Wireless Communication: WLAN and WPA2 (IEEE 802.11 and IEEE 802.11i)

Jan Philipp Behrens

Universität Potsdam
jabehrens@uni-potsdam.de

Zusammenfassung. Drahtlose lokale Netzwerke (WLAN) sind aus dem Alltag längst nicht mehr wegzudenken und gewinnen stetig an Bedeutung, da immer mehr Geräte von der Uhr bis zum Kühlschrank WLAN-fähig werden. Durch die Verwendung von WLAN wird lästige Verkabelung überflüssig und die Bewegung der Benutzer nicht mehr eingeschränkt. Im Folgenden soll zuerst eine Einführung in WLAN im Allgemeinen, mit dem Fokus auf die verschiedenen Betriebsmodi, Standards, das MAC-Protokoll und den Frame, gegeben werden. Anschließend sollen mit WEP und WPA die Vorgänger des WPA 2 Sicherheitsstandards betrachtet sowie deren Sicherheitslücken aufgezeigt werden. Zuletzt schauen wir uns das WPA 2 Protokoll und dessen Sicherheitslücken Hole196, KRACK und Kr00k an.

Schlüsselwörter: WLAN · WEP · WPA2 · IEEE 802.11 · IEEE 802.11i · Hole196 · KRACK · Kr00k · Wireless Communication

1 IEEE 802.11 / WLAN

1.1 Betriebsmodi

WLAN bietet eine Reihe verschiedener Betriebsmodi. Die beiden wichtigsten sind der Infrastruktur- (Abb. 1) und der Ad-hoc-Modus (Abb. 2). Der Gängigste ist der Infrastrukturmodus, bei dem Verbindungen stets über einen zentralen Access Point aufgebaut werden [8]. Der Ad-hoc-Modus hingegen verbindet die Teilnehmer über Punkt-zu-Punkt Verbindungen direkt miteinander [6].

1.2 Standards

Seit der Einführung des IEEE 802.11 Standards im Jahr 1997 kamen eine Vielzahl neuer Standards hinzu. Diese führten unter anderem neue Frequenzbänder (802.11a,b,g,n,...), Sicherheitsstandards (802.11i) und Quality of Service Verbesserungen (802.11e) ein. Zu den verwendeten Frequenzbereichen gehören der 0,9 GHz, 2,4 GHz, 5 GHz und 60 GHz Bereich. Da die Durchdringung von Objekten schlechter wird je höher die Frequenz ist, kommen die Frequenzbereiche in

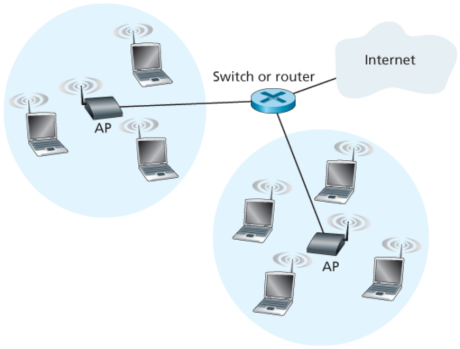


Abb. 1. Infrastrukturmodus (Quelle: [8]).

Abb. 2. Ad-hoc-Modus (Quelle: [8]).

unterschiedlichen Szenarien zum Einsatz. Der sub-GHz Bereich spielt beim Internet of Things (IoT) und der Machine to Machine (M2M) Kommunikation eine Rolle, während der 2,4 und 5 GHz Bereich für den alltäglichen Gebrauch zum Beispiel im Haus und auf der Arbeit zum Einsatz kommt. Der 60 GHz Bereich bleibt Großrechenanlagen vorbehalten und besitzt nur wenige Meter Reichweite. Die Datenrate hat seit 1997 stetig zugenommen, einerseits durch effizientere Kodierungen, jedoch auch durch Kanalbündelung (MIMO) und Richtfunktechnik (Beamforming). Die heute möglichen Datenraten liegen zwischen 5 und 176 GBit/s [1,7].

