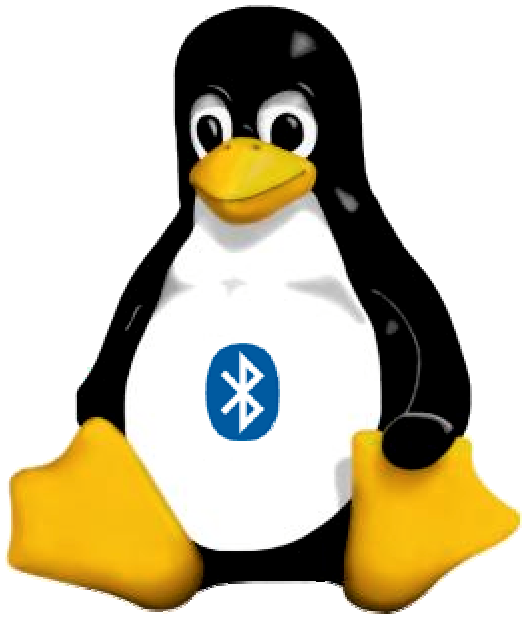
Wissenschaftliches Experiment



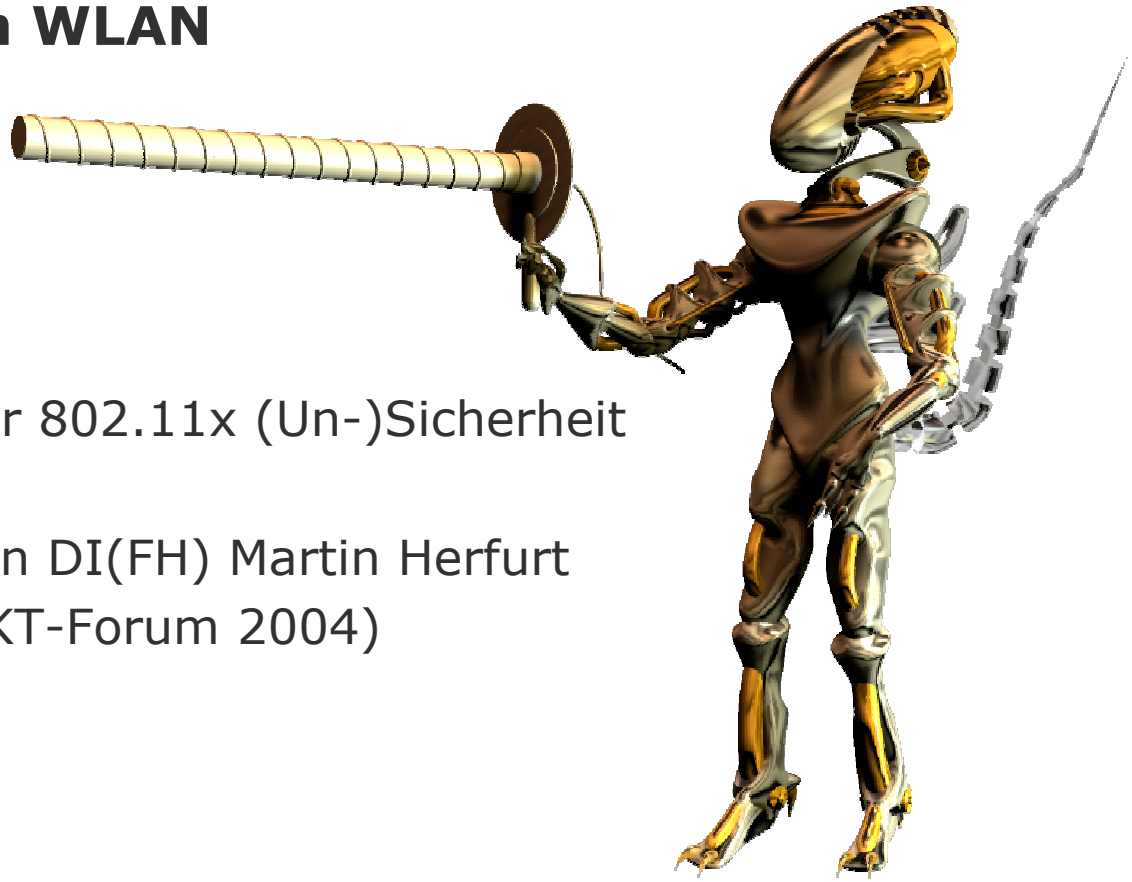
Aktivieren Sie Bluetooth auf ihrem Telefon!

Ändern sie ggf. den Bluetooth-Modus auf “sichtbar”!

Machen sie sich keine Sorgen!

salzburg research

War-Driving im WLAN



Die Verwertung der 802.11x (Un-)Sicherheit

Ein Kurzvortrag von DI(FH) Martin Herfurt
am 26.02.2004 (IKT-Forum 2004)

Salzburg Research Forschungsgesellschaft m.b.H.| Jakob-Haringer-Str. 5/III | A-5020 Salzburg
T +43.662.2288-200 | F +43.662.2288-222 | info@salzburgresearch.at | www.salzburgresearch.at

Was man wissen sollte

- 802.11b/g wird sehr viel eingesetzt
  - immer mehr auch in privaten Haushalten
- WEP Verschlüsselung ist bei allen Schlüssel-Längen unsicher
  - Initialisatios-Vektor-Schwäche
- 2002 verwendeten rund 75% aller gefundenen WLANs keinerlei Verschlüsselung (Manhattan, Northern Virginia, Salzburg)
  - Unverschlüsselte Netzwerke gibt es auch heute noch!

