Erledigt Schwere Sicherheitslücke in WPA2

Beitrag von „aufdenschlips“ vom 16. Oktober 2017, 10:34

Quelle: arstechnica.com

Severe flaw in WPA2 protocol leaves Wi-Fi traffic open to eavesdropping

KRACK attack allows other nasties, including connection hijacking and malicious injection.

https://arstechnica.com/inform…ic-open-to-eavesdropping/

Beitrag von „Doctor Plagiat“ vom 16. Oktober 2017, 11:54

Dazu sollte man erwähnen, dass sich der Angreifer in Funkreichweite zum Client und zum Access Point befinden muss.
Des Weiteren haben die Netzwerkausrüster Aruba und Ubiquiti schon fertige Sicherheitspatches. So steht das bei heise.

Beitrag von „aufdenschlips“ vom 16. Oktober 2017, 14:56

Man sollte sich generell in Funkreichweite eines Wlans befinden um WPA2 benutzen zu können.

Zwei Hersteller von wie vielen Consumer-Wlan-Router/AP-Herstellern?

Genau 0.

Beitrag von „revunix“ vom 16. Oktober 2017, 15:06

Hab ich mir auch gerade angesehen... ganz schön heftig, deswegen nur mit VPN in öffentlichen WiFi's!

https://www.youtube.com/watch?v=Oh4WURZoR98

Beitrag von „Schorse“ vom 16. Oktober 2017, 18:23

Moin,
deshalb WLAN-Zugang auf die bekannten WLAN-Geräte beschränken!

Beitrag von „Mocca55“ vom 16. Oktober 2017, 18:30

Stichwort MAC-Filter.
Läuft bei mir. 👍

Beitrag von „Moorviper“ vom 16. Oktober 2017, 18:32

@Un!x

wpa2 sicherheitslücke und öffentliche Wlans

Vielleicht findest du den Fehler in deiner Logik

Beitrag von „kelevra“ vom 16. Oktober 2017, 18:42

> Zitat von Mocca55
>
> Stichwort MAC-Filter.
> Läuft bei mir.

MAC Filter sind nutzlos. Kann man sich genau so sparen, wie SSID Broadcast abzuschalten.

Beitrag von „cobanramo“ vom 16. Oktober 2017, 18:44

ach @Mocca55, denkst du wirklich jemand der sowas auf die Beine stellen kann nicht einen MAC Adresse ändern könnte?
MAC Filter ist nur ein kosmetischer Schutz

Beitrag von „Mocca55“ vom 16. Oktober 2017, 19:21

@kelevra
@cobanramo
Ich weiß das man einen MAC-Filter auch umgehen kann aber das ist immernoch besser wie

ohne. Und Sicherheit fängt ja schon beim WPA2 Passwort an, das schonmal nicht nur ein Name sein sollte. Dann wäre noch der MAC-Filter zu überbrücken und dann könnte noch ein IP Konflikt enstehen da ich meine IP Adressen fest nach MAC Adressen vergebe. Und dann kommt noch das Router Passwort und zu guter letzt ist noch jedes Gerät im WLAN mit einem Passwort gesichert. Also viel Arbeit für den der rein will. Und zu holen gibts bei mir auch nicht wirklich was.

Ich denke wenn jemand ins WLAN will kommt er rein ist nur ein Frage der Zeit.

Beitrag von „Patricksworld“ vom 16. Oktober 2017, 19:28

Die Frage wäre. Ist die Lücke nur im WPA2? Denn dann kann man ja auch vorrübergehend auf WPA wechseln.

Beitrag von „revunix“ vom 16. Oktober 2017, 20:41

> Zitat von Moorviper
>
> Vielleicht findest du den Fehler in deiner Logik

Gut vielleicht habe ich mich da auch etwas blöd ausgedrückt Aber es gibt ja auch von McDoof und co. WiFi mit Passwort und trotzdem ist das öffentlich.

