Rechtliche Aspekte beim Einsatz eines WLAN

Telemed 2003, 08. November 2003 in Berlin

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

Fachhochschule
Dortmund
University of Applied Sciences

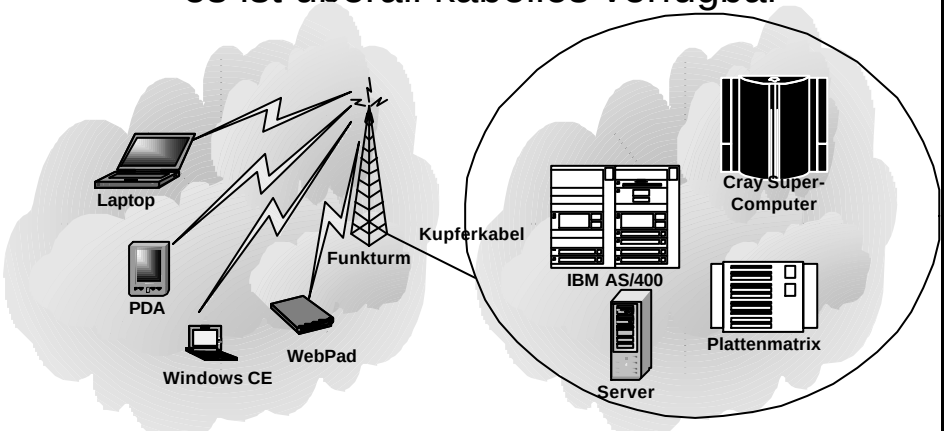
Sie erwartet im Folgenden

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

Fachhochschule
Dortmund
University of Applied Sciences

Motivation

Das Gute am WLAN:
es ist überall kabellos verfügbar



WLAN-Anbindung

Klinisches Rechenzentrum

Fachhochschule
Dortmund
University of Applied Sciences

Motivation

Das Schlechte am WLAN:
es ist überall kabellos verfügbar

Fachhochschule
Dortmund
University of Applied Sciences

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

Fachhochschule
Dortmund
University of Applied Sciences

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)

Fachhochschule
Dortmund
University of Applied Sciences

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

Fachhochschule
Dortmund
University of Applied Sciences

Normen und Anbieter (1)

Kriterien zur Herstellerauswahl 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

Fachhochschule Dortmund
University of Applied Sciences

Normen und Anbieter (2)

Von 44 Herstellern blieben 6 potentielle Anbieter übrig:

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

Fachhochschule Dortmund
University of Applied Sciences

Datenschutzbestimmungen

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

Fachhochschule
Dortmund
University of Applied Sciences

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)

Fachhochschule
Dortmund
University of Applied Sciences

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.

Fachhochschule
Dortmund
University of Applied Sciences

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.

Fachhochschule
Dortmund
University of Applied Sciences

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 Erefahrung bringen.

Fachhochschule
Dortmund
University of Applied Sciences

Sicherheit im WLAN (1)

Wired Equivalent Privacy

Authentisierung mittels MAC-Adressen

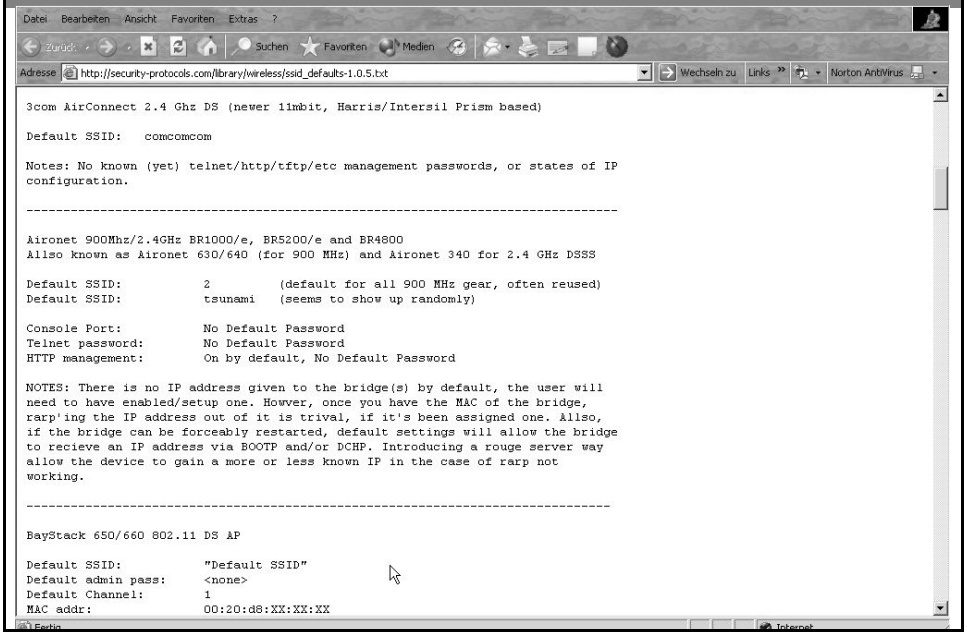
Verbergen der ESSID

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.

