Determining Wireless Local Area Network (WLAN) Vulnerabilities on Academic Network

Fazli Azzali, Amran Ahmad, Ali Yusny Daud

College of Arts and Sciences
Universiti Utara Malaysia,06010 Sintok, Kedah
{fazli, amran, aliyusny}@uum.edu.my

ABSTRACT

The advancement and proliferation of wireless local area network nowadays have driven for an alarm on the whole network operation. The concern applies to both business and academic computer network environments. This paper describes our research and experiences in performing network vulnerabilities analysis in academic local area network. The research uses network vulnerability analysis methodology to perform vulnerability analysis on Academic and Administration building. From the analysis, the overall network security level can be determined. Remedies and solution to counter any vulnerability can also be prescribed and this will reduce network vulnerability threat to academic local area network.

Keywords
WarDriving, network vulnerabilities, vulnerability analysis

1.0 INTRODUCTION

Wireless technology gives users the freedom of mobility, gives network designers more options for connectivity, and gives many new devices the capability to connect to network. However, wireless technology brings significantly more threats or vulnerability than traditional wired networks. The issue of network vulnerabilities of wireless Local Area Network (LAN) is very demanding in managing computer network. With increasing faults and attacks on network infrastructure, there is an urgent need to analyze networks and services vulnerabilities under organize fault attack.

Vulnerability is flaw or weakness in a system's design, implementation or operation and management that could be exploited (Qu et al., 2001). Network vulnerabilities refer to the impact of attacks and fault on computer network. It is a point where the network is susceptible to attack. The network vulnerabilities analysis is systematic examination of computer network to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

Identifying organizational network vulnerabilities is a part of vulnerability risk assessment. Identifying vulnerabilities in enterprises can be divided into two step vulnerabilities by asset and vulnerabilities by class (Myerson, 2002). Traditional assets are consists of hardware, software, network and communications, human resource, facilities, data mechanism, disaster recovery procedures, and organizational resources. Each assets have a different vulnerabilities and poses different set of test. Vulnerabilities by class is identified by a group of assets into classes that from a threat. Network vulnerabilities analysis (NVA) performs a systematic test on the wireless network to identify any threats.

One way of protecting the corporate information system is to reduce, mitigate or eliminate the risk of actual threats from occurring by doing some good risk management program and treat it as number one priority for security policy and each risk assessment process consists of five variables: assets, threats, vulnerabilities, risks and control (Myerson, 2002).

2.0 WLAN VULNERABILITIES

The security services are provided largely by the Wired Equivalent Privacy (WEP) protocol to protect link-level data during wireless transmission between clients and the access points. WEP does not provide end-to-end security, but only for the wireless portion of the connection (Karygiannis & Owens, 2002).

WLANs are vulnerable and it is a good idea to follow a few simple tips to better protect your WLAN. Hackers are smart too but when your WLAN is protected, they may get frustrated and give up. Key problem with existing 802.11 are listed below (Karygiannis & Owens, 2002)

- Security features in vendor products are frequently not enabled - Security features, albeit poor in some cases

are not enabled when shipped, and users do not enable when installed. Bad security is generally better than no security.

- Initial Vector (IV)s are short (or static) - 24-bit IVs cause the generated key stream to repeat. Repetition allows easy decryption of data for a moderately sophisticated adversary.
- Cryptographic keys are short - 40-bit keys are inadequate for any system. It is generally accepted that key sizes should be greater than 80 bits in length. The longer the key, the less likely a comprise is possible from a brute-force attack.
- Cryptographic keys are shared - Keys that are shared can compromise a system. As the number of people sharing the key grows, the security risks also grow. A fundamental tenant of cryptography is that the security of a system is largely dependent on the secrecy of the keys.
- Cryptographic keys cannot be updated automatically and frequently - Cryptographic keys should be changed often to prevent brute-force attacks.
- Rivest Cipher 4 (RC4) has a weak key schedule and is inappropriately used in WEP - The combination of revealing 24 key bits in the IV and a weakness in the initial few bytes of the RC4 key stream leads to an efficient attack that recovers the key. Most other applications of RC4 do not expose the weaknesses of RC4 because they do not reveal key bits and do not restart the key schedule for every packet. This attack is available to moderately sophisticated adversaries
- Packet integrity is poor - Cyclic Redundancy Check 32 (CRC32) and other linear block codes are inadequate for providing cryptographic integrity. Message modi cation is possible. Linear codes are inadequate for the protection against advertent attacks on data integrity. Cryptographic protection is required to prevent deliberate attacks. Use of non-cryptographic protocols often facilitates attacks against the cryptography.
- No user authentication occurs - Only the device is authenticated. A device that is stolen can access the network.
- Authentication is not enabled; only simple Service Set Identifier (SSID) identification occurs - Identity-based systems are highly vulnerable particularly in a wireless system because signals can be more easily intercepted.
- Device authentication is simple shared-key challenge-response - One-way challenge-response authentication is subject to “man-in the-middle” attacks. Mutual authentication is required to provide verification that users and the network are legitimate.
- The client does not authenticate the access point (AP) - The client needs to authenticate the AP to ensure that it is legitimate and prevent the introduction of rogue APs.