1.3 MAC Protokoll

Als Media Access Control (MAC) Protokoll kommt beim WLAN das sogenannte Carrier Sense Multiple Access / Collision Avoidance (CSMA/CA) zum Einsatz. Dieses soll, wie der Name schon sagt, Kollisionen vermeiden. Im Gegensatz dazu wird beim Ethernet das CSMA/CD (Collision Detection) verwendet. Um Kollisionen zu vermeiden horcht der Sender zuerst, ob der Empfänger beschäftigt ist. Falls dies nicht der Fall ist, sendet er und wartet auf die Empfangsbestätigung. Erhält der Sender keine Empfangsbestätigung wiederholt er diesen Vorgang. Ist der Empfänger jedoch beschäftigt, so wartet der Sender bis dies nicht mehr der Fall ist und startet dann das Herunterzählen eines zufälligen Backoff-Zählers, um gleichzeitiges Senden mehrerer wartender Clients zu verhindern. Dies führt jedoch zum Problem der Hidden Station [8].

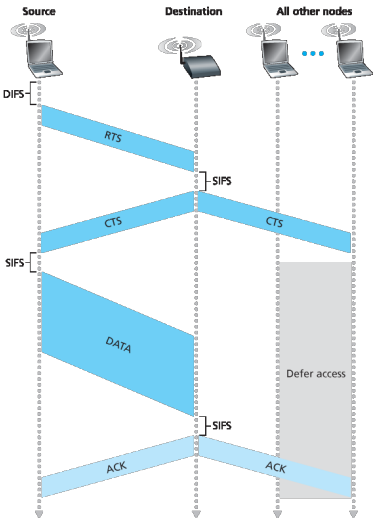


Abb. 3. Reservieren des Kanalzugriffs (Quelle: [8]).

Hidden Station Problem Das Hidden Station Problem tritt auf, wenn sich mehrere Sender nicht sehen und gleichzeitig senden. Um dies zu verhindern, werden Request to Send (RTS) und Clear to Send (CTS) Control Frames verwendet, um den Kanalzugriff zu reservieren (Abbildung 3) [8].

1.4 Frame

Der Frame besteht beim WLAN im Wesentlichen aus einer 4 Byte Prüfsumme, 2312 Byte Payload, vier Adressfeldern für je eine 6 Byte große MAC-Adresse und der Sequenznummer (Abbildung 4). Die Prüfsumme dient zum Korrigieren von Übertragungsfehlern, die beim WLAN wesentlich häufiger auftreten als beim Ethernet. Zwei der vier Adressfelder sind für den Sender und Empfänger, während die anderen beiden Adressfelder nur im Falle einer Weiterleitung verwendet werden. Weiterleitungen können beispielsweise im Ad-hoc- und im Infrastrukturmodus auftreten, wenn zum Beispiel nicht direkt sondern über einen AP mit dem Router kommuniziert wird. Die Sequenznummern dienen zur Unterscheidung neuer Frames von Retransmission-Frames [8].

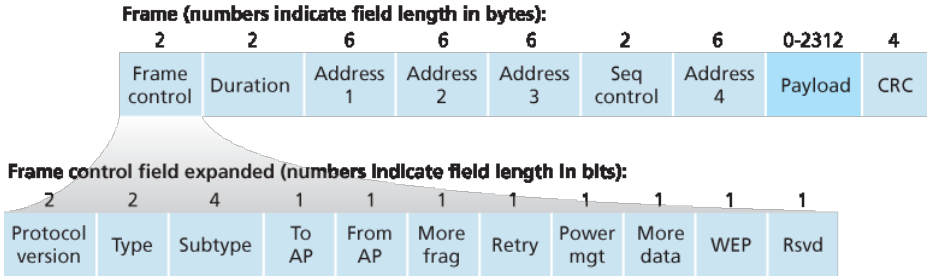


Abb. 4. WLAN Frame (Quelle: [8]).

1.5 Probleme / Nachteile

Privatssphäre Das Wi-Fi Positioning System erlaubt dezimetergenaue Ortung.

Gesundheitsschäden Es wird immernoch kontrovers diskutiert wie stark die Schäden, insbesondere durch oxidativen Stress, durch die Strahlung des WLANs sind.

Reichweite Die Reichweite bis zu der WLAN-Signale noch empfangbar sind liegt bei etlichen Kilometern, was dazu führt, dass man nicht mehr nur lokal angreifbar ist.

