Assignment 1-3-5

Project Whitepaper

ITEC495-V1WW

Instructor: Wayne Smith

Jim Patterson

Table of Contents

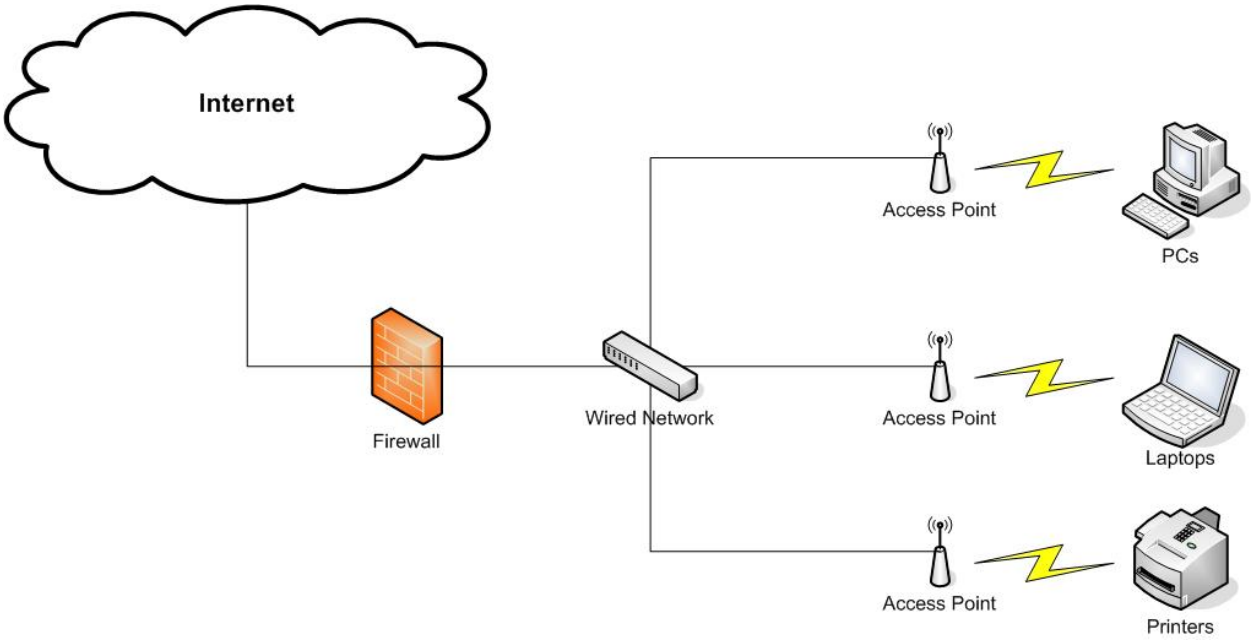
1. Abstract

Wi-Fi networks or W-LANs have been employed by home users to create an instant home network due to their flexibility and mobility, ease of installations and lower implementation costs compared to installing wired cables for several years. This surge in popularity and the numerous advantages has created a desire by companies to harness these abilities for the use in an enterprise environment. Wi-Fi's (Wireless Fidelity's) explosion though has caused demand to push ahead of solid security practices and the availability of IT professionals able to manage these wireless networks. To add to the mix there are several frequencies in which these networks can operate in with different security implementations. This white paper looks to identify they best balance of security and usability to support the mobile needs of companies.

2. Introduction

The purpose of a WLAN network is the same as the wired network. It provides a way for users to connect to a network but with WLAN it is provided without having a physical network cable attached to the users' computer. Data is transmitted over air via radio frequencies. W-LANs are made up of one or more access points that act as connectors between a companies wired and wireless Ethernet. Wireless network standards used today The WLAN (802.11) specifications are defined by IEEE (Institute of Electrical and Electronics Engineers). These standards include 802.11a,

802.11b, 802.11g, 802.11n, 802.1x, 802.11e and 802.11i. The most common standard and the ones that will be discussed in this white paper are 802.11a, 802.11b, 802.11g, and 802.11n. 802.11n was recently ratified by the IEEE as a standard on September 11, 2009. The most common standard used in today's industry is the 802.11g standard. It operates in the 2.4GHz spectrum and can allow for data transfers of up to 54Mbps.



Basic Wireless Network Diagram

3. Analysis

a. Wireless Strengths

- Faster, Cheaper and Easier to Deploy – There is no need to run Ethernet wires to each endpoint.

