

Sicherheit im Wireless LAN

Jessica Jobski
Fachbereich Informatik der Universität Hamburg (Student)
Vogt-Kölln-Straße 30
Hamburg, Germany

5jobski@informatik.uni-hamburg.de

ABSTRACT

Mit der steigenden Nachfrage nach Mobilität auch im Bereich der EDV wird die Vernetzung mobiler Systeme immer wichtiger. Dazu gibt es verschiedene Möglichkeiten, Funknetzwerke aufzubauen. Vorteile von Funknetzen sind die hohe Mobilität, Flexibilität und eine schnelle Installation. Aber es gibt häufig auch Probleme im Bereich der Sicherheit. In diesem Paper werden die so genannten WLANs (wireless local area networks) unter der Problemstellung betrachtet, wie eine sichere kabellose Übertragung von Daten gewährleistet werden kann.

Categories and Subject Descriptors

C.2.1 [Computer-Communication Networks]: Network Architecture and Design – *wireless communication*

D.4.6 [Operating Systems]: Security and Protection – *access controls, authentication*

K.6.5 [Management of Computing and Information Systems]: Security and Protection – *authentication, unauthorized access (e.g., hacking, phreaking)*

General Terms

Security

Keywords

WLAN

1. EINLEITUNG

In den vergangenen Jahren hat die Anzahl der WLANs weltweit zugenommen. Dass diese häufig leider nur unzureichend gesichert sind, wird regelmäßig von den so genannten 'Wardriven' gezeigt, die bei ihren Testfahrten in den Städten viele schlecht gesicherte WLANs finden – einige wenige WLANs werden sogar ungesichert in der Standardkonfiguration betrieben. Das, obwohl es bei den heutigen Accesspoints viele Möglichkeiten gibt, schnell eine Grundsicherheit herzustellen und damit die Sicherheit des WLANs zu erhöhen. Eine gute Möglichkeit zur Einarbeitung in dieses Thema bieten die Paper [1] und [2].

2. GRUNDSICHERHEIT

Bereits die WLAN-Geräte der ersten Generation boten Möglichkeiten an, eine Grundsicherheit des Netzwerkes herzustellen. Diese Optionen sind in heutigen Geräten immer noch (teilweise verbessert) zu finden und sollten für eine Grundsicherheit des WLANs genutzt werden.

2.1 SSID-Broadcast

Die SSID ist ein vom Administrator des WLANs beliebig gewählter Name zur Bezeichnung des WLANs. Häufig unterschätzt wird die Möglichkeit, das Senden der SSID im Accesspoint zu unterbinden, bei einer Testfahrt durch die Hamburger Innenstadt wurde von siebzig Prozent der empfangenen Accesspoints die SSID gesendet. Ein

Unterbinden des Sendens der SSID bewirkt, dass das WLAN u.a. unter Netstumbler (ein Programm, das die Funkwellen der WLANs auffängt und von Wardriven häufig genutzt wird um WLANs aufzuspüren) nicht mehr erkannt wird. Es ist zwar mit einigen Programmen trotzdem möglich, das WLAN zu finden, zumindest aber kann man verhindern, einige 'Gelegenheits'-Wardriver auf sich aufmerksam zu machen. Das bedeutet, es besteht eine geringere Gefahr, dass jemand versucht in das WLAN einzudringen. Bei Accesspoints, die immer die SSID senden, besteht immerhin noch die Möglichkeit, einen unauffälligen Namen für das WLAN zu wählen. Denn WLANs, bei denen ein Angreifer schon an der SSID erkennen kann, dass es sich um einen Hochgeschwindigkeits-Internetzugang handelt, haben einen höheren Reiz als ein WLAN mit unbekannter Geschwindigkeit und unbekanntem Standort bzw. Besitzer.

2.2 MAC-Adressen-Filter

Wenn es schon nicht möglich ist, ein WLAN gänzlich zu verstecken, kann man es doch potentiellen, ungebetenen 'Gästen' schwieriger machen, auf das Netzwerk zuzugreifen. So ist es bei den meisten heutzutage genutzten Accesspoints möglich, nur bestimmten WLAN-Karten den Zugriff zu erlauben. Dies funktioniert über die MAC-Adresse, die zur eindeutigen Identifikation eines Netzwerkgerätes in einem Netzwerk dient und im Accesspoint eingegeben werden kann. Andere als die dort aufgeführten Adressen werden abgelehnt. Allerdings ist bei den meisten WLAN-Karten die MAC-Adresse veränderbar (z.B. mit SMAC für Windows), sodass eine bei der Kommunikation zweier ins WLAN integrierter Geräte mitgelesene MAC-Adresse missbraucht werden kann, um auf ein durch MAC-Adressen-Filter geschütztes Netzwerk zuzugreifen.

