

Rechtliche Aspekte beim Einsatz eines WLAN

Telemed 2003, 08. November 2003 in Berlin

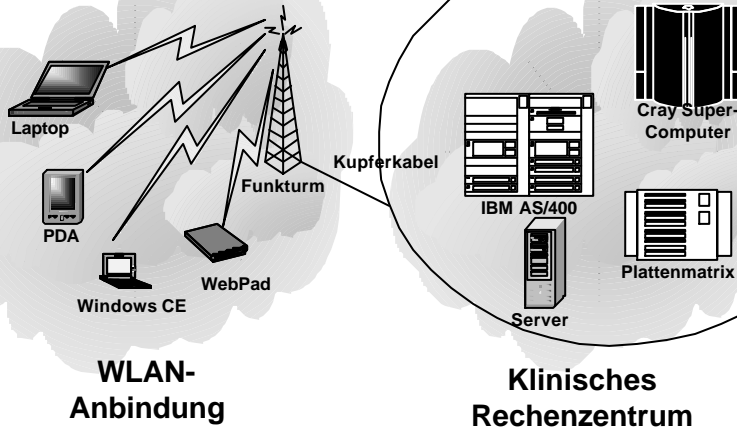
B. Schütze, M. Kroll, T. Geisbe, T. J. Filler

Sie erwartet im Folgenden

- Motivation
- Normative Regelungen
- Datenschutz-Aspekte
- Folgerung(en)
- Zusammenfassung

Motivation

Das Gute am WLAN:
es ist überall kabellos verfügbar



Motivation

Das Schlechte am WLAN:
es ist überall kabellos verfügbar



Übersicht Normen

Notwendig für eine CE-Zulassung

- a) Elektromagnetische Verträglichkeit und
Funkspektrumangelegenheiten (ERM:
EN 300 328-2 v.1.1.1 (7-2000)
- b) Gesetz über die elektromagnetische Verträglichkeit
von Geräten“ (EMVG)
- c) Zulassungsvorschrift für Funkanlagen für Breitband-
Datenübertragungen im Frequenzbereich 2400 -
2483,5: BAPT 222 ZV 126

Übersicht Normen

Vorgeschrieben beim Einsatz eines WLAN im medizinischen Umfeld

- d) Einrichtungen der Informationstechnik in medizinischer
Anwendung: EN 60601-1-2
- e) Grenzwerte und Messverfahren für Funkentstörung:
EN 55011 (1991) bzw. DIN EN 55011 (1997)
- f) Änderung A1 zu EN 55011:
EN 55011/A1 (1997) bzw. DIN EN 55011 A1 (1997)
- g) Änderung A2 zu EN 55011:
EN 55011/A2 (1996) bzw. DIN EN 55011 A2 (1996)
- h) Funk-Entstörung von elektrischen Betriebsmitteln und
Anlagen:
EN 55014 (1993) bzw. DIN EN 55014 (1993)

Übersicht Normen

Normen, die dem Personenschutz dienen –
eine Einhaltung ist nicht vorgeschrieben

- i) Sicherheit in elektromagnetischen Feldern - Schutz von Personen
DIN VDE 0848, Teil 2 (Oktober 1991)
- j) Schutz von Personen mit aktiven Körperhilfsmitteln im Frequenzbereich 0Hz bis 300GHz
DIN VDE 0848, Teil 3 (Mai 2002)
- k) 26. Verordnung zum Bundes-Immissionsschutzgesetz (26.BImSchV), Frequenzbereich 10 MHz bis 300 GHz

Normen und Anbieter (1)

Kriterien zur Herstellerwahl von
WLAN-Hardware:

- Unterstützung von Standard-PC-Software
- Unterstützung von 802.11b und 802.11g
- Möglichkeit zum Aufrüsten auf die kommenden Standards, insbesondere auf die schon angekündigten Standards 802.11h und 802.11i
- Authentisierung von MAC-Adressen
- Broadcast deaktivierbar
- Administration über http und Telnet möglich

Normen und Anbieter (2)

Von 44 Herstellern blieben 6 potentielle Anbieter übrig:

Anbieter	Normenerfüllt
1st Wave	Ja
3Com	Ja
Artem	Ja
Cisco Systems	Ja
Lancom Systems	Nein, sind aber z. Zt. im Zertifizierungsprozess
Zyxel	Ja

