Der WPA2 KRACK

In den vergangenen Tagen hat eine Schwachstelle im WPA2 Protokoll für Aufsehen gesorgt. Einer Gruppe belgischer Forscher der Universität Löwen ist es gelungen, die unüberwindbare Verschlüsselung des WPA2-Protokolls zu umgehen. Durch diesen Trick ist es möglich, den verschlüsselten Datenverkehr mitzulesen und zu verändern.

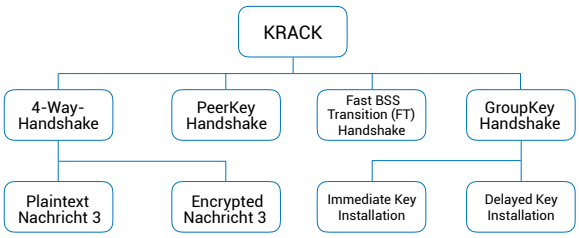
Zusammenfasung

Belgische Forscher haben einen Angriff auf das *Wi-Fi Protecetd Acess 2* (WPA2) Protokoll vorgestellt, welches das Mitlesen und Verändern des Datenverkehrs ermöglicht. Üblicherweise wird dieses Protokoll zum Schutz von *Wireless Local Area Networks* (WLAN) eingesetzt. Aktuell kann davon ausgegangen werden, dass ein Großteil aller WLAN-fähigen Geräte von dieser Sicherheitslücke betroffen ist.
Aufgrund einer Vielzahl von kontroversen Artikeln, die derzeit publiziert werden, hat sich die mVISE AG dem Thema angenommen, um den Angriff im Detail zu analysieren und dessen Auswirkungen aufzuzeigen.
Der Angriff wird als *Key Reinstallation Attack* (KRACK) bezeichnet und zielt auf Schwächen bzw. Ungenauigkeiten in der Implementierung von WPA2 ab. Im Folgenden wird aufgezeigt, wo die Schwächen der Implementierung liegen, welche Ungenauigkeiten den Angriff ermöglichen und welche Maßnahmen eine Organisation ergreifen muss, um sich vor den Auswirkungen dieser Schwachstelle zu schützen.

Problem

KRACK vereint vier verschiedene Ansätze mit der Gemeinsamkeit, die dritte Nachricht[1] des 4-Way-Handshakes zurückzusetzen bzw. diese wiederzuverwenden. Durch diesen Vorgang hat ein Angreifer die Möglichkeit, Rückschlüsse auf den verschlüsselten Inhalt der übertragenen Daten zu ziehen. Doch so einfach, wie sich dies in der Theorie anhört, ist es nicht.
Um einen KRACK Angriff durchführen zu können, müssen die WLAN-fähigen Geräte dem Standard IEEE 802.11 entsprechen und von der Sicherheitslücke betroffen sein.

Eine weitere Voraussetzung für den Angriff ist die Positionierung des Angreifers als „Man-in-the-Middle“. Dies setzt voraus, dass er sich in unmittelbarer Nähe des WLAN aufhalten muss. Problemfelder von KRACK:

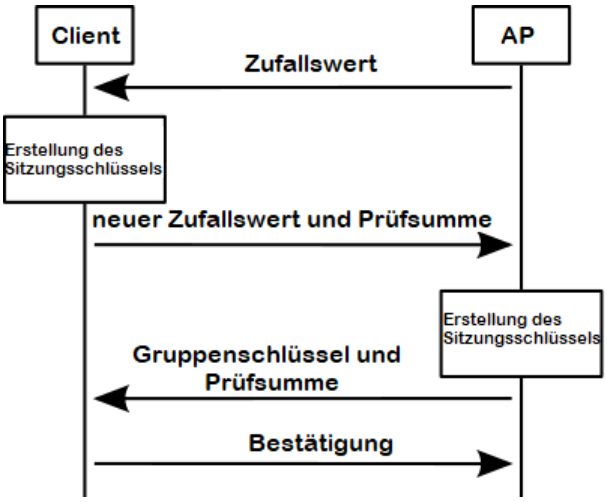


> ***“NO! Keep using WPA2”***
>
> ***“Finally, although an unpatched client can still connect to a patched AP, and vice versa, both the client and AP must be patched to defend against all attacks!“ // Mathy Vanhoef***

