

Drahtlose Netze - neue Gefahren zwingen zum Paradigmenwechsel (Sebastian Schreiber <Schreiber@SySS.de>

1. Einleitung

In den letzten zehn Jahren hat mobile Kommunikation immer mehr an Bedeutung gewonnen. Zunächst hielten die Funktelefone (später: vom Typ DECT) Einzug in Büros und Privatwohnungen. Innerhalb weniger Jahre sind GSM-Handys zu einem gängigen Kommunikationsmedium geworden. Bei der Versteigerung der UMTS-Lizenzen in Deutschland wurden im Sommer 2000 knapp 100 Mio DM investiert (sieheⁱ). WLAN-Hot-Spots schießen wie Pilze aus dem Boden und Handys ohne Bluetooth lassen sich kaum mehr verkaufen.

Fest steht: der Siegeszug der mobilen Kommunikation ist nicht zu stoppen.

These Bei sich rapide entwickelnden Technologien denken die Hersteller zunächst an Markteroberungsstrategien, dann an Technologie und zu aller letzt an Sicherheit.

2. Bluetooth

Bluetooth wird für kurze Distanzen eingesetzt. Aufgrund des geringen Preises für Bluetooth-Komponenten werden sie zunehmend in verschiedenste Endgeräte eingebaut: Laptops, PDAs, Digitalkameras, Handys, Diktiergeräte, Headsets - aber auch in Kraftfahrzeuge. Üblicherweise erfolgt die Authentifizierung über ein „Pre-Shared Secret“ und die Daten werden verschlüsselt.

Leider ist die Verschlüsselung oft alles andere als ausreichend: im Nokia-Prospekt zu den Bluetooth-Handys wird mit dem Einsatz von Bluetooth-Verschlüsselung geworben. Wirft man aber einen Blick in die Spezifikation von Nokiaⁱⁱ, so stellt sich heraus, dass die Verfahren mit einer Schlüssellänge zwischen 8 und 128Bit arbeiten. Die Computerzeitschrift C't (sieheⁱⁱⁱ) hat gemessen, dass das Nokia-Handy 6310 von sich aus nur 56Bit Schlüssellänge vorschlägt - in der Praxis ist das viel zu wenig. Flächendeckende Scans auf Bluetooth-Komponenten ist aufgrund der kürzeren Reichweite viel schwieriger als beim *WAR-Driving*.

3. DECT

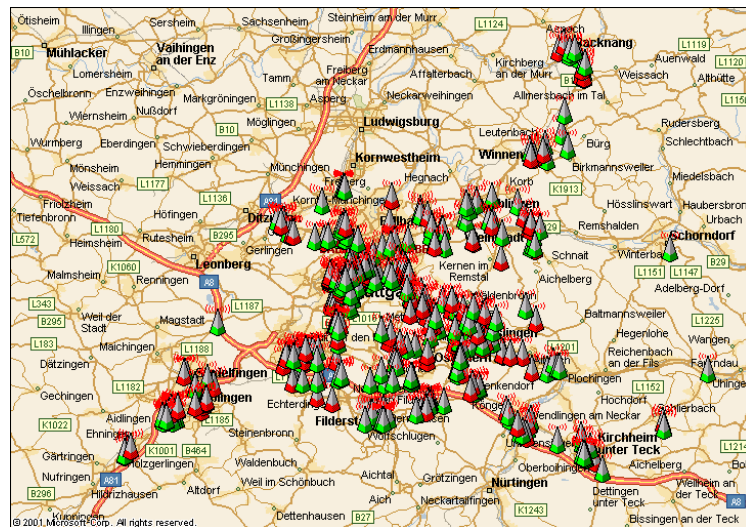
DECT wird heute für die mobile ISDN- oder Analogtelefonie eingesetzt und verfügt über eingebaute Sicherheitsmechanismen. Im Vergleich zu WLAN-Infrastrukturen und IP-Telefonie ist DECT in vielen Unternehmen schon seit geraumer Zeit im Einsatz.

These Langfristig wird DECT durch IP -Telefonie und WLAN abgelöst werden.

