

Wireless – aber sicher!

Mobile & Wireless Konferenz 06, 27.09.06
Martin Rutishauser

Wie «sicher» ist «sicher» ?



(Beispiel: Tresor)

Sicherheit ist niemals 100%!



Ein Tresor hält (gem. seinem Härtegrad) beispielsweise 30, 45 oder 60 Minuten den gängigsten Angriffen stand. Aber es wird immer jemanden geben, der ihn mit viel Aufwand brechen kann.

Vorstellung

□ **Martin Rutishauser**

- Senior Consultant / Branch-Manager Bern bei OneConsult GmbH
- Security-Audits, Sicherheitskonzepte, Policies
- OSSTMM-Zertifizierungen: OPST, OPSA, Trainer
- Windows, Linux und Securitytools

□ **OneConsult GmbH**

- IT Security Consulting und strategische Beratung
- Unabhängigkeit & Neutralität
- Nutzenoptimierung & Knowhow-Transfer
- Fachwissen & Erfahrung



Agenda

- 1. Einführung Technologien**
2. Gefahren und Massnahmen Wireless
3. Gefahren und Massnahmen Bluetooth
4. Zusammenfassungen

1 Einführung



□ Wireless

- Computer, Notebooks, Kombigeräte (ADSL-Router), PDA's
- Reichweite: 50 – 500 m
- Sicherheit: WEP (RC4 40 Bit), WPA (RC4 TKIP = Temporal Key Integrity Protocol), WPA2 (AES 256 Bit), 802.11i (Enhanced Security)

<u>Standard</u>	<u>Frequenz</u>	<u>Durchsatz</u>
802.11a	5 GHz	bis 54 Mbps
802.11b	2.4 GHz	bis 11 Mbps
802.11g	2.4 GHz	bis 54 Mbps
(802.16 (WiMAX))	2 – 66 GHz	ca. 70 Mbps)

1 Einführung

□ Bluetooth Bluetooth

- Computer, Notebooks, Mobiltelefone, Headsets
- Drei mal mehr Umsatz derzeit als Wireless-Produkte
- Reichweite: 10 – 100 m
- Sicherheit : non-secure, service level enforced security, link level enforced security

<u>Standard</u>	<u>Frequenz</u>	<u>Durchsatz</u>
1.0(b),1.1,1.2	2,402 - 2,480 GHz	ca. 720 Kbps
2.0	2,402 - 2,480 GHz	ca. 2.1 Mbps

1 Einführung

□ Infrarot

- Fernbedienungen, Computer, PDA, Mobiltelefone
- SIR (Serial InfraRed) mit bis zu 115,2 Kbps (9,6 Kbps)
- FAST-IR (seit 2002) mit bis zu 4 Mbps (250Kbps)
- Reichweite ca. 1 – 10 m
- Sender/Empfänger müssen sich „sehen“ (line of seight)

□ Funk

- Drahtlose Telefone (Basisstation und Mobilteil)
- DECT (Digital Enhanced Cordless Telecommunications)
- 1880 MHz bis 1900 MHz, ca. 1 Mbps Durchsatz
- Reichweite ca. 30 – 3000 m
- Sicherheit: Anmeldung, Authentifikation, Verschlüsselung

Agenda

1. Einführung Technologien
2. **Gefahren und Massnahmen Wireless**
3. Gefahren und Massnahmen Bluetooth
4. Zusammenfassungen

2 Gefahren und Massnahmen Wireless




□ Gefahr: Detektion

- Wireless-LAN können passiv erkannt werden
- Auch ohne SSID-Broadcasts
- (liegt in der Natur der Technologie)

□ Massnahme gegen Detektion

- Auf Einsatz Wireless-LAN verzichten

Wardriving + Warchalking =>

let's warchalk..!	
KEY	SYMBOL
OPEN NODE	ssid  bandwidth
CLOSED NODE	ssid 
WEP NODE	ssid access contact  bandwidth
blackbeltjones.com/warchalking	

2 Gefahren und Massnahmen Wireless

□ **Gefahr: Lauschangriffe**

- Ohne Verschlüsselung werden die Daten im Klartext über die Luft übertragen -> Gefahr von „Mithörern“
- (liegt in der Natur der Technologie)

□ **Massnahme gegen Lauschangriffe**

- Übertragungsverschlüsselung einsetzen
- VPN-Technologie einsetzen
- Verschlüsselte Dienste einsetzen (SSH, HTTPS)

2 Gefahren und Massnahmen Wireless

□ **Gefahr: Identitätsdiebstahl**

- MAC-/IP-Adressen können gefälscht werden
- ARP-Umleitung (Ersatz Default Gateway)
- Benutzung Wireless-Netzwerk (und dazugehörigen Internet-Anschluss) für illegale Aktivitäten

