Beyond WEP - WLAN Security Revisited

Rolf Sotzek
Betreuer: Holger Kinkelin
Seminar Future Internet SS2012
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
Email: sotzekr@in.tum.de

KURZFASSUNG

Computer werden in der heutigen Zeit immer wichtiger und sind aus unserem Alltag nicht mehr wegzudenken, seien es Smartphones oder Laptops. Die Vernetzung von Computern zu Netzwerken war eine bahnbrechende Entwicklung, die zum Erfolg der Computer beigetragen hat. Neue Erkenntnisse in der Funk-Technologie ermöglichten nicht nur kabelgebundene, sondern auch drahtlose Netzwerke (WLANs). Jedoch mussten auch neue Sicherheitsmechanismen für WLANs entworfen werden. Denn bei diesen sind Angreifer nicht mehr auf den physikalischen Zugriff auf das Kabel angewiesen. Wired Equivalent Privacy (WEP) war ein erster Standard, bei dem sehr schnell gravierende Sicherheitsmängel gefunden wurden. Wi-Fi Protected Access (WPA) ist eine überarbeitete Version von WEP. Es besitzt zwar weniger Mängel als WEP, jedoch wird noch immer ein nicht sicheres Kryptographie-Verfahren verwendet. Wi-Fi Protected Access 2 (WPA 2) ist die Weiterentwicklung von WPA und gilt aus heutiger Sicht bei einer richtigen Konfiguration als sicher. Aber in letzter Zeit werden ständig neue Schwachstellen bei WLANs gefunden, mit denen die Sicherheitsmechanismen von WPA 2 umgangen werden können.

Schlüsselworte

WPA, WPA 2, WPS, WPS Sicherheit, Hole 196

1. EINLEITUNG

Das 1997 vorgestellte WEP sollte in WLANs, die nach IEEE 802.11 Standard spezifiziert sind, die Geheimhaltung der Daten sicherstellen. Mögliche Dritte, die versuchen, die Geheimhaltung zu umgehen, werden als Angreifer bezeichnet. Jedoch wurden schon 2 Jahre nach der Entwicklung Sicherheitslücken im verwendeten Kryptographie-Verfahren, dem RC4 Algorithmus, entdeckt. Die vier Ziele der WEP Sicherheitsmechanismen sind die Vertraulichkeit, die Zugriffskontrolle, die Nachrichtenauthentisierung und -integrität. Die Vertraulichkeit ist gebrochen, sobald Angreifer Nachrichten mitlesen können. Der Cyclic Redundancy Check (CRC) ist für die Überprüfung der Nachrichtenintegrität ungeeignet. Durch Einschleusen neuer Nachrichten kann die Zugriffskontrolle umgangen werden. WEP sollte unter keinen Umständen mehr eingesetzt werden, da keines der Sicherheitsziele erreicht werden konnte. S. Fluhrer, I. Mantin und A. Shamir stellten 2001 einen Angriff auf den RC4 Algorithmus vor [1]. Mittlerweile kann WEP in weniger als 60 Sekunden geknackt werden [2].

Bei der Entwicklung von WPA im Jahr 1999 wurde speziell darauf geachtet, dass die Angriffe, die bei WEP möglich waren, nicht auf WPA anwendbar sind. Dafür wurde das Temporal Key Integrity Protocol (TKIP) entwickelt. Eine zentrale Neuerung war, dass jedes versendete Paket mit einem neuen Schlüssel chiffriert wird. Des Weiteren wurde der CRC Algorithmus durch einen verschlüsselten Message Integrity Check (MIC) (auch oft Michael genannt) abgelöst. Leider verwendet TKIP aber immer noch den unsicheren RC4-Algorithmus.

Im folgendem Kapitel 2 wird die Funktionsweise von WPA 2 erklärt. Dies beinhaltet die Betriebsarten von WPA 2, das Schlüsselmanagement und die Erläuterung der Sicherheitsprotokolle. Eine Auswahl von möglichen Angriffen auf WPA 2 wird in Abschnitt 3 vorgestellt. Hierbei wird zuerst ein Angriff auf den Advanced Encryption Standard (AES) erläutert. Des Weiteren werden Angriffe, die auf der Unbedarftheit des Nutzer beruhen, beschrieben. Es werden zudem protokollbasierte Angriffe dargestellt. Auf die verwandten Arbeiten wird in Paragraph 4 hingewiesen. Zum Abschluss der Arbeit wird in Kapitel 5 ein Resümee gezogen.

2. WPA 2

Der Begriff „WPA 2“ bezeichnet die Implementierung des IEEE 802.11i Standards. Durch den IEEE 802.11i Standard [11] gab es gravierende Neuerungen, wie zum Beispiel die Trennung von Authentifizierung der Clients und der Geheimhaltung und Integrität der Daten. Es musste also eine robuste und skalierbare Netzwerkarchitektur entworfen werden. Diese neue Architektur für WLANs wird unter dem Oberbegriff Robust Security Network (RSN) zusammengefasst. RSN benutzt den IEEE 802.1X Standard für die Authentifizierung, eine sichere Verteilung der Schlüssel und neue Integritäts- und Verschlüsselungsverfahren. Kommt bei der Authentifizierung oder dem Verbindungsaufbau ein Four-Way Handshake zum Einsatz, so spricht man auch von einer Robust Security Network Association (RSNA).