4. WLAN

Als Systemadministrator sind wir es gewohnt, mit teuren, unzuverlässigen und instabilen Systemen zu arbeiten. Die neue Technologie des WLANs hingegen ist preisgünstig, verfügbar und komfortabel - kurz: äußerst attraktiv. Moderne Laptops (selbst die aus den Discount-Supermärkten) werden bereits ab Werk mit WLAN-Karten ausgestattet. Leider sind die im Einsatz befindlichen Verschlüsselungs- und Authentifikationstechnologien (WEP) nicht ausreichend; die proprietären Erweiterungen sind untereinander inkompatibel. Oft vertrauen Administratoren auf die physische Distanz als Sicherheitsbarriere. Es zeigt sich aber, dass man bereits mit legal erhältlichen Antennen Distanzen von einigen Kilometer überbrücken kann. Beim so genannten *War-Driving* zeigt sich, dass nach wie vor ein großer Teil der Unternehmen ihre Netze überhaupt nicht schützen, d.h. auf Verschlüsselung durch WEP verzichten. Obwohl die verfügbare WEP-Verschlüsselung mittels im Internet verfügbarer Software leicht überlistet werden kann, macht ihr Einsatz durchaus Sinn: zum einen ist eine

niedrige Hürde immer noch besser als gar keine - zum anderen ist der Einsatz von Verschlüsselung erforderlich, um einen Vertraulichkeitsanspruch zum Ausdruck zu bringen: das Abhören und Ausspähen eines unverschlüsselten WLANs steht in Deutschland keinesfalls unter Strafe.



5. Öffentliche WLANs: „Hot-Spots“

In Hotels, Flughäfen und Bahnhöfen schließen öffentliche WLANs (so genannte Hot-Spots) wie Pilze aus dem Boden. Der Siegeszug der öffentlichen WLANs ist nicht mehr aufzuhalten: die Mitarbeiter *werden* öffentliche WLANs nutzen - selbst wenn dies durch eine IT Security Policy verboten wird.

Eine Vielzahl von Herstellern wie beispielsweise Cisco hat das Standard-WLAN nach IEEE 802.11 um eigene Sicherungsmechanismen erweitert. Firmenintern lassen sich WLANs so relativ einfach sichern - öffentliche Hot-Spots lassen sich aufgrund mangelnder Kompatibilität allerdings nicht schützen.

Der Autor empfiehlt, den Gefahren durch Wireless-LANs mit folgendem 3-Punkte-Plan zu begegnen:

1. **Etablierung von VPNs über WLANs**
Die unsichere WEP-Verschlüsselung lässt sich durch den Einsatz von etablierter VPN-Technologie absichern. Nutzt man zudem eine Personal Firewall, so kann dem Mitarbeiter erlaubt werden, auch öffentliche WLANs zu nutzen.
2. **Ausstattung der Laptops mit Personal Firewalls**
Einige VPN-Hersteller haben in Ihren VPN-Clients einfache Firewalls eingebaut: ein Anwender erhält nur dann Zugang zum Firmennetz, wenn die Client-Firewall korrekt konfiguriert ist.
3. **Regelmäßige Scans nach wilden WLANs**
Mit Tools wie dem Netstumbler lassen sich die Räumlichkeiten eines Unternehmens effizient nach unerwünschten WLANs scannen.

These Die Technologie WLAN bereitet UMTS ernsthafte Konkurrenz und wird sich beim Datenfunk durchsetzen. WLAN-Hot-Spots nehmen den Platz der ausgedienten Telefonzellen ein und werden überall verfügbar sein (Restaurants, Cafes, Hotels, Bahn- und Busbahnhöfe, Flughäfen, öffentliche Plätze, etc.).

6. UMTS/GRPS

Im Gegensatz zu WLANs haben die paketvermittelnden Netze GRPS und UMTS drei große Nachteile: Zum einen sind Netze sowie Endgeräte momentan kaum verfügbar; zweitens ist die Internetnutzung momentan nahezu unbezahlbar; drittens ist die zur Verfügung stehende Bandbreite von 2 MBit im Vergleich zu den bei modernen WLAN-Hardware üblichen 56 MBit-Karten gering.

