I. J. Computer Network and Information Security, 2013, 7, 9-20
Published Online June 2013 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2013.07.02

Wi-Fi Networks Security and Accessing Control

Tarek S. Sobh
Information Systems Department, Egyptian Armed Forces, Cairo, Egypt
tarekbox2000@yahoo.com

Abstract—As wireless networks access gains popularity in corporate, private and personal networks, the nature of wireless networks opens up new possibilities for network attacks. This paper negotiating Wi-Fi security against scanning of rogue Wi-Fi networks and other related activities and considers the monitoring of Wi-Fi traffic effects. The unauthorized access point (AP) problem has raised more attention and resulted in obtaining wireless access without subscriber permission.

This work assumes Wi-Fi AP under attack specially rogue AP and/or ad-hoc client. It provides a solution for detecting and preventing this attack. In addition, it provides the required user permissions to allow/block access of the files on the user of ad-hoc client. The experiments include the rogue AP attack are maintained and the effectiveness of the proposed solution are tested.

***Index Terms*—**Mobile Internet Devices, WLAN Networks, Rogue Access Point, Wi-Fi 802.11

I. Introduction

With advances in wireless networks, networked mobile systems are becoming increasingly prevalent. There is also growing demand for ubiquitous services. These two factors are fueling a wide scale deployment of wireless networks including the IEEE 802.11 Wireless Local Area Network (WLAN). Wireless technology allows a computer to be connected to a WLAN by means of ''Access Points'' (AP) through radio waves without the need for cables or wires. This allows multiple users to share the same Wi-Fi1 AP or 'hotspot' within a WLAN coverage range as shown in Fig. 1. The popularity of wireless networking is a function of convenience [1, 2]. It provides the mobility that presents one of the most important features in the advanced computing technology. Wireless technologies may be categorized in a variety of ways depending on their function, frequencies, bandwidth, communication protocols involved, and level of sophistication [3, 4]. WLAN is what most of us think of Wireless technology. It includes the now-ubiquitous 802.11 family of protocols, as well as a few others. While the fact that Wi-Fi technology has a few security vulnerabilities is not news, the extent of these vulnerabilities may be surprising [2, 5, 6].

Most mobile devices now have the ability to connect via Wi-Fi. Therefore, it is very easy to find Wi-Fi hotspots scattered all over the place (see Fig. 1) [7, 8]. If you are traveling, sitting on beach or sitting on a bench somewhere, you will be able to connect to the number of free Wi-Fi networks and you will see a list of available networks.

Nowadays, online security experts have found several hacking schemes where cyber criminals use rogue Wi-Fi hotspots to lure people into using their network and then using the connection to attack users' laptop or mobile device [2, 5]. Wi-Fi security has become a serious concern, making unsuspecting mobile computing device folk vulnerable to attack [7, 8, 9]. User of mobile may think that there is nothing valuable in his laptop or Smartphone but he will be surprised at what attacker can steal with his private information [10].

Laptop
DKS 1812
Router
Power
Power
Power
Smartphone
DKS Adapter
DKS Adapter
At the door/gate
In your home

Figure. 1: Wireless Components

An unsecured Wi-Fi network connection can be tapped into and the communication intercepted by others, stolen, modified or deleted as it travels over the network. The unsecured connection can also be used for unlawful or undesirable purposes. Rogue AP, Wi-Fi mooching, war driving, piggybacking, joyriding or hitchhiking are common risks of an open Wi-Fi connection [2, 6].

Internet coffee offers a free Wi-Fi service as a marketing strategy so people will buy their coffee; restaurants do the same as well [5]. On a more creepy note, there are also Rogue Wi-Fi networks or also called rogue AP, which are those not associated with a place you are currently in that offer free, public and sometimes even faster internet connection.

In this work, a solution is proposed to monitor Wi-Fi network that is under unauthorized access attack specially rogue AP. Also, it provides the required user permissions to allow/block connect and access files on the secure ad-hoc client. The experiment results show the effectiveness of the proposed solution.

In this paper a problem definition and its solution is provided. Section 2 discusses the wireless network security. Section 3 negotiates rogue problem and its threats. Section 4 presents the related works to the wireless security. In section 5, the proposed model to defend the victim network is presented and experimental results are discussed. The conclusion is presented in section 6.