Der Aufbau einer sicheren Verbindung nach IEEE 802.11i [11] erfolgt in vier Schritten:

- Aushandlung der verwendeten Sicherheitsmechanismen
- Authentifizierung
- Ableitung und Verteilung der Schlüssel
- Verschlüsselung und Integritätsschutz der Datenkommunikation

doi: 10.2313/NET-2012-08-1_03

2.1 Aushandlung der verwendeten Sicherheitsmechanismen

Damit ein Client sich an einem Netzwerk anmelden kann, muss er erst einmal wissen, welche Netzwerke sich in seiner Umgebung befinden. Dies wird erreicht, indem der Client auf jedem Kanal einen Probe Request sendet. Alle Access Points in Reichweite antworten dem Client mit einer Probe Response, die ein RSN Information Element (IE) enthält. Durch das RSN IE wird dem Client mitgeteilt, welches Authentifizierungsverfahren und Sicherheitsprotokoll der Access Point benutzt und ob eine Wiederaufnahme der vorherigen Verbindung möglich ist. [16]

2.2 Authentifizierung

Bei der Authentifizierung während des RSNA-Handshakes gibt es verschiedene Arten. Eine erste Unterscheidung bieten die zwei verschiedenen Betriebsarten von WPA und WPA 2:

WPA-Personal wird auch WPA-PSK genannt und wurde für private Haushalte und kleine Firmen entworfen, die keinen Authentifizierungsserver besitzen. Jeder Client authentifiziert sich durch einen geheimen Text, den Pre-Shared Key (PSK). Dieser PSK ist für alle Clients im WLAN gleich.

WPA-Enterprise wurde für Unternehmen entworfen und dabei wird ein Authentifizierungsserver benötigt. Durch die komplexere Struktur wird mehr Sicherheit gewährleistet. Für die Authentifizierung empfiehlt der IEEE 802.1X Standard das Extensible Authentication Protocol (EAP).

2.3 Ableitung und Verteilung der Schlüssel

Die RSN Netzwerkarchitektur besitzt im Gegensatz zu WEP ein Schlüsselmanagement. Bei WEP wird ein einziger Schlüssel für die Verschlüsselung und die Authentifizierung verwendet. Im Gegensatz dazu gibt es bei WPA 2 verschiedene Schlüssel, die in einer Schlüsselhierarchie angeordnet sind. In der Kryptographie muss sich der Benutzer ausweisen, zum Beispiel durch die Kenntnis von einem Geheimnis, woraufhin er einen neuen Schlüssel bekommt, mit dem er auf die vom ihm gewünschten Dienste zugreifen kann. Diese neuen Schlüssel sind meistens nur temporäre Schlüssel, die nach der Nutzung des Dienstes ungültig werdem. Das vereinbarte Geheimnis wird ebenfalls durch einen Schlüssel repräsentiert. Dieser wird aufgrund seiner Wichtigkeit auch Master Key genannt. [3]

Zum einen soll jeder Client des Netzwerkes mit dem Access Point in einer einzelnen, sicheren Verbindung kommunizieren. Zum anderen soll der Access Point aber auch Daten an alle Clients gleichzeitig schicken können. Aus diesen beiden unterschiedlichen Anwendungsfällen ergeben sich die zwei Schlüsselarten des Schlüsselmanagements. Für jede Adressierungsart werden somit auch verschiedene Schlüssel gebraucht. Bei der Kommunikation von einem Access Point mit einem Client kommt ein paarweiser Schlüssel zum Einsatz. Dieser paarweise Schlüssel ist ausschließlich dem Access Point und dem Client bekannt. Zur Kommunikation vom Access Point zu allen Clients wird ein Gruppenschlüssel festgelegt, der allen Clients und dem Access Point bekannt ist. Dieser Gruppenschlüssel schützt somit Broadcast und Multicast Daten. [3]

2.3.1 Paarweise Schlüssel

In der Schlüsselhierarchie steht beim paarweisen Schlüssel der 256 Bit lange Pairwise Master Key (PMK) an der Spitze. Der gleiche PMK muss sowohl dem Access Point als auch dem Client bekannt sein. Hierbei spielt das verwendete Authentifizierungsverfahren von WPA 2 eine wichtige Rolle. Bei WPA-Personal wird aus dem PSK der PMK berechnet. Bei WPA-Enterprise wird der IEEE 802.1X Standard verwendet, um auf beiden Seiten den PMK zu erzeugen. Jeder Client und der Access Point besitzen ihren eigenen PMK, da bei der Berechnung des PMK Zufallszahlen benutzt werden. In der Hierarchie unter dem PMK ist der Pairwise Transient Key (PTK). Der PTK wird mittels eines Pseudo-Random Number Generators (PRNG) aus dem PMK erzeugt. Dieser PTK zerfällt wieder in kleinere, temporäre Schlüssel. Diese kleineren Schlüssel haben das Ziel, die Schlüssel- und die Datenübertragung zu schützen. Die Schlüsselhierarchie des paarweisen Schlüssels ist in Abbildung 1 verdeutlicht.

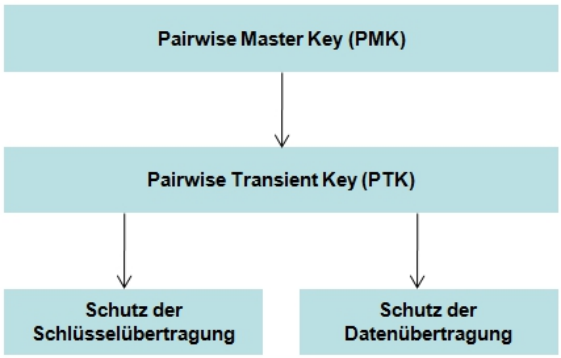

Abbildung 1: Ableitung des PTK

Damit sowohl der Access Point als auch der Client den gleichen PTK erzeugen, wird ein Four-Way Handshake benutzt. Dabei erzeugen beide Kommunikationspartner jeweils eine Pseudozufallszahl und tauschen diese aus. Aus dem PMK, den beiden Pseudozufallszahlen und den MAC-Adressen wird durch dieselbe Pseudo-Random Function (PRF) der gleiche PTK gewonnen. Bei dem gesamten Four-Way Handshake wird das EAP over Lan (EAPoL) Protokoll verwendet. Das EAPoL Protokoll regelt die Verwendung von EAP in Netzwerken und somit auch in WLANs. Nach dem Abschluss des Four-Way Handshakes besitzen beide Kommunikationspartner die nötigen temporären Schlüssel und aktivieren die Verschlüsselung. Die Verwendung des PTK zur Datenverschlüsselung ist in Abbildung 2 veranschaulicht. [3]

