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.