II. Wireless Network Security

Hacking wireless hardware is an endeavor steeped in a rich history of experimentation [11]. The wireless hardware hacker of today pursues his/her craft with a passion not seen since the amateur radio operators of the last generation. Many wireless enthusiasts are, in fact, connected with the ham community. Once solely the domain of a small group of Radio Frequency (RF) engineers becomes available, wireless gear has never been so inexpensive and accessible as it is today. By small investment, you can own wireless hardware due to rapidly declining hardware costs, then anybody can learn and experiment with 802.11 equipment. There are several wireless hacks, tricks, and hardware modifications, such as D-Link DWL650 card modification for adding an external antenna, OpenAP (Instant802) reprogramming of AP to run an open-source version of Linux, and Dell 1184 AP exploring the embedded Linux operating system [12].

WLANs attacker operated clients: using a wireless enabled laptop and couple of tools an attacker can successfully disrupt wireless service in networks few feet away. Most such Denial of Service (DoS) attacks aim at exhausting AP resources such as the client-association-table.

Wi-Fi devices can monitor and record data in case of encryption-free. Such network devices may use a Virtual Private Network (VPN) or secure Hypertext Transfer Protocol (HTTPS) over Transport Layer Security. Attackers are only out to log and gather information about the wireless network they find while scanning WLAN [13, 14, 15].

Table 1 summarizes common 802.11 and 802.1X attack Categories, giving examples of available attack methods used by wireless intruders.

Table 1: Wireless attacks and available methods

Attack Category	Attack methods
Authentication Attacks Steal credentials to penetrate wired network and services	PSK Cracking
	LEAP Cracking
	Password Capture
	VPN Login Cracking
Access Control Attacks Circumvent filters and firewalls to obtain unauthorized access	War Driving
	MAC Spoofing
	Rogue Access Points
	Unauthorized Ad Hocs
Confidentiality Attacks Intercept sensitive or private data sent over wireless associations	Eavesdropping
	WEP Key Cracking
	Evil Twin
	AP Phishing
Integrity Attacks Modify packets sent over wireless to mislead attacker	802.11 / EAP Replay
	802.11 / EAP Injection
	Response Poisoning
Denial-of-Service Attacks Inhibit or prevent legitimate use of WLAN services	RF Jamming
	Management/Control DoS
	Beacon Flood
	Deauth Flood
	EAP-of-Death
Station Attacks Crash or compromise laptop, phone, or other Wi-Fi endpoint	Wireless D Station Attacks river Exploits
	Wireless Station Probes

In this work, our concern related to access control attacks specially rouge AP. Traditional firewall is the first line of defense against network access control attacks but is not completely effective as Wi-Fi network protection because it works at traffic transfer point between LAN and Internet as shown in Fig. 2 [16]. It does not detect Rogue AP. It does not see traffic through Rogue AP. In this section, we will discuss some examples of wireless access without permission and Wi-Fi access protection solutions. While next section we will negotiate about rogue threats

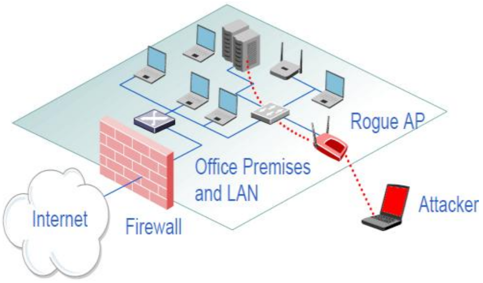


Figure 2: Firewall and Rogue AP [17]

2.1 Examples of Wireless Access Control Attacks

These different names describe the same activity of obtaining wireless access without the permission or knowledge of the subscriber such as War Chalking, Wi-Fi Mooching, Joyriding, War Driving, Piggybacking, or Hitchhiking [2, 5, 6, 18].

2.1.1 War Chalking

War chalking is a practice of marking a series of symbols on sidewalks and walls to indicate nearby wireless access as shown in Fig. 3. That way, other computer users can pop open their laptops and connect to the Internet wirelessly. It involves marking free websites for use by wireless hobos [14, 19]. Smart Phones, mobile devices and wireless vendors, have condemned as bandwidth theft the placing of chalk symbols on walls and pavements at places where free wireless network access is available [7, 9, 10]. It becomes a security threat when attackers freely browse corporate networks and access private information or use a network to dispatch millions of spam [18].