Datenschutzbestimmungen

Musterberufsordnung (MBO)
Bundesdatenschutzgesetz (BDSG)
Landesdatenschutzgesetz (LDStG)
Landeskrankenhausgesetz (LKHG)
Telekommunikationsdatenschutzgesetz
Ggf. Krankenhausdatenschutzgesetz
Ggf. Gesundheitsdatenschutzgesetz
Ggf. Katholisches Datenschutzgesetz
Ggf. Evangelisches Datenschutzgesetz

Geheimniswahrung

- Zeugnisverweigerungsrecht des Arztes (§53 Abs.2.1 StPO)
- Beschlagnahmeverbot von Patientendaten (§97 Abs.1 StPO)
- Eingeschränktes Durchsuchungsrecht (§103 Abs.1 StPO)
- Verpflichtung zur Geheimniswahrung des Arztes (§203 Abs.1 StGB)



Sicherheit im WLAN (1)

Wired Equivalent Privacy

WEP nutzt RC4 zur Verschlüsselung → potentiell unsicher:
Die Projektgruppe „Local Wireless Communication“ des Bundesamtes für Sicherheit in der Informationstechnik (BSI) hat bei einer Übertragungsgeschwindigkeit von 5 Mbit/s und einer Datenmenge von 2,86 GB im Juli 2002 nur **10 Minuten** zur Entschlüsselung benötigt.

Sicherheit im WLAN (1)

Wired Equivalent Privacy

Authentisierung mittels MAC-Adressen

Mac-Adressen können mittels gängiger Tools gefälscht werden, ein Sniffen des Netzwerkverkehrs ermöglicht das Herausfinden einer zu fälschenden MAC-Adresse.

Sicherheit im WLAN (1)

Wired Equivalent Privacy

Authentisierung mittels MAC-Adressen

Verbergen der ESSID

Das Verbergen der Extended Service Set Identifier (ESSID) bringt nur wenig Schutz, da beim Handshake die ID im Klartext übermittelt wird.

D.h. der Angreifer kann die ESSID durch Protokollierung des Netzwerk-Verkehrs schnell in Erfahrung bringen.

Sicherheit im WLAN (1)

Wired Equivalent Privacy

Authentisierung mittels MAC-Adressen

Verbergen der ESSID

IEEE 802.11i

Zur Schlüsselverwaltung und -verteilung für AES (Advanced Encryption Standard) setzt IEEE 802.11i wiederum IEEE802.1x voraus (Abwärtskompatibilität). Letztlich daher nur wenig sicherer als IEEE802.1x.

Sicherheit im WLAN (2)

The screenshot shows a web browser window with the address bar containing the URL `http://security-protocols.com/library/wireless/ssid_defaults-1.0.5.txt`. The main content area displays technical specifications for three types of wireless devices:

- 3com AirConnect 2.4 Ghz DS (never 11mbit, Harris/Intersil Prism based)**
 - Default SSID: `comcomcom`
 - Notes: No known (yet) telnet/http/tftp/etc management passwords, or states of IP configuration.
- Aironet 900MHz/2.4GHz BR1000/e, BR5200/e and BR4800**
 - Also known as Aironet 630/640 (for 900 MHz) and Aironet 340 for 2.4 GHz DSSS
 - Default SSID: `2` (default for all 900 MHz gear, often reused)
 - Default SSID: `tsunami` (seems to show up randomly)
 - Console Port: No Default Password
 - Telnet password: No Default Password
 - HTTP management: On by default, No Default Password
 - NOTES: There is no IP address given to the bridge(s) by default, the user will need to have enabled/setup one. However, once you have the MAC of the bridge, rarp'ing the IP address out of it is trivial, if it's been assigned one. Also, if the bridge can be forceably restarted, default settings will allow the bridge to receive an IP address via BOOTP and/or DHCP. Introducing a rouge server way allow the device to gain a more or less known IP in the case of rarp not working.
- BayStack 650/660 802.11 DS AP**
 - Default SSID: `"Default SSID"`
 - Default admin pass: `<none>`
 - Default Channel: `1`
 - MAC addr: `00:20:d8:XX:XX:XX`

Sicherheit im WLAN (3)

Internet Explorer browser window showing a website with a table of wireless nodes and a topographic map of Berlin.

