Is your WLAN secure?

George Bailey
Ivy Tech Community College
Information Security

Topics

- **Overview**
  - Availability
  - WLAN standards
- **Best Practices – Home/SOHO user**
  - Access Control
  - Monitoring
  - Privacy
- **Enterprise Initiatives**
  - 802.1X Authentication Standard
  - 802.11i Security Standard
  - Vulnerability Assessment
  - AP Management
- **Enterprise Risks**
  - Rogue APs
  - Ad-Hoc Networks
  - Bridging

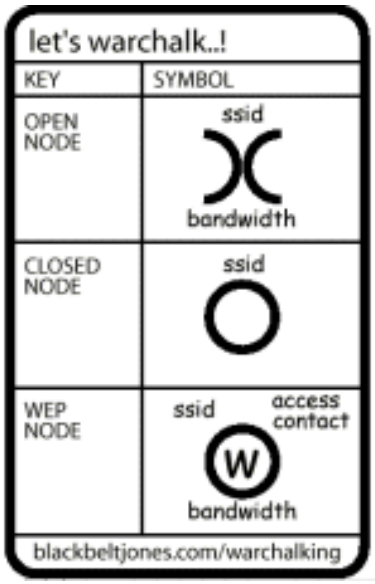
Wireless **Overview**

- Availability - Common place
  - Home
  - School
  - Public Access (Starbucks, Libraries, Airports, etc).

- Standards
  - 802.11 – First WLAN standard. Operated on 2.4Ghz band and provided up to a 2Mbps link.
  - 802.11b – An extension of 802.11, increased the bandwidth to 11Mbps.
  - 802.11a – Created to increase wireless bandwidth. Operates on the 5Ghz band and provides up to a 54Mbps link. Not interoperable with 802.11b. Not widely deployed.
  - 802.11g – Backwards compatible with 802.11b devices, but with improved security enhancements over 802.11. Up to a 54Mbps link over the 2.4Ghz band.

Best **Practices**

- **Access Control**
  - Who can access your WLAN?
- **Monitoring**
  - How do you know that others aren't accessing your WLAN?
- **Privacy**
  - OK, access is restricted what about your data?



Access **Control**

- **Broadcasting SSID – turn OFF**
  - SSID is an acronym for Service Set Identifier. In other words, this is the name of the network. (i.e. Smith's Network, Starbucks, TCPL, etc).
  - Not full proof, but good first defensive layer.
- **MAC Authentication – turn ON**
  - Media Access Control (MAC) Address is a unique address that each network device has burned into it by the manufacturer.
  - Again not full proof, but very good defensive move.
- **Lock down your WLAN router!**
  - Change the default password.
  - Turn off remote access if you know you won't use it.

WLAN **Monitoring**

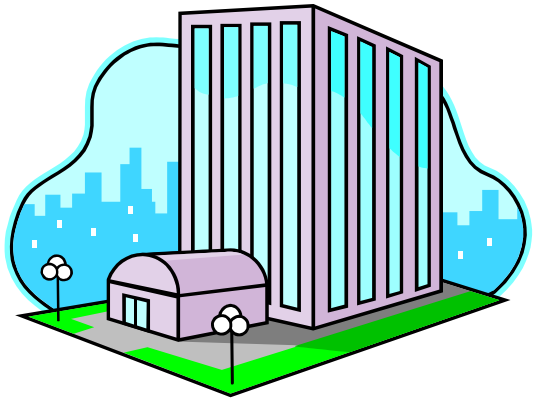
- **DHCP listing**
  - See what addresses are being used. Limit them to number of authorized devices.
- **Access logs**
  - See what web sites have been visited.
  - Good way to track down Spyware too.

Data **Privacy**

- **Encryption**
  - Turned OFF by default…turn it ON!
  - 104bit WEP is better than nothing…
- **WEP Vs WPA-PSK**
  - Wired Equivalent Privacy
    - 40/64/104 bit encryption
    - Static keys
  - WiFi Protected Access – Preshared Key
    - WEP replacement, Ideal for home/SOHO environments
    - Individual, dynamic WEP keys.

Enterprise **Initiatives**

- Based on Standards
  - Site Survey
  - AAA
  - Confidentiality
  - Monitoring
  - Vulnerability Assessment
  - AP Management



Site **Survey**

- Where to place your access points?
  - Common areas, meeting rooms, classrooms, libraries
- Actual AP placement in a room?
  - Away from electronic interference
  - RF

Access, Authentication, **Accounting**

- IEEE 802.1X Standard
  - User and device authentication
    - LDAP and RADIUS
  - Role based access control
    - Who has access to what, when do they have access to it, from where can they access it?
  - Improved audit trail
    - Time stamp network access and traffic to a particular user and particular device.

Data **Privacy**

- IEEE 802.11i Standard
  - Wifi-Protected Access
    - AES256 encryption
    - Support for client certificates
    - No shared secrets with clients
  - Authentication - device or user, both
  - Accounting - When & what
  - Access – Limiting resource access

WLAN **Monitoring**

- Capacity planning
  - What APs are being used, which aren't?
- Quality of service
  - Detection of signal interference
  - Bandwidth degradation
- Security concerns
  - Who, when, what, why and how?

Vulnerability **Assessment**

- Viruses, Trojans, Worms, Oh My!
  - Goal - Keeping the network clean
  - Mobile devices, where have they been?
  - Patch level
  - Software inquiry
    - Virus scanner
    - Firewall
    - Hacker tools

AP **Management**

- One network…
  - Many APs, single configuration
    - Multi-vendor, varying models, common settings
  - Making modifications across the entire enterprise
    - Eg. Changing the address of the DHCP server for 1800+ APs

Enterprise **Risks**

- Different than Home/SOHO
- Many different entry points into the network
- Various resources needing protection
- Various devices, multitude of users

Rogue APs

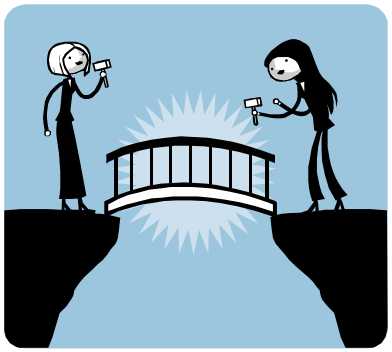
- Unauthorized APs
  - Access point allowing open access
- Authorized but misconfigured APs
  - Access point that may be interfering with normal network operations (DHCP, etc)
- Neighboring APs
  - Not on your network, but luring your users away

Ad-Hoc **Networks**

- User to user networking
  - Technology is good, security is weak
  - Users generally unaware it's happening
  - Awareness is #1 protective measure

Bridging

- Bridging the gap between WLAN & LAN
  - Devices attached to the LAN and participating on the WLAN
  - Direct access to the LAN via user's WLAN antenna



Recap

- WLAN availability is growing…
- Access control important to WLAN implementation
- Encryption is **WORTH** the extra effort!
- Proactive monitoring will reduce support costs and lower security risks
- Stick to the standards!!!

Questions / **Comments?**

Contact **Information**

George Bailey

Information Security

Ivy Tech Community College of Indiana

Email: gbailey@ivytech.edu

Phone: (317) 921-4526