[1] Bei einem 4-Way-Handshake werden vier verschiedene Nachrichten für die Authentifizierung zwischen Client und Access Point ausgetauscht. KRACK zielt dabei auf die dritte Nachricht ab.

PROBLEMFELD 1: 4-WAY-HANDSHAKE

Das Ziel des *4-Way-Handshakes* ist die Generierung eines gemeinsamen Sitzungs- und Gruppenschlüssels durch Client und Access Point. Dies passiert mittels vier semantisch vordefinierten Nachrichten. Zu Beginn sendet der Access Point einen einmaligen Zufallswert an den Client. Dieser kann dadurch einen Sitzungsschlüssel generieren.



4-Way Handshake

In einem weiteren Schritt kommuniziert der Client mit dem Access Point. Dieser sendet diesem einen neuen, einmaligen Zufallswert inklusive einer Prüfsumme. Dadurch kann dieser ebenfalls einen Sitzungsschlüssel erstellen.

Im Anschluss sendet der Access Point einen Gruppenschlüssel mit der dazugehörigen Prüfsumme an den Client. Die Prüfsumme wird dabei mit dem vereinbarten Sitzungsschlüssel gesichert.

Abschließend bestätigt der Client den korrekten Empfang des Gruppenschlüssels an den Access Point.
Von besonderer Bedeutung ist, dass die dritte Nachricht des *4-Way-Handshakes* so definiert ist, dass diese immer nur einen Gruppenschlüssel mit dazugehöriger Prüfsumme beinhaltet. Dennoch kann diese mehrmals hintereinander gesendet werden. Grundsätzlich werden bei diesem Angriff zwei Angriffsszenarien unterschieden. Im ersten Szenario wird die dritte Nachricht unverschlüsselt an den Client gesendet, der diese wiederum akzeptiert. Dies bezeichnet einen Angriff auf den *Plaintext* (dt. Klartext). Im zweiten Szenario wird die dritte Nachricht verschlüsselt versendet.

ANGRIFF AUF DEN PLAINTEXT

Der Angreifer leitet die ersten beiden Nachrichten weiter. Anschließend fängt er die dritte Nachricht ab und blockiert sie. Dadurch wird vom Client keine Empfangsbestätigung (Nachricht 4) an den Access Point versandt. Er wartet, bis der Access Point nach einem Timeout erneut die dritte Nachricht verschickt. Im weiteren Verlauf werden beide Nachrichten an das Opfer weitergeleitet. Falls das Opfer die unverschlüsselte dritte Nachricht akzeptiert, werden beide Nachrichten verarbeitet. Dies führt dazu, dass ein Reset durchgeführt wird, Zufallszahlen und Schlüssel werden „Re-installiert“ (Key Reinstallation) und können somit erneut verwendet werden.

