FORENSIC ANALYSIS OF WIRELESS NETWORKS

Dyah Anggraini[1]
Syahbuddin
Fakultas Ilmu Komputer, Universitas Gunadarma
Jl. Margonda Raya No. 100 Depok 16424
[1]*d_anggraini@staff.gunadarma.ac.id*

ABSTRACT

Wireless communications has been accepted by many organizations and users as it allows to be flexible and portable with increased productivity and lower installation costs. It can be moulded and designed to address different usage and user needs. WLAN able devices allow users to move their wireless devices from place to place within the office without the need of wires and without losing network connectivity. It is a well known fact that the wireless networks are vulnerable to many attacks. Some of the attacks may include interception of sensitive information that is not encrypted and transmitted between two wireless devices. Ad hoc transmissions within the network can even compromise the security of a network. Intruders can interfere from inside or out of the network in order to gain connectivity to network management controls and thereby disrupting network resources. In most cases the attackers cannot be traced or the purpose of the attack is not known. Even though we have access to the AP's log files, it has very less information stored in it. Most of the AP's do not provide syslog facilities so that the logs can be stored at some other server. With the increase in the number of attack tools, security of wireless technologies has become a primary concern. This paper is all about building a device that would be able to watch all the WLAN data and analysing all the traffic coming and going out of the wireless AP.

Keywords: Wireless local area network (WLAN), Access Point (AP), Forensic, Wi-Fi Tools, WEP, WPA, 802.11

INTRODUCTION

Wireless networks are very common in most of the organizations and has now seen a sudden surge in the individual market. Most of laptops and other devices are wireless enabled and can be configured to any wireless networks. Wireless networks usually called as Wireless Local Area Networks (WLAN) has gained wide scale acceptance in organizations and as individual users for it allows users to be more flexible. It also increases portability and users can move from one place to another without the use of wires thus decreasing wiring costs and increasing flexibility. Wireless technologies can be designed to address user's needs and usage requirements. Ad hoc networks, allow data synchronization with network systems and application sharing between wireless devices. These wireless technologies can offer dramatic cost savings and new capabilities to diverse applications. As the service has become more and more popular and widely accepted the risks in using the wireless technologies has exponentially increased. Some of the risks involved are similar to the wired technology.

As wireless signals travel through air the risks of getting attacked by intruder's, remains extremely high. The loss of confidentiality and integrity and the threat of Denial of Service (DoS) attacks are risks typically associated with wireless communications. Unauthorized may gain

access to the internal network and may launch attacks on other system in and out of the network. As the signal is available free to air in most of the cases the intruders cannot be traced and the purpose of the attack is not known. Even though we have access point log files, it does not contain the required information. Most of the Access Points do not even provide *syslog* facilities so that the log files can be redirected to some other computer running *syslog* server. Moreover, many attack tools are available free for download that can be used easily to compromise any wireless networks. This paper would try to emphasize on computer forensic techniques used in wireless networks so that the ambiguity of intruders can be traced and purpose of the attack be known. For experimentation purposes Netgear's WG102 Wireless Access Point has been utilized along with Airtraf for wireless network analysis

THEORITICAL BACKGROUND

Threats and Vulnerabilities. The inherently open nature of wireless access compared to the wired world creates significant security concerns, chief among them are user authentication and rights enforcement. Signals may be sent indiscriminately if the access points are not configured correctly and if these signals go into the public areas can be accessed by eavesdropping. Specific threats and vulnerabilities in wireless devices have been identified as follows: All the vulnerabilities found in the wired technologies has been identified in wireless technologies as well. Intruders may gain unauthorized access to an agency's computer network through wireless connections, bypassing any firewall protections. Specific information can be intercepted and disclosed with the use of poor encryption techniques that can be easily decrypted. DoS attacks can be carried over on the wireless devices thus disrupting the service. Man-in-the-middle

attacks can be carried out to gain unauthorized access to the sensitive information being transmitted. Network injection attacks can bring down the whole network and require rebooting or even reprogramming of all intelligent networking devices. Data may be extracted without detection from improperly configured devices. Viruses and other malicious codes may corrupt data on a wireless devices and subsequently be introduced to a wired network connection. MAC address spoofing is possible to gain access to the wireless networks. Many programs are available that have network sniffing capabilities and when combined with other softwares can allow the computer to pretend it have any MAC address.(Wright, 2003)

802.11 Architecture. WLAN technology has improved drastically from its advent in the mid 1980s when the Federal Communications Commission (FCC) first made the RF spectrum available to industry. In the early days, it was relatively slow and but has improved over the years with the 802.11 technology as it provides increased bandwidth.