According to CERT® Coordination Center the number of vulnerability reports rose from 171 in 1998 to 1090 by 2000 and 633 by first quarter of 2001 (Myerson, 2002). According to Fortinet Inc’s director, today’s wireless security standards such as Wired Equivalent Privacy (WEP) and Wi-Fi protected access (WPA) protect the privacy of wireless connection via encryption, and ensure that only authorized users can connect to a wireless access point but once connected, even if encrypted can easily deliver content threats into wired network. One of the biggest communications company in country also follows the same step by not having a hotspot security applications in place because it is a public service and users have to take their own security.

3.0 RELATED WORK

Mobility that wireless technology provides has facilitated some security vulnerabilities and malicious attacks. Even with good internal security practices such as firewalls and virus protection, campus networks are still vulnerable to malware, since wireless access on college campuses allows the spread of computer viruses and worms due to laptops moving between campus and less-protected networks (Higby & Bailey, 2004). The traditional ways of protecting network for wired environments are no longer sufficient (Zhang et al., 2003).

Wireless local area networks provide a luxury of mobility to clients so that they may roam without the restriction of wires, room and/or buildings. At the same time, wireless local area networks have given birth to a new breed of network weaknesses that are compounding and exploiting current local area network vulnerabilities (Higby & Bailey, 2004).

Wireless access on college campuses facilitates the spread of computer viruses and worms due to laptops that do not have current software patches and/or antivirus protection connecting to the network (Higby & Bailey, 2004).

The nature of mobile computing environment makes it very vulnerable to an adversary’s malicious attacks. The use of wireless links renders the network susceptible to attacks ranging from passive eavesdropping to active interfering. Unlike wired networks where an adversary must gain physical accesses to the network wires or pass through several lines of defense at firewalls and gateways. Attack on a wireless network can come from all directions and target at any node. Damages can include leaking secret information, messages contamination and node impersonation. It means wireless network will not have a

clear line of defense, and every node must be prepared for encounters with an adversary directly or indirectly (Zhang et al., 2003).

WarDriving is "the act of moving around a specific area and mapping the population of wireless access points for statistical purposes" (Hurley et al., 2005). WarDriving, also called access point mapping, is the act of locating and possibly exploiting connections to wireless local area networks while driving around a city or elsewhere. It is important to note that the definition of WarDriving is not exclusive to driving around in a car. (Hurley et al., 2005) explained that "WarDriving can be accomplished by anyone moving around a certain area looking for data." People have "war drived" simply by walking around a neighborhood with a Personal Digital Assistant (PDA), or using a laptop while taking a taxi or the subway.

WarDriving is a process which an individual uses a wireless device such as a laptop or PDA to drive around looking for wireless networks (Johnson, 2005). Some people do this as a hobby and map out different wireless networks which they found. Other people, who can be considered hackers, will look for wireless networks and then break into the networks. If a wireless is not secure, it can be fairly easy to break into the network and obtain confidential information. Even with security, hackers can break the security and hack.

According to (Duntemann, 2003), a WarDriving is gathering of statistics about wireless networks in a given area by listening for their publicly available broadcast beacons. Wireless access points (APs) announce their presence at set intervals (usually 100 milliseconds) by broadcasting a packet containing their service set identifier (SSID) and several other data items. A stumbling utility running on a portable computer of some sort (a laptop or PDA) listens for these broadcasts and records the data that the AP makes publicly available.

The term is the offspring of the term wardialing, which was the practice of dialing random phone numbers via computer to find an answer modem. WarDriving provides a unique opportunity to gauge the growth of a technology market segment by direct inspection. In other words, we do not have to take a vendor's or research firm's word for how many wireless networks are out there.