2.3 WEP

Teil des WLAN-Standards IEEE 802.11 ist WEP. WEP bedeutet "Wired Equivalent Privacy" und ist eine Standard-Verschlüsselungsart für WLANs. WEP basiert auf dem RC4-Algorithmus. Wenn WEP verwendet wird, muss am Accesspoint und an den Clients jeweils derselbe Key (bestehend aus einem beliebigen Hex-Wert oder einer beliebigen Zeichenkette) definiert werden, um miteinander in Verbindung treten zu können. Abhängig vom Accesspoint kann ein 40 Bit oder 104 Bit oder bei einigen Geräten auch 232 Bit WEP-Key eingetragen werden. Von den Geräten wird der Key dann um 24 Bit erweitert und aus einem 40 Bit ein 64 Bit, aus einem 104 Bit ein 128 Bit und aus einem 232 Bit ein 256 Bit Key. Je länger der Key ist umso sicherer ist er. Um sich den WEP-Key leichter merken zu können gibt es auch Programme, welche bei den Accesspoint Konfigurations-Tools dabei sind und eine kurze Phrase in einen bestimmten Key wandeln.

WEP gilt jedoch schon lange als nicht besonders sicher und wurde bereits Ende 2001 erstmals geknackt [3]. Inzwischen kursieren eine Menge an Programmen im Internet

mit welchen WEP-Keys mit Hilfe von aufgezeichnetem Netzwerkverkehr geknackt werden können.

3. ERHÖHUNG DER SICHERHEIT

Spätestens als WEP geknackt wurde, wurde deutlich, dass neue Verschlüsselungstechniken entwickelt werden mussten, um das nun unsichere WEP abzulösen. Da dies aus Sicherheitsgründen schnell vor sich gehen sollte, wurde zuerst eine Verbesserung von WEP basierend auf demselben Verschlüsselungsalgorithmus entwickelt (WPA). Um auch in Zukunft sichere WLANs betreiben zu können, wurde später die Entwicklung des neuen Sicherheitsstandards IEEE 801.11i in Angriff genommen.

3.1 WPA

'WiFi Protected Access' (WPA) ist ein Verschlüsselungsverfahren, das die enormen Sicherheitsprobleme mit WEP bis zum Standard IEEE 802.11i überbrücken soll und über ein Softwareupdate auf den bisherigen Geräten lauffähig ist. WPA basiert ebenso wie WEP auf dem RC4-Algorithmus. Um eine höhere Sicherheit zu erreichen, wird eine Extensible-Authentication-Protocol (EAP) gestützte Authentifizierung genutzt, sowie das Temporal-Key-Integrity-Protocol (TKIP) für die Nutzung eines dynamischen Keys und PSK (Pre-Shared-Key) für die Authentifizierung von Nutzern. Dies steht im Gegensatz zu den besonderen Schwächen von WEP, nämlich der Nutzung eines konstanten Keys und die ungenügende Integritätssicherung. Außerdem werden nun die Daten im Funkverkehr durch den Message-Integrity-Check (MIC) auf ihre Vertrauenswürdigkeit geprüft. Hierzu werden die Datenpakete fortlaufend nummeriert und im verschlüsselten Teil mitgesendet. Wenn beim Empfänger Pakete ohne die richtige laufende Nummer ankommen, werden sie verworfen.

Da sich in diesem Fall kurz der Empfänger ausschaltet, besteht allerdings die Gefahr, dass der MIC missbraucht wird, um einen sogenannten Denial-of-Service (DOS) Angriff auf den Router auszuführen, also den Router durch wiederholtes Senden von Paketen mit falscher Nummer lahmzulegen.

3.2 WPA 2

Da die Schwächen des von WPA genutzten RC4-Algorithmus bereits veröffentlicht worden sind [4] wurde am 2. Februar die Erweiterung von WPA, WPA2 ins Leben gerufen, um WPA ersetzen zu können. WPA2 nutzt den Verschlüsselungsalgorithmus AES (Advanced Encryption Standard), der in den USA sogar für staatliche Dokumente mit höchster Geheimhaltungsstufe zugelassen ist, und implementiert die grundlegenden Funktionen des neuen Sicherheitsstandards IEEE 802.11i.

Für WPA2 ist ebenso wie bei WPA bisher nur die Möglichkeit von Passwortattacken bei den Pre-Shared-Keys bekannt, damit besteht solange kaum Gefahr für das Netzwerk, wie ein 'starker' Key genutzt wird, in dem kein Wort, aber Zahlen und Sonderzeichen vorkommen.