2.3.2 Gruppenschlüssel

Genau wie beim PMK ist der Group Master Key (GMK) an der ersten Stelle in der Hierarchie der Gruppenschlüssel. Die Handhabung mit dem GMK ist viel einfacher als bei den paarweisen Schlüsseln, da an der Erstellung nur der Access Point beteiligt ist. Für den GMK wählt der Access Point einfach eine Zufallszahl. In der Hierarchie folgt unter dem GMK der Group Transient Key (GTK). Der GTK

doi: 10.2313/NET-2012-08-1_03

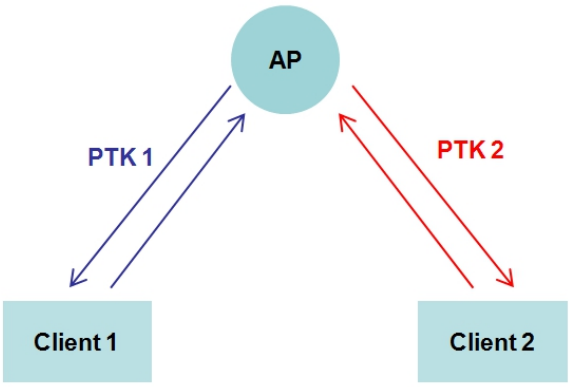

Abbildung 2: Verwendung des PTK

zerfällt wieder in temporäre Schlüssel, mit denen Multicast-Datenübertragungen geschützt werden können. Der GTK wird aus dem GMK, der MAC-Adresse des Access Points und einem Zufallswert unter Verwendung einer PRF erzeugt. Die Hierarchie des Gruppenschlüssels ist in der Abbildung 3 dargestellt.

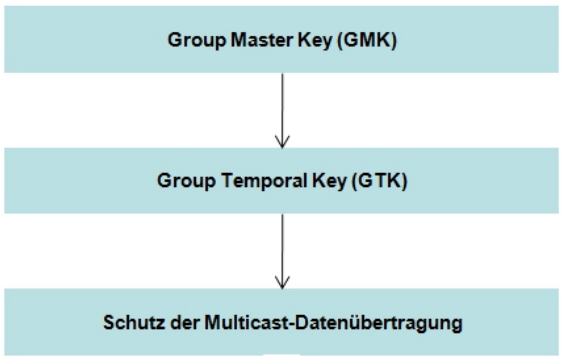

Abbildung 3: Ableitung des PTK

Die Verteilung des GTK an alle Clients ist einfacher, da die bestehende Absicherung durch den PTK benutzt wird. Die Verwendung des GTK zur Datenverschlüsselung von Multicasts ist in Abbildung 4 veranschaulicht. [3]

Bei WPA 2 wurde auch ein Schlüsselwechsel hinzugefügt. Verliert der GTK eines Netzwerks seine Gültigkeit, wird vom Access Point an alle Clients ein neuer GTK verteilt. Der GTK muss zum Beispiel erneuert werden, sobald ein Client das Netzwerk verlässt, damit der Client nicht mehr die Multicast und Broadcast Daten des Access Points empfangen kann. Der Group Key Handshake, der in IEEE 802.11 [11] definiert ist, kümmert sich um die Aktualisierung des GTK. Er ist einem Two-Way Handshake sehr ähnlich:

1. Der Access Point teilt jedem Client des Netzwerks den neuen GTK mit. Der neue GTK ist dabei durch die Schlüsselübertragung des PTK verschlüsselt.
2. Jeder Client bestätigt den GTK und antwortet dem Access Point.

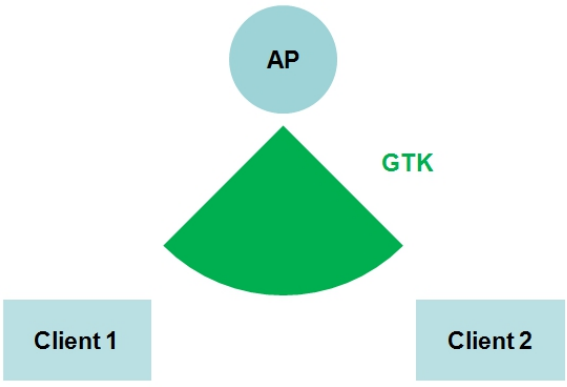

Abbildung 4: Verwendung des GTK

2.4 Verschlüsselung und Integritätsschutz der Datenkommunikation

WPA 2 unterstützt aus Kompatibilitätsgründen sowohl das Temporal Key Integrity Protocol (TKIP) als auch das Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP). Die Unterstützung von CCMP ist bei WPA 2 fest vorgeschrieben. Die beiden Sicherheitsprotokolle für WPA 2 unterscheiden sich stark:

TKIP benutzt den RC4-Algorithmus mit einer Schlüssellänge von 128 Bit. Zur Sicherung der Nachrichtenintegrität wird der Michael Algorithmus verwendet.

CCMP verwendet den Advanced Encryption Standard (AES) mit einer Block- und Schlüssellänge von 128 Bit. Die Nachrichtenintegrität wird durch einen Cipher Block Chaining - Message Authentication Code (CBC-MAC) gesichert.