It is important to understand the common threats that wireless network can face (Microsoft, 2006). The issues of vulnerabilities are explained below:

1) Disclosure of data through eavesdropping - Eavesdropping attacks on wireless traffic that is not secure can result in the disclosure of confidential data, discovery of user credentials, and can even lead to identity theft. Sophisticated attackers can use information collecting by eavesdropping to mount attacks on systems that would not otherwise be vulnerable.
2) Interception and modification of transmitted data An attacker who can gain access to network resources is also capable of inserting rogue systems into a network that can intercept and modify data en-route between two legitimate systems.
3) Spoofing - Access to an internal network provides an attacker with the opportunity to forge data so that it appears to be legitimate traffic. Such attacks can include spoofed e-mail messages that would be trusted by internal users more readily than communications from outside sources, thus providing a platform for social engineering attacks and Trojan insertions.
4) Denial of services (DoS) - No matter what security solution is implemented; a WLAN is uniquely susceptible to DoS attacks whether purposeful or accidental. Such disruptions can be the result of something as simple as a microwave oven or a device set to flood a network with indiscriminate traffic.
5) Free-loading (resource theft) - Some intruders might be after nothing more than free access to the Internet. Though not directly malicious or damaging, such activities can result in slower network connectivity for legitimate users or an unmanaged vector for malware test.
6) Accidental threats and unmanaged connections – In unsecured WLAN environments any visitor can gain access to the internal network simply by starting up a device that is capable of accessing wireless networks. Such unmanaged devices could already be compromised or supply an attacker with vulnerable point of attack against a network.
7) Rogue WLAN access points - Even if a business has no wireless network it can still be vulnerable to security threats from unmanaged wireless networks. Wireless hardware is relatively inexpensive so any employee could possibly set up an unmanaged and unprotected network within an environment.

4.0 VULNERABILITIES DISCOVERY

To do WarDriving, we need a vehicle, a computer; which can be a laptop, a wireless Ethernet card set to work in promiscuous mode, and some kind of an antenna which can be mounted on top of or positioned inside the car. Because a wireless LAN may have a range that extends beyond an office building, an outside user may be able to intrude into the network, obtain a free Internet connection, and possibly gain access to company records and other resources.

What most needed to WarDriving includes the following (Duntemann, 2003): A computer you can haul around with you. Most people use laptops. Some use PDAs based on the

PocketPC OS or Linux.

• A "stumbler" utility. By far the best known is Marius Milner's Network Stumbler for Windows, which most people call NetStumbler. Most major operating systems have stumbler programs available. Linux has Kismet; MAC OS has MacStumbler. Marius has ported NetStumbler to PocketPC, for which it's called MiniStumbler.
• A Wi-Fi client adapter supported by your chosen stumbler utility.
• An external antenna attached to your client adapter. Ideally, this is an omnidirectional vertical mounted on the vehicle roof. These are small and resemble cell phone antennas. We can wardrive with nothing more than a PC card's built-in antenna, but these antennas are wretched and will be shielded from signals to some extent by the vehicle's metal structure.
• A Global Positioning System (GPS) receiver that emits National Marine Electronics Association (NMEA) 183 formatted data. This allows the stumbler program to record where stumbled stations are located in the physical world. Technically, GPS is optional, but the stumbled data is much less useful without GPS information.
• Wireless Network Interface Card (Lucent ORiNOCO cards recommended)

5.0 VULNERABILITIES ASSESSMENT

Wireless Vulnerabilities Assessment (WVA) can be divided into two phases which are Vulnerability Testing and Vulnerability Analysis.

5.1. Vulnerability Testing

Network penetration testing means using tools and processes to scan the network environment for vulnerabilities. This helps refine an enterprise's security policy, identify vulnerabilities, and ensure that the security implementation actually provides the protection that the enterprise requires and expects. Regularly performing penetration tests helps enterprises uncover network security weaknesses that can lead to data or equipment being compromised or destroyed by exploits attacks on a network, usually by "exploiting" a vulnerability of the system),Trojans (viruses), denial of service attacks, and other intrusions. Testing also exposes vulnerabilities that may be introduced by patches and updates or by misconfigurations on servers, routers, and firewalls.