- Mobility and Flexibility – Endpoints can access the network from anywhere in range of the wireless network. This can improve productivity through ease of access to resources.
- Reduced Cost-of-Ownership – In dynamic environments requiring frequent moves and changes, endpoints can be moved around dynamically without the tether of an Ethernet cable.
- Scalability – Additional access points can be quickly added where connections are needed with minimal setup time.

b. Wireless Weaknesses

- Rogue Access Points
    i. Employee Implementations – employees can setup access points with no security that can allow anyone to connect to the internal network that has a wireless card.
    ii. Hacker Implementations – Hackers can setup access points to trick employees into connecting to their network instead of the secure company network.
- Poor Security Implementation on Access Points – With wireless networks visible to anyone with in range, security holes are more vulnerable to attack from hackers.

- Limited Bandwidth – W-LANs offer a reduced speed over wired networks therefore any network intensive activities are more likely to adversely affect others on the WLAN.
- Knowledge – WLAN security knowledge requires a new set of skill over what is required to secure a wired network. This knowledge is often missing or lacking.

c. Wireless Security Types

Type	Key Type	Encryption Scheme	Additional Authentication
Wired Equivalent Privacy (WEP)	Shared key	RC4 encryption 24bit	None
Wi-Fi Protected Access (WPA)	Temporal Key Integrity Protocol (TKIP) – dynamic key	RC4 encryption 48bit	Extensible Authentication Protocol (EAP) - allows for external authentication.
Wi-Fi Protected Access 2 (WPA2)	Variable cipher key lengths of 128, 192 or 256 bits.	Advanced Encryption Standard (AES) 128bit	Wireless Robust Authentication Protocol (WRAP) and Counter with Cipher Block Chaining Message authentication code Protocol (CCMP).

d. Wireless Standards

Type	Frequency	Maximum Speed	Maximum Range (meters)	Compatibility	Security Types Available
802.11a	5GHz	54 Mbps	15m	None	WEP, WPA, WPA2
802.11b	2.5GHz	11 Mbps	45m	802.11a	WEP, WPA, WPA2
80211.g	2.5GHz	54 Mbps (up to 108 Mbps with extensions)	45m	802.11a 802.11b	WEP, WPA, WPA2
802.11n	5 GHz	600Mbps	91m	802.11b 802.11g	WEP, WPA, WPA2

4. Solution Discussion

Evaluating wireless technology is a three fold process. The first selection that must be made is a selection of a wireless standard. Available choices are 802.11a, 802.11b, 802.11g, and 802.11n. Important factors to consider when choosing a wireless standard are speed, range, compatibility and possible interference. 802.11a and 802.11n both operate in the 5GHz frequency range. Operating in this range reduces the interference from such devices and cordless phones, microwaves, and Bluetooth devices to name a few. 802.11n offers the best speed and range of the selected standards. 802.11g and 802.11n presents the greatest compatibility with the other standards each with the ability to support two other standards other than its own. Using these criteria 802.11n

offers the best combination of speed, range, and compatibility, with the least amount of possible interference.

The second choice that must be made is the security implementation. Available choices are WEP, WPA, and WPA2. All of the security technologies are vulnerable to DoS (Denial of Service) attacks such as RF jamming, data flooding, or Layer 2 session hijacking. While these attacks will not compromise the network, they will disrupt communication. WEP is the oldest of the technologies and is by far the least secure. A team at the Technische Universität Darmstadt has been able to get the key for a WEP enable access point with a 95 percent probability of success in as little as two minutes. (Bangeman, 2007) This makes this security technology completely unacceptable in an enterprise environment. Additionally each computer that connects uses this shared key to connect. Once the vulnerabilities in WEP are exploited a hacker has complete access to the network and can launch attacks against other network resources from the inside.

The next step up in wireless security is WPA. WPA was created to correct the vulnerabilities in WEP. While it performs admirably it is not without its own vulnerabilities. While vulnerabilities exists in WPA such as in the Temporal Key Integrity Protocol (TKIP) of WPA with proper security implementations these can be mitigated. For the majority of wireless setups WPA is adequate. The problem is adequate security is only a step away from vulnerable. WPA and WPA2 both offer up ways for clients to authenticate with a network device. By authenticating, security is improved due to a secondary level of security. The more layers of security available the harder it is for a hacker to get through. Lastly, WPA2 was created as an improved version of WPA.