Beitrag von „kelevra“ vom 16. Oktober 2017, 20:43

@Mocca55
Damit hast du dein Möglichstes getan. Üblicherweise würde man sich ein einfacheres Netz suchen. Außer man hat es explizit auf deines abgesehen, aber dann hast du ganz andere Probleme.

Beitrag von „jboeren“ vom 16. Oktober 2017, 21:27

Laut Zeit klingt es schlimmer als es ist:

http://www.zeit.de/digital/dat…a2-krack-verschluesselung

Beitrag von „hackiFan“ vom 16. Oktober 2017, 21:34

Immer diese Diskussionen
Es ist Fakt das immer irgendwo Sicherheitslücken gibt und geben wird
WPA2 konnte man schon lange mit Hilfe von GPU “schneller“ cracken
Dafür gibt's auch diverse Linux distros
Also hin oder her
Spielt das absolut keine Rolle wo was gefunden wird
Oder habt ihr im Netzwerk geheime Daten die Millionen wert sind dass jemand sich dafür interessieren würde

Beitrag von „jboeren“ vom 16. Oktober 2017, 21:38

Die Geheimdienst braucht kein wlan zum ausspionieren!

Beitrag von „Nio82“ vom 16. Oktober 2017, 21:39

Ganz ehrlich, zusagen MAC Filter oder andere Sicherheits Mechanismen sind Quatsch & sinnlos zu nutzen ist genau so blödsinnig wie zu sagen: "*Ich baue in meinen Laden keine Tür ein, weil Einbrecher mit genug Wille zum Erfolg kommen trotzdem rein!*"

Merkt ihr den Blödsinn?

Nichts ist unknackbar, doch kann man den Angreifern immerhin soviel Barrieren in den Weg stellen wie möglich. Was dann nicht so versierte Hobbyhacker abschreckt. Und wenn ich das Maximale an Sicherung umsetze, wo wird der Hacker eher versuchen rein zu kommen? Bei mir wo es schwerer ist? Oder bei meinem Nachbarn der sich keinen Plan über WLAN Absicherung macht & zB WPA & WPA2 gleichzeitig aktive hat oder sogar nur WEP nutzt?

Beitrag von „kelevra“ vom 16. Oktober 2017, 22:31

> Zitat von Nio82
>
> Ganz ehrlich, zusagen MAC Filter oder andere Sicherheits Mechanismen sind Quatsch & sinnlos zu nutzen ist genau so blödsinnig wie zu sagen: "*Ich baue in meinen Laden keine Tür ein, weil Einbrecher mit genug Wille zum Erfolg kommen trotzdem rein!*"
> Merkt ihr den Blödsinn?

Blödsinn ist es zu glauben, dass ein MAC Filter schützt.

Selbstverständlich soll man sein Netz verschlüsseln, und zwar möglichst mit langen Passwörtern, die nicht mit Wörterbuchattacken angreifbar sind. Ebenso sollte man WPS deaktivieren, da dies in Version 1.0 (welche noch auf vielen Routern aktiv ist) ein erhebliches Sicherheitsrisiko darstellt.

Vielleicht sollte man sich erst mit der Materie beschäftigen, bevor man "Tipps" gibt.

> Zitat von hackiFan
>
> Oder habt ihr im Netzwerk geheime Daten die Millionen wert sind dass jemand sich dafür interessieren würde 😉

Die übliche "ich hab' nichts zu verbergen" Denke...

Beitrag von „Nio82“ vom 16. Oktober 2017, 22:54

@hackiFan

> Zitat von hackiFan
>
> Oder habt ihr im Netzwerk geheime Daten die Millionen wert sind dass jemand sich dafür interessieren würde

Klar doch, ich habe das Rezept für CocaCola, den Lageplan vom Versteck des Bernsteinzimmers, die Formel für Kalte Fusion, die GPS Koordinaten von Jimmy Hoffers Grab & die Baupläne vom 1947 in Rosswell abgestürzten UFO auf meinem Rechner!

...Nah wer kann das überbieten? 

@kelevra

Nah, da is wohl einer auf Krawall gebürstet?