2.4.1 TKIP

Die zentralen Verbesserungen von WEP zu TKIP sind [3]:

- In die Berechnung des MIC wird ein geheimer Schlüssel, welcher ein Teilschlüssel des PTK ist, miteinbezogen. Der Michael Algorithmus hat den Vorteil, dass die Prüfsumme von der gesamten Nachricht berechnet wird. Diese beinhaltet somit auch die Ziel- und Quelladresse.
- Das bereits beschriebene Schlüsselmanagement wird eingeführt.
- Jedes Paket wird mit einem neuen Schlüssel chiffriert.
- Sollten MIC-Fehler auftreten, werden Gegenmaßnahmen eingeleitet.
- Der von WEP bekannte Initialisierungsvektor (IV) wird durch einen erweiterten IV ersetzt.

2.4.2 CCMP

Bei CCMP wird AES in Counter Modus zur Verschlüsselung von Daten benutzt. Ein weitere Betriebsart von AES ist der Counter with CBC-MAC Modus (CCM Modus). Dieser wird

doi: 10.2313/NET-2012-08-1_03

für die Berechnung des CBC-MAC gebraucht. Der berechnete CBC-MAC, quasi eine verbesserte Prüfsumme, bietet sowohl Authentifizierung als auch Integrität. Für die weitere Arbeit hat das CCMP eine geringe Bedeutung, deswegen sei der Vollständigkeit halber auf J. Edney und W. A. Arbaugh [3] verwiesen.

3. ANGRIFFE AUF WPA 2

Sucht man heute danach, wie man ein WPA 2 Netzwerk knacken kann, wird man meistens zu Aircrack-ng [9] weitergeleitet. Bei WPA 2 kann mit Aircrack-ng nur die WPA-PSK Betriebsart gebrochen werden. Das Knacken des Schlüssels von WPA-Enterprise ist so gut wie unmöglich, weil ein Schlüssel mit der maximalen Länge verwendet wird. Bei WEP können statistische Lösungsverfahren die Rechenzeit verkürzen. Im Gegensatz dazu muss bei WPA 2 der komplette Schlüsselraum ausprobiert werden. Der Angriff kann nicht beschleunigt werden, da die Schlüssel bei WPA 2 dynamisch sind. Die einzige Information, die man über den PSK erhält, ist in dem Four-Way Handshake enthalten. Der Angreifer muss also die Anmeldung eines Clients an dem Access Point mitschneiden. Ungeduldige Angreifer täuschen einem mit dem Netzwerk verbundenen Client einen Verbindungsabbruch vor, woraufhin sich der Client wieder mit dem Access Point verbindet und somit auch ein neuer Four-Way Handshake stattfindet. [10]

In den Unterkapiteln werden verschiedene Angriffe auf WPA 2 erläutert. Zuerst werden Angriffe auf den AES vorgestellt, gefolgt von Angriffen, die aufgrund der Unvorsichtigkeit von Nutzern ermöglicht werden. Als Letztes werden Protokolle oder Auszüge eines Protokolls gezeigt, die die Sicherheit eines WPA 2 WLANs gefährden können.

3.1 Angriffe aus AES

2011 stellten A. Bogdanov, D. Khovratovich und C. Rechberger den ersten Angriff auf den vollen AES-Algorithmus vor. Mit Hilfe von vollständigen bipartiten Graphen wird eine viermal höhere Geschwindigkeit als mit der Brute-Force-Methode erreicht. In der Kryptographie wird eine Verschlüsselung als geknackt bezeichnet, wenn es ein Verfahren gibt, dass schneller als Brute-Force ist. Statt 2^{128} werden $2^{126,1}$ Operationen benötigt, um einen AES-128 Schlüssel zu brechen. Zwar ist der Rechenaufwand immer noch viel zu groß, aber dennoch gelang ein wichtiger theoretischer Durchbruch. [5]

3.2 Unbedarftheit der Nutzer

Ein großes Problem bei der Sicherheit von WLANs ist, dass sich viele Nutzer der Risiken einer falschen Konfiguration des Access Points nicht bewusst sind. Mögliche Anwender wissen meist nur wenig über die verwendeten kryptographischen Verfahren oder haben keine Ahnung, was ein 256 Bit Schlüssel ist. Bei einem 256 Bit Schlüssel beträgt der Schlüsselraum 2^{256}. Allgemein kann man sagen, dass wenn man die Anzahl der Bits des Schlüssels erhöht, man also einen längeren Schlüssel nimmt, auch die Anzahl der möglichen Schlüssel zunimmt. Angreifer brauchen somit länger, um alle möglichen Schlüssel auszuprobieren. Jedoch sollte man im Umgang mit Schlüsseln nicht vergessen, dass die Sicherheit eines WLANs durch die kryptographische Verschlüsselung erreicht wird und nicht durch den Schlüssel.

Bei WPA-Personal kann der PSK mit 64 Hexadezimalzahlen oder über ein Passwort von 8 bis 63 ASCII Zeichen eingegeben werden. Der PBKDF 2 (ein kryptographisches Verfahren zum Ableiten von Schlüsseln) berechnet aus dem PSK, der SSID und der Länge der SSID mit Hilfe von Hashing den PMK. Ist der PSK n ASCII Zeichen lang, so liefert der PBKDF 2 eine sicherheitsrelevante Schlüssellänge von $2,5 * n + 12$ Bit. [11]

Viele private Haushalte verwenden einfache Wörter als PSK für ihre WLANs. Dies stellt ein großes Problem dar, weil diese mittels Wörterbuch-Attacken schnell erraten werden können. Leider sind diese einfachen PSKs meistens auch noch sehr kurz und somit auch gut durch Brute-Force-Angriffe brechbar. Maßgeblich für die Sicherheit eines WLANs ist immer die Wahl eines guten PSK. Der PSK sollte mindestens 13 Buchstaben lang sein, Zahlen und bestenfalls Sonderzeichen enthalten. A. Ku empfiehlt nach seinen Tests [18] eine Mindestpasswortlänge von acht Zeichen mit mindestens einem Sonderzeichen, einer Zahl und einem Groß- und Kleinbuchstaben. Allerdings scheint ein PSK mit 13 Groß- und Kleinbuchstaben auch sicher zu sein.