ANGRIFF AUF DIE VERSCHLÜSSELTE NACHRICHT

Bei dieser Form des Angriffs wird die dritte Nachricht ausschließlich dann vom Client akzeptiert, wenn diese verschlüsselt ist. In einem ersten Schritt lässt der Angreifer das Opfer einen vollständigen *4-Way-Handshake* vollziehen. Anschließend wartet der Angreifer auf einen erneuten Handshake, um die dritte Nachricht vorzuenthalten. Der Access Point sendet nach einem Time-out die dritte Nachricht noch einmal an den Client. Diesmal werden beide Nachrichten an den Client weitergeleitet. Der Client verschickt für jede der beiden erhaltenen Nachrichten eine Empfangsbestätigung. Der Client bemerkt auch hier seinen Fehler und führt einen Reset durch. Laut Aussage der belgischen Forscher hat der Zufallswert dadurch den Wert eins. Aufgrund dieser Aussage ist der Zufallswert nicht mehr von Bedeutung. Die Längen der Nachrichten sind vordefiniert, dadurch lassen sich Rückschlüsse auf die Art der Nachrichten ziehen. Dies ist auch bei der dritten Nachricht möglich. Der Reset und das daraus entstehende Wiederverwenden der Zufallszahl haben zur Folge, dass anschließend der Datenverkehr mittels bekannter Techniken entschlüsselt werden kann.

ANDROID NULLER-SCHLÜSSEL

Unter Android 6.0, Android Waer 2.0 und höher, findet eine *all-zero* Verschlüsselung statt. Dies bedeutet, dass der Schlüssel nach seiner Nutzung im Speicher durch eine Folge von Nullen überschrieben wird. Nach einer „Key Re-Installierung“ kommt somit ein Schlüssel nur aus „0en“ bestehend zum Einsatz. Diese Verschlüsselung ist damit leicht zu überwinden. Google arbeitet daran, Patches zur Behebung dieser Schwachstelle, zu veröffentlichen.

PROBLEMFELD 2: PEER KEY HANDSHAKE

Der *Peer Key Handshake* ist mit dem *4-Way-Handshake* verwandt. Durch seine ähnliche Form und dem ähnlichen Verhalten kann der Angriff des *4-Way Handshakes* in abgewandelter Form auf diesen angewendet werden. Da der *Peer Key Handshake* nicht so weit verbreitet ist, lässt sich daraus eine geringere Angriffswahrscheinlichkeit ableiten.

PROBLEMFELD 3: FAST BSS TRANSITION HANDSHAKE

Generell gilt, dass der *Fast BSS Transition Handshake*, so wie er im Standard von 802.11r definiert ist, nicht vom KRACK-Angriff betroffen ist. Abweichende Implementierungen von diesem Standard führen jedoch dazu, dass dieser Angriff durchgeführt werden kann. Gruppen- und Sitzungsschlüssel werden demnach neu initialisiert, obwohl dies nicht notwendig ist. Ein *Fast BSS Transition Handshake* wird durchgeführt, wenn ein Client von einem zum anderen Access Point weitergeleitet wird. Nicht jeder Hersteller von Access Points unterstützt diese Technik.

PROBLEMFELD 4: GROUP KEY HANDSHAKE

Der *Group Key Handshake* dient dazu, ausschließlich zugelassenen Clients einen Zugriff auf den Gruppenschlüssel zu ermöglichen. Aus diesem Grund wird die Netzwerkverbindung mit dem Gruppenschlüssel periodisch erneuert. Auch hier gelten einige Einschränkungen für einen Angreifer. Beispielsweise muss dieser im Besitz der ersten Nachricht des Handshakes sein. Die Nachricht muss vom Access Point bereits genutzt werden und der Client muss diese noch akzeptieren. Falls dies dem Angreifer gelingt, so wird ein Zähl-Wert im Ablauf zurückgesetzt und es können Nachrichten erneut versendet werden. Es wird zwischen einer *„Immediate Key Installation“* und einer *„Delayed Key Installation Attack“* unterschieden.

Sicherheitsziele

Grundsätzlich ist die Aussage falsch, dass die Sicherheit des *„4-Way-Handshakes“* nicht mehr gewährleistet werden kann. Die Angriffe richten sich nicht gegen die im Protokoll designten Sicherheitsziele. Die ausgetauschten Schlüssel des *4-Way-Handshakes* werden dem Angreifer nicht offenbart. Eine Änderung der Schlüssel kann somit einen Angriff nicht verhindern. Des Weiteren muss der Angreifer für den Angriff die Nachrichten weiterleiten, damit der Handshake beendet wird. Auch dies verletzt nicht die designten Sicherheitsziele des Protokolls. Vergleichbar ist der Angriff mit einer falschen Verwendung von Gegenständen. Ein Personen-Aufzug ist nur für den Transport von Personen zugelassen und eignet sich nicht zur Verteilung von geheimen Dokumenten, wie beispielsweise eine Röhrenpost.

