

Wireless LAN Security Issues and Solutions

Cliff Skolnick, BAWUG

Topics

- Security Issues
- WLAN Models
- Access, Authentication, Accounting
- Securing Your Data
- Securing an Open Access Point

Wireless LAN Security

- All the normal Internet issues and more
- Open WLANs are everywhere
- Vendor defaults are usually open
- Many types of attacks
- Attackers can be miles away

Common WLAN Security Needs

- Private - Homes & Companies
 - Information Security
 - Access Monitoring
 - Firewall

Common WLAN types (cont.)

- Public - Hot Spot, Hot Zones, Open AP
 - Access Monitoring
 - Accounting
 - Firewalling w/ resource allocation

Access, Authentication, Accounting

- Beacon Frames
 - Closed networks do not advertise
 - Good 802.11b sniffers can pick up the SSID (network name) anyways
- MAC Address Filtering
 - Static list or high end units via Radius server
 - Trivial to clone an allowed MAC address

AAA (cont.)

- Shared Password
 - No individual responsibility
 - Lost key, every device must be changed
 - Can be sniffed with some luck
- WEP Key
 - Shared password problems from above
 - Can be broken with some effort

AAA (Cont.)

- 802.1x
 - Individual password required for access
 - Per-session wep key (harder to sniff, harder to break)

Securing Data

- Common Types of Attacks
 - Man in the middle
 - Authentication forging
 - Rogue access points
 - Brute force attack
- Too Many to be Safe!
- Mitigation is the Best Policy

Securing Data (cont.)

- Options
 - Tunneling protocols (ssh, ssl, etc.)
 - VPN (pptp, gre, etc.)
 - Layer 2 encryption
 - IPSEC

Open AP Issues

- Is There a Real Threat?
- AP outside firewall
- Bandwidth limiting
- Some type of logging
- Captive Portal

Open AP Issues (cont.)

- Is There a Security Policy in Place?
 - Terms of service for use of an open AP

Open AP Issues (cont.)

- Securing an Open AP
 - Logging in place?
 - Bandwidth limiting?
 - Firewall?
 - Captive portal?

References