SECURITY
PROFESSIONAL SERVICES
www.securityps.com

Strategic Information Security.

Wireless Network Security

Technologies, Guidelines & Management

By: Steve A. Rodgers

Partner, Information Security Consultant

NebraskaCERT 2003 - August 6th

Objectives

- Overview of Wireless Networking
- Wireless Security Risks
- Technologies to Mitigate Risk
- Guidelines for Secure Wireless Implementation and Management
- Wireless Network Security Resources

Ó 2003 Security Professional Services, Inc. All rights reserved.

SECURITY
PROFESSIONAL SERVICES
www.securityps.com

Strategic Information Security.

Overview of Wireless Networking

Overview of Wireless Networking

Types of Wireless Networks

- 900 MHz
- HomeRF
- Bluetooth
- WiFi™ – 802.11 Technologies

Ó 2003 Security Professional Services, Inc. All rights reserved.

Overview of Wireless Networking

802.11 Technologies

Wireless Standard	802.11b	802.11a	802.11g
Speed	11 Mbps	54 Mbps	54 Mbps
Frequency	2.4 GHz	5 GHz	2.4 GHz
Encryption	64, 128-bit	64, 128, 152-bit	64, 128-bit
Hotspots	Yes, and growing rapidly	Very Few	Compatible with 802.11b Hotspots
Compatibility	Only 802.11b	Only 802.11a	802.11g and 802.11b

Ó 2003 Security Professional Services, Inc. All rights reserved.

Overview of Wireless Networking
Growth of Wireless Networks

- **Gartner predicts there will be 4.2 Million WLAN users by the end of 2003**
- **By 2007 they predict more than 31 Million**

At least Seven fold growth in just four years!!!

Ó 2003 Security Professional Services, Inc. All rights reserved.

Overview of Wireless Networking
Why Such Growth?

- **Mobility**
- **Convenience**
  - **Ease of network setup (Access Point)**
  - **Speed and simplicity of client installation (Laptop, PDA, etc.)**
- **Increased Productivity**
- **Ubiquitous Hotspots:**
  - **Cometa Networks and McDonalds – "The Extra Value Meal" including Free Wireless Access?**
  - **SBC Communications – plans to deploy 2,000 hot spots**
  - **Sprint just announced PCS Wi-Fi service in 800 locations by the end of the summer**
  - **Gartner forecasts 9.3 Million Hotspot visitors in 2003, up from 2.5 Million in 2002**

All these benefits should be balanced against the risk…

Ó 2003 Security Professional Services, Inc. All rights reserved.

SECURITY
PROFESSIONAL SERVICES
www.securityps.com

Strategic Information Security.

Wireless Security Risks

Wireless Security Risks

Security Issues are Numerous…

- Packet capture and analysis
- Network mapping
- Target profiling and identification
- Information/identity theft
- Denial of Service (DoS)
- Peer-to-peer hacking
- Social engineering
- Unauthorized access and/or control

Ó 2003 Security Professional Services, Inc. All rights reserved.

Wireless Security Risks

Primary Concerns

- **Access to internal resources from remote locations**
- **Capturing information – sensitive emails, credit card numbers, usernames and passwords**

This puts at risk the organizations:
Confidentiality, Integrity, and Availability…

Ó 2003 Security Professional Services, Inc. All rights reserved.

Wireless Security Risks
A History of Security Problems…

- WEP, the link encryption mechanism used by 802.11b was flawed from the design stages:
  - Two Universities cracked WEP… In one case it only took them eight hours
  - It took AT&T Labs only 15 minutes
- Tools such as AirSnort or WEPCrack are readily available
- May of 2002 – Best Buy pulled its wireless point-of-sale systems after an anonymous hacker captures credit card numbers

Ó 2003 Security Professional Services, Inc. All rights reserved.

Wireless Security Risks
Denial of Service (DoS)

- **Wireless networks are extremely vulnerable to DoS attacks**
- **2.4 GHz frequency range used by 802.11b and 802.11g is very susceptible to interference from cordless phones and microwaves**
- **System criticality?**
  - **POS**
  - **Inventory and shipping**
  - **Wireless Security Cameras**
  - **VoIP?**

Ó 2003 Security Professional Services, Inc. All rights reserved.

