss der User die betroffenen Produkte so schnell wie möglich updaten, falls das Security-Update vorhanden ist. Der KRACK zielt auf den „Four-Way“ Handshake des WPA2 Protokolls ab und vertraut darauf, dass das Ziel-Gerät einen bereits vorhandenen Key benutzt. Diese geschickte Vorgehensweise wird durch Manipulieren und Wiedergeben von kryptografischen Handshake-Nachrichten erreicht. Es basiert darauf das man Datenpakete klaut, die vom aktuell benutzten Key sind, die der Client benutzt.

Wie die Reinstallation von PTK & GTK funktioniert

Die Installation des PTK geschieht, indem man die vierte Nachricht des FourWay Handshakes abfängt und dann der Client denkt, dass damit der Fourway Handshake beendet ist. Damit wird die Installation des Pariwaise-Transient-Key eingeleitet(PTK). Als Ergebnis wird ein Frame gesendet der nun als Transmitter gilt und damit kann man dann den Sicherheitslayer Encrypthen.

Fourway Handshake KRACK

Der erste Schritt ist, dass man als „Hacker“ einen Multi-Channel (MitM) (man in the middle Position) erlangen muss. Von hier aus kann man NICHT die decryption der Frames starten. Hier kann man nur Nachrichten zwischen AP und Client blocken und verzögern. Um in den MitM zu kommen, zwingt man das Opfer sich in einen so genannten rogue channel zu verbinden. Dies erfolgt durch ein Tool. Einmal in dieser Position leitet man die ersten drei Nachrichten des FourWay Handshakes unverändert weiter, nicht jedoch die vierte Nachricht. Jedoch denkt der Client, dass der Handshake komplett ist was wiederum heißt, dass er den Negotiated-Session Key installiert hat. Als Ergebnis kommt zustande, dass alle Daten des Clients, die gesendet werden, unverschlüsselt sind, aber, weil der Router die vierte Message nicht bekommen hat, ist der Handshake nicht abgeschlossen und somit sendet er eine neue Message 3 mit erhöhtem Counter. Wenn der Client die Nachricht bekommt sendet er eine neue Message 4. Dazu kommt, dass er den PTK reinstalliert und somit die Variablen reseted und auch den Counter reseted. Das löst aus, dass der Client die Variablen wieder benutzt und als Datenframe sendet. Dazu kommt, dass man Frames selber senden kann, da der replay counter reseted wurde.