The 802.11 standards permit devices to operate in either peer to peer or on the basis of fixed access points to which the mobile devices or units may connect. The infrastructure mode can be used to increase the range of wireless network. The clients configured in this mode can move freely from one zone to another between the two access points without loosing any connectivity. The first access point attached to the router acts in a basic infrastructure mode that helps in serving the clients which fall under its network range. If we need to extend the range of wireless network, then multiple access points are used so that the signals can overlap allowing the wireless devices to move freely between two access points.

The WLAN infrastructure consists of wireless client stations that use radio signals in order to communicate with the wireless access points. The wireless client

stations are equipped with wireless network interface cards, which have the ability to transmit and receive radio signals with the logic of decoding the messages carried with the signals.

Typically WLANs operate in infrastructure mode. Another type of connection is an ad-hoc connection. In this type of connection mode wireless devices are connected to each other without using any access point infrastructure. This type of communication made is similar to the peer-to-peer network in the wired technology. In peer-to-peer network every computer is connected to each other and can share files and folders between each other. In this type of network there is

Wireless Lan Components. A WLAN is comprised of two essential devices – a wireless client station and access point. A station or a client is typically a notebook or a laptop with a wireless network card to communicate with the wireless access point or it may even consist of wireless enabled handheld devices such as PDA etc. The wireless network cards can be obtained in different forms. There are PCMCIA wireless cards which can be slotted in the PCMCIA card slot of notebook. One can get wireless network card in the USB format as well. These cards are used to connect the wireless client device to the WLAN network. The wireless access point is a device that connects wireless communication devices together to form a wireless network. The access point, which acts like a bridge between the wireless network and the wired network typically comprises of radio, facility to connect to wired network and the software to drive the wireless communication (Karygiannis, 2002). The AP functions as a base station to which different wireless devices can be connected.

The reliable coverage range of 802.11 WLAN depends on several factors, including data rate required and capacity, source of RF interference, physical area and characteristics, power, connectivity, and antenna usage. Theoretical ranges are from 29 meters for 11Mbps in a closed office area to 485 meters for 1Mbps in an open area. The range of WLAN can be increased by using special high gain antennas. The bridging connection of AP's allows them to communicate to exchange network traffic. Bridging involves either a point-to-point or a multipoint configuration. In point-to-point architecture two LANs are connected to each other via the LANs respective access points. Whereas, in multi-point architecture on subnet of a LAN is connected to two or more different subnets simultaneously.

Security of 802.11 Wireless Lans. The three basic security features required by a device are as follows: *Confidentiality*: The intent of confidentiality is to prevent information compromise from casual eavesdropping. *Integrity*: It was developed to ensure that messages are not modified in transit between the wireless clients and the access point in an active attack. *Authentication*: This service provides a security service to verify the identity of communicating client stations. In short, it provides the access control to the network by denying access to client stations.

Over the years many such standards such as WEP, WPA and 802.1x authentication methods were developed in order to improve the authentication and thus overall improving the security of the wireless signals.

Wired Equivalent Privacy (WEP): WEP is a widely used network security method. When you enable WEP, you set up a network security key. This key encrypts the information that one computer sends to another computer across the network. The receiving computer needs the key to decode the information so that it's difficult for some on another computer to get onto the network and access files without the users permission.

Wi-Fi Protected Access (WPA): WPA was created to improve the security of

WEP. Like WEP, WPA encrypts information, but it also checks to make sure that the network security key has not been modified. WPA also authenticates users to help ensure that only authorized people can access the network. There are two types of WPA authentication: WPA and WPA2(Alliance, 2005). WPA is designed to work with all wireless network adapters, but it might not work with older routers or access points. WPA2 is more secure that WPA, but it will not work with some older network adapters. WPA is designed to be used with an 802.1x authentication server, which distributes different keys to each other. This is referred to as WPA-2. It can also be used in a pre-shared key (PSK) mode, where every user is given the same pass phrase

802.1 x authentications: 802.1 x authentications can help enhance security for 802.11 wireless networks and wired Ethernet networks. 802.1x uses an authentication server to validate users and provide network access. On wireless networks, 802.1x can work with Wired Equivalent Privacy (WEP) or Wi-Fi Protected Access (WPA) keys. This type of authentication is typically used when connecting to a workplace network.

