Sicherheitsempfehlungen für Public Wireless Hotspots

ECO − Verband der deutschen Internetwirtschaft e.V. Arbeitskreis WLAN / AG Sicherheit

Patrick Postel − Datenaura GbR
Holger Zuleger − Arcor AG

17. April 2003

Die Arbeitsgruppe Sicherheit im Arbeitskreis WLAN des Verbandes der deutschen Internetwirtschaft e.V. (ECO) beschäftigt sich mit dem Thema der unbedenklichen Datenübertragung mittels Wireless LAN. Wie das Wort „unbedenklich“ bereits ausdrückt, gilt es dabei nicht das sicherste aller möglichen Verfahren zu finden, sondern es wird eine Empfehlung gesucht, die eine Kombination aus Sicherheit und Praktikabilität darstellt. Alle Hinweise beziehen sich dabei ausschließlich auf das Umfeld der sogenannten „Public Hotspots“.
Ziel ist es, sowohl gegenüber den Betreibern als auch den Nutzern der Public Hotspots, Empfehlungen bezüglich der Authentifizierung, der Integrität und der Vertraulichkeit der Daten auszusprechen.

1. Sicherheit bei Public Wireless Hotspots

Bei der Beurteilung der Datensicherheit im Bereich von Wireless Hotspots wurden die folgenden Punkte berücksichtigt.

a. Authentifizierung
   Die Authentifizierung der beteiligten Kommunikationspartner ist Voraussetzung für die Datenintegrität das Accounting und die Datenverschlüsselung. Sie sollte immer beidseitig stattfinden (mutual authentication) um sog. Man-in-the-Middle Angriffe auszuschließen.

b. Datenintegrität
   Die Datenintegrität gewährleistet, dass über den einmaligen Authentifizierungsvorgang hinaus, eine Zuordnung der Datenpakete zu einer authentifizierten „Session“ möglich ist. Sie verhindert die Übernahme einer Session durch einen Angreifer und ist Voraussetzung für die Datenverschlüsselung und das Accounting.

c. Accounting
   Im Wesentlichen geht es hierbei um das sichere Erkennen des Start- und Endezeitpunktes einer Nutzersession sowie die korrekte Zuordnung der Datenpakete. Dies ermöglicht sowohl eine zeit- als auch volumenbasierte Abrechnung der Session. Voraussetzung für ein korrektes Accounting sind sowohl die Authentifizierung (Sessionstart), als auch die Sicherstellung der Datenintegrität, um einen Schutz gegen eine Sessionübernahme zu gewährleisten. Zusätzlich wird ein Mechanismus für die Signalisierung des Sessionendes benötigt.

d. Verschlüsselung
   Verschlüsselung ist die Gewährleistung der Vertraulichkeit der Daten gegenüber Dritten. Im Fall eines Public Hotspot kann die Verschlüsselung lediglich die Vertraulichkeit der Daten auf der Funkstrecke gewährleisten. Sie dient dazu, eine dem Dialzugang vergleichbare Sicherheit zu gewährleisten.
   Voraussetzung für die Verschlüsselung, ist eine beidseitige Authentifizierung sowie die Gewährleistung der Datenintegrität.

2. Verfahren zur Nutzerauthentifizierung bei Wireless Hotspots

Im folgenden sollen unterschiedliche technische Verfahren zur Nutzerauthentifizierung und Verschlüsselung bei Public Wireless Hotspots näher beleuchtet werden. Die Liste ist keineswegs vollständig sondern stellt eine Auswahl von sicheren und praktikablen Verfahren dar.

2.1 Webauthentifizierung

Wie durch den Namen bereits angedeutet, handelt es sich hierbei lediglich um ein Authentifizierungsverfahren. Es basiert auf einer Webschnittstelle, die über SSL/TLS verschlüsselt sein sollte. Über diese wird der Nutzer seine Zugangsdaten eingeben und bei erfolgreicher Authentifizierung wird die IP-Adresse des Client auf einem Access-Gateway (Paketfilter) zur Internetnutzung freigegeben. Dem Client muß bereits vor der Authentifizierung eine IP-Adresse zugeordnet werden. Dies geschieht in der Regel über DHCP.