Wireless Security Risks

Signal Propagation and Wardriving

- **Signals from the Access Points and Clients travel through building structures**
- **Hacking 802.11b can be done for under $1000!**

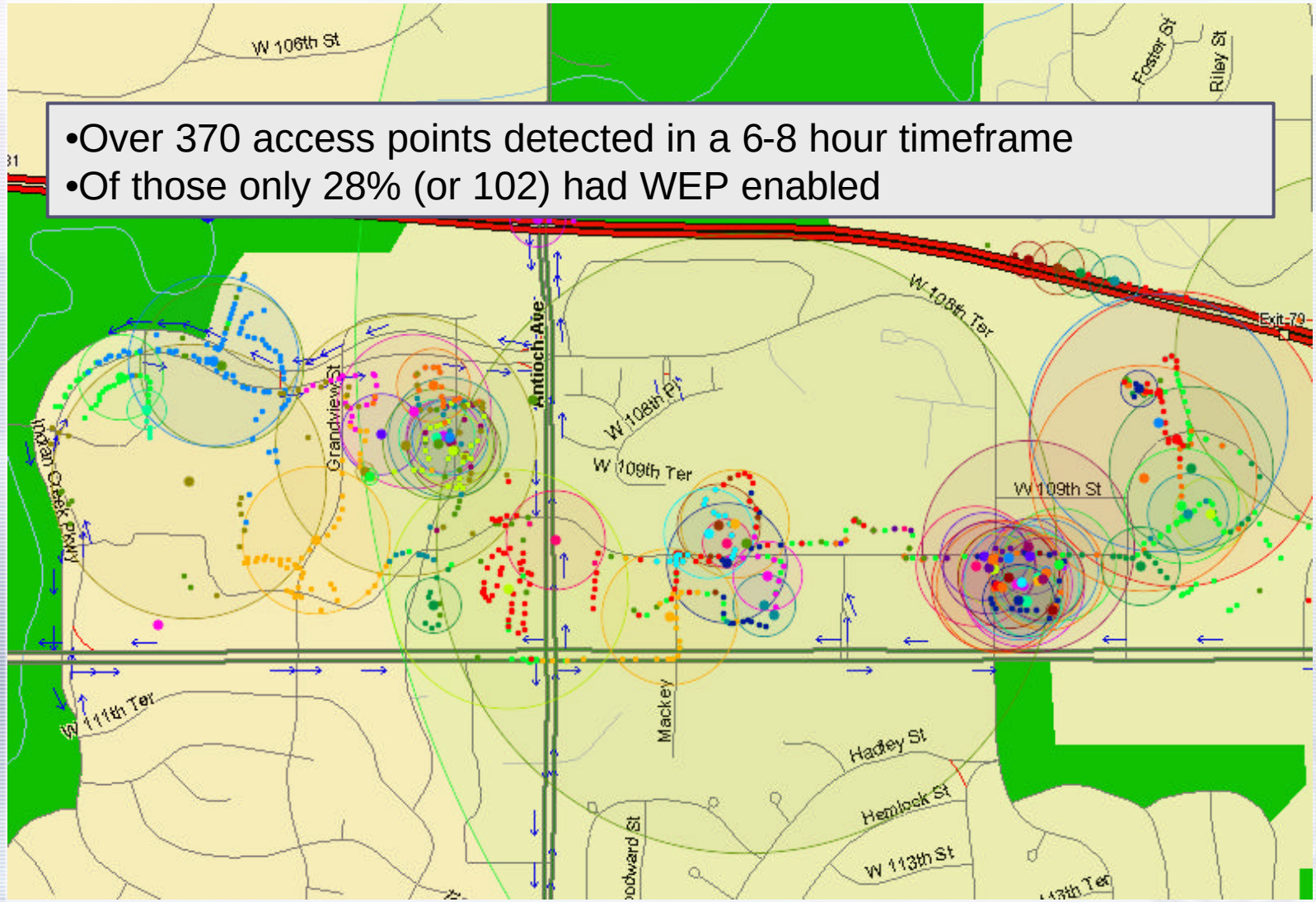
	Description	Cost
Hardware	**Wireless NIC**	**~ $70**
	Laptop (used)	**~ $600**
	Omni Antenna	**~ $60**
	GPS (optional)	**~ $200**
Software	**Kismet, NetStumbler, BSD Airtools**	**Free**
	Ethereal	**Free**

Or, just use a PDA, wireless NIC, and some free software for under $500!