WPA2 works to further the security of wireless networks by offering greater encryption, an improved authentication method using Wireless Robust Authentication Protocol (WRAP) and Counter with Cipher Block Chaining Message authentication code Protocol (CCMP). This combination with the improvements included from WPA makes WPA2 the best choice for securing a wireless network.

A final consideration when choosing a wireless network technology is cost. The nice thing about cost of wireless technology is that the price difference is negligible. Device today primarily come in two varieties: 802.11a,b,g and 802.11b,g,n with some covering all four of the primary standards. In this category there is no winner. It primarily comes down to the standards a company wants to offer to its users. In private wireless networks the standard can be controlled and only specified standard can be allowed. This not only reduced the implementation time it also improves security by reducing the possible standards that can be used.

5. Evaluation Criteria

The technologies were evaluated primarily on the following criteria listed in order of importance.

- Security/Vulnerabilities – Types of security implementations available. Number of vulnerabilities.
- Speed – Data transfer rate.
- Availability – Market availability of hardware.

- Support – documentation/community information.
- Range – Quality of service vs. range of access point.
- Cost – Infrastructure costs.

6. Solution Selection and Reasoning

a. Standard – 802.11n

- Offers the highest available security in WPA2.
- Backwards compatible with 802.11b and 802.11g devices. (802.11a compatibility available on more expensive devices.)
- Greatest maximum range at 70 meters.
- Less interference with other common devices such as cordless phones and Bluetooth.

b. Security Model – WPA2

- Has the fewest number vulnerabilities of possible choices.
- Offers the highest encryption rate.
- Network keys are variable and dynamic.
- Offers multiple authentication modes.
- Highest possible security available.

7. Conclusion

Choosing 802.11n as the wireless standard has developed into the go to choice with finalization of a standard on September 11, 2009. It is backward compatible with older 802.11g or 802.11b gear. Additionally, it supports much faster wireless connections over a longer distance. The thing to note is that older standards such as 802.11g or 802.11b will not benefit from the faster speed or greater range. Most laptops today that come with a wireless card have an 802.11g/b card. This is rapidly changing and in the not so distant future all laptops will come with 802.11n cards.

As more corporations start to implement wireless networks due to user demand, the IT staff for the organization must recognize the security threats wireless poses. Businesses need to plan and take proper security measures before during, and after implementing a wireless networks in their environment to protect valuable data against any potential attack. WEP security is full of vulnerabilities and for a basic hacker can be compromised in a matter of seconds. It should be avoided at all costs. WPA while better still has its vulnerabilities and should be used with caution. If at all possible WPA2 should be used. The key to securing the wireless network is implementing best practices from endpoint to the network layer. An additional key is frequent auditing of security policies and practices. This will help strengthen the wireless security and keep information up to date and relevant.

While choosing the latest and greatest in technology is not always a wise choice, when dealing with wireless it pays off. The latest standard offers the best combination of speed and range while offering the highest available security options. Lastly selecting

the latest standard means that the current hardware will be usable a lot longer. Reducing the hardware turnover can greatly improve its return on investment.

8. References

Bangeman, E. (2007, April 4). *New Attack Cracks WEP in Record Time*. Retrieved from http://arstechnica.com/hardware/news/2007/04/new-attack-cracks-wep-in-record-time.ars

Cerruzi, P (2003). A history of modern computing. (2nd). Cambridge, MA, MIT Press.

Miller, B. (2009). *WPA2 Security: Choosing the Right WLAN Authentication Method for Homes and Enterprises*. Retrieved from http://viewer.bitpipe.com/viewer/viewDocument.do?accessId=10963901

Moscaritolo, A. (2008, November 7). Vulnerability Discovered in WPA Encryption . Retrieved from http://www.securecomputing.net.au/News/127719,vulnerability-discovered-in-wpa-encryption.aspx

Neoh, D. (2003, December 12). *Corporate Wireless LAN: Know the Risks and Best Practices to Mitigate Them*. Retrieved from http://www.sans.org/reading_room/whitepapers/wireless/corporate_wireless_lan_know_the_risks_and_best_practices_to_mitigate_them_1350

Reynolds, G (2007). Ethics in Information Technology. (2nd). Boston, MA, Thomson.

Whitman, M., & Mattord, H. (2009). Principles of information security (3rd ed.). Boston: Thomson Course Technology, Inc.