Die Datenintegrität der Session beruht bei diesem Verfahren auf IP-Adressen. Bei einigen Realisierungen wird zusätzlich die Hardwareadresse (MAC-Adresse) überprüft.

Die Erkennung des Sessionendes erfolgt meist zeitgesteuert (Idletime) in Kombination mit einem Logout-Fenster.

Eine Verschlüsselung des Datenverkehrs ist verfahrensbedingt nicht möglich.

Der Vorteil des Verfahrens liegt in der einfachen Handhabung und der Möglichkeit, dem Benutzer eine Informationsplattform zur Verfügung zu stellen. Auch ein Zugriff auf eine „Free-Access-Area“ läßt sich damit relativ leicht realisieren. Dies dürfte zur Zeit das am weitesten verbreitete Verfahren sein.

2.2 PPTP (Point to Point Tunnel Protocol)

Dieses Protokoll wurde (unter anderem) von Microsoft für den Zugriff auf das Firmennetzwerk über Dailup-Netzwerke entwickelt. Es existieren zwei Versionen des Protokolls, wobei aufgrund von Sicherheitsproblemen in der ersten Version lediglich PPTPv2 zum Einsatz kommen sollte.

Die Authentifizierung erfolgt geschützt über MS-CHAPv2. Sie wird durch den Aufruf des Dial-Interfaces initiiert.

Die Gewährleistung der Datenintegrität erfolgt über kryptographische Verfahren. Jeglicher Datenverkehr wird bis zum Access-Gateway getunnelt und verschlüsselt übertragen.

Das Sessionende kann sehr gut erkannt werden, da der Client zu dem Authentifizierungssystem einen Tunnel aufbaut, der durch das Beenden des Dialerinterfaces wieder abgebaut wird.

Das Protokoll ermöglicht eine Verschlüsselung der Datenpakete. Das eingesetzte Verschlüsselungsverfahren gilt für die Verschlüsselung der Funkstrecke als ausreichend sicher, wenn mit 128 Bit Verschlüsselung, ausreichend langen Passworten, und MS-CHAPv2 gearbeitet wird [SMW].

Das gesamte Verfahren zur An- und Abmeldung entspricht der Vorgehensweise beim Einrichten eines DFÜ-Netzwerkes und dürfte daher vielen Nutzern bekannt sein.

2.3 WEP, 802.1x, WPA, TKIP, 802.11i

Diese Verfahren versuchen die Datenintegrität und eine Verschlüsselung auf der Funkstrecke zu gewährleisten. Hierzu ist eine Authentifizierung am AccessPoint[1] notwendig. Alle Verfahren arbeiten auf Layer 2, sodass lediglich ein authentifizierter Nutzer überhaupt einen Zugang zum Netz bekommt. Einen ersten Überblick über die Funktionsweise liefert [Cra] und [Puz].

Die genannten Verfahren sind jeweils Teilgebiete eines Mechanismus, der dazu gedacht ist eine Benutzerauthentifizierung durchzuführen (802.1x) und auf dieser Grundlage eine Verschlüsselung der Datenpakete (WEP) mit automatischer Schlüsseländerung (TKIP) zu erreichen. Die Zusammenführung dieser Teilaspekte nennt sich WPA und wird, nachdem die verwendeten Verschlüsselungsalgorithmen durch AES ersetzt wurden, im Standard 802.11i enden. Mit der Verabschiedung dieses Standards ist nicht vor dem vierten Quartal 2003 zu rechnen. Da das gesamte Verfahren auf einer leistungsfähigeren Verschlüsselung basiert, wird der Einsatz von neuer Hardware notwendig werden, wodurch sich die Einführung der Technik weiter verzögern wird.

Die zur Verfügung stehenden Authentifizierungsverfahren sind sehr vielseitig, allerdings eignen sich nicht alle für die Verwendung im Umfeld eines Public Hotspot. Als geeignete Verfahren sind lediglich EAP-TTLS, PEAP [Rei02] sowie SIM zu nennen. Der Verbreitungsgrad dieser Verfahren dürfte zur Zeit jedoch noch sehr gering sein.