In der heutigen Zeit des Internet-Zeitalters gibt es aber auch ein weiteres Problem bei der Sicherheit von Schlüsseln. Weil die Produktion von Computern immer billiger wird, kaufen große Firmen ganze Rechenzentren, in denen sie tausende von Prozessoren zu einem Super-Computer vernetzen. Meistens brauchen die Firmen nicht die ganze Kapazität des Super-Computers und verkaufen somit Rechenzeit an Kunden. Die EC2 von Amazon ist ein Beispiel dafür [17]. Auf solchen Super-Computern geht das Knacken eines Schlüssels sehr viel schneller. Das Knacken eines Schlüssels ist somit eher eine Frage des Geldes anstatt der Zeit.

3.2.1 Unbemerkte Windows-Ad-hoc-Netzwerke

2006 entdeckte S. Nomad ein abnormes Verhalten von Windows-Ad-hoc-Netzwerken [4]. Ein Beispielszenario dieses Verhaltens ist:

- Zuhause besitzt Alice einen Access Point mit der SSID „Netgear“. Sie hat ihren Laptop so eingerichtet, dass er sich automatisch mit diesem Netzwerk verbindet.
- Weil Alice viel reist und ihren Laptop zum Arbeiten nutzt, arbeitet sie auch unterwegs. Das kann beispielsweise an Flughäfen sein.
- Zufällig hat der neben Alice sitzende Bob einen Laptop, der ein Ad-hoc-Netzwerk mit dem Namen „Netgear“ hat.
- Der Laptop von Alice sucht nach dem Netzwerk mit der SSID „Netgear“ und verbindet sich mit Bobs Ad-hoc-Netzwerk.
- Beim nächsten Booten von Alices Laptop ohne angeschlossenes Netzwerkkabel und ohne ein Netzwerk mit der SSID „Netgear“ in Reichweite, erstellt der Laptop von Alice ein Ad-hoc-Netzwerk mit dem Namen „Netgear“.

Angreifer können sich somit gezielt mit den betroffenen Computern verbinden, wodurch weitergehende Attacken ermög-

doi: 10.2313/NET-2012-08-1_03

licht werden. Dieses Szenario basiert auf einem Konfigurationsfehler und er kann sich virusartig von PC zu PC verbreiten. Microsoft hat diesen Fehler mittlerweile behoben. Der beste Schutz vor diesem Fehler ist, die WLAN Karte im Laptop abzuschalten, wenn man kein WLAN benötigt. Die meisten Laptops besitzen sogar eine Taste oder Tastenkombination, mit der man die WLAN Karte abschalten kann. Auch sollte man aus diesem Fehler lernen, dass man sein Betriebssystem und alle Treiber immer auf dem aktuellsten Stand halten sollte.

3.2.2 Karma Attacke

Karma [12] greift die automatische Anmeldung an schon bekannten Netzwerken an.

Generell läuft die Suche nach WLANs unter Windows XP SP 2 wie folgt ab [13]:

- Der Client erstellt eine Liste mit allen verfügbaren Netzwerken in Reichweite, indem ein Broadcast Probe Request auf jedem Kanal gesendet wird.
- Die Access Points in der Umgebung antworten mit ihren Probe Response.
- Der Client besitzt eine Preferred Networks List (PNL). Diese ist eine geordnete Liste von Netzwerken, zu denen sich der Client in der Vergangenheit verbunden hat.
- Sollte ein Netzwerk aus der PNL in Reichweite sein, verbindet sich der Client mit diesem.
- Wenn keines der gefundenen Netzwerke in der PNL ist, werden spezifische Probe Requests für jedes Netzwerk aus der PNL gesendet. Dies ermöglicht, sich mit versteckten Netzwerken zu verbinden.
- Falls immer noch keine Verbindung hergestellt werden konnte und es ein Ad-hoc-Netzwerk in der PNL gibt, wird dieses Netzwerk erstellt und der PC wird der erste Client.
- Ist die Option „Verbindung zu unbekannten Netzwerken herstellen“ gewählt, wird in der Reihenfolge, in der die Netzwerke entdeckt wurden, versucht, sich mit jedem erreichbaren Netzwerk zu verbinden. Diese Option ist standardmäßig ausgeschaltet.
- Sollte immer noch keine Verbindung bestehen, wird die SSID der Netzwerkkarte auf eine Zeichenkette aus 32 zufälligen char-Werten festgesetzt und für eine Minute gewartet, bis der Algorithmus von neuem gestartet wird.

Angriffe auf den Algorithmus:
Angreifer können die SSID aller Netzwerke in der PNL herausfinden, indem sie die Probe Requests des Clients mithören. Angreifer können gefälschte Verbindungsabbrüche an den Client senden, wodurch der Client den Algorithmus neu startet. Dies bewirkt, dass der Client die spezifischen Probe Requests für jedes Netzwerk in der PNL sendet. Angreifer können mit dem Wissen der PNL einen gefälschten Access Point mit der SSID eines Eintrages aus der PNL erstellen. Karma macht sich dieses Verhalten zu Nutze und erstellt diese gefälschten Access Points automatisch. Sucht ein Client ein Netzwerk mit der SSID „FritzBox“, wird ihm durch Karma ein unverschlüsseltes Netzwerk mit dem Namen „FritzBox“ angeboten. Entscheidend ist nun, ob der Client ein verschlüsseltes Netzwerk erwartet oder nicht. Ist in der PNL das Netzwerk mit einer Verschlüsselung gespeichert, wird die Verbindung zu dem von Karma erstellten Netzwerk fehlschlagen, da dieses unverschlüsselt ist. Sollte das Netzwerk in der PNL nicht verschlüsselt sein, verbindet sich der Client mit dem Karma Netzwerk. Über weitere gefälschte Services, wie zum Beispiel DHCP und HTTP, kann man relativ einfach einen Man-in-the-middle-Angriff ausführen. [12]

Bei Mac Systemen funktioniert die automatische Anmeldung bei Netzwerken anders als unter Windows XP SP 2. Jedoch bleiben fast die gleichen Probleme erhalten. So geben auch Mac System ihre PNL preis. [13]

Nutzer sollten bei der Verwendung von WLANs also immer alle unverschlüsselten Netzwerke aus der PNL löschen. Des Weiteren sollten die Nutzer vorsichtig im Umgang mit WLANs werden und in unsicheren Umgebungen, wie zum Beispiel öffentlichen Plätzen, nicht einfach ein offenes WLAN benutzen.

