Hacking The Invisible Network

The Risks and Vulnerabilities Associated with Wireless Hotspots

Michael Sutton <msutton@idefense.com>
Pedram Amini <pamini@idefense.com>
Purpose

• Study security from two points of view
  – Providers
  – End users

• A variety of implementations
  – Cafés
  – Hotels

• Tools
  – Laptops, Dell Axim
  – Hermes and Prism chipsets
  – Various software tools
  – Tolerant bladder
Wireless Internet Service Providers
– aka Hotspots

What are they?
• Where are they?
  – Airports
  – Hotels
  – Retail stores
  – Coffee Shops
• Why go wireless?
  – Cost
  – Convenience
Industry

• Startups
  – Boingo
  – WayPort
  – NetNearU
  – HotSpotzz
  – Airpath Wireless
  – Surf and Sip
  – HereUAre
  – Deep Blue Wireless
  – Joltage (defunct)
Industry (cont’d)

• Telecomm
  – T-Mobile
  – AT&T (Cometa)
  – Sprint (Boingo)

• Hardware
  – Intel (Cometa)
  – IBM (Cometa)
Provider Risks

• Business risks
  – Financial loss
  – Launch pad for anonymous attacks

• Network level attacks
  – Privacy
  – Confidentiality
  – Data integrity

• Denial of service attacks
  – Availability
End User Risks

- Node vs. Network level security
  - “Crunchy on the outside, Chewy on the inside”

- Untrusted networks
  - Intranet safe services
  - Information leakage
  - Spoof attacks

- End user awareness
Security Implementations

- Access control
  - Firewall restricts connectivity
  - Web requests redirected to login screen
  - Authentication takes place over SSL
  - Internet access is granted
Security Implementations (cont’d)
Security Implementations (cont’d)

• IP address filtering
  – Everyone

• MAC address filtering
  – T-Mobile

• IPSec VPN
  – Deep Blue Wireless
    – Optional

• DHCP lease expiration
  – ?
Revenue Loss

• Tunneling data through unfiltered protocols
  – Bypassing access controls

• Connection hijacking
  – Stealing legitimate connections

• Connection sharing
  – Multiple unauthorized connections piped through one legitimate connection
Tunneling

IP Traffic

Loki Server
Internet
External Sites
ICMP Traffic
Loki Client
Access Point
Firewall Gateway
IP Traffic

Copyright © 2003 iDEFENSE Inc.
Connection Hijacking

Internet Access Point
Target IP \( \rightarrow \) Y.Y.Y.Y
MAC \( \rightarrow \) Y:Y:Y:Y:Y:Y
Permitted

Attack IP \( \rightarrow \) Y.Y.Y.Y
MAC \( \rightarrow \) Y:Y:Y:Y:Y:Y
Blocked

Connection Hijacking

Internet Access Point
Target IP \( \rightarrow \) Y.Y.Y.Y
MAC \( \rightarrow \) Y:Y:Y:Y:Y:Y
Permitted

Attack IP \( \rightarrow \) X.X.X.X
MAC \( \rightarrow \) X:X:X:X:X:X
Blocked

Connection Hijacking

Internet Access Point
Target IP \( \rightarrow \) Y.Y.Y.Y
MAC \( \rightarrow \) Y:Y:Y:Y:Y:Y
Permitted

Attack IP \( \rightarrow \) Y.Y.Y.Y
MAC \( \rightarrow \) Y:Y:Y:Y:Y:Y
Permitted

Internet Access Point
Target IP \( \rightarrow \) Y.Y.Y.Y
MAC \( \rightarrow \) Y:Y:Y:Y:Y:Y
Permitted

Attack IP \( \rightarrow \) X.X.X.X
MAC \( \rightarrow \) X:X:X:X:X:X
Permitted
Connection Sharing

Share 1

Router

Access Point

Internet

Share 2
Network Level Attacks

- Traffic monitoring
  - Passive attack

- DNS Hijacking
  - Active attack
    - Man in the middle attacks
    - Auto update hijacking

- Public IP addresses
  - WayPort
  - Remote attack

- ARP Spoofing
  - Active attack
    - Network crossover
WayPort Layout

- Internet
- WayPort
- Gateway
- Access Points
- 64.134.81.168 (Linux)
- 64.134.81.169 (Windows)
- 64.134.81.129
Denial of Service Attacks

- Physical layer (1)
  - Interference
- Data layer (2)
  - ARP spoofing
- Network layer (3)
  - AirJack
End User Countermeasures

- VPN
- Encryption w/ validation
- O/S hardening
- Node level firewall/IDS
- Dedicated travel hardware
Improved WISP Security

• Non Internet addressable IPs
  – Network Address Translation (NAT)
• Filter all protocols
• 802.1x
• Intrusion Detection System (IDS)
  – Spoof detection (ARP, IP, DNS, …)
• Intrusion Prevention System (IPS)
Questions?