Ein Problem bei der Umstellung von WPA auf WPA2 wird allerdings insofern entstehen, als dass sie im Gegensatz zur Umstellung von WEP auf WPA nicht durch ein Firmwareupdate durchführbar ist. Denn für die neue AES Verschlüsselung ist zum Teil die Hardware zu langsam, so dass neue und am Anfang eventuell sehr teure Spezialhardware benötigt wird.

3.3 VPN

Ebenfalls als eine sehr sichere Lösung wird ein Virtual Private Network (VPN) betrachtet. Hierbei wird der Accesspoint vor einer Firewall angeschlossen, die nur verschlüsselte VPN-Daten in das lokale Netz und zum Server, dem VPN-Endpunkt

durchlässt. Erst die weitere Übertragung arbeitet dann unverschlüsselt (Abbildung 1). Der große Vorteil an der VPN-Lösung ist, dass man damit auch über das Internet einen sicheren Zugang in das eigene LAN aufbauen kann.

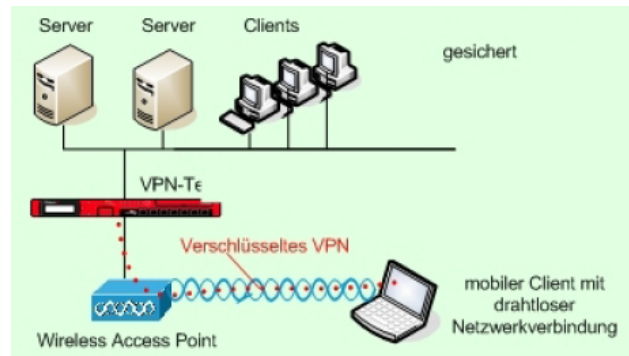


Abbildung 1: Zugriff auf lokales Netz über VPN [2]

4. AUSBLICK

Mit der Einführung von neuer Hardware, die dem IEEE 802.11i Standard entspricht, wird die Sicherheit von WLANs größer werden, auch, da dann nicht mehr der RC4-Algorithmus genutzt wird. Ob und wie schnell sich damit WPA2 durchsetzt wird man abwarten müssen, schließlich bedeutet es auch eine Neuanschaffung von Hardware, die vermutlich gerade Privatanwender am Anfang nicht tätigen wollen, besonders wenn ihr eventuell vorhandenes privates WLAN auch mit 'alter Technik' funktioniert und die Möglichkeit eines fremden Zugriffs als unwahrscheinlich und relativ ungefährlich (da der Eindringling nicht Zugriff auf äußerst vertrauliche Firmendaten bekommt) angesehen wird.

5. ABSCHLUSS

Die Sicherheitstechniken WPA und vor allem WPA2 als Ablösung von WEP als Verschlüsselungstechnik führen zu einer deutlich höheren Sicherheit der WLANs. Völlige Sicherheit wird es allerdings nicht geben können, solange nicht einige allgemeine Probleme von WLANs beseitigt werden: Zum einen ist es noch nicht möglich DoS-Attacken wirkungsvoll abzuwehren, zum anderen lässt sich die Ausbreitung von Funkwellen – die entscheidet, ob ein potentieller Eindringling überhaupt erst in Reichweite des WLANs gelangen kann – nicht gut kontrollieren, da sie von vielen Faktoren (z.B. Wänden und Mikrowellen) abhängt.

6. REFERENZEN

- [1] Bhagyavati, Summers, W. C., and DeJoie, A. Wireless security techniques: an overview. In *Proceedings of the 1st Annual Conference on Information Security Curriculum Development* (Kennesaw, Georgia, October 08 - 08, 2004), 82-87., InfoSecCD '04., New York, NY, 2004. ACM Press
- [2] Michael Lichtensteiger, Diplomarbeit: Wireless LAN - Sicherheit im Home- und KMU-Bereich. 2005. http://homepage.hispeed.ch/michiboa/docs/WLAN_Diplomarbeit.pdf, am: 08.01.2006.
- [3] Stubblefield, A., Ioannidis, J., and Rubin, A. Using the Fluhrer, Mantin, and Shamir attack to break WEP. In *Proceedings of the 2002 Network and Distributed Systems Security Symposium*, 17-22, 2002.
- [4] Fluhrer, S., Mantin, I., and Shamir, A. Weaknesses in the key scheduling algorithm of RC4. In *Eighth Annual Workshop on Selected Areas in Cryptography*, Toronto, Canada, 2001.