---

1. Tatsächlich wird der AccessPoint die Authentifizierungsdaten lediglich zu einem Authentisierungsserver (Radius) weiterleiten. Die Authentifizierung erfolgt daher eigentlich gegenüber dem Authentisierungsserver und nicht gegenüber dem AccessPoint.

Verfahren	Authentifizierung		Dyn. WEP-Key	Hotspot geignet	Standard
	von	über			
EAP-MD5	Client	hashed Passwort	nein	schlecht	RFC2284
EAP-TLS	Client/Server	Zertifikate	ja	schlecht	RFC2716
EAP-TTLS	Client	Passwort o.ä.	ja	sehr gut	draft-ietf-ppext-eap-ttls(01)
	Server	Zertifikat			
PEAP	Client	MS-Chap Passwort	ja	sehr gut	draft-josefsson-pppext-eap-tls-eap(05) (Cisco/Microsoft)
	Server	Zertifikat			
OTP Generic Token	Client	One Time Passwort Token	nein	bedingt	draft-ietf-eap-otp(00)
EAP-SIM	Client/Server	GSM SIM-Card	ja	sehr gut	draft-haverinen-pppext-eap-sim(03) (Nokia)
Kerberos	Client/Server	3DES-Key	ja	schlecht	draft-aboba-pppext-eapgss(12)

Die eingesetzten Verfahren zur Gewährleistung der Datenintegrität sind nicht ohne Mängel, aber für den vorgesehenen Verwendungszweck ausreichend und bei weitem sicherer, als Verfahren die lediglich auf IP-Adressen beruhen.

2.4 IPsec

IPsec bietet eine beidseitige Authentifizierung der Kommunikationspartner, die in der Regel auf Zertifikaten basiert. Dies stellt im Umfeld eines Public Hotspot ein gewisses Hindernis dar, da dem Clientsystem vorab keine Zertifikate zugeordnet werden können. Die Authentifizierung über Serverzertifikat und Benutzername (Hybrid XAUTH), die im Umfeld eines Public Hotspot geeignet wäre, ist zur Zeit nicht standardisiert [Phi]. Sogenannte „Shared-Secret“ Authentifizierung ist für diesen Anwendungszweck völlig ungeeignet.

Die Datenintegrität wird durch starke kryptographische Verfahren gewährleistet.

Das Sessionende kann gut erkannt werden, da die meisten IPsec-Clients eine Möglichkeit bieten die IPsec-Verbindung explizit zu beenden.

Zur Verschlüsselung stehen diverse als sicher einzustufende Verfahren zur Verfügung.

Aus sicherheitstechnischer Sicht handelt es sich hierbei um das beste Verfahren. Allerdings ist es für die Absicherung der Funkstrecke nur eingeschränkt verwendbar, da die Authentifizierungsverfahren für dieses Einsatzgebiet nicht geeignet sind.
Für den Zugriff des Nutzers auf ein Firmennetz wird ebenfalls der Einsatz von IPsec-Software erforderlich sein. In diesem Fall müßte IPsec in IPsec getunnelt werden. Dies ist zwar prinzipiell möglich, stellt sich allerdings aus Sicht des Anwenders recht kompliziert dar.

2.5 Zusammenfassung der unterschiedlichen Verfahren

Das zur Zeit am häufigsten anzutreffende Verfahren zur Nutzerauthentifizierung an Wireless Public Hotspots, die Authentifizierung über eine Webschnittstelle, bietet aus sicherheitstechnischer Sicht leider die geringsten Möglichkeiten. Insbesondere ist keine Verschlüsselung der Funkstrecke zu erreichen. Dies mag für viele Anwendungen ausreichend sein, setzt jedoch eine hohe Eigenverantwortung und auch technisches Know How auf Seiten der Nutzer voraus, da kritische Anwendungen (z.B. Email) auf Applikationsebene verschlüsselt werden sollten.