□ **Massnahme gegen Identitätsdiebstahl**

- Einbruchserkennung im Wireless-LAN (www.airdefense.net)
- IDS, Filterung Verkehr Wireless-LAN -> Internet
- Protokollierung (und Auswertung) von DHCP und ARP

2 Gefahren und Massnahmen Wireless

□ **Gefahr: Datendiebstahl**

- Daten, welche ungeschützt übertragen werden, können „kopiert“ werden
- Computer im LAN oft unzureichend geschützt
- Computer mit Wireless-LAN und LAN (dual-homed) präferenzierte Ziele (Weg um die Firewall zwischen Internet und LAN)

□ **Massnahme gegen Datendiebstahl**

- Computer im LAN: Firewall, Antivirus, Updates, Passwörter
- Übertragungsverschlüsselung Wireless-LAN einsetzen
- Verschlüsselte Dienste einsetzen (SSH, HTTPS)

2 Gefahren und Massnahmen Wireless

□ Gefahr: Verschlüsselungsschwächen

- WEP: Initialisierungsvektor, Bruteforce Passwort
- WPA: Bruteforce Passwort
- WPA2: gilt noch als ungeknackt
- GRE: Remote Sniffing (Router/Endpunkt)
- IPSec: Man-in-the-Middle, Remote Sniffing (Encapsulating)

□ Massnahme gegen Verschlüsselungsschwächen

- VPN für Wireless-Clients konfigurieren (gegenseitig stark authentifiziert)
- WPA2/IPSec verwenden (kein 100%-iger Schutz)
- Verschlüsselte Dienste verwenden (SSH, HTTPS)

Agenda

1. Einführung Technologien
2. Gefahren und Massnahmen Wireless
- 3. Gefahren und Massnahmen Bluetooth**
4. Zusammenfassungen

3 Gefahren und Massnahmen Bluetooth

□ Gefahr: **Blueprinting**

- Erkennung und Identifizierung von Geräten
- MAC-Adresse MM:MM:MM:XX:XX:XX
- SDP Service Discovery Protocol



□ Massnahme gegen **Blueprinting**

- Bluetooth-Gerät im versteckten Modus (hidden/undiscoverable) betreiben
- Bluetooth ausschalten

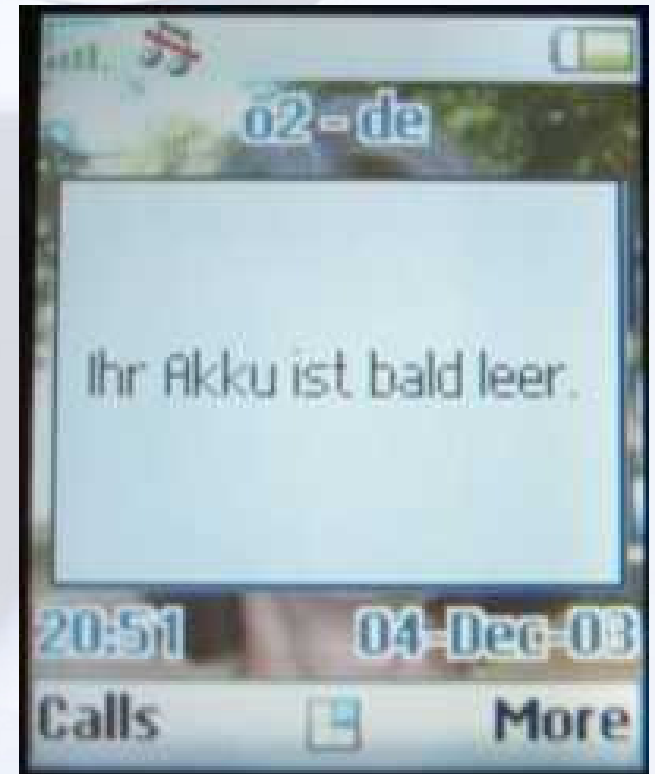
3 Gefahren und Massnahmen Bluetooth

□ Gefahr: Bluejacking

- Kontakt/Notiz/Bild erstellen und via Bluetooth an benachbarte Geräte senden
- Nicht gefährlich, nur lästig