© 2003 Security Professional Services, Inc. All rights reserved.

Wireless Security Risks

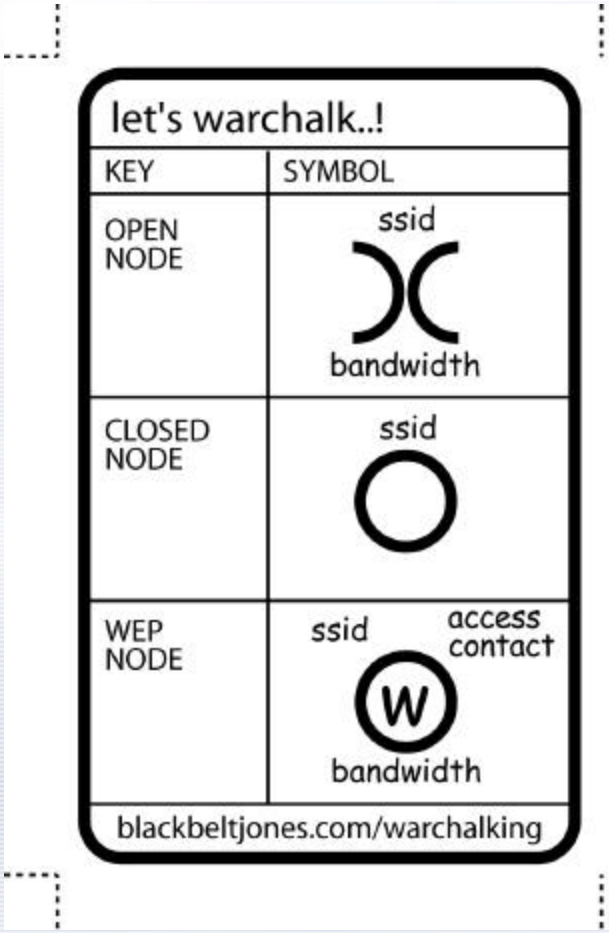
Security PS Wireless Security Survey – Dec 2003



- Over 370 access points detected in a 6-8 hour timeframe
- Of those only 28% (or 102) had WEP enabled

© 2003 Security Professional Services, Inc. All rights reserved.

Wireless Security Risks
Warchalking Example



Source: www.warchalking.org

© 2003 Security Professional Services, Inc. All rights reserved.

SECURITY
PROFESSIONAL SERVICES
www.securityps.com

Strategic Information Security.

Technologies to Mitigate Risk

Wireless Security Technologies

Authentication Mechanisms

- **802.1X – Currently available**
  - **Extensible Authentication Protocol (EAP) over a LAN or WLAN**
  - **Typically uses a RADIUS server**
- **802.11i – Standard still being ratified**
  - **Comprised of two primary components:**
    - **Robust Security Network (RSN) – provides authentication component**
    - **Wi-Fi Protected Access (WPA) – provides encryption component**

© 2003 Security Professional Services, Inc. All rights reserved.

Wireless Security Technologies

Encryption Mechanisms

- **WEP – Wired Equivalent Privacy**
  - **Numerous security issues**
  - **Flawed from the initial design phase**
- **WPA – Wi-Fi Protected Access™**
  - **Designed to address security weaknesses found in WEP**
  - **Harder to "crack" with increased key size and life**
  - **Generates and distributes encryption keys automatically using Temporal Key Integrity Protocol (TKIP)**
  - **Introduces integrity check on the header**
  - **Can be implemented one of two ways:**
    - **Enterprise Mode - Using 802.1X and a RADIUS Server**
    - **Home Mode – Uses Pre-shared Keys (PSK)**

Ó 2003 Security Professional Services, Inc. All rights reserved.