Beitrag von „cobanramo“ vom 16. Oktober 2017, 23:00

Na ich, im Moment ist nichts wichtiger als die Iranische Atomprogramm 

Beitrag von „kelevra“ vom 17. Oktober 2017, 06:01

> Zitat von hackiFan
>
> @kelevra
>
> Nah, da is wohl einer auf Krawall gebürstet? 

Nein, ganz und gar nicht. Wenn man aber ganz eindeutig mit Halbwissen um sich wirft, muss man eben auch mit einer Gegenreaktion rechnen.

Zum Thema schützensweerte Daten: Wenn die werten Gesprächspartner hier keine schützesnwerten Daten in ihren Netzwerken haben, wozu dann überhaupt das WLAN verschlüsseln? Think about it!

Ich finde es erstaunlich, wie leichtfertig das Thema Sicherheit angegangen wird. Daher auch mein, zugegeben stichelnder, Kommentar, man hätte "ja nichts zu verbergen". Ich möchte ja keinesfalls den Teufel an die Wand malen, aber etwas ernsthafter sollten solche Themen durchaus diskutiert werden, auch wenn es heute wahrscheinlicher ist sich einen Trojaner einzufangen, als sein WLAN Netz gehackt zu bekommen.

Beitrag von „umax1980“ vom 17. Oktober 2017, 10:25

Es ist wirklich scary was da möglich ist, habe mir gerade mal ein paar Videos angesehen die sich mit WLAN Sicherheit beschäftigen.

Davon ausgehend kann man sich auch gleich keine Verschlüsselung einstellen.

Echt heftig.

Wie habt ihr denn eure Netzwerke gesichert?

Beitrag von „DataV“ vom 17. Oktober 2017, 11:38

bei mir wirds per Gruppenmitgliedschaft im AD und einem RAS-Server gesichert

---

Beitrag von „jboeren“ vom 17. Oktober 2017, 11:45

@umax1980 Nur über wpa2 gesichert.

Das Problem ist aber nicht meine iGäte oder MacOS geräte sondern das ander wlan zeugs das sich im Haus befindet zum beispiel die Airports oder Kameras. Ich glaube nicht das alle hersteller ihre Produkte updaten werden...

Beitrag von „umax1980“ vom 17. Oktober 2017, 12:10

Ist denn da grundsätzlich jedes endgerät betroffen? Oder nur der Router ?

Beitrag von „jboeren“ vom 17. Oktober 2017, 12:36

Sowieich es lese kann jedes wlan gerät betroffen sein:

”Da es sich bei Krack um eine Schwäche im WPA2-Standard selbst handelt, sind praktisch alle WLAN-fähigen Geräte betroffen, vom Router über Smartphones und Desktoprechner bis zu

vernetzten Geräten im Internet der Dinge.“

Beitrag von „umax1980“ vom 17. Oktober 2017, 12:42

Herzlichen Glückwunsch !!!

Beitrag von „Nio82“ vom 17. Oktober 2017, 16:42

@kelevra

Es ist schon sehr hochmütig & Egozentrisch von dir alle Anderen hier "Halbwissen" zu unterstellen. Wo du selber erst kurz im Forum bist & die Leute ja wohl noch nicht kennst! Wenn du meinst ein Anderer liege falsch, dann überzeuge mit Argumenten! Doch bisher kann man von dir nur lesen: "*Der sieht es anders als ich? Also liegt er falsch!*"

...Ach & wenn du mit Humor nicht umgehen kannst, dann wirds dir bei uns nicht gefallen. 

@umax1980

> Zitat von umax1980
>
> Wie habt ihr denn eure Netzwerke gesichert?

Wie ich schon auf Seite 1 sagte, nichts ist unknackbar, doch kann man dem Angreifer immerhin so viele Steine wie möglich in den Weg legen um es ihm zu erschweren.
Ich habe alles an Sicherheitsmaßnamen getroffen das bei mir möglich ist. WPA2 ohne zusätzlich WPA1, WPS aus, MAC Sperre, Maximale Passwortlänge von 63 Zeichen mit kryptisches PW bestehend aus Groß-& Kleinbuchstaben & Sonderzeichen von Zufallsgenerator erzeugt. Und das wichtigste überhaupt, wenn nicht benötigt, ist WLAN deaktiviert.