ID	Name	Ort	Karte	ifs	Status	Alter
76	angeldamm	Kreuzberg/Mitte			wartet	
7	l3	Friedrichshain			vollap	148d
8	subnet	Friedrichshain			aufbau	341d
79	rs10	Mitte			aufbau	294d
12	themm	Mitte			voll	346d
?	berlinwireless	Friedrichshain			vollap	283d
?	Wöhlichstr.8	Fhain			wartet	
14	gart23	Fhain			kein_node	327d
19	s20f	FHAIN			aufbau	4d
21	workan	Prenzlauer Berg			vollap	190d
24	mikromag				aufbau	
25	jung19	Fhain			wartet	320d
26	treptow-net				vollap	
27	BambiBar	Prenzlauerberg			vollap	309d
28	pirates	FHAIN			aufbau	306d
29	Holteistr.13	Friedrichshain			interessiert	
30	nuka				wartet	190d
31	hennar				wartet	196d
32	antennenschirmade	fhain			aufbau	258d
33	Kreisausdian	Berlin			vollap	246d
34	W18	Berlin			wartet	233d
35	42box	fhain			aufbau	202d
36	Wlan-Family.org	Berlin-Kreuzberg			testbetrieb_ap	219d
37	leo34	Lichtenberg			vollap	19d
38	dan17	Berlin-Friedrichshain			wartet	204d
39	Jung_42				wartet	202d
40	bsdgeeks	Tiergarten			wartet	196d
41	Wlan_Trebar	Berlin			aufbau	173d
42	box110	Berlin			wartet	148d
43	mkip-weissensee				offline	134d
44	WlanHain			1	vollap	8d
45	WlanHain2			1	vollap	8d

The right side of the browser shows a topographic map of Berlin with various WLAN nodes marked. The map includes labels for districts like Kreuzberg, Prenzlauer Berg, and Friedrichshain, and major roads like the A10 and A100. A scale bar indicates 5 km.

Sicherheit im WLAN (4)

Internet Explorer browser window showing a forum post from WarDriving-Forum.de.

WarDriving-Forum.de
Deutschlands WarDriving-Forum
WarDriving in Deutschland

wardriving-forum.de im IRC:
#wardriving_germany

wardriving-forum.de [Board Regeln](#)

Leckere 200K downstream am Potsdamer Platz

new topic | post reply | WarDriving-Forum.de Foren-Übersicht -> Wardriving in Berlin

Vorheriges Thema anzeigen :: Nächstes Thema anzeigen

Autor	Nachricht
Kasmus	<p>Verfasst am: Do Okt 16, 2003 1:01 am Titel: Leckere 200K downstream am Potsdamer Platz</p> <p>Hallo zusammen,</p> <p>Am Potsdamer Platz steht im SonyStyle Laden in der zweiten Etage ein offener, unverschlüsselter 11Mbit/s AP, der über den ganzen Innenhof rund um den Brunnen vor dem CineStar/IMAX strahlt.</p> <p>Wir hatten heute Downloadgeschwindigkeiten um die 200K (getestet mit http://kernel.org/pub/linux/kernel/v2.4/linux-2.4.22.tar.bz2).</p> <p>Die IPs werden aus dem Range 192.168.44.9-? wie üblich per DHCP vergeben.</p> <p>.1 bis .8 sind für einen Cisco Router reserviert.</p> <p>Auf der .1 läuft das Gateway und als besonderes Leckerli haben die Herren Admins auf der .8 auf Port 80 das HTTP-Interface des Cisco Routers offen gelassen, so dass man problemlos alle Parameter *lesen* kann. Hehe.</p>

Information about the author Kasmus:
Anmeldungsdatum: 16.10.2003
Beiträge: 2
Wohnort: Berlin & Umgebung :)

Folgerungen

- Nicht jeder Hersteller liefert Hardware, mittels derer im medizinischen Umfeld ein WLAN aufgebaut werden darf.
- Die Schutzmechanismen des Standards reichen zum Schutz der Patientendaten nicht aus.
- Daher müssen proprietäre Maßnahmen zum Schutz der Daten getroffen werden.

Schutzmaßnahmen

z.B. ein VPN wird aufgebaut....

IPSec-VPN mit Linux
und FreeSWAN

(K)ein PPTP



z.B. verschlüsselter Datentransfer....

durch ein Java-Applet mit
Cryptix oder BouncyCastle



Zusammenfassung

- Wenige Hersteller erfüllen die normativen Anforderungen zum Einsatz eines WLAN im medizinischen Umfeld.
→ sorgfältige Anbieter-Auswahl erforderlich
- Daten aus dem Gesundheitswesen müssen vor unbefugtem Zugriff geschützt werden.
- Die im WLAN-Standard z. Zt. enthaltenen Verfahren gewährleisten keinen Schutz.
- Zur Nutzung eines WLANs müssen weitergehende Maßnahmen ergriffen werden, z.B. Implementierung eines Virtual Private Network (VPN).