Wireless Security Technologies

Virtual Private Networks (VPNs)

- **VPNs provide end-to-end encryption and in many cases enterprise level authentication**
- **VPNs typically use protocols such as:**
  - **IPSec**
  - **SSL**
  - **L2TP**
  - **PPTP**
- **Defense-in-depth:**
  - **Using WPA and a VPN together will create a very strong security barrier on your wireless network**
- **Leverage existing VPNs if they are already deployed in your environment**

VPNs provide increased security, but may add complexity and cost if not already deployed

Ó 2003 Security Professional Services, Inc. All rights reserved.

Wireless Security Technologies

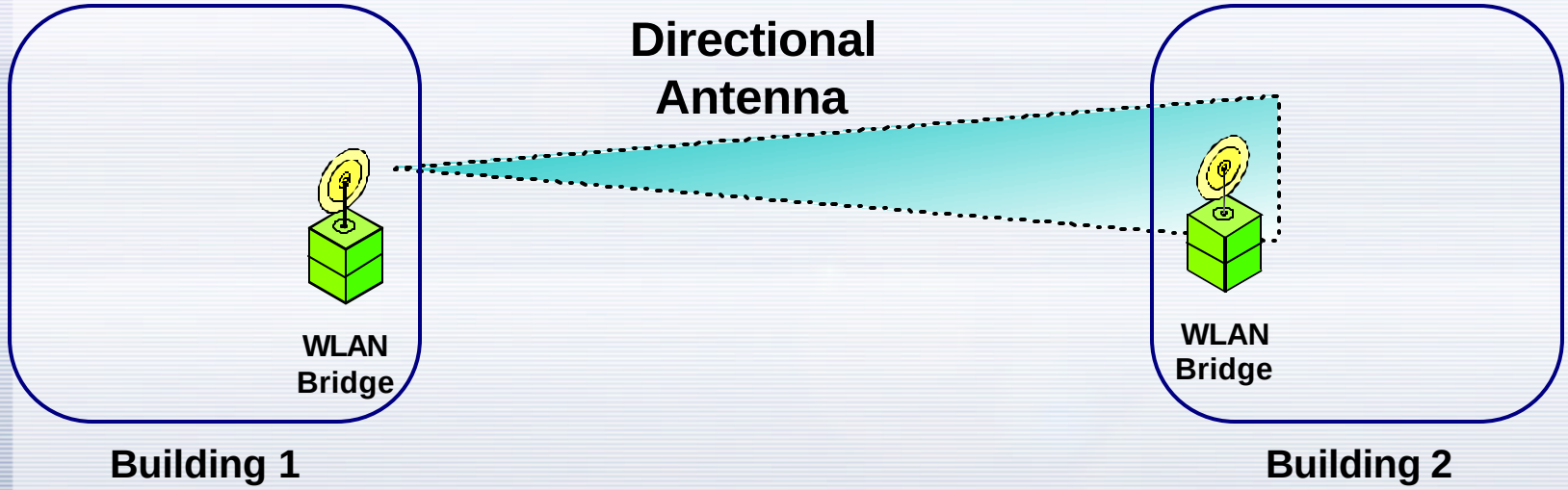
Antennas and Signal Propagation

- Signal propagation can be controlled with antenna selection
- Three primary types of antennas:
  - Omni
  - Sector
  - Directional
- Signal strength can be configured on the Access Point (AP) or client wireless card

Ó 2003 Security Professional Services, Inc. All rights reserved.

Wireless Security Technologies

Antenna Type and Placement



Ó 2003 Security Professional Services, Inc. All rights reserved.