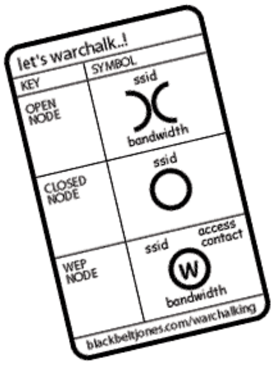


Figure 3: War Chalking Symbols

2.1.2 Wi-Fi Mooching

You are become a mooch user if you are one of those people who think an unsecured Wi-Fi connection is an open invitation to come on in, you are not alone [2, 18]. Ter Kah Leng [18] said, "If you are the sort that likes to mooch off of his neighbor's unsecured Wi-Fi connection, surfing the Internet or on their dime, you might want to think about ponying up for some access of your own". Wi-Fi theft, it turns out, can land you in the clink.

2.1.3 Joyriders

When Wi-Fi connections belonging to subscribers are opened without their prior consent, this action is called ‘Joyriders’ [18]. Roaming Wi-Fi users include " Joyriders" that use an open Wi-Fi connection to access the Internet. Joyriders find and use a Wi-Fi connection outside of their home or office for a variety of purposes, including checking e-mail, web surfing, or connecting to a corporate network [5, 14, 19]. The motive is to connect to the Internet without having to pay for the service.

2.1.4 War Driving

War Driving is an extension of the concept of War Dialing that deserves some explanation. It is a method popularized by a character played by Matthew Broderick in the film WarGames, and named after that film. The term originates from a phone hacking technique used in the 1980s - war dialing. War dialing consists of dialing every phone number in a specific sequence in search of modems [4, 10].

War Driving is the act of searching for Wi-Fi wireless networks by a person in a moving vehicle, using a portable computer, Smartphone or Personal Digital Assistant (PDA). The basic idea behind War Driving is to “sniff” 802.11 traffics with a wireless card set in “monitor” mode so that it accepts all traffic on frequency irrespective of intended target. The “War Driving” approach is considered as an example of attacks that exploit such Wi-Fi network vulnerabilities [20].

2.1.5 Piggybacking

Piggybacking refers to access to a wireless Internet connection by bringing one's own computer within the range of another's wireless connection, and using that service without the subscriber's explicit permission or knowledge. During the early popular adoption of 802.11, providing open access points for anyone within range to use was encouraged to cultivate wireless community networks, particularly since people on average use only a fraction of their downstream bandwidth at any given time. Recreational logging and mapping of other people's AP has become known as war driving. It is also common for people to use open (encryption-free) Wi-Fi networks as a free service, termed piggybacking [6, 21].

2.1.6 Hitchhiking

Hitchhiker is a utility that checks all public Wi-Fi APs near to your current position, and automatically configure your Pocket PC to allow you to connect quickly [6, 18]. This utility is perfect to Wi-Fi user when he or she out of his or her Wi-Fi AP coverage and about and discover that he or she needs some vital online information. Hitchhiker takes away the problems of manually searching for open APs then configuring Wi-Fi user Pocket PC to connect to nearest AP.

2.2 WLAN Security Solutions and Access Protections

Nowadays the main issue with wireless network security is its simplified access to the network compared to traditional wired networks such as Ethernet. Wi-Fi technology was built based on the IEEE 802.11 standards [2, 5, 6]. The IEEE develops and publishes some of these standards, but does not test equipment for compliance with them. The non-profit Wi-Fi Alliance formed in 1999 to fill this void to establish and enforce standards for interoperability and backward compatibility, and to promote WLAN technology. As of 2010, the Wi-Fi Alliance consisted of more than 375 companies from around the world. With wired networking, one must either gain access to a building or break through an external firewall. Most business networks protect sensitive data and systems by attempting to disallow external access. Thus gaining wireless connectivity provides an attack vector, particularly if the network lacks encryption or if the intruder can defeat any encryption.

End users benefit from a zero-configuration device that works with defaults does not enable existing wireless security options, providing open wireless access to a LAN. To turn security on requires the user to configure the device, usually via a software interface. The attacker can simply use a search engine to discover default system settings for a firmware installed wireless AP. Therefore, he can detect default system settings such as Service Set Identifier (SSID) and LAN IP address.