Was man vorausetzt

- Anfälliges 802.11b oder 802.11g Netz
- Schlecht geschirmte Wände
- bei WEP Verschlüsselung
  - möglichst viele Geräte
  - möglichst viel Datenverkehr am Netz
- Idealerweise **kein** Virtual Private Network (VPN)
- Kein aufmerksamer Netzwerk-Administrator ;)

Was man benötigt

- Laptop mit freiem PCMCIA Slot
- 802.11b oder 802.11g WLAN-Karte mit Antennen-Buchse und geeignetem Chipset
  - ORINOCO Karten bzw. Karten mit PRISM2-Chipset
- tragbare 2,4 GHz Antenne mit Anschlusskabel (optional)
- Spezialsoftware zum
  - Detektieren von WLANs (NetStumbler , Wellenreiter)
  - Abhören von WLANs (Ethereal, AiroPeek)
  - Brechen der WEP Verschlüsselung (AirSnort, WEPCracker)

Was man alles anstellen kann

- Netzwerk abhören
  - Passwörter von Mitarbeitern stehlen
- Pakete einschleusen
  - Kommunikation stören (Verbindungen beenden)
- Man-in-the-middle
  - Sich als vermeindlich sicherer Rechner tarnen und anvertraute Geheimnisse an den echten Rechner weitervermitteln
- Spoofing
  - Sich als anderer Rechner ausgeben
- Connection Hijacking
  - Vermeindlich sichere Verbindung übernehmen ohne dass der Server das merkt
- Denial of Service und Flooding Attacken
  - Lahmlegen von Rechnern und Services durch extensives Zugreifen auf dessen Resourcen

Was man dagegen tun wollte

- 802.11i Security (WPA - WiFi Protected Access)
- Standard ausschliesslich für Sicherheit
- Release war im Herbst 2003
- Neue Sicherheitsmechanismen
  - TKIP - Temporary Key Integrity Protocol
  - MIC - Message Integrity Check
  - Schlüssel Mix - MAC Adresse ist Teil des Schlüssels
  - Erweiterter IV - Mehr Möglichkeiten bei Verschlüsselung
  - Schlüsselerneuerung - Schlüssel wechselt automatisch
- Too late - too little
- Auf lange Sicht soll auch bei physikalischer Verschlüsselung AES verwendet werden

Was man selbst dagegen tun kann

- Gegen Abhören (Network-Sniffing)
  - Verwendung eines Virtual Private Networks (VPN)
  - Bei Verwendung von WEP in regelmäßigen Abständen den Schlüssel erneuern
- Gegen unerlaubte Mit-Benutzung
  - Authentifikationslösung (wie an Flughäfen)
  - MAC filtering
  - DHCP deaktivieren
- Gegen Störung der End-Geräte
  - Sicheres Betriebssystem verwenden (patch me if you can ;)
  - Installation einer „Personal Firewall"

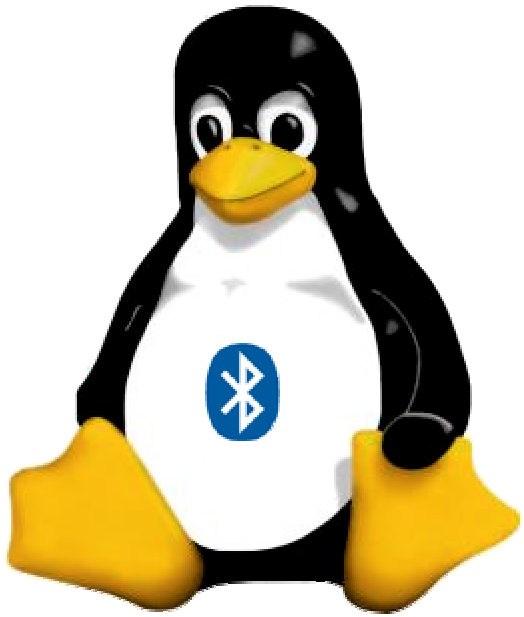
Was man in Zukunft oft hören wird

- Bluejacking/Bluesnarfing (Wardriving im WPAN)
  - Bluetooth-Geräte weisen natürlich auch Sicherheitsmängel auf
  - Unbekannte können sich „Sicherheitskopien" der gespeicherten Dinge anfertigen (notwendige Distanz: ~10m)
    - Telefonbuch
    - Kalender
    - Klingeltöne
    - Nachrichten :)
  - Man schützt sich durch
    - Wechsel in den „Hidden"-Modus
    - Abschalten von Bluetooth am Gerät
    - Unglaubliche Paranoia

Vielen Dank für die Aufmerksamkeit

TKS 2000 - MDF Labor - Helix-Antennenbau - Gruppe B

Vielen Dank für ihre Hilfe !



Sie sollten Bluetooth auf ihrem Telefon jetzt wieder deaktivieren ;)