Proseminar Kryptographische Protokolle
WLAN

Danilo Bürger

7. Juli 2009

1 Motivation

Wireless Local Area Network (WLAN) hat in unserer Gesellschaft mittlerweile einen hohen Stellenwert erreicht. Seit Herbst 2007 wurden im so genannten EMEA-Bereich, bestehend aus Europa, Mittlerer Osten, und Afrika, mehr Notebooks als Desktops verkauft. Dies umfasst bei einem Wachstum von 48 % gegenüber dem Vorjahr 11,2 Millionen Notebooks gegenüber 10,7 Millionen Desktops.[1] Es stehen alleine in Deutschland mehr wie 14.000 Hotspots zur Verfügung.[2] 46 % aller EU Haushalte nutzen mittlerweile ihren Internetanschluss über WLAN[3] und 54 % aller großen Unternehmen investieren mehr Geld in Funknetze für ihre Datenübertragung als in konventionelle Kabel.[4] Die Schattenseite daran folgt zugleich: Nur 47 % aller Unternehmen schützen ihr WLAN Netzwerk überhaupt durch geeignete Verschlüsselung wie zum Beispiel WEP, WPA, oder ähnlichem. Noch schlechter sieht es bei Intrusion Detection und Prevention Systemen aus, die bei weniger als 30 % der Unternehmen im Einsatz sind.[5] Aus diesen Gründen lohnt es sich einen Blick auf die Sicherheit von WLAN Netzwerken zu richten.

2 WLAN Standard

Fast immer wenn über WLAN geredet wird, ist damit der Standard 802.11 des Institute of Electrical and Electronics Engineers (IEEE) gemeint. Dieser Standard definiert WLAN seit 1997 und befindet sich in ständiger Weiterentwicklung. Zur Zeit besteht diese Familie offiziell aus 11 Normen. Dabei sind die Normen 802.11b und 802.11g beim Einsatz von WLAN am verbreitetsten. Als neuste Norm befindet sich 802.11n in der Entwicklung. Eine kleine Übersicht von den Normen zeigt den Trend zu höheren Datentransferraten auf. Dies ist

[1] Quelle: International Data Corporation (IDC)
[2] Quelle: Deutsche Presse Agentur (DPA), 2008
[3] Quelle: Deutsche Presse Agentur (DPA), 2008
[4] Quelle: Motorola, 2008
[5] Quelle: Motorola und Vanson Bourne, 2009

auch der Grund warum sich der Ursprungsstandard 802.11 nie durchgesetzt hat.

Standard	Datentransfer	Frequenz	Reichweite	Akzeptanz
802.11	2 Mb/s	ISM 2,4 GHz	n.a.	Veraltet
802.11a	54 Mb/s	5 GHz	10 - 15m	Geringe Verbreitung
802.11b	11 Mb/s	ISM 2,4 GHz	30 - 50m	Weite Verbreitung
802.11g	54 Mb/s	ISM 2,4 GHz	30 - 50m	Weltweit am verbreitetsten
802.11n	600 Mb/s	ISM 2,4 Ghz / 5Ghz	50 - 70m	Geräte schon verfügbar
802.11p	27 Mb/s	5,85 GHz	n.a.	Favorisiert vom C2C-CC

Standard	Bedeutung
802.11d	Anpassung an die regulatorischen Bestimmungen verschiedener Länder
802.11e	Unterstützung von Quality-of-Service
802.11f	Interoperabilität zwischen Basisstationen
802.11h	Reichweitenanpassung, Indoor- und Outdoor-Kanäle
802.11i	Erweiterungen bezüglich Sicherheit und Authentifizierung
802.11j	4,9 - 5 GHz Operation in Japan
802.11s (Draft)	Mesh-Netzwerke

Die Sendeleistung der einzelnen Normen wird in Deutschland durch die Bundesnetzagentur reguliert. Dabei darf auf ISM 2,4 GHz mit maximal 100mW und auf 5 GHz mit maximal 30mW (802.11a) bzw. 200mW (802.11h) gesendet werden. In anderen Ländern sind diese Maximalwerte wesentlich höher gelegt und gehen bis zu 1 Watt. ISM 2,4 GHz ist dabei wesentlich weniger stark reguliert als die 5GHz Frequenz. Ausserdem ist ISM kostenfrei nutzbar und dank der hohen Verbreitung fallen die Gerätekosten weitaus geringer aus als bei der 5 GHz Frequenz. Allerdings kommt es bei ISM 2,4 GHz zu mehr Störungen und Interferenzen da Bluetooth, Mikrowellen und ähnliche Geräte auf der selben Frequenz arbeiten. Ein störungsfreier Betrieb ist zu dem bei nur maximal 3 Netzwerken am selben Standort möglich (und zwar auf den Kanälen 1, 7, 13).