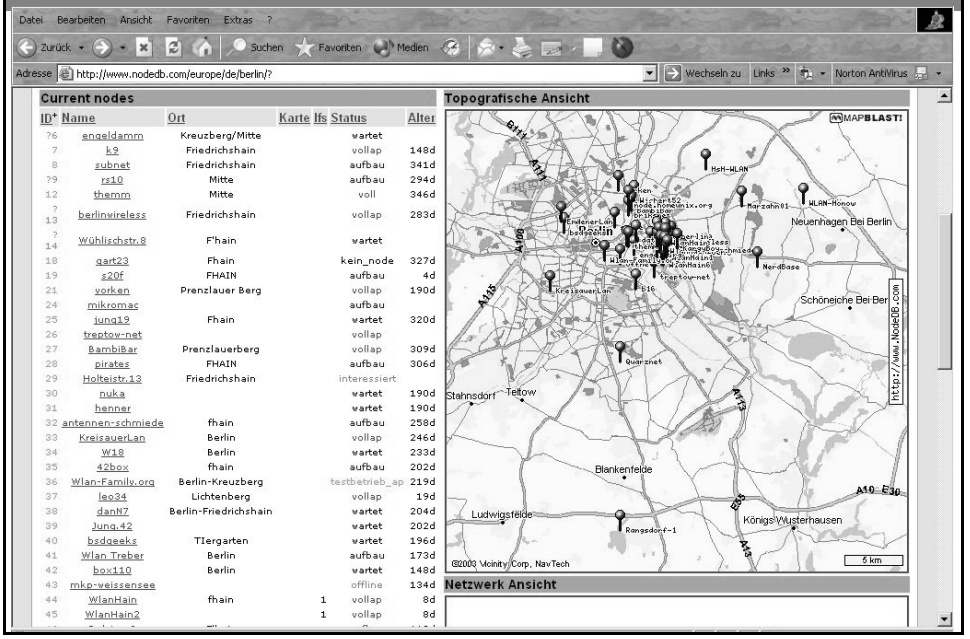
Fachhochschule
Dortmund
University of Applied Sciences

Sicherheit im WLAN (2)



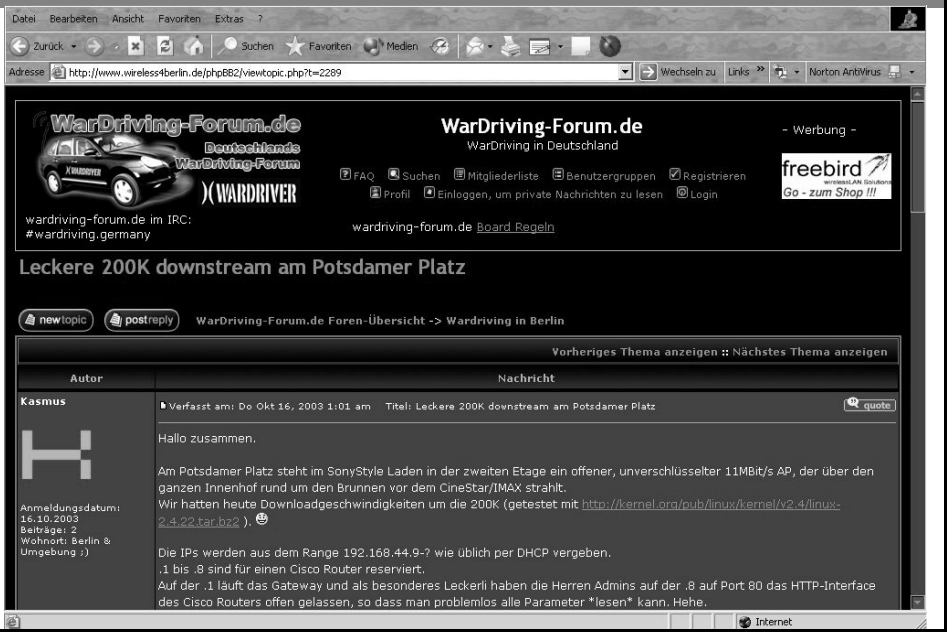
Fachhochschule
Dortmund
University of Applied Sciences

Sicherheit im WLAN (3)



Fachhochschule
Dortmund
University of Applied Sciences

Sicherheit im WLAN (4)



Fachhochschule
Dortmund
University of Applied Sciences

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.

Fachhochschule
Dortmund
University of Applied Sciences

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

Fachhochschule
Dortmund
University of Applied Sciences

Literatur

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

Fachhochschule
Dortmund
University of Applied Sciences

Literatur

2) Datenschutz:

c) Internet-Adressen

- Datenschutzbeauftragte
  (Bundesbeauftrate 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,
  Niedersachen 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 ttp://www.datenschutz.de/(de)/

Literatur

3) WLAN-Sicherheit:

- Fluhrer S, Mantin I, Shamir A. [Online] Weaknesses in the Key Sxheduling 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

Fachhochschule
Dortmund
University of Applied Sciences

Vielen Dank für Ihre Aufmerksamkeit!

Kontakt: schuetze@medizin-informatik.org