3.3 Protokollbasierte Angriffe

Entwickler von neuen Protokollen sind nicht perfekt. Dadurch kommt es zu Design- und Implementierungsfehlern. Diese Fehler sind tief im Protokoll verankert und dadurch später schwer zu kompensieren und aufzufinden.

3.3.1 WPS

Wi-Fi Protected Setup (WPS), früher Wi-Fi Simple Config genannt, ist eine Zertifizierung von der Wi-Fi Alliance [7], die beim Hinzufügen von Geräten zu schon bestehenden Netzwerken hilft. Anfang 2007 wurde dieser Standard von der Wi-Fi Alliance entwickelt, mit dem Ziel, dass auch Leuten ohne umfangreiche Computerkenntnisse eine einfache Möglichkeit geboten wird, neue Clients unkompliziert in ein vorhandenes Netzwerk hinzuzufügen. Unerfahrene Anwender sollten vor der Eingabe von langen PSKs verschont bleiben. Auch könnten Anwender von der Anzahl der verschiedenen Kryptographieverfahren, wie WEP, WPA und WPA 2 verwirrt sein. Mittlerweile bieten fast alle großen Hersteller von Access Points (Cisco, Netgear, D-Link, usw.) Geräte mit WPS-Zertifizierung an. Heutzutage gibt es schon mehr als 200 Produkte, die eine WPS-Zertifizierung von der Wi-Fi Alliance besitzen. Die Wi-Fi Alliance vergibt die WPS-Zertifizierung auf Grundlage der Wi-Fi Simple Configuration Specification (WSC). [6]

Der Standard beinhaltet drei verschiedene Methoden, wie Anwender neue Geräte in ein Netzwerk integieren können [8]:

Push Button Configuration. Bei diesem Verfahren können neue Geräte durch das Drücken von Knöpfen angemeldet werden. Der Access Point besitzt einen physikalischen Knopf. Die anzumeldende Gegenstelle kann entweder einen physikalischen oder einen Software implementierten Knopf aufweisen. Um neue Geräte am Access Point anzumelden,

doi: 10.2313/NET-2012-08-1_03

muss zuerst der Knopf am Access Point gedrückt werden. Hiernach beginnt ein zweiminütiger Countdown, während dem sich neue Geräte anmelden können. Die Verbindung wird durch das Drücken des Knopfs an dem anzumeldenden Gerät hergestellt.

Pin. Bei der Pin-Variante muss beim Hinzufügen eines Gerätes ein Pin eingegeben werden. Der Pin kann aus einer fest voreingestellten Zahlenkombination bestehen. Jedoch sind auch Implementierungen mit einem dynamischen Pin möglich. Mit Hilfe eines Monitors kann man sich den generierten, dynamischen Pin anzeigen lassen. Beim fest voreingestellten Pin befindet sich zum Beispiel ein Aufkleber auf der Unterseite des Access Points mit dem Pin. Will sich zum Beispiel ein neuer Client zum Netzwerk verbinden, erscheint bei ihm ein Fenster. In diesem muss der Pin eingeben werden. Ist der Pin richtig, wird der Client anschließend mit dem Access Point verbunden. Sollte der Pin falsch sein, tritt ein Fehler auf.

Near Field Communication (NFC). Die NFC ermöglicht die drahtlose Übertragung von Daten über eine Strecke von einigen Zentimetern. Sie baut auf der Technologie von RFID-Chips auf. Hierbei wird die Konfiguration des WLANs im RFID-Chip gespeichert. Durch ein entsprechendes Lesegerät kann die Konfiguration durch den Client ausgelesen werden.

Die letzte Methode wird auch oft als Out-of-band Methode bezeichnet, da bei ihr die Informationen nicht über den WLAN Kanal übertragen werden. Die Wi-Fi Alliance vergibt die WPS-Zertifizierung für Access Points, wenn sie die Push Button Methode und die Pin-Eingabe unterstützen. Die drahtlosen Clients müssen nur die Pin-Methode ermöglichen.

Wenn man die verschiedenen Methoden nach ihrer Sicherheit unterscheidet, ergibt sich folgende Übersicht:

Push Button Configuration. Durch das Drücken des Knopfes am Access Point kann sich jeder beliebige Client innerhalb eines Zeitfensters von zwei Minuten anmelden. Angreifer könnten sich in dieser Zeit mit ihren Computern anmelden. Sie müssen nur wissen, dass der Button gedrückt wurde.

Pin. 2011 entdeckte S. Viehböck eine Schwachstelle bei der Pin Methode, wenn der Access Point einen fest voreingestellten Pin besitzt [6]. Die genaue Erläuterung, wie man den Pin wiederherstellen kann, folgt nach dieser Auflistung.

Near Field Communication (NFC). Angreifer müssen bis auf einige Zentimeter an den Access Point herankommen, damit sie den RFID-Chip lesen können.

Im nächsten Abschnitt wird gezeigt, wie man die fest voreingestellte Pin aufgrund eines Design-Fehlers des WPS Protokolls knacken kann.