The most common wireless encryption-standard, Wired Equivalent Privacy (WEP), has been shown to be easily breakable even when correctly configured. WEP encryption was designed to protect against casual snooping, but is now deprecated by using some open source tools [22]. Wi-Fi Protected Access (WPA and WPA2) encryption, which became available in devices in 2003, aimed to solve this problem [13, 15]. Wi-Fi access points typically default to an open mode (i.e. encryption free). The current version of Wi-Fi WPA2 is considered secure, provided users employ a strong pass phrase. New protocols for quality-of-service (WMM) make Wi-Fi more suitable for latency-sensitive applications, and powers saving mechanisms to improve battery operation.

Attackers who target the wireless networks may face the secured networks, which use WEP keys. A common but unproductive measure to deter unauthorized users involves suppressing the access point's SSID broadcast, "hiding" it. This is ineffective as a security method because the SSID is broadcast in the clear in response to a client SSID query. Another unproductive method is to only allow computers with known MAC addresses to join the network. However, network attacker can defeat this method because they can often set MAC addresses with minimal effort by using MAC spoofing. If eavesdroppers have the ability to change their MAC address, then they may join the network by spoofing an authorized address.

From the above description the solutions is to monitor WLAN traffic and use the effective Wireless Intrusion Detection System (WIDS) that contains the analysis engine for this attack and other attacks. This engine automatically analyzes wireless network to proactively identify many threats. The WIDS enables wireless security beyond WEP by identifying vulnerabilities and attacks that cannot be protected simply by the use of encryption. One such vulnerability that cannot be prevented with WEP is the presence of rogue wireless devices, including honeypot APs, where a hacker mimics a known AP to lure unsuspecting users. Once connected, the hacker can download a virus or steal confidential data. An example attack, which circumvents WEP, is WEPWedgie. This toolkit determines 802.11 WEP keystreams and injects traffic with known keystreams. Table 2 provides a brief comparison of the available WLAN security options.

Table 2: Comparison of the available WLAN security options

	WEP	WPA	WPA2
Security Level	Less Secure	Secure	Highly Secure
Encryption	Open Key, Shared Key	TKIP	TKIP, AES
Authentication	Open Key	EAP over 802.1X	EAP over 802.1X
Key Length	64 bit (10 digit key) 128 bit (26 digit key)	TKIP	• 128 bit (default) • 192 bit • 256 bit
Key Type	Static Key	Dynamic Key	Dynamic Key
Application	Small home Networks	• Small- to - medium sized environments • Local LANs	• Defense • Government • Industrial Plants • Enterprise

Currently 802.1x standard implementations must use one of several authentication protocols called Extensible Authentication Protocol (EAP). EAP is responsible for establishing how the authentication process should be carried out. This establishes the rules so that both client and AP know the rules and appropriate responses for a successful authentication. The most popular EAP types are LEAP, PEAP, TTLS, and Cisco's FAST [www.airmagnet.com] [23]. Each of these authentication methods has their own unique strengths and considerations, and choosing the correct method for underlying network can be one of the most important steps of the security design process [www.airmagnet.com]. Fig. 4 presents RADIUS mediated Authentication Process using EAP.

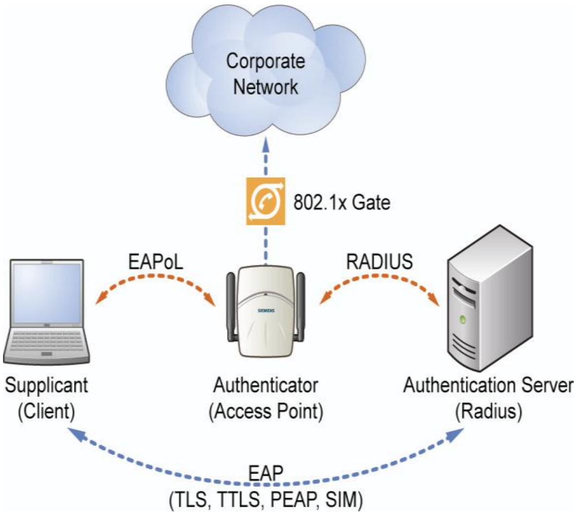


Figure 4: RADIUS mediated Authentication Process using EAP [24]

Table 3 provides a brief overall comparison of the various EAP types.

Table 3: EAP authentication types [www.airmagnet.com]

EAP Type	Client Certificate?	2 Way Authentication	Susceptible to Dictionary Attack?
MD5	Password	No	Yes
LEAP	Password	Yes	Yes
TLS	Yes	Yes	No
PEAP	No	Yes	No
TTLS	No	Yes	No
FAST	No	Yes	No

MD5 – This is the weakest of the possible EAP methods and typically should not be employed in a WLAN inasmuch as it provides negligible benefits over WEP.