Wireless Security Technologies
Wireless LAN Monitoring and Probes

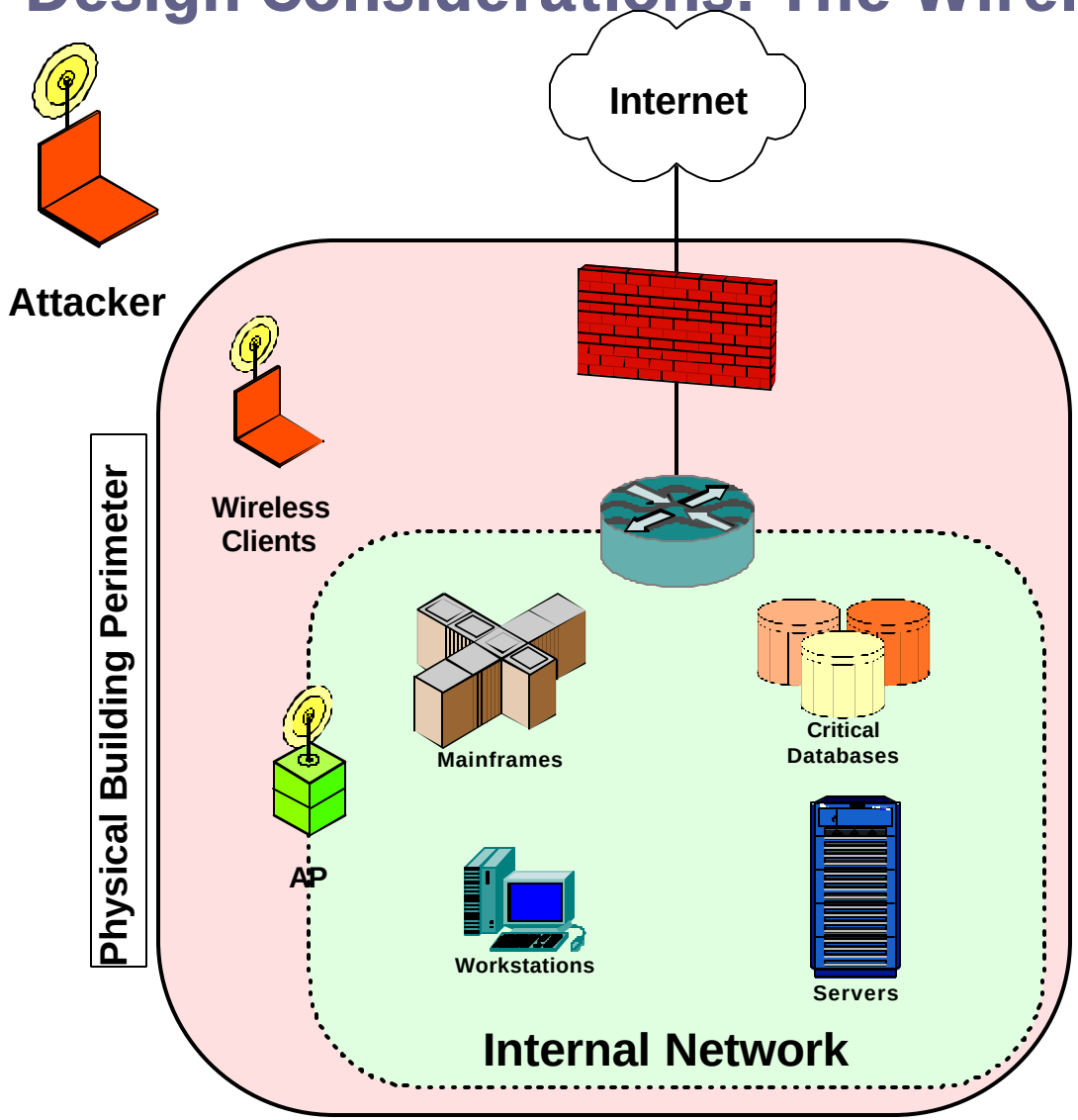
- **These probes determine the presence and location of Wireless APs:**
  - **AirDefense – RogueWatch**
  - **AirMagnet – AirMagnet Distributed**
  - **WiMetrics - WiSentry**

Monitoring Probes can run from $3,000 to $7,000 per probe and up. Is this solution overkill? It depends…

Ó 2003 Security Professional Services, Inc. All rights reserved.