Literatur

1) Normen:

Sämtliche Normen sind im Beuth-Verlag erhältlich:

<http://www.beuth.de>

2) Datenschutz:

a) Bücher

- Hermeler AE (2000) Rechtliche Rahmenbedingungen der Telemedizin. Verlag C. H. Beck, ISBN 3 406 46875 6
- Dierks C, Feussner H, Wienke A (2001) Rechtsfragen der Telemedizin. Springer Verlag, ISBN 3-540-67927-8
- Datenschutz-Jahrbuch (2002) Datakontext-Fachverlag, ISBN 3-89577-220-8
- Klug C (2002) BDSG-Interpretationen. Datakontext-Fachverlag, ISBN 3-89577-255-0
- Geis I, Helfrich M (2003) Datenschutzrecht. Verlag C. H. Beck, ISBN 3 406 470742

2) Datenschutz:

b) Journals

- (Muster-)Berufsordnung für die deutschen Ärztinnen und Ärzte (1997) Deutsches Ärzteblatt 94 (37): A2354 – A 2363
- Rieser S (1999) Ärztliche Schweigepflicht: Druck von allen Seiten. Deutsches Ärzteblatt 96 (17): A253 – A 254
- Jentsch P (2001) Transparenzgesetz: Datenschützer laufen Sturm. Können sie den -glasernen Arzt- verhindern? Fortschr. Med. 43(8): 50 – 51
- Ulsenheimer K.(2003) Wenn der Staatsanwalt kommt - Rechte und Pflichten des Arztes bei einer Durchsuchungsaktion. Manuelle Medizin 41: 129 – 133
- Wienke A, Sauerborn J (2000) EDV-gestützte Patientendokumentation und Datenschutz in der Arztpraxis. MedR 11: 517 - 519

2) Datenschutz:

c) Internet-Adressen

- Datenschutzbeauftragte
(Bundesbeauftragte für Datenschutz <http://www.bfd.bund.de/>,
Bayern <http://www.bayern.de/DSB/>,
Berlin <http://www.datenschutz-berlin.de/>,
Brandenburg <http://www.brandenburg.de/land/lfdbbg/>
Rheinland Pfalz <http://www.info-mainz.de/datenschutz-rp/>,
Niedersachsen <http://www.lfd.niedersachsen.de/>,
NRW <http://www.lfd.nrw.de/>,
Niedersachsen <http://www.lfd.niedersachsen.de/>
Hamburg <http://www.hamburg.de/Behoerden/HmbDSB/>
Hessen <http://www.hessen.de/hdsb/>
Saarland <http://www.datenschutz.hessen.de/>)
- Evangelische Kirche http://www.ekd.de/datenschutz/1618_4586.html
- Katholische Kirche <http://www.datenschutz-kirche.de/>
- Virtuelles Datenschutzbüro [http://www.datenschutz.de/\(de\)/](http://www.datenschutz.de/(de)/)

3) WLAN-Sicherheit:

- Fluhrer S, Mantin I, Shamir A. [Online] Weaknesses in the Key Scheduling Algorithm of RC4 [zitiert 2003 Oktober 22]; Verfügbar unter <http://citeseer.nj.nec.com/fluhrer01weaknesses.html>
- Stubblefield A, Ionnidis J, Rubin AD [Online] Using the Fluhrer, Martin and Shamir Attack to break WEP [zitiert 2003 Oktober 22]; Verfügbar unter http://www.cs.rice.edu/~astubble/wep/wep_attack.html
- Borisov N, Goldberg I, Wagner D [Online] Intercepting Mobile Communications – The Insecurity of 802.11 [zitiert 2003 Oktober 22]; Verfügbar unter <http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf>
- Vogelsberger M. (2003) Kismet & Co. – WLAN-Sicherheit unter der Lupe. Linux Magazin 12: 36 – 43
- Yoshihiro A, Nakata N, Harada J, Tada S (2002) Wireless local area networking for linking a PC reporting system and PACS: clinical feasibility in emergency reporting. Radiographics 22(3): 721 - 728

**Vielen Dank
für Ihre
Aufmerksamkeit!**

Kontakt: schuetze@medizin-informatik.org