Die für das Anwendungsszenario aus sicherheitstechnischer Sicht beste Lösung stellt das 802.11i Verfahren dar. Es bietet eine praktikable und sichere Authentifizierung sowie eine ausreichende Sicherheit um die Funkstrecke zu verschlüsseln. Für die Gewährleistung der Vertraulichkeit der Daten bis zum Endsytem, sollte der Nutzer bei Bedarf zusätzliche Verfahren anwenden (z.B. IPSec).
Leider kann zur Zeit weder von einer Verfügbarkeit der Technik ausgegangen werden, noch von einer breiten Akzeptanz auf Anwenderseite. Da es sich hierbei jedoch um einen Standard handelt, ist zu erwarten, dass sich dies in absehbarer Zeit ändern wird. Auch die vermehrte Nutzung im privaten Bereich dürfte die Akzeptanz der Technik erhöhen.

In der Zwischenzeit sollte jede Möglichkeit genutzt werden um dem Benutzer eine größere Sicherheit anzubieten. Das PPTP-Verfahren ist hierfür hervorragend geeignet.

IPsec ist unerlässlich um eine Vertraulichkeit der Daten für den Nutzer zu gewährleisten. Allerdings scheint es für die Absicherung der Funkstrecke eher ungeeignet zu sein. Um den Zugang zu einem Firmennetzwerk über ein VPN-Gateway zu verschlüsseln ist es jedoch ein ideales und etabliertes Verfahren. Die technische Realisierung des Public Hotspot sollte so beschaffen sein, dass einem Einsatz von IPsec von Seiten des Nutzers nichts im Wege steht.

3. Richtlinien

Die ausgeführten Überlegungen sollen in Form von einfachen Richtlinien, sowohl für die Hotspot Betreiber als auch für die Hotspot Nutzer zusammengefasst werden.

3.1 Sicherheitsempfehlungen für Wireless Hotspot Betreiber

- Die Authentifizierungsdaten sollten über die Funkstrecke immer verschlüsselt übertragen werden. Bei der Übertragung der Daten zu den Authentifizierungssystemen (RADIUS-Server) über öffentliche Netze sind geeignete Verschlüsselungsverfahren anzuwenden (SSL, IPsec).
- Die für das Authentifizierungssystem verwendeten Zertifikate sind von einer geeigneten Zertifizierungsinstanz zu signieren. Der Fingerprint des Serverzertifikats ist zu veröffentlichen.
- Die eingesetzten Sicherheitsverfahren sollten dem Nutzer vorab, spätestens jedoch nach erfolgter (sicherer) Authentifizierung in Form eines Sicherheitshinweises bekannt gemacht werden. Dabei sollte der Nutzer auf die Risiken der Nutzung einer Funkstrecke hingewiesen werden. Ein Verweis auf eine Webseite ist hierfür als ausreichend anzusehen.
- Um die Privatsphäre des Nutzers zu schützen, sollte der Hotspot Betreiber mindestens ein geeignetes Verfahren zur Verschlüsselung der Funkstrecke anbieten.
- Die Nutzung dieser Verschlüsselung kann optional sein, insbesondere wenn das Verfahren zusätzliche Software auf der Clientseite voraussetzen würde.
- Der Nutzer ist auf die Möglichkeit der verschlüsselten Übertragung hinzuweisen.
- Für die Gewährleistung einer korrekten Abrechnung (accounting) sollten geignete Verfahren zur Datenintegrität eingesetzt werden.
- Der Aufbau des Public Wireless Hotspot und die eingesetzte Technik darf die Verwendung von Verschlüsselungssoftware (z.B. IPsec) auf Nutzerseite nicht behindern (NAT oder PAT).

3.2 Sicherheitsempfehlungen für Wireless Hotspot Nutzer

Jeder Nutzer eines Wireless Hotspot sollte sich über seine Sicherheitsanforderungen im Klaren sein und danach entscheiden ob, bzw. unter welchen Bedingungen eine Nutzung des Hotspot möglich ist.