LEAP – It provides an easy way to get 2-way authentication without using certificates. The weakness is that it requires users to remember a user password, and is thus susceptible to dictionary attacks.

TLS – It provides a very secure solution, but requires the use of certificates on the client.

PEAP– It is very secure solution. Uses TLS to create a secure tunnel where a second authentication mechanism can be used. Does not require a certificate on the client, but will use a certificate on the server.

TTLS – It is very secure solution. It is very similar to PEAP; it uses TLS to create a tunnel to avoid using certificates on the client.

FAST – It is very secure. Creates a secure tunnel, then uses AAA server to authenticate the server and client.

III. Rogue Problem

The problem of rogue APs has garnered more attention than any other security issue. A rogue AP defined as any AP in your network that was not intentionally deployed by your network staff (see Fig. 5). Rogue AP may be well-meaning employees who bring in devices from home, they can be devices used by hackers, or they can be neighboring devices that simply overlap with your WLAN. These devices can have many effects and none of them is good in terms of network security. In short, a rogue device is any untrusted or unknown device running in your WLAN.

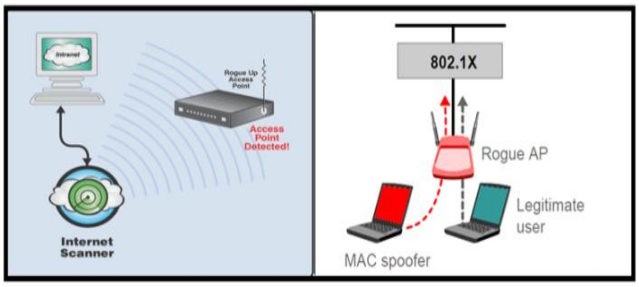


Figure 5: Unsecured Rogue Access Point Allows Anyone to Connect to the Network [17]

The well-known scenario of rogue AP is to plug it into a wired switch port and now rogue AP has wireless access to the larger wired network. Unfortunately, so does any Wi-Fi device within range of the AP including the wireless lurker in the parking lot. This provides a chance of unauthorized access to the entire enterprise network. An attacker could avoid organization security policy by planting a rogue device inside the building.

In such mobile environment, it is hard to trust any device completely. A wireless mobile device beaming signals into your network be either a harmless neighbor AP or an attacker-operated device trying to steal proprietary information from your WLAN [7, 9, 25]. Moreover, a poorly configured AP or a client can either open up access to outsiders or get associated with attacker. Fig. 6 illustrates some scenarios rogues AP attacks.

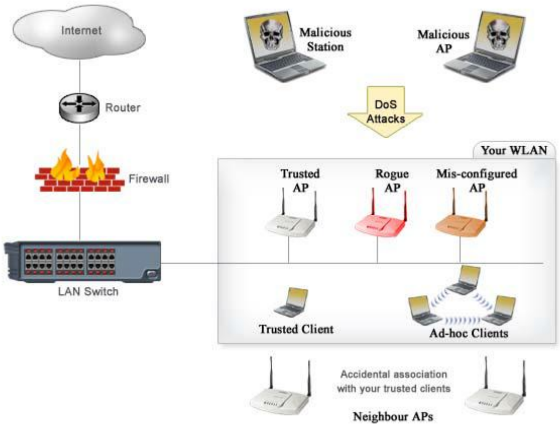


Figure 6: Malicious Rogue Devices and Associated Threats [25]

Though the term rogue is often referred to devices that are external to an organization, for clarity, in this work the term may refer to any unauthorized device irrespective of its real intent. The rogue threats are listed as follows:

3.1 Employee installed unauthorized Access Points

Driven by the convenience of wireless home networking some employees plug grade access points to corporate LAN [26]. The cheap AP may not follow enterprise standard deployment procedures thus compromising security on the WLAN and wired network.

Users and visitors inside organization building (Wi-Fi network) and hackers outside organization building can connect to such unauthorized APs to steal network traffic, send objectionable content to others, retrieve private data, attack company assets, or use organization network to attack others.

3.2 Misconfigured Access Points

Sometimes an authorized AP accidently turns into a rogue device due to configuration flaw [17]. Change in SSID, authentication settings, encryption settings etc., should be taken seriously as they could enable unauthorized associations if not configured properly. For example, in open mode authentication any wireless client device in state of unauthenticated and unassociated can send authentication requests to an AP and on successful authentication would move to state of authenticated but unassociated. If an AP does not validate the client properly, an attacker can send lot of such authentication requests, overflow the AP client access list, and make it reject access to other clients.