Die Übertragung an sich erfolgt dabei stets über Funkwellen obwohl der Standard auch Infrarot erlaubt. Das hat sich aber aufgrund der geringen Reichweite von nur 10 Metern nicht durchsetzen können. Es gibt für die Funkübertragung zwei verschiedene Verfahren auf der ISO-OSI Schicht 1 (Bitübertragung): Das Frequenzsprungverfahren Frequency Hopping Spread Spectrum und das heutzutage eingesetzte Bandspreizverfahren Direct Sequence Spread Spectrum.

Ein WLAN Netzwerk operiert entweder im Ad-hoc Modus, also von Endgerät zu Endgerät, oder über den weitaus verbreiteteren Infrastruktur Modus. Dabei wird ein Access Point als Brücke zwischen den Endgeräten eingesetzt. Die Brückenfunktion wird auf ISO-OSI Schicht 2 (Data Link Layer) umgesetzt. Access Points lassen sich auch zu einem Basic oder Extended Service Set zusammenfassen. Jeder Access Point hat ausserdem einen zugewissenen Service Set Identifier (SSID) welcher für die Kontaktaufnahme vom Endgerät zum Access

Point relevant ist. Ist ein Access Point im Modus Open Network, so akzeptiert er jegliche SSID bei der Kontaktaufnahme. Anders bei einem Closed oder Cloaked Network wo die SSID dem Endgerät bekannt sein muss. Allerdings sendet der Access Point im Closed Network Modus sogenannte Beacon Frames in regelmäßigen Abständen aus um sich bekannt zu machen. Ein Cloaked Network Access Point tut das nicht und antwortet auch nicht auf Endgeräte die mittels einer Probe Nachricht die SSID erfahren möchten.

3 WLAN Sicherheit

Da sich Funkwellen auch durch Mauern hindurch verbreiten, kann ein WLAN Netzwerk nicht auf gewisse Räumlichkeiten beschränkt werden. Daher ist die Sicherheit von WLAN extrem wichtig. Denn der Hacker Kongress DEFCON hat im Jahre 2005 einen Weltrekord beim Übertragen von WLAN Signalen auf 200 km mit handelsüblichen WLAN Karten und Parabolspiegeln aufgestellt. Selbst mit einfachsten Hilfsmitteln aus dem Baumarkt kann städtisch eine Abhörung über mehrere Hundert Meter realisiert werden.

Die Vermutung liegt jetzt natürlich nahe einfach die SSID von einem Cloaked Network Access Point als Passwort zu verwenden. Allerdings erfolgt die Kontaktaufnahme zu einem Access Point durch sogenannte Management Nachrichten welche immer im Klartext übertragen werden. Ein Angreifer kann so also die SSID abhören und danach selber verwenden. Eine Cloaked Network setzt also nur die Hemmschwelle für einen Angriff höher, trägt aber nicht zur eigentlichen Sicherheit bei. Das ist ein sehr gutes Beispiel für das kontroverse Prinzip Security over Obscurity.

Zudem sollten sich kritische Anwendungen nie auf WLAN verlassen, denn eine Denial of Service Attacke ist jederzeit durch das Design von WLAN möglich: Endgeräte müssen jederzeit mit Interferenzen rechen und verzögern ihre Datenübertragung für eine bestimmte Zeit bei Störungen. Sollte ein Angreifer nun in einer festen Zeitspanne Störsignale aussenden, kann keine Datenübertragung mehr stattfinden. Ausserdem besteht immer die Möglichkeit gezielt Endgeräte durch entsprechende Management Nachrichten vom Access Point abzumelden.