Einige allgemeine Richtlinien sollen den Hotspot Nutzer dabei unterstützen:

- Die Authentifizierung an dem Wireless Hotspot sollte immer verschlüsselt erfolgen. Eine Ausnahme kann die Verwendung einer zeitlich limitierten Prepaid-Karte darstellen, allerdings nur dann, wenn die Nutzungsdauer nicht unterbrochen werden kann. In diesem Falle kann auch eine unverschlüsselte Authentifizierung akzeptiert werden, da die Userkennung als eine Art One-Time-Passwort angesehen werden kann.
- Der Nutzer sollte die Korrektheit des von der Authentifizierungsstelle vorgelegten Zertifikats überprüfen. Hierzu zählt die Überprüfung des Fingerprints, die Gültigkeitsdauer, den Inhaber sowie die Zertifizierungsinstanz des Zertifikates.
- Eine Nutzung des Wireless Hotspot ohne Verschlüsselung auf der Funkstrecke kann lediglich empfohlen werden, wenn auf eine Übertragung von personenbezogenen Daten (Passwörter, Email) verzichtet wird. Jeder Nutzer muß dabei selbst definieren wie groß seine Privatsphäre ist. Der Nutzer sollte sich immer bewußt sein, dass der gesamte Datenverkehr mit einfachsten Mitteln für jedermann im Funkbereich des Hotspot einsehbar ist.

- Für personenbezogene Daten (Passwörter, Email) sind unbedingt zusätzliche Vorkehrungen, z.B. durch eine Verschlüsselung auf Anwendungsebene durchzuführen. Ein Beispiel hierfür ist das sichere Bearbeiten von Emails über eine HTTPS Webschnittstelle bzw. über die hierfür vorgesehenen sicheren Internetprotokolle (Secure POP, IMAPS, SMTP mit TLS).
- Ist die Funkstrecke des Hotspots verschlüsselt, **kann** auf die Verschlüsselung auf der Applikationsebene verzichtet werden. Die Übertragung von Passworten sollte jedoch auch hierbei, wie generell im Internet, **nicht** im Klartext erfolgen. Die Nutzung von CHAP oder MD5 Passworten wird **dringend** empfohlen. Die Sicherheit eines Hotspots mit verschlüsselter Datenübertragung entspricht in etwa der eines Dialup-Internetzugangs.
- Die Nutzung eines Wireless Hotspots zum Zugriff auf ein Firmennetzwerk sollte **ausschließlich** über eine verschlüsselte Verbindung zu dem vertrauenswürdigen Access-Gateway der Firma erfolgen [BSI]. Eine Verschlüsselung der Funkstrecke ist hier **keinesfalls** als ausreichend anzusehen.

4. Adressen und Literaturverzeichnis

[Rei02] *A Technical Comparison of TTLS and PEAP*, O'Reilly, Oktober 2002
http://www.oreillynet.com/pub/a/wireless/2002/10/17/peap.html

[BSI] *Sicherheit im Funklan (WLAN, IEEE 802.11)*,
Bundesamt für Sicherheit in der Informationsverarbeitung, Juni 2002
http://www.bsi.de/fachthem/funk_lan/wlaninfo.pdf

[SMW] B. Schneier, Mudge, D. Wagner,
Cryptanalysis of Microsoft's PPTP Authentication Extensions (MS-CHAPv2), Oktober 1999
http://www.counterpane.com/pptpv2.pdf

[Cra] J. Philip Craiger, *802.11, 802.1x and Wireless Security* , Juni 2002
http://www.sans.org/rr/wireless/80211.php/

[Abo] Bernard Aboba, *The Unofficial 802.11 Security Web Page*, März 2000
http://www.drizzle.com/˜aboba/IEEE/

[Puz] Rita Puzmarova, *Wireless Hotspot Security*, Computer Bits, Februar 2003
http://www.computerbits.com/archive/2003/0200/hotspotsecurity.html

[Phi] Lisa Phifer, *The Remote Access Condrum Part1: Extended Authentication*,
internet.com ISP-Planet, November 2000
http://www.isp-planet.com/technology/remote_access_conundrum-1-1.html

Verband der deutschen
Internetwirtschaft e.V.
Arenzhofstraße 10
50769 Köln
info@eco.de

Patrick Postel
Datenaura GbR
Pinnasberg 29-33
20359 Hamburg
postel@datenaura.com

Holger Zuleger
Arcor AG
Alfred-Herrhausen-Allee 1
65760 Eschborn
Holger.Zuleger@arcor.net