Man the Harpoons

mth

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.