Most of the access points available for home use usually do not come with the new encryption technologies developed such as WPA and 802.1x authentications. The network cards even do not support the WPA and the recent 802.1x authentication standards. The manufacturing companies of these access points and wireless network cards release new firmware that supports these standards but normal users who are not technically sound don't even update the firmware to enjoy the benefits of these authentication standards. Most of the home networks even do not make use of the basic authentication type WEP which is not considered to be strong form of security measure. WEP can easily be cracked by numerous tools available freely for download. In order to secure the wireless networks people need to be encouraged to use some sort of security methods and policies.

Even though there are strong encryption techniques available to secure wireless technologies they can be cracked and the information passing through them can be exposed. Moreover, these encryption techniques only encrypt the data, but what data is being transmitted is not known. Any compromised access point can be used for sending data maliciously without the knowledge of the owner of the access point. Devices must have the ability to monitor the data being passed between two wireless devices. This poses a serious security threat and hence must be reduced in order to make wireless networks a safer technology.

Attacking Wireless Lans. The attackers can be categorized into two different categories: targeted attackers and other attackers of opportunity.

Targeted attackers are small in number and they are more dangerous than other attackers, because their aim is to attack the target system for which they are paid for. The goal of attacker of opportunity is to intrude into as many syster..s as possible with the least amount of effort. (Spitzner, 2003). The attackers usually take the opportunity of the disable security settings of the wireless networks in the home environment. The third category of attackers is called as script kiddies who just attack the system for the sake of attacking with no motive behind.

The biggest security threat in wireless LANs is the loss of confidentiality through eavesdropping. Anyone with the capability of receiving a wireless signal can potentially eavesdrop a signal between the wireless access point and a wireless client. The attack can be big drastic as private information such as passwords, financial data can be exposed. Using WEP minimizes the threat of eavesdropping, but there are numerous tools available freely on the internet to crack the WEP key.

In practice, most wireless LAN intrusions are simply an attempt to gain Internet access (Potter, 2003). Although intruders can launch attacks from the internal network to the external resources and the owners of the network could be liable for attacks launched by intruders.

Integrity of the wireless LAN is also at high stake as attackers can gain an unauthorized access to a wireless LAN and could potentially spoof the wired network so that the traffic from the wired network can be redirected to the attackers machine.

Wireless LANs are susceptible to DoS attacks. Such attacks are carried out to disrupt the transmission of certain packets so that transmission device behaves as if the channel was busy.

RESEARCH METHODS

War driving is the most commonly followed technique in order to gain access to the wireless networks in range. In this types of attacks attackers search for wireless networks and check the security of the networks. Once the target has been identified and enough data has been collected to crack the WEP key the attacker can execute an attack.

Edney (2004) identified few tools that are commonly used in carrying out these attacks, i.e. netstumber, kismet, and airtraf. Netstumbler is one of the most popular program used for war-driving as it is easy to use and install. It gives ample amount of information regarding a wireless signal such as SSID of each access point discovered, whether or not it has encryption enabled, and the channel on which it is operating. Kismet is based on Unix Operating System. It is a passive system and hence cannot be detected. It can gather almost the same information as netstumbler. Moreover, it can even collect all received packets for further analysis. Airtraf is a wireless sniffer that can detect and determine of exactly what is being transmitted through these wireless signals. It even has the capability of tracking rogue

access points and even stores the information at a different location for further analysis. This is another tool which is gain a lot of popularity in this field.

RESULT AND DISCUSSION

Studies of Wireless LAN. Study reveals that inspite of many security flaws in the wireless technology much more severe problems exist. The manufactures of the wireless access points turn off the security features available in these APs when they ship their products to the customers thus failing to implement even basic security feature available in the AP. (Shipley, 2001)

Five Components of Wireless Intrusion Protection. Thus the wireless networks must be protected from external attacks by implementing the following features in the Wireless Access Points.

Rogue Detection: The device must have the ability to accurately detect all types of rogue wireless devices – rogue APs, AP software for laptops, rogue clients, rogue bridges, ad-hoc networks on all the frequencies. Immediate notification must be given for the detected anomaly. The device must be intelligent enough to identify authorized AP, rouge AP devices

Vulnerability Assessment: A proper scanning tool must be implemented which would identify any mis-configurations occurring in the wireless setup. A proper scanning tool must be implemented to scan wireless clients for threats such as worms and viruses or any other sniffer tools.

Intrusion Detection: Real-time detection must be performed and must be intimated when any compromise has been detected. A database of wireless attacks must be maintained and it symptoms stored so that the device can immediately identify the threat. Wireless activity must be monitored constantly and proper action must be taken in case of any malfunctions

Usage Auditing: Facility to automatically audit the number of access points and wireless clients connected must

be displayed. Detection and notification scheme for an malicious activities must be maintained.