These WLAN -Hot-Spots werden bis ins Jahr 2010 für mobiles Internet eine größere Bedeutung haben als UMTS.

7. D.o.S-Attacken

Attacken gegen die Verfügbarkeit von drahtlosen Netzen ist systeminhärent hoch: Sender/HF-Generatoren mit entsprechender Sendeleistung können jegliche Kommunikation unmöglich machen. Zu beachten ist, dass sich solche Störsender billig herstellen und auf kleinstem Raum unterbringen lassen.

Ist ein Unternehmen von der Verfügbarkeit eines Netzes abhängig, so empfiehlt es sich, nicht allein auf drahtlose Netze zu vertrauen.

8. IRDA

Infrarot wurde zunächst zur Fernsteuerung von Radio und Fernseher eingesetzt. Heute wird Infrarot auch zwischen PDA, Handy, Drucker und Laptop eingesetzt. Mittlerweile kann man per Infrarot problemlos Daten mit bis zu 4MBit übertragen. IRDA selbst bietet kaum Sicherheit: Authentifikation und Verschlüsselung ist nicht Bestandteil des Standards und müsste in höheren OSI-Layern implementiert werden - was leider nicht üblich ist. Das Abhören einer über Infrarot verbundenen Tastatur beziehungsweise eines über Infrarot an den Laptop angeschlossenen Handy ist dann einfach, wenn Sichtverbindung besteht: Schließlich ist Infrarot nichts anderes als Licht aus einem für den Menschen unsichtbaren Spektralbereich.

These Infrarot wird von Bluetooth (zunächst im IT -Bereich, später auch bei HiFi-Geräten) zurückgedrängt und verliert seine Bedeutung.

9. Ad-hoc-Netze

Unter einem Ad-hoc-Netzwerk versteht man einen IT-Verbund bei einer gewissen räumlichen Nähe nahezu *automatisch* zustande kommt. So meldet sich ein Bluetooth-Headset beim nächsten Handy an; eine entsprechend konfigurierter Bluetooth- oder WLAN-PDA verbindet sich mit dem nächsten Access-Point, der als Internet-Hotspot dient. Das Anwendungsspektrum von Ad-hoc-Netzen ist nahezu unbegrenzt; folgende Anwendungen sind in naher Zukunft denkbar:

1. Handys unterstützen bereits heute Computerspiele zweier über Bluetooth kommunizierender Handys. Denkbar ist, dass Handys in Zukunft permanent die Umgebung absキャンen. Sobald ein spielwilliger im Umkreis von 15m auftritt, signalisieren dies die beiden Handys und ein Spiel beginnt.
2. Betritt man einen Bahnhof, so verbindet sich der PDA mit dem Reiseinformationssystem der Bahn. Hat man bereits ein Ticket erworben, so wird man automatisch auf drohende Verspätungen aufmerksam gemacht. Verfügt man über kein Ticket, so werden einem gleich die Verbindungen vom entsprechenden Startbahnhof angebunden.
3. Möchte man im Restaurant Speisen und Getränke bestellen, so ist dies mit dem eigenen PDA und einem Ad-hoc-Netzwerk möglich.

4. Der PDA bedient über Bluetooth das heimische Fernsehgerät fern. Der PDA kennt dabei die Vorlieben des Anwenders, sowie das aktuelle Fernsehprogramm.

These Ad-hoc-Netze werden stark an Bedeutung gewinnen.

10. Personal Firewalls

Der geschäftlich genutzte Computer (Laptop oder PDA) wird traditionell über eine Netzwerkkarte oder über einen Dial-In-Zugang mit dem Firmennetz verbunden. Gegenüber Angriffen aus dem Internet ist er hierbei durch die Corporate recht gut gesichert. Die moderne Welt sieht anders aus: der Firmenlaptop wird unterwegs im Hotel oder Flughafen kurz ans Internet angeschlossen, erhält beim Besuch bei fremden Unternehmen Internetzugang über ein fremdes Firmennetz,

Als einzig mögliche Konsequenz muss sich der Laptop heute selbst schützen und kann sich nicht mehr auf die (zweifelsohne erforderliche) Firmenfirewall verlassen. So genannte *Personal Firewalls* (oder *Desktop Firewalls*) werden unverzichtbar. Leider sind die Begriffe nicht scharf definiert: meist ist eine Kombination von folgenden Technologien gemeint:

- Paketfilter
- Virens Scanner für Mail und Festplatte
- Layer-7-Proxy mit http-Filter
- Sandbox-Umgebung für diverse Client-Programme gemeint.