Ein vereinfachter Ablauf des WPS Protokolls bei der Pin Eingabe sieht wie folgt aus [6]:

- Verbindungsaufbau zwischen Access Point und Client.
- EAP Initiation unter Verwendung von EAPoL zwischen Access Point und Client.
- Diffie-Hellman Schlüsselaustausch zum Aufbau einer sicheren Verbindung.
- Der Client sendet den ersten Teil des beim ihm eingegebenen Pins.
- Der Access Point bestätigt den ersten Teil.
- Der Client sendet den zweiten Teil des beim ihm eingegebenen Pins.
- Der Access Point bestätigt den zweiten Teil.
- Der Access Point sendet seine Konfiguration (SSID, Verschlüsselungsart, WLAN Schlüssel, usw.) an den Client.
- Der Client baut eine Verbindung zum Access Point mit den übermittelten Information auf.

Sollte bei diesem Ablauf ein Fehler auftreten, antwortet der Access Point sofort mit einer Fehlermeldung. Durch die sofortige Antwort des Access Points ist es einem Angreifer möglich, die Richtigkeit der Teile des Pins abzuleiten [6]:

- Erhält der Angreifer nach dem Senden des ersten Teils des eingegebenen Pins eine Fehlermeldung, weiß er, dass der erste Teil des eingegebenen Pins falsch ist.
- Ebenso verhält es sich mit dem zweiten Teil des Pins.

Wenn man den voreingestellten Pin genau betrachtet, stellt man fest, dass der achtstellige Pin in zwei Teile zerlegt werden kann. Es werden zuerst alle möglichen Kombinationen der ersten vier Stellen ausprobiert. Bei vier Stellen entspricht dies lediglich 10^4 Kombinationen. Der zweite Teil des Pins kann noch schneller erraten werden, da die achte Stelle des Pins eine Prüfsumme (Checksum) ist und somit aus den restlichen sieben Stellen berechnet werden kann. Die Aufteilung des Pins in zwei Teile ist in Abbildung 5 verdeutlicht. Aus dem zweiten Teil des Pins folgen also nur 10^3 Kombinationen, welche durchprobiert werden müssen. Insgesamt müssen nur 11000 Kombinationen ausprobiert werden bis der richtige Pin gefunden ist. S. Viehböck brauchte durchschnittlich 1,3 Sekunden pro Pin Versuch, das Ausprobieren aller Pins dauert somit circa vier Stunden. [6]

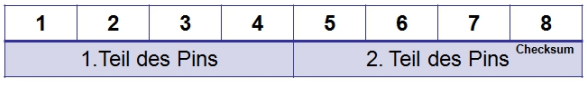

Abbildung 5: Aufteilung des WPS Pins in zwei Teile

Aufgrund dessen, dass WPS die Konfiguration des Access Points dem Client mitteilt, funktioniert dieser Angriff unabhängig von der verwendeten Verschlüsselungsart des

doi: 10.2313/NET-2012-08-1_03

WLANs. Das reine Ausprobieren vieler Pins funktioniert nicht bei alle Access Points, weil manche Hersteller nach einer gewissen Anzahl von Pin-Eingabe-Versuchen die WPS Funktion automatisch für eine kurze Zeit deaktivieren. Der einzige Schutz vor dem Herausfinden des WPS Pins ist, die WPS Funktion im Access Point auszuschalten. [6]

3.3.2 Hole 196

Hole 196 ist eine andere Art eines Angriffs auf WLANs als die bisher vorgestellten. Das Besondere, was Hole 196 von den meisten Angriffen unterscheidet, ist, dass man Mitglied des Netzwerks sein muss. Es wird also nicht der Schlüssel des Netzwerks oder die AES Verschlüsselung angegriffen, sondern ein fehlendes Management ausgenutzt. Studien zeigen, dass die Zahl der internen Angriffe auf Netzwerke zunehmen und diese sehr hohe finanzielle Schäden verursachen können.

Die Lücke, die Hole 196 ermöglicht, wurde von AirTight Networks [14] auf Seite 196 des IEEE 802.11 Standard (2007) [11] gefunden, daher auch der Name „Hole 196“. Bei Hole 196 wird das fehlende Management des GTK ausgenutzt. Bei Datenpaketen, die mit dem PTK verschlüsselt sind, kann ein Client erkennen, ob die MAC-Adresse gefälscht oder der Inhalt verändert wurde. Jedoch hat der GTK keine dieser Eigenschaften. Normalerweise sollte nur der Access Point Daten mit dem GTK verschlüsseln und die Clients die Daten mit dem GTK entschlüsseln. Aber nichts im IEEE 802.11 Standard verhindert, dass ein Client gefälschte, mit dem GTK verschlüsselte Pakete verschickt. Dadurch ergeben sich drei mögliche Angriffe: Denial of Service, Einschleusen von Schadcode in andere Clients und ARP Poisoning. Das Besondere bei dieser Art des ARP Poisoning ist, dass dieses verschlüsselt erfolgt und über Funk übertragen wird. Beim bisherigen ARP Poisoning wurden die gefälschten ARP Pakete über den Access Point weitergeleitet und die Attacke konnte somit erkannt werden. Im Gegensatz dazu werden bei Hole 196 die gefälschten ARP Pakete direkt von Client zu Client geschickt. Ein weiteres Problem ist, dass die gefälschten ARP Pakete in der Luft existieren und verschlüsselt sind. Kabelgebundene Sicherheitssoftwarelösungen können diese Art der Attacke also nicht erkennen. Zudem erkennen existierende Access Points kein abnormes Verhalten. Die einzige Möglichkeit, sich vor dem Angriff zu schützen, wäre bei der Verteilung des GTK jedem Client einen eigenen GTK zuzuweisen. [15]

In Abbildung 6 wird die Man-in-the-middle-Angriffsvariante von Hole 196 veranschaulicht. Zuerst (Schritt 1) sendet der Angreifer einem Client ein gefälschtes ARP Paket, das mit dem GTK verschlüsselt ist. Daraufhin sendet der Client die Daten wie üblich an den Access Point, wobei diese mit dessen PTK verschlüsselt sind (Schritt 2). Jedoch ist die Ziel-MAC-Adresse die des Angreifers. Der Access Point sendet die Daten mit dem PTK des Angreifers verschlüsselt an den Angreifer, da dies die Ziel-MAC-Adresse ist (Schritt 3). Als Letztes leitet der Angreifer die gesamten Daten wieder zum Access Point, damit dem Client keine Beeinträchtigung auffällt (Schritt 4).