2 IEEE 802.11i / WPA 2

2.1 Vorgänger

Wired Equivalent Privacy Das 1999 eingeführte IEEE 802.11 Wired Equivalent Privacy (WEP) Protokoll war das erste Sicherheitsprotokoll für WLAN. Es basiert auf einer Stromchiffre, die den Klartext sowie die Prüfsumme bitweise mit dem Schlüsselstrom XOR-verknüpft, dem sogenannten RC4 Verfahren. Wobei die Sicherheit von Stromchiffren auf der Einmalverwendung der Schlüssel basiert. Die Schlüssellänge des WEP betrug zunächst 64, später 128 und zuletzt 256 Bit und setzt sich aus zwei Komponenten zusammen: dem Initialisierungsvektor und dem symmetrischen Schlüssel. Der 24 Bit große Initialisierungsvektor (IV) wird für jeden Frame neu generiert und steht unverschlüsselt im Header des Frames. Der symmetrische Schlüssel (auch WLAN-Passwort genannt) ist vorher festgelegt und muss einmalig über einen sicheren Kanal ausgetauscht werden. Da der symmetrische Schlüssel sich nicht ändert, reicht er alleine nicht aus, um das Sicherheitskriterium von Stromchiffren zu erfüllen und muss daher mit dem zufälligen IV kombiniert werden. Um, die bei funkübertragungen häufiger auftretenden, Übertragungsfehler finden und korrigieren zu können, beinhaltet das WEP Protokoll einen 32 Bit Cyclic Redundancy Check (CRC32). Da diese jedoch nur eine vergleichsweise einfache lineare Funktion ist, eignet sie sich nicht als sogenanntes Message Authentication Protocol. Das heißt Angreifer können unbemerkt Schlüsseltext und Prüfsumme verändern. Ein weiteres Problem des WEP Protokolls ist der IV der mit 24 Bit zu klein bemessen ist und sich, bei nur 2^{24} Möglichkeiten, zu schnell wiederholt. Das der IV außerdem unverschlüsselt im Header steht, macht es Angreifern zusätzlich einfach, da diese so direkt einen sich wiederholenden IV bemerken. In Abbildung 5 ist der schematische Ablauf der Verschlüsselung dargestellt [5,6,7,8,9].

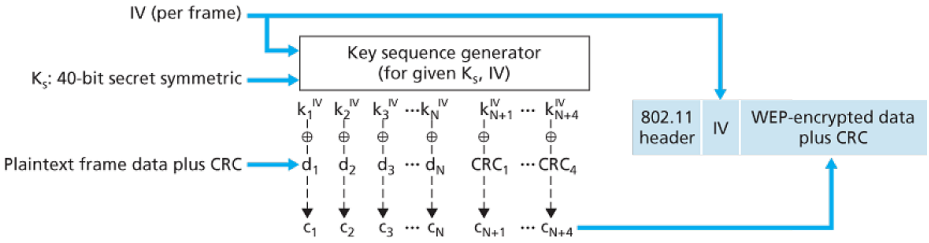


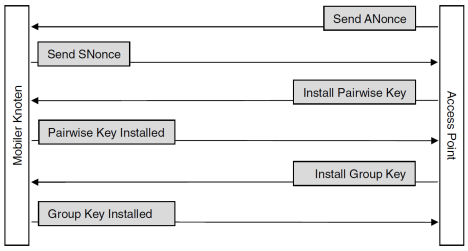
Abb. 5. WEP Protokoll (Quelle: [8]).

WPA Der Nachfolger des WEP war das Wi-Fi Protected Access (WPA) Protokoll, welches als Zwischenlösung diente bis Geräte für WPA 2 zur verfügung standen. Es benutzte weiterhin das RC4-Verfahren zur Verschlüsselung, da es auf der gleichen Hardware laufen musste wie WEP. Verbessert wurde das Protokoll um das sogenannte Temporal Key Integrity Protocol (TKIP), dass die Berechnung eines Message Integrity Codes (MIC), einen größeren 48 Bit IV, die Einführung von Sequenznummern sowie die Erzeugung unterschiedlicher Schlüssel je Frame vorsah. Das Berechnen eines MIC sollte die Schwächen des zuvor beim WEP verwendeten CRC32 beheben, während sich der größere IV im Vergleich zu dem des WEPs seltener wiederholte. Die Erzeugung unterschiedlicher Schlüssel für jeden Frame, lässt nicht direkt Rückschlüsse auf den symmetrischen Schlüssel zu, da dieser nur indirekt zum generieren der temporären Schlüssel verwendet wird. Und die Einführung von Sequenznummern sollte Replayattacken erschweren, in dem nun neue Frames von Retransmits unterschieden werden konnten [5,6,7,9].