Mag sein das vieles davon umgangen werden kann, doch die Masse machts. Ein Angreifer wird

sich nicht ewig mit dem WLAN aufhalten das stärker geschützt ist als die 5, 6 anderen ringsherum.

Beitrag von „umax1980“ vom 17. Oktober 2017, 17:40

Das ist das indentische Konzept, wie man bei Einbruchs-Vorsorge vorgeht, möglichst viele Steine in den Weg legen, damit das Ziel einfach durch den "Zeitdruck" nicht erreicht werden kann.

Beitrag von „jboeren“ vom 17. Oktober 2017, 17:49

Frage mich wie das funktionieren soll... Wie weiss man als benutzter welches gerät ein sicherheitsupdate hatte oder sicher ist? Besser wäre mmn einen neuen standart “wpa3”?

Beitrag von „kelevra“ vom 17. Oktober 2017, 17:57

> Zitat von Nio82
>
> @kelevra
>
> Es ist schon sehr hochmütig & Egozentrisch von dir alle Anderen hier "Halbwissen" zu unterstellen. Wo du selber erst kurz im Forum bist & die Leute ja wohl noch nicht kennst! Wenn du meinst ein Anderer liege falsch, dann überzeuge mit Argumenten! Doch bisher kann man von dir nur lesen: "*Der sieht es anders als ich? Also liegt er falsch!*"

> *...Ach & wenn du mit Humor nicht umgehen kannst, dann wirds dir bei uns nicht gefallen.* 

Keine Sorge...mit Humor komme ich ganz gut zurecht. 

Anscheinend sind meine Posts aber missverständlich angekommen.

Worauf ich ursprünglich hinaus wollte, war es einzelne Features, wie MAC Filter, nicht als "Sicherheitsfeature" darzustellen. Weniger versierte Leser könnten das falsch interpretieren und schlussfolgern, dass sie alleine damit massgeblich ihr Netzwerk schützen.

Natürlich kann man es in der Summe mit diversen Einstellungen, wie du sie beschreibst, einem potenziellen Angreifer unnötig schwierig machen, sodass er sich ein leichteres ziel sucht.

Aber Schwamm drüber, wir müssen das jetzt sicherlich nicht unnötig strapazieren. Ich denke im Kern sind wir einer Meinung.

Beitrag von „Nio82“ vom 17. Oktober 2017, 19:29

Das Thema ist jetzt auch bei SemperVideo angekommen:

https://youtu.be/sLwpls3mTW8

Beitrag von „Schorse“ vom 17. Oktober 2017, 20:16

@jboeren nein, es geht um das Gerät welches das WPA2 (Protokoll) im WLAN bereitstellt.

Beitrag von „jboeren“ vom 17. Oktober 2017, 21:25

also den router? 

Beitrag von „Schorse“ vom 17. Oktober 2017, 22:41

Genau! Jetzt wird es natürlich brisant wenn der Hersteller kein patch liefert

Beitrag von „Noir0SX“ vom 18. Oktober 2017, 14:49

... https://avm.de/aktuelles/kurz-…bandanschluss-ist-sicher/ ...

Beitrag von „Kabelaffe“ vom 18. Oktober 2017, 18:38

Betroffen sind nur Netze die das Fast Roaming nutzen mit mehr als einem AP

IEEE 802.11r sorgt dafür, dass sich bewegende WLAN-Clients beim Roaming ohne aufwändige Neuanmeldung und damit weitgehend störungsfrei von einem AP zum nächsten wechseln können. Das Ziel ist, die Anzahl der Datenpakete für die Anmeldung am AP wieder auf die vom IEEE 802.11 bekannten vier bis sechs Pakete zu verringern.