4. VERWANDTE ARBEITEN

Lehembre gibt in seiner Ausarbeitung [16] eine gute Einführung zum Thema WLANs und deren Sicherheit. Die vielen Grafiken veranschaulichen die Abläufe sehr gut und bilden

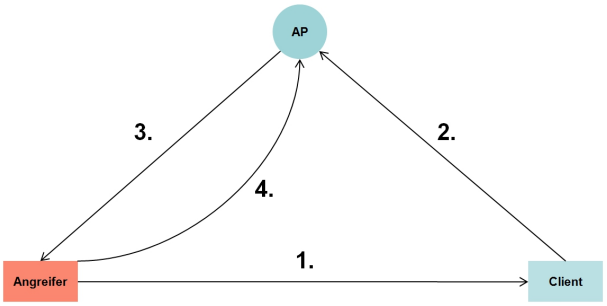

Abbildung 6: Man-in-the-middle-Angriffsvariante von Hole 196

ein Nachschlagewerk. Jedoch werden manchmal umfangreiche Details nicht genau erklärt.
A. Müller, H. Kinkelin, S. K. Ghai und G. Carle stellen in ihrer Arbeit [19] ein System vor, mit dem X.509 Zertifikate für neue Geräte eines Netzwerks ausgestellt werden können. Durch diese Zertifikate kann der Zugriff auf das Netzwerk geregelt werden.

Diese Ausarbeitung stellt die Funktionsweise von WPA 2 in einer vereinfachten Form dar. Des Weiteren werden verschiedene Angriffe auf WPA 2 erläutert. Das Ziel dieser Arbeit ist, dass man sich der Risiken und einhergehende Gefahren von WLANs bewusst wird und weiß, wie man sich gegen einige davon schützen kann.

5. ZUSAMMENFASSUNG

Aus heutiger Sicht gilt WPA 2 als sicher, wenn der Access Point richtig konfiguriert ist. Es sollte im privaten Umfeld ein möglichst langer und komplexer PSK gewählt werden, damit dieser nicht erraten werden kann. Als Verschlüsselungsart sollte WPA 2 mit CCMP gewählt werden, weil diese heutzutage als sicher gilt. Des Weiteren sollten der Access Point als auch alle Clients auf einem aktuellen Stand gehalten werden. Nicht verwendete Protokolle, wie WPS, sollte man am besten ausschalten oder nur kurz, wenn man sie benötigt, einschalten. Auch sollte bei Laptops das WLAN vollkommen ausgeschaltet sein, wenn es nicht gebraucht wird. Es bleibt abzuwarten, ob neue Schwachstellen gefunden werden.

6. LITERATUR

[1] S. Fluhrer, I. Mantin und A Shamir: *Weaknesses in the Key Scheduling Algorithm of RC4*, 2001

[2] E. Tews, R.-P. Weinmann und A. Pyshkin: *Breaking 104 bit WEP in less than 60 seconds*, In WISA'07 Proceedings of the 8th international conference on Information security applications, pages 188-202, Springer, 2007

[3] J. Edney und W. A. Arbaugh: *Real 802.11 Security: Wi-Fi Protected Access and 802.11i*, Boston, MA, Addison-Wesley, 2004

[4] *Microsoft Windows Silent Adhoc Network Advertisement*, `http://www.nmrc.org/pub/advise/20060114.txt`, S. Nomad, Nomad Mobile Research Centre, 2006

[5] A. Bogdanov, D. Khovratovich und C. Rechberger: *Biclique Cryptanalysis of the Full AES*, 2011

doi: 10.2313/NET-2012-08-1_03

[6] S. Viehböck: *Brute forcing Wi-Fi Protected Setup*, 2011
[7] *Wi-Fi Alliance*, http://www.wi-fi.org
[8] *Wi-Fi Alliance FAQ*, http://www.wi-fi.org/knowledge-center/faq
[9] *Aircrack-ng*, http://www.aircrack-ng.org/
[10] *Aircrack-ng Cracking WPA*, http://www.aircrack-ng.org/doku.php?id=cracking_wpa
[11] IEEE 802.11: *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications*, 2007
[12] *Karma*, http://www.theta44.org/karma/index.html
[13] D. A. D. Zovi und S. A. Macaulay: *Attacking Automatic Wireless Network Selection*, In Proceedings from the Sixth Annual IEEE SMC, pages 365-372, 2005
[14] *AirTight Networks*, http://www.airtightnetworks.com
[15] *AirTight Networks - WPA2 Hole196 Vulnerability*, http://www.airtightnetworks.com/WPA2-Hole196
[16] G. Lehembre: *Wi-Fi security - WEP, WPA and WPA2*, 2005
[17] *Amazon Elastic Compute Cloud (Amazon EC2)*, http://aws.amazon.com/de/ec2/
[18] *Tom's Hardware, A. Ku*, http://www.tomshardware.de/WLAN-Einbruch-Hacken-Brute-Force,testberichte-240879.html
[19] A. Müller, H. Kinkelin, S. K. Ghai und G. Carle: *An Assisted Device Registration and Service Access System for future Home Networks*, 2009

doi: 10.2313/NET-2012-08-1_03