5.2 Vulnerability Analysis

The result generated from the report is needed to be analyzed. The report provides host by host security risk information and also overall security weakness in the network. It can provide us much more detail vulnerabilities on the network. From the analyzed report, the overall conclusion can be used as guideline in determine the security level faces by the organization and the types of remedies and prevention can be taken to secure the network. In practice, the need for vulnerability analysis is universally acknowledged. Commercial vulnerability scanners are good at identifying known vulnerabilities in the software. However, identifying vulnerabilities is only a small part of securing a network, and a significant issue is identifying which vulnerabilities an attacker can take advantage of through a chain of exploits. There are numerous examples of such chains in the research literature. In summary, each host on a network (hosting services or client to network services, or even accessing email messages) is expected to expose vulnerabilities to the outside world. Plugging all network vulnerabilities based on the output of a vulnerability scanning tool may render a network unusable to bonafide users. Hence there is a need for vulnerability analysis of the complete network (combining all the network applications and hosts) to chain exploits on each host to find out the reach of the attacker. Such analysis is useful since it not only pin points most serious vulnerabilities on a network which must be plugged, but also gives a basis for decision making on the placement and security of valuable resources.

6.0 RESULT

Figure 1 showed the locations of every APs available.

Figure 1. GPS Map

Table I shows the summary of the data capture such as total of access point and ad hoc, encryption off/on, and default SSID.

Table 1: *Data Captured*

Categories	No.
ALL (AP & Ad-hoc)	45
Encryption OFF	45
Encryption ON	0

Access Point	38
Ad-hoc	7
Default SSID	4
Authorize AP	29

Based on the data, total of access point were 38 units and ad hoc were 7 units. However, all of the numbers (access point and ad hoc devices) are Encryption OFF (open mode) which means no access security key (password) is needed and anybody can easily access through the access point device. Four access points had been detected for using default of the service set identifier (SSID). Moreover from 45, 29 were legal APs and the rest were unauthorized APs (rogue AP).

7.0 CONCLUSION AND RECOMM ENDATIONS

From the discussion we conclude that the vulnerabilities are elsewhere waiting to be manipulated. Some action should be taken before it is become worst. We suggest two types of solution to overcome the problems: Using WPA or WPA2 and implementing 802.1x Remote Authentication Dial In User Service (RADIUS).

• Using WPA or WPA2
Instead of OPEN and Shared AP, with 100% vulnerabilities, the management should change to CLOSE AP which implementing encryption as a secure access to each user. WEP is not a good choice encryptions mechanism however WPA/WPA2 is better as a security barrier between WLAN and LAN.

• Implementing 802.1X (RADIUS)
Another option is implementing 802.1X. As an enterprise security perimeter, this option is crucial in preventing any unauthorized user from entering into network environment.

Placing APs without proper configuration will increase the vulnerabilities to network environment. During WarDriving session a few important factors had been found such as the number of APs and Ad-hoc that not used any security method and several used default SSID. Some action should be taken aggressively to negate the problem in near future especially by implementing either WPA/WPA2 or 802.1X as the enterprise solution to prevent unauthorized user.

REFERENCES

Duntemann, J. (2003). Wireless LAN security and wardriving, from http://wardrive.net

Higby, C. & Bailey, M. (2004). Wireless security patch management system. *CITC5 '04: Proceedings of the 5th conference on Information technology education* New York, NY, USA: ACM. 165–168.

Hurley, C., Rogers, R., & Thornton, F. (2005). *WarDriving: Drive, Detect, and Defend*. Syngress Publishing.

Johnson, R. (2005). Wardriving ethics, from http://www.rjcomputerconsulting.com

Karygiannis, T. & Owens, L. (2002). *Wireless network security: 802.11, Bluetooth and handheld devices*. In National Institute of Standards and Technology: National Institute of Standards and Technology.

Microsoft (2006). *Secure Wireless Access Point Configuration*. Technical Report, Microsoft.

Myerson, J. (2002). Identifying enterprise network vulnerabilities. *International Journal of Network Management*, 135–144.

Qu, G., JayaPrakash, Ramkishore, Hariri, S., & Raghavendra (2001). *A Framework for Network Vulnerabilities Analysis*. From http://ww.ece.arizona.edu/~hpdc/projects/nvat/NV-framework.pdf

Zhang, Y., Lee, W., & Huang, Y.-A. (2003). Intrusion detection techniques for mobile wireless networks. *Wireless Network*, 9(5), 545–556.