Die meisten Router unterstützen das noch nicht einmal

Beitrag von „Altemirabelle“ vom 18. Oktober 2017, 20:06

Ich schütze mich so: mein router ist so schwach (eingestellt), dass der Angreifer nicht nur einen Lapi mitbringen muss sondern auch gleich eine Brechstange. Wenn es aber soweit ist hab ich für den Angreifer eine nette Überraschung, nämlich einen Hund, nein nicht meinen Golden Retriever, sondern eine Flinte, die Hund heisst. Ich bin sicher!

Beitrag von „derHackfan“ vom 18. Oktober 2017, 20:23

> Zitat von Altemirabelle
>
> nicht meinen Golden Retriever, sondern eine Flinte, die Hund heisst. Ich bin sicher!

Mich schützen meine drei Chihuahua, die sind nämlich nicht auf Wade sondern auf Kehle abgerichtet, ich empfehle jedem Besucher den Kopf oben zu lassen.

Beitrag von „Nio82“ vom 18. Oktober 2017, 20:28

@Altemirabelle

Der Witz wäre noch Cooler wenn du gesagt hättest, du hast 2 Hunde zu Hause & die heißen "Smith & Wesson"!

@derHackfan

Da fällt mir gerade spontan der Witz ein wo ein Chihuahua einen Pitbull tötet. Wie hat er das

geschafft? Ganz einfach, er ist dem Pitbull beim runter schlucken im Hals stecken geblieben!

Beitrag von „Altemirabelle“ vom 18. Oktober 2017, 20:46

@Nio82

Wir müssen aber doch etwas realistischer sein. Smith & Wesson ist hier schwer zu kaufen. Hab überall nachgefragt, war sogar bei Lidl. Nix, nur Bratwurst, aber bei Weitem nicht so gefährlich. Und eine Flinte hat doch jeder .... im Garten vergraben. Heheh

---

Beitrag von „aufdenschlips“ vom 18. Oktober 2017, 20:54

Also hier geht dies relativ leicht - Platz am Dokument und Kohle vorrausgesetzt. Sind ja nicht gerade billig.

Stoße lieber an mit einem großzügigen Schluck aus der Gluck, 9er Murmeln passen einfach mehr rein und schneller raus

---

Beitrag von „cobanramo“ vom 18. Oktober 2017, 21:09

Also ehrlich gesagt bin grad bisschen erschrocken, seit Ihr tatsächlich bereit bei einem "WLAN Einbruch" mit Kanonen zu hantieren?
Bei dieser Einstellung dürft Ihr aber euch nicht wundert wenn der nächste Nachbar euren Chihuahua mit Leopard 2 überfährt weil dessen Gartenzaun angepinkelt wurde

---

Beitrag von „Nio82“ vom 18. Oktober 2017, 21:16

@cobanramo

Ne ne, der Chihuahua bekommt eine Blaue Hundeweste vom Nachbarn & dann muss er als Übungsmunition für den Leo herhalten!

(Übungsmunition = Blau gekennzeichnet)

Beitrag von „derHackfan“ vom 18. Oktober 2017, 21:29

@Nio82 du kommst gleich an die Flexi Leine.

Beitrag von „aufdenschlips“ vom 19. Oktober 2017, 07:41

> Zitat von cobanramo
>
> Also ehrlich gesagt bin grad bisschen erschrocken, seit Ihr tatsächlich bereit bei einem "WLAN Einbruch" mit Kanonen zu hantieren?
> Bei dieser Einstellung dürft Ihr aber euch nicht wundert wenn der nächste Nachbar euren Chihuahua mit Leopard 2 überfährt weil dessen Gartenzaun angepinkelt wurde

Nun ja, da der Angreifer eh schon in räumlicher Nähe sein muss

Würde die Murmeln nicht einmal per Hand schmeissen, weiß ja nicht ob der Empfänger überhaupt eine Berechtigung zum Besitz hat

Beitrag von „Altemirabelle“ vom 19. Oktober 2017, 08:36

Chihuahua ist für einen Panzer eine ernsthafte Bedrohung. Es reicht dass der Chihuahua ihn täglich etwas anpinkelt und das verdammte Ding rostet, und wird Schrott.