Wireless LAN security

Philippe Langlois, WaveSecurity Inc.
Langlois@onebox.com
Different Wireless Networks

- WLAN for SOHO / enterprise
  - 802.11b, 11Mbit, 2.4GHz (WiFi)
  - 802.11a, 54Mbit, 5GHz
  - HiperLAN, 54Mbit, 5GHz
- HomeRF for Home users
- Bluetooth for Personal Area Network (PAN)
Do I need a Wireless LAN?

- Quick operationnal needs
  - Start Ups where speed > security
- Temporary operations
  - Trade shows
- Mobility requirements
  - Consultants
- Expensive wiring costs
  - Old or preserved buildings
  - Distributed areas
  - Zone with a street or railroad crossing
802.11b security features

- **SSID**
  - Network name, not encrypted
- **Association**
  - Capability to register a station with a WLAN
- **WEP**
  - Encryption at 64bits or 128bits
  - Broken due to bad use of the cipher
  [Walker, Berkeley Team, Arbaugh, Fluhrer]
Problem: Insecure WLAN setup

- Standard configuration with no security enabled
  - Anybody can “associate” and join the network
- Common & identifiable SSID
  - Company name
  - “default”
- No WEP by default
  - Even if WEP is crackable, it blocks a large number of attackers
Problem: Rogue WLAN

- Gives access to the internal network
- Installed without knowledge of the CIO
  - Installation is as easy as a hub or a router
- Typical cases:
  - Test lab
  - Permanent “temporary” networks
  - Integrators
Problem: Bad WLAN architecture

- Located inside the firewall
- No authentication done
- Antenna located near company’s building boundary
How attacks take place?

• War driving
  • Passing by cars, pedestrians…
  • Several programs automates this “hunt”
  • GPS location to pinpoint networks

• Targeted attacks
  • Attacker has a specific target
  • He goes to the different locations of the company
  • He stays as long as he wants

• Company damages & responsibility
How to secure?

- Detect networks
- Secure them
  - Basic security features
  - Authentication
  - Cryptography
- Monitor the activity
Detection

- WLAN level
  - Infrastructure or ad-hoc?
  - WEP or not?
  - Open association or MAC restricted?
- Network level
  - TCP/IP, IPX, …?
  - DHCP or static IP?
- Security level
  - Captive portal?
  - IPsec?
Basic security features

- **WEP**
  - Enable WEP to make attacks difficult
  - Choose a WEP key not in dictionaries

- **Association**
  - Block association by MAC addresses
  - Restrict DHCP to selected MAC addresses

- **Filter by the firewall:**
  - On a “need to know” basis
  - Isolate on a specific segment
Auth: Captive portal

- **Synopsis:**
  - Intercepts first HTTP connection
  - Redirect to authentication page using SSL
  - Does access control based on login / password

- **Products**
  - NoCatAuth (freeware)
  - Vernier Networks (commercial)

- **Costs:**
  - Not intrusive nor expensive
Auth: 802.1X

- **Synopsis:**
  - authentication before giving access to the network
  - Requires a PKI certificate on each client
  - Requires a central RADIUS server with EAP

- **Products:**
  - CISCO
  - Microsoft Windows XP

- **Costs:**
  - Deployment is intrusive
  - Maintenance is expensive
  - Can be a corporate wide solution
Crypto: VPNs

• To replace flawed WEP
  • Not mutually exclusive
• Products:
  • SSH
  • FreeSWAN
  • Proprietary VPNs (ie: CheckPoint SecuRemote, …)
  • IPSEC
• Costs:
  • Deployment costs are expensive
  • Maintenance expensive
  • Can be a corporate wide solution
Monitoring

- LAN level
  - Snort, Real Secure, Dragon
- Wireless level
  - AirIDS
- Access Point & Captive Portal logging
  - SNMP traps
  - Syslog
Comprehensive solutions

- WLAN client + outside firewall + SSL
  - Minimum
- WLAN Test Tool + Captive Portal + SSH
  - Low end solution
- Wireless Scanner + 802.1X + IPSEC
  - High end solution
Conclusion

- Basic security features are not enough
- Security for WLAN needed anyway
- Corporate wide
- Secure WLAN exists
Demonstration
Questions & Answers