Nach der Lehrmeinung soll auf Firewall-Systemen keinerlei andere Programme als die Firewall selbst laufen¹. Dieses Paradigma kann beim Einsatz der oft noch nicht ganz ausgereiften Produkte natürlich nicht eingehalten werden.

These Personal Firewalls müssen auf alle mobilen Computer .

11. Vergleich der wichtigsten Technologien:

	Geeignet für öffentliche (ö) oder Firmennetze (f) oder individuelle Netze (i)	Verfügbare Infrastrukturen	Verfügbare Hardware	Gebühren für den Datentransport	Bandbreite
DECT	ö/f/i	ja	Ja	Keine	Niedrig
WLAN	ö/f/-	ja	Ja	Keine/niedrig	Sehr hoch
IRDA	-/f/i	ja	Ja	Keine	Mittel
Bluetooth	-/f/i	ja	Ja	Keine	Mittel
GSM/HSCSD/GRPS	ö/-/-	Ja	Ja	Hoch	Niedrig-mittel
UMTS	ö/-/-	Im Aufbau	teilweise	Verm. hoch	Hoch

12. Paradigmenwechsel: weg vom Burggraben

Traditionell bauten Firmen ihre Netze nach dem Burggrabenparadigma auf: innerhalb eines Corporate Networks befinden sich vertrauenswürdige **Mitarbeiter** die es durch wirksame Firewalls vor Angriffen aus dem Internet zu schützen galt.

Bald wurde begonnen, in Einzelfällen gegen das Paradigma zu verstoßen: so verbinden sich Partner oft über RAS oder VPN mit dem eigenen Corporate Network:

Wartung der TK-Anlage, Druckern, Storage

- Wartung von Maschinen (Hochregallager, Werkzeugmaschinen, etc.)
- Den OSS-Support von SAP
- Fern-Administration durch Systemhäuser.

Das Privileg, Zugriff aufs Corporate Network zu erhalten, kommt nun nicht mehr nur Mitarbeitern, sondern auch **Partnern** zu; das Burggrabenparadigma wird aufgeweicht.

¹ Siehe unter anderem das Grundschutzhandbuch Kap. M2.72

WLANs hebeln das Paradigma völlig aus: betreibt ein Unternehmen ein schlecht geschütztes WLAN, so kann jeder, der sich in der Nähe befindet, ins Firmennetz gelangen. Mit der zunehmenden Verbreitung drahtloser Netze gewinnt auch die *interne* Sicherheit an Bedeutung.

13. Fazit

Dass mobile Connectivity ein Hauptthema der nächsten Jahre sein wird, ist klar. Welche Standards sich durchsetzen, ist heute noch offen. Es liegt nahe, dass parallel verschiedene Technologien eingesetzt werden, und dass häufig Standards durch neue abgelöst werden. Es liegt nahe, dass unter anderem auch Technologien eingesetzt werden, die die Authentizität des Benutzers sowie die Vertraulichkeit der transportierten Daten nicht ausreichend sichern werden. Verschlüsselung, starke Authentifikation sowie Laptop- (oder PDA-) Sicherheit sind daher unbedingt erforderlich: Unternehmen sind für den Schutz ihrer Daten selbst verantwortlich.

ⁱ Webpage der Regulierungsbehörde: <http://www.regtp.de/aktuelles/pm/00116/index.html>.

ⁱⁱ Siehe: http://ncsp.forum.nokia.com/downloads/nokia/documents/N6310_BT_Spec.pdf

ⁱⁱⁱ Michael Schmidt **Blaufunk-Spion Bluetooth-Analyzer Tektronix BPA 105**
c't 21/02, Seite 206