2.2 WPA 2

Das IEEE 802.11i WPA 2 Protokoll wurde entwickelt, um die Schwachstellen des WEP zu beheben. Es verwendet den aufwändigeren Advanced Encryption Standard (AES) zum verschlüsseln, weshalb neue Hardware mit Coprozessoren nötig wurde. Das Protokoll unterscheidet zwischen einer Authentifizierung mittels Pre-Shared Key (PSK) dem sogenannten Personal Mode und einer Authentifizierung mittels des Extensible Authentication Protocols (EAP), bei dem der Access Point (AP) die Anfrage an einen Authentifizierungsserver weiterleitet, dem Enterprise Mode. Bei der Authentifizierung mittels Pre-Shared Key kommt ein vorher festgelegtes 8 bis 63 Zeichen langes Passwort zum Einsatz, aus dem sich dann durch 4096-fache Anwendung der SHA1 Hashfunktion der Pairwise Master Key (PMK) berechnet.

Auf die Authentifizierung folgt die Key Generation and Distribution (KGD) Phase. Diese sieht einen 4-Way sowie einen Group Handshake vor (Abbildung 6). Beim 4-Way Handshake tauschen sich Client und AP zunächst einen Nonce sowie einen Message Integrity Code (MIC) aus. Letzterer dient zur Erkennung von Übertragungsfehlern und dem Verhindern von Forging. Der Nonce (number only used once) ist eine Zahl die nur einmal verwendet wird und für den ersten Frame zufällig generiert und danach inkrementiert wird. Nach dem Austausch von Nonce und MIC berechnen Client und AP den Pairwise Transient Key (PTK) aus dem PMK, beiden Nonce und den MAC-Adressen. Bei dem Group Handshake kommt hingegen kein MIC zur Anwendung und der Group Master Key (GMK) wird zufällig generiert. Aus dem GMK leitet sich dann der Group Transient Key (GTK) ab. Eine Übersicht über die bei WPA 2 verwendeten Schlüssel ist in Abbildung 7 dargestellt [5,6,7,9].



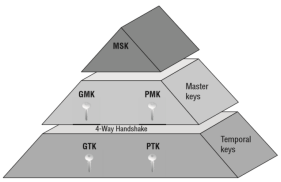


Abb. 6. Handshakes KGD Phase (Quelle: [5]). **Abb. 7.** Schlüsselhierarchie WPA 2 [1].

2.3 Schwachstellen

Hole 196 Die Hole 196 genannte Sicherheitslücke wurde so benannt, da sie auf Seite 196 der IEEE Spezifikation steht und bezeichnet das Fehlen eines MIC beim Group Handshake. Diese Lücke führt dazu, dass keine Möglichkeit besteht zu überprüfen, ob Adressen gefälscht oder Daten manipuliert wurden. Dadurch wird es jedem Netzwerkteilnehmer ermöglicht unbemerkt selbst gefälschte Broadcast-Nachrichten anstelle des AP zu versenden [4].

KRACK Die 2017 entdeckte Key Reinstallation Attack (KRACK) basiert auf der erzwungenen Wiederverwendung der Nonce. Dazu sendet der Angreifer zunächst die dritte Nachricht des 4-Way Handshakes erneut. Woraufhin das Opfer den bereits verwendeten Schlüssel reinstalliert und dabei den Nonce zurücksetzt. Der Angriff beinhaltet verschiedene Varianten, denn nicht jede Implementation erlaubt einen Retransmit im Klartext, sodass zusätzlich zum Beispiel Racing Conditions ausgenutzt werden müssen. KRACK ermöglicht letztlich das Entschlüsseln von Paketen und wenn nur WPA TKIP verwendet wird sogar Zugriff auf den MIC und somit Forging. Zu bemerken ist außerdem, dass sowohl iOS 10.3.1 als auch Windows 7 und 10 nicht anfällig für diesen Angriff sind, da diese die WPA 2 Spezifikation nicht komplett umsetzten in dem sie Retransmits der dritten Handshake-Nachricht verboten [10].