□ Massnahme gegen Bluejacking

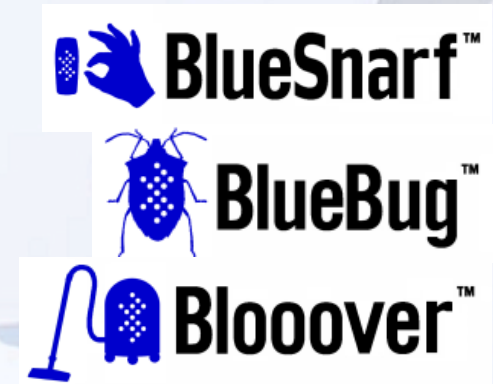
- Empfang ablehnen wenn möglich
- Bluetooth-Gerät im versteckten Modus (hidden/undiscoverable) betreiben
- Bluetooth ausschalten



3 Gefahren und Massnahmen Bluetooth

□ Gefahr: Bluesnarfing/Bluebug

- Firmware-Problem Mobiltelefone 2003/2004
- Unbemerktetes Herunterladen von Kontakten
- Lesen/Senden/Empfangen SMS
- Anrufe tätigen
- Bluesnarf++ neu, voller Lese-/Schreibzugriff
- Bloover kombiniert Bluesnarf/Bluebug



□ Massnahme gegen Bluesnarfing/Bluebug

- Bluetooth im versteckten (hidden/undiscoverable) Modus betreiben
- Firmware-Aktualisierung
- Bluetooth ausschalten

3 Gefahren und Massnahmen Bluetooth

□ Gefahr: Denial-of-Service

- Äquivalent Ping-of-Death in der IP-Welt
- IPAQ-PDA reagiert bei 600bytes (l2ping/L2CAP)



□ Massnahme gegen Denial-of-Service

- Bluetooth im versteckten (hidden/undiscoverable) Modus betreiben
- Bluetooth ausschalten

Agenda

1. Einführung Technologien
2. Gefahren und Massnahmen Wireless
3. Gefahren und Massnahmen Bluetooth
4. **Zusammenfassungen**

4 Conclusio Business

- ❑ Kein Einsatz Wireless/Bluetooth in sensitiven Bereichen (Tastaturen!)
- ❑ Wireless/Bluetooth nicht immer eingeschaltet lassen
- ❑ Wireless-LAN restriktiv vom internen Netzwerk trennen, Computer im LAN schützen
- ❑ VPN für Wireless-Clients einsetzen mit gegenseitiger starker Authentifikation
- ❑ Wireless-Verschlüsselung (WPA2, IPSec) unbedingt einsetzen (kein 100%-iger Schutz), komplexe Schlüssel regelmässig wechseln
- ❑ MAC-Adressen-Filterung für Wireless aktivieren (kein 100%-iger Schutz)
- ❑ Keine Wireless-Verbindungen mit leerer SSID zulassen und SSID nicht broadcasten (Detektion dennoch nicht 100% verhinderbar)
- ❑ Einbruchserkennung Wireless-LAN (Wireless -> Internet)
- ❑ Bluetooth-Gerät im versteckten Modus (hidden/undiscoverable) betreiben
- ❑ Regelmässige Audits durchführen (lassen)

4 Conclusio Private

□ **Wireless**

- Wireless-LAN nicht immer eingeschaltet lassen
- Wireless-LAN mit Firewall/NAT-Funktionalität separieren und interne PC's mit Host-Firewall/Antivirus schützen
- Wireless-LAN nicht unverschlüsselt betreiben (keine 100%-ige Sicherheit), möglichst WPA2/WPA anstelle von WEP einsetzen, komplexe Schlüssel regelmässig wechseln

□ **Bluetooth**

- Bluetooth nicht immer eingeschaltet lassen
- Gerät im versteckten Modus (hidden/undiscoverable) betreiben
- Bei empfangenen Daten nicht gleich „OK“ oder „SPEICHERN“ drücken

Besten Dank...

...für Ihre Aufmerksamkeit!

Martin Rutishauser

OSSTMM-Trainer, OPSA, OPST
Senior Consultant / Branch Manager Bern

info@oneconsult.com
+41 79 323 99 07

OneConsult[®]

Hauptsitz:

OneConsult GmbH
Zürcherstrasse 73
8800 Thalwil
Schweiz

<http://www.oneconsult.com>
info@oneconsult.com
Tel. +41 43 443 52 52
Fax +41 43 443 52 62

Filiale Bern:

OneConsult GmbH
Aarstrasse 98
3005 Bern
Schweiz

<http://www.oneconsult.com>
info@oneconsult.com
Tel. +41 31 318 25 25
Fax +41 31 318 25 35

Vertretung Deutschland:

Vertretung der OneConsult GmbH
in Deutschland
Parkstraße 2
89231 Neu-Ulm
Deutschland

<http://www.oneconsult.com>
info-de@oneconsult.com
Tel. +49 731 977 191 70
Fax +49 731 977 191 99