Auswirkungen

Microsoft hatte bereits vor Veröffentlichung der WPA2-Schwachstelle seine aktuellen Betriebssysteme mit einem Patch versorgt. Den Angaben zufolge waren die folgenden Betriebssysteme betroffen:

- Windows 7
- Windows 8.1
- Windows 10
- Windows Server 2008
- Windows Server 2012
- Windows Server 2016

Anwender dieser Betriebssysteme, die die automatischen Updates aktiviert haben, seien demzufolge nicht betroffen. Mittels der KB-Nummer (Knowledge Base), können nähere Informationen in der Microsoft-Support-Datenbank eingesehen werden. Darunter auch Security-Updates. KB-Nummern:

- KB4042895 - Windows 10
- KB4041693 & KB4041687 - Windows 8.1
- KB4041681 & KB4041678 - Windows 7

Auch die Entwickler des Betriebssystems Ubuntu haben bereits am 16.10.2017 für verschiedene Sicherheitslü-

cken im wpa_supplicant ein Sicherheitspatch veröffentlicht. Genauere Informationen lassen sich unter dem Begriff *„Ubuntu Security Notice USN-3455-1“* finden.

Apple hat die Sicherheitslücke für seine Betriebssysteme bereits in den Beta-Versionen 11.1 seiner Betriebssysteme gepatcht. Die Updates sollen zeitnah verteilt werden.

Für Android wurde ein Sicherheitspatch am 06.11.2017 verteilt. Sicherheitsupdates für Geräte anderer Hersteller, die unter dem Betriebssystem Android laufen, können sich verzögern. Lineage OS, der Nachfolger des beliebten CyanogenMod, hat bereits sein Custom Android Betriebssystem gepatcht.

Laut AVM sind die eigenen WLAN-Router (Fritzbox) nicht von KRACK betroffen. Nach weiteren Untersuchungen des Problems bietet AVM nun aktuelle Updates für WLAN-Repeater und WLAN/Powerline-Produkte an. Für das Betriebssystem OpenBSD wurde bereits im August ein Sicherheitspatch veröffentlicht. Cisco hat seine Geräte getestet und stellt, für die meisten von ihnen, Sicherheitsupdates zur Verfügung. Dennoch wurden nicht alle Cisco Access Points durch dieses Update vollständig geschützt. Diese Geräte erhielten am 22. und 23. Oktober 2017 ein zusätzliches Update. Genauere Informationen können unter „cisco-sa-20171016-wpa“ eingesehen werden. Einige Intel Produkte sind ebenfalls betroffen. Für aktuelle Geräte sind Updates verfügbar.

Angaben von Apple:
Die aktuellen Betaversionen von iOS 11.1,
MacOS 10.13.1, watchOS 4.1 und tvOS 11.1 haben den Angriff bereits herausgepatcht.
Die Beta wurde am 01.11.2017 mit dem Update iOS 11.1 ausgerollt.
Ob ältere Geräte ein Sicherheitsupdate erhalten, ist unklar.

Lösung

Für ein Unternehmen oder eine Privatperson ist es schwer, vorab zu entscheiden, ob eine eingesetzte Technologie ausreichend gegen bislang unbekannte Angriffe geschützt ist. Wird allerdings WLAN genutzt, so muss klar sein, dass sich eine Organisation oder Privatperson das Übertragungsmedium Luft mit dem Angreifer teilt. Dies sollte beim mobilen Arbeiten beachtet werden, um entsprechende Gegenmaßnahmen ergreifen zu können.
Für Mobile Devices wie Smartphones und Tablets, gibt es bereits Lösungen, um Angriffen wie KRACK die Schlagkraft zu nehmen. Dabei wird sich nicht auf die Verschlüsselung des Transportweges (hier WLAN) verlassen, sondern eine Ende-zu-Ende-Verschlüsselung sichergestellt. Gleichzeitig ist es möglich, Angriffe auf diese Weise zu erkennen.