Forensic analysis: Activity logging and reporting of connection status, activity patterns, and activity transitions to monitor for acceptable use and/or analyse the footprints of a wireless hacker must be directed to a syslog server so that it can be stored for further analysis. Real-time traffic must be captured in order to detect any malicious activity going on in the network

Oasis in Desert. Consider a situation where the above mentioned war driving tools can be used for security purposes and be implemented in the AP for packet analysis, rouge AP detection and to identify other security related threats. How about developing a device that will actually be able to read the wireless associations between the wireless LANs and Access points? A very beneficial tool can be developed combining all the best features of the above mentioned tools. It must be implemented in the IOS of the router softwares so that people can take advantage of these tools and make their network secure from external attacks. Moreover, apart from making the network more secure, such devices would be of immense help in carrying out forensic analysis of the Wireless LANs. The device must have the capability of detecting other Access Points so that it can identify as a genuine or a non-genuine system.

The following screenshot shows the activity log page of a typical Wireless Access Point. With the current setups the only information shown in these logs is about the login and logoff details. Apart from this information all the information is not known. If at all we could implement a version of Airtraf into this Wireless Access Point it would be an immense help in carrying out forensic analysis as the packets captured from it can be directed to the syslog server and can be stored at a different location for later detailed analysis.

Figure 1: The screenshot is taken from Netgear WG102 wireless access point.

The screenshot is taken from Netgear WG102 wireless access point. This access point has Syslog server facility but the data captured by this syslog server is not sufficient to carry out any forensic analysis because the data collected in these logs only inform about the administrative login times.

It does not have any facilities to detect any rogue access points being attached to the system. The logs do not inform whether the network key has been compromised or not and what kind of traffic is flowing through the system. If, anyone wants to carry out a forensic analysis the current information is not sufficient at all. The solution is to implement a type of intrusion detection system within the wireless access point so that it can monitor and record the activities of the wireless signal originating from the access point.

Implementing airtraf in these access points would help in carrying out forensic activities. The advantage of implementing network packet analyser is discussed in the section of Intrusion Protection. After implementing airtraf in these wireless access points it may look as follows:
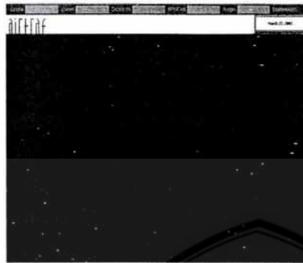
Figure 2: The example of airtraft Implementation in a wireless AP (a)

Figure 3: The example of Airtraft Implementation in a wireless AP (b)
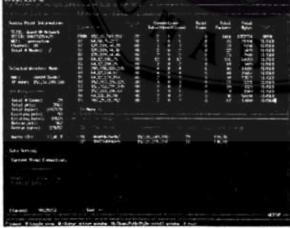

Figure 4: The example of airtraft Implementation in a wireless AP (c)

Once all the features of the tools are included then the forensics of the wireless networks is possible. In order to store for later analysis these records would then be routed to a syslog server.

CONCLUSION

The tools such as netstumbler, airtraf and numerous others are considered to be wireless hacking tools but in disguise these tools can be utilized for enhancing the wireless security. Thus modify these rules so that they can be used with the IOS of the router software would help devices to be more secure and reliable. This paper describes the conceptual design of a wireless forensic device.

REFERENCES

Alliance, W. F. (2005). Deploying WPA and WPA2 in the Enterprise [Electronic Version]. Retrieved 15/10/06 from http://www.wifialliance.com/OpenSection/white_papers/whitepaper-022705-deployingwpawpa2enterprise/.

J Edney, A. (Ed.). (2004). *Real 802.11 security: Wi-Fi protected access and 802.11i*. Boston: Addison-Wesley.

Potter, B. (2003). Wireless security's future. *IEEE Security & Privacy, 1*(4), 68-72.

Shipley, P. (2001). Open WLANs: the early results of wardriving. Retrieved 5/10/06, 2006, from http://www.dis.org/filez/openlans.pdf

Spitzner, L. (2003). Honeypots: catching the insider threat. *Proceedings of 19th Annual Computer Security Applications Conference*.

T Karygiannis, L. O. (2002). Wireless Network Security. *Recommendations of the NIST*

Wright, J. (2003). Detecting Wireless LAN MAC Address Spoofing.