Wireless Security Guidelines

Design Considerations: The Wireless LAN



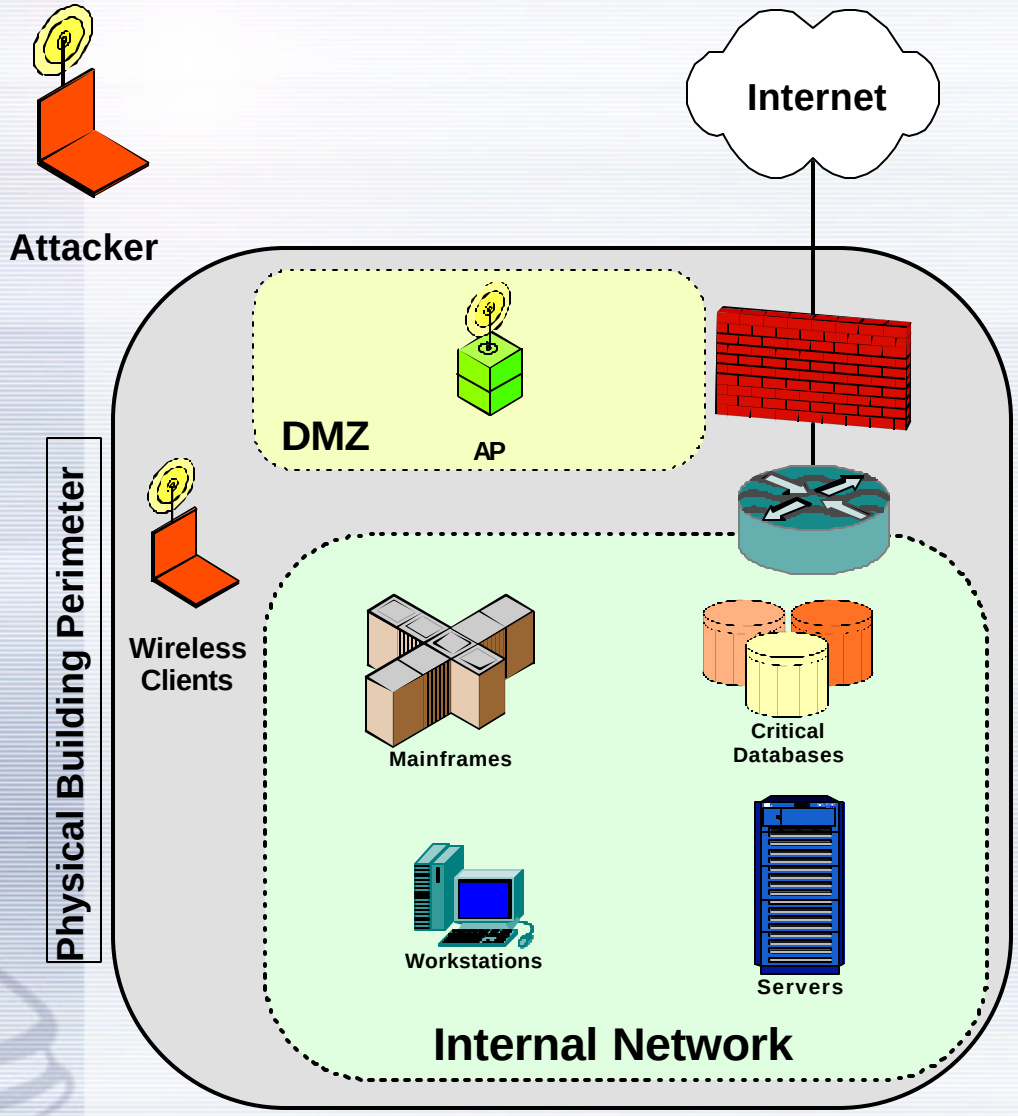
What's wrong here?

- Wireless connects to Internal network
- Little ability to protect, monitor and enforce policy

Ó 2003 Security Professional Services, Inc. All rights reserved.