Neben dem Versuch eine gewisse Sicherheit durch Cloaked Networks zu erreichen, besteht die Möglichkeit nur gewisse Endgeräte über eine Zugriffskontrollliste der MAC Adressen zu realisieren. MAC Adressen werden aber zu jeder Zeit im Klartext übertragen. Das kann sich ein Angreifer zu nutze machen und gültige MAC Adressen abhören, die er dann in seiner WLAN Karte übernimmt um sich als ein anderes Endgerät auszugeben. Dieser Angriff ist auch unter MAC Spoofing bekannt.

Da sich Endgeräte immer mit dem Access Point mit der größten Signalstärke verbinden, ist es für einen Angreifer möglich einen Access Point mit identischer

SSID und einer Signalstärke über dem zulässigen Grenzwert aufzustellen um eine Man in the Middle Attacke zu realisieren. Dabei können Daten des Endgeräts zur späteren Analyse aufgezeichnet werden.

Um all diese Angriffe und Schwachstellen zu vermeiden, kann eine Verschlüsselung eingesetzt werden. Der Ursprungsstandard sieht dafür Wired Equivalent Privacy (WEP, 802.11) vor. Dieser wurde in 802.11i durch WPA (Wi-Fi Protected Access) bzw. WPA2 abgelöst. Es wird im folgenden trotzdem WEP zur Veranschaulichung einiger Designfehler aufgezeigt:

Zur Verschlüsselung teilen sich der Sender und Empfänger einer Nachricht M den gemeinsamen Schlüssel K. Der Sender berechnet daraufhin die Prüfsumme $CRC(M)$ (Cyclic Redundancy Check). Der Sender wählt einen 24 Bit langen Initialisierungsvektor IV. Mittels RC4 wird ein Schlüsselstrom $Key = RC4(IV|K)$ erzeugt. Mit dem Schlüsselstrom wird nun die Nachricht verschlüsselt: $C = (M|\ CRC(M)) \oplus Key$. Die verschlüsselte Nachricht C wird mit dem Initialisierungsvektor IV an den Empfänger übertragen. Der Empfänger generiert nun aus K und IV seinen eigenen Schlüsselstrom Key und entschlüsselt die Nachricht $C \oplus Key = M|\ CRC(M')$. Solle $CRC(M) = CRC(M')$ gelten, so ist diese korrekt.

Diese Vorgehensweise offenbart schon einige offensichtliche Design Fehler: WEP ist ein Shared Key Autentifikationsschema. Einzelne Benutzer sind also nicht individuell autentifizierbar. Der Schlüssel ist in der Praxis vielen Administratoren oder sogar allen Mitarbeitern eines Unternehmens bekannt. Dadurch verliert der Schlüssel seine Eigenschaft als Geheimnis und da kein Schlüsselmanagement vorgesehen ist, wird der Schlüssel nicht periodisch erneuert. Eine manuelle Schlüsselerneuerung ist dagegen sehr aufwendig und Kosten intensiv. Desweiteren ist WEP ein einseitiges Challenge-Response Protokoll. Das heißt, dass der Access Point sich gegenüber dem Endgerät nicht autentifizieren muss. Das kann für eine Man in the Middle Attacke, wie vorher beschrieben, ausgenutzt werden. Ausserdem ist CRC-32 eigentlich nur für Bitübertragungsfehler und nicht als starke Hashfunktion vorgesehen. Das kann sich ein Angreifer zu nutze machen und Nachrichten manipulieren, denn es gilt: $CRC(M \oplus M') = CRC(M) \oplus CRC(M')$. Dadurch kann der Angreifer sich eine Nachricht und Prüfsumme D bzw. $CRC(D)$ berechnen um gewisse Bits von M abzuändern: $C' = C \oplus (D|CRC(D))$. Da RC4 und CRC linear arbeiten ist das manipulieren einer Nachricht jederzeit möglich. Darüber hinaus gibt es weitere Angriffe auf WEP zum umlenken, einschleusen und entschlüsseln von Nachrichten. WEP Schlüssel können mittlerweile in unter 60 Sekunden entschlüsselt werden.

WEP sollte also nicht mehr zur Verschlüsselung eingesetzt werden. WPA bildet auch nur ein Übergansprotokoll von WEP auf das noch sichere WPA2, da der Standard 802.11i sehr umfangreich ist und nicht rechtzeitig fertig gestellt werden konnte.