Kr00k KRACK führte zwei Jahre nach seiner Entdeckung zu der Entdeckung einer weiteren Schwachstelle, der Kr00k. Beim Testen der eigentlich bereits gepatchten zweiten Generation der Amazon Echo geräte bemerkte man, dass diese immernoch angreifbar waren, der Grund war diesmal jedoch Kr00k. Bei Kr00k handelt es sich im Vergleich zu KRACK nicht direkt um einen Angriff, sondern um einen Hardwarefehler der WLAN-Chips von Cypress und Broadcom. Dieser tritt nach einer Verbindungstrennung auf bei der der Session Key aus dem Speicher gelöscht (mit Nullen überschrieben) wird und führt dazu, dass restliche Pakete aus dem Transmit Buffer, mit diesem All-Zero-Key verschlüsselt,

[1] Quelle (abgerufen: 2020-05-24): https://www.wifi-professionals.com/wp-content/uploads/2019/01/Hierarchy-768x489.png

übertragen werden. Eine Verbindungstrennung und damit der Fehler, tritt auf wenn man sein WLAN abschaltet, die Verbindung manuell trennt, sich außerhalb der Reichweite des AP befindet, der AP oder sein WLAN abgeschaltet werden oder beim Roaming zwischen zwei APs. Außerdem kann eine Trennung von einem Angreifer, durch das Senden von Management Frames, auch absichtlich herbeigeführt werden, da diese unverschlüsselt verschickt werden. Dieser Schwachpunkt wurde mit IEEE 802.11w durch Protected Management Frames (PMF) behoben, welche beim Nachfolger WPA 3 pflicht sind. Der Fehler betraf Milliarden von Geräten verschiedenster Hersteller, ließ sich jedoch mit einem Softwareupdate beheben [2,3].

Konklusion

Die WLAN Spezifikation IEEE 802.11 zeigt beispielhaft auf, dass Standards im IT-Bereich einer häufigen Anpassung und Erweiterung bedürfen, um auf neue Begebenheiten zu reagieren und anfänglich nicht bedachte Szenarien abzudecken. Außerdem bieten Sicherheitsstandards nie absolute Sicherheit und sind manchmal sogar erst der Grund für eine potentielle Angreifbarkeit (Hole196 bzw. KRACK).

Literatur

1. IEEE 802.11 WLAN Standards im Vergleich, https://www.welotec.com/de/wlan-standards-vergleich, abgerufen: 2020-05-24
2. Kr00k: How kracking amazon echo exposed a billion+ vulnerable wifi devices, https://www.rsaconference.com/usa/agenda/kr00k-how-kracking-amazon-echo-exposed-a-billion-vulnerable-wifi-devices, abgerufen: 2020-05-27
3. Kr00k white paper, https://www.welivesecurity.com/wp-content/uploads/2020/02/ESET_Kr00k.pdf, abgerufen: 2020-05-24
4. WPA2 Hole196 Vulnerability: Exploits and Remediation Strategies. A Whitepaper by AirTight Networks, Inc., http://securedsolutions.com.my/pdf/WhitePapers/WPA2-Hole196-Vulnerability.pdf, abgerufen: 2020-05-24
5. Bless, R., Mink, S., Blaß, E.O., Conrad, M., Hof, H.J., Kutzner, K., Schöller, M.: Sichere Netzwerkkommunikation: Grundlagen, Protokolle und Architekturen. Springer-Verlag (2006)
6. Eckert, C.: IT-Sicherheit: Konzepte-Verfahren-Protokolle. Walter de Gruyter (2013)
7. Frankel, S., Eydt, B., Owens, L., Scarfone, K.: Establishing wireless robust security networks: a guide to IEEE 802.11 i. NIST Special Publication pp. 800–97 (2007)
8. Kurose, J.F., Ross, K.W.: Computer networking: a top-down approach. Pearson (2017)
9. Schmeh, K.: Kryptografie: Verfahren, Protokolle, Infrastrukturen. dpunkt.-Verlag (2016)
10. Vanhoef, M., Piessens, F.: Key reinstallation attacks: Forcing nonce reuse in wpa2. In: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. pp. 1313–1328 (2017)