Wireless Security Guidelines

Design Considerations: The "Improved" Wireless LAN



Benefits:

- Segmented WLAN network governed by firewall
- Ability to enforce network policy
- Improves ability to securely manage Internal network(s)

© 2003 Security Professional Services, Inc. All rights reserved.

Wireless Security Guidelines

Wireless Client Security

- Security of the wireless clients is critical!
- Even if you have:
  - Wireless DMZ
  - WEP and/or WPA
  - Even if you isolate APs in a DMZ don't forget about the individual security of the clients
- The attackers can go right after the clients themselves
- Make sure the client are hardened
- Install on each client:
  - Personal Firewall/IDS
  - Anti-virus

© 2003 Security Professional Services, Inc. All rights reserved.

Wireless Security Guidelines

Securely Deploying APs

- **Change the SSID**
- **Disable SSID Broadcast**
- **Change the default password for AP Management**
- **Enable MAC Address Filtering (depending on your environment)**
  - **Default deny - use "Permit Only" and NOT "Prevent"**
- **Configure Encryption (WEP or WPA)**
- **On 802.11g devices configure mode of operation:**
  - **802.11g only**
  - **Mixed mode (802.11b and 802.11g)**

SSID changes don't increase security levels much, but will keep clients configured with "default" settings from accessing your AP

Ó 2003 Security Professional Services, Inc. All rights reserved.

Wireless Security Guidelines
Antenna Type and Placement

- **Choose the best antenna for the situation:**
  - **Omni**
  - **Sector**
  - **Directional**
- **Aim sector and directional antennas towards the inside of the building**
- **Test signals from both inside building and outside**
- **Possibly adjust transmitter power on AP to keep signals inside building**

Ó 2003 Security Professional Services, Inc. All rights reserved.

Wireless Security Guidelines

Education is Critical

- **Educate end-users (security awareness):**
  - **Make sure they understand security policies pertaining to WLANs**
  - **Connect only to "known" APs**
  - **No "ad-hoc" connections**
- **Educate Network/System Admins**
  - **Policies**
  - **No rogue APs should be installed**
  - **How to securely deploy APs and clients**
- **Educate Help Desk**
  - **How to troubleshoot authentication issues**
- **Educate Security Analysts**
  - **How to test for rogue APs**
  - **How to review configurations and setting for policy compliance**

Ó 2003 Security Professional Services, Inc. All rights reserved.

Wireless Security Guidelines

Other Issues to Consider

- **Easy to deploy does not = secure**
- **Make provisions for:**
  - **Security complexities**
  - **Management complexities**
  - **Periodic wireless security site surveys and assessments**
  - **Other issues?**

Ó 2003 Security Professional Services, Inc. All rights reserved.

Conclusion
Final Thoughts

- **Treat wireless users like “remote” users**
- **Don’t forget to secure the wireless clients**
- **Wireless Security Technologies are quickly changing**
- **Investigate and choose the right technology combinations that meet your security requirements**
- **Conduct periodic wireless security site surveys and assessments**

Ó 2003 Security Professional Services, Inc. All rights reserved.

SECURITY
PROFESSIONAL SERVICES
www.securityps.com

Strategic Information Security.

Wireless Network Security Resources

Wireless Network Security Resources

URLs

- The Unofficial 802.11 Security Web Page
  http://www.drizzle.com/~aboba/IEEE/
- Wi-Fi Alliance - Wireless Protected Access™
  http://www.weca.net/OpenSection/protected_access.asp
- Wireless/802.11 Security and Wardriving Resources
  http://www.wardrive.net/
- NIST 802.11 Wireless LAN Security Workshop
  http://csrc.nist.gov/wireless/
- Security PS Web Site, Resources:
  http://www.securityps.com

© 2003 Security Professional Services, Inc. All rights reserved.

SECURITY
PROFESSIONAL SERVICES
www.securityps.com

Strategic Information Security.

Thank You!

Steve A. Rodgers, CISSP

Further Questions, Comments, or Suggestions Email:
srodgers@securityps.com