Bei der Entwicklung von mobilen Anwendungen ist darauf zu achten, dass diese mit ausreichendem Schutz versehen sind. Neben dem defensiven Programmieren sollte darauf geachtet werden, dass die Nutzung der Transportlayer ausreichend Schutz bietet. Das Einbauen von TLS – oder anderer guter Ende-zu-Ende-Verschlüsselungen – ist dafür unverzichtbar.
Generell gilt jedoch, dass eine Übertragung von Daten mittels sicherer Ende-zu-Ende-Verschlüsselung, über alle Übertragungsstationen hinweg, gewährleistet werden kann. Weiterhin sollte darauf geachtet werden, dass nach Möglichkeit immer eine verschlüsselte Verbindung gewählt wird. Beim Benutzen von Webseiten ist HTTPS der Indikator für eine geschützte Verbindung. HTTPS nutzt TLS und verschlüsselt damit die übertragenen Daten zusätzlich.

Profitieren Sie von qualifizierten Lösungen

Die mVISE AG berät, unterstützt und setzt um! Bei den Herausforderungen des Schutzes Ihres Unternehmens, unterstützen wir Sie in vollem Umfang.

Unsere IT-Security Experten haben seit Jahren umfassende Erfahrungen aus vielen verschiedenen IT-Umfeldern sammeln können. Mittels umfangreichen und auf Ihre Bedürfnisse zugeschnittenen Workshops helfen wir Ihnen, bei dem Aufbau einer geeigneten Sicherheitskultur. Dabei lernen Ihre Mitarbeiter unter anderem Handlungsanweisungen kennen, die sie beim Eintreten von IT-Sicherheitsvorfällen schützen können. Gleichzeitig haben wir die Möglichkeit, durch umfangreiche Penetrationstests Ihre mobilen Anwendungen auf Sicherheitslücken zu untersuchen.

ÜBER DEN AUTOR

Bernhard Borsch ist seit 2014 für die mVISE AG tätig. Als Manager für das IT-Security Consulting beraten sein Team und er Kunden zum Thema IT-Security im Zuge der Herausforderungen der Digitalisierung. Zu seinen persönlichen Themenfeldern gehört neben den klassischen Themen, wie Enterprise- & Cloud-Security, PKI und Kryptographie, auch Zukunftsthemen der IT Security, wie Blockchain und Deception Technology. Professionelle und fachkompetente Beratung sind sein Schlüssel zum Erfolg.

mVISE

Wir unterstützen mittelständische und große Unternehmen aller Branchen dabei, von der digitalen Revolution zu profitieren. Die besondere Kombination aus firmeneigenen Software-Lösungen mit ausgewählten Experten-Teams in den relevanten und aktuellen IT-Themengebieten schafft nachhaltige Wettbewerbsvorteile für unsere Kunden.

Unsere Experten bestimmen, gestalten, kreieren und steuern IT-Infrastrukturen und Software-Lösungen für Datenintegrations- und Enterprise-Data-Management-Projekte, mit dem Ziel, die aktuellen Geschäftsmodelle unserer Kunden zukunftssicher zu machen und gleichzeitig neue Geschäftsmodelle zu identifizieren.

Sprechen Sie uns an – gerne stellen wir Ihnen unser Angebot
in einem persönlichen Gespräch näher vor.
service@mvise.de | www.mvise.de

mVISE AG
Wahler Straße 2
40472 Düsseldorf
Fon: +49 211 78 17 80 – 0