3.3 Attacker Access Points

802.11 clients automatically choose the best available AP nearby and connect with them. Currently, Windows platforms connect automatically to the best connection possible in the vicinity. Due to this behavior, authorized clients of one organization can connect to Access points from the neighboring organization. Though the neighbors APs have not intentionally lured the client, these associations can expose sensitive data [27].

Ad-hoc devices are wireless clients that can communicate among themselves without requiring a

LAN bridging device such as Access Point [17]. Though such devices can essentially share data among themselves, they pose significant threat to the enterprise as they lack the necessary security measures such as 802.1x user authentication and the dynamic key encryption. As a result, ad-hoc networks risk-exposing data in the air. In addition, weak authentication may allow unauthorized devices to associate. If the ad-hoc mode clients are also connected to the wired network, the entire enterprise wired network is at risk.

3.4 Unauthorized Access Points

WLANs are also becoming targets of a variety of attacks. One of the ways in which a WLAN can be attacked is by introducing one or more unauthorized fake Access Points (APs) in the network [http://www.proxim.com/]. Unauthorized AP can be set up by a malicious attacker to masquerade as an authorized AP by spoofing the authorized AP's MAC address.

Organizations can set security policies on what constitutes an authorized AP. The basic security policy depends on MAC addressed filtering. Organizations can pre-configure the list of authorized wireless devices [17, 27]. MAC and identification of any other device outside the MAC list will signify the presence of a rogue device. Also, if an organization standardizes on specific vendor APs then AP from any other vendor can be deemed rogue [23]. Similarly, enterprises can set various policies including SSID, Radio Media Type, and Channel. Whenever a new access point is discovered in the network that falls outside the pre configured authorized LIST, it can be assumed a rogue AP, as we will see in the proposed model.

3.5 Attacker operated Access Points

WLANs are prone to numerous attacks especially with freely available attacking tools. Attackers can install APs with the same ESSID as the authorized AP. Clients receiving stronger signal from the attacker operated AP would then attract legitimate clients to associate with it and launch a man-in-the-middle attack.

Table 4 presents a summary of the types of rogue APs and a number of possible scenarios [28].

Table 4: Rogue AP Taxonomy and Scenarios [28]

Rogue AP Class	Possible Scenarios

1. Improperly configured	Insufficient security knowledge;
	Faulty driver;
	Physically defective;
	Multiple network cards

2. Unauthorized	Connected to internal LAN without permission; External neighborhood AP
3. Phishing	Fabricated by adversary
4. Compromised	Disclosure of security credentials

IV. RELATED WORKS

Rogue AP security threats for corporate Wi-Fi networks are critical; detecting such rogue APs is one of the most important tasks of network security staff. Traditional rogue AP detection relies on network enumeration tools such as NetStumbler running on computer (laptop or other mobile device). This auditing approach is both time-consuming, unreliable and fails when a rogue AP is spoofed such as the MAC address and SSID of a legitimate AP.

Two online rogue AP detection algorithms are proposed in [29]. The basic idea of these two algorithms is the sequential hypothesis tests applied to packet-header data that are passively collected at a monitoring point. Algorithms use the properties of the 802.11 CSMA/CA and the half duplex of wireless channels to distinguish between wired and wireless connection. Once TCP ACK-pairs are observed, prompt decisions are made with little computation and storage overhead.

A layer-3 rogue AP detection approach is proposed by Yin et al. [27]. It uses the both verifier and sniffers. A verifier is employed on the internal wired LAN to send test traffic towards wireless edge. If sniffers capture an AP relaying from the test packets, the AP is marked as rogue. In addition, binary hypothesis testing is used to improve the detection rogue AP.

Several commercial products have been developed to help automate scanning process and continuous monitoring. The main product in the market today is AirDefense [www.airdefense.net] and provides an IDS capability specifically for the Wi-Fi environment using an integrated system of sensors and a management console. It uses a combination of radio frequency sensors and an intrusion detection/protection server appliance to capture, process, and correlate network events. Also, AirDefense [www.airdefense.net] stated that Security conscious enterprises are fortifying their wireless LANs with a layered approach to security that closely resembles the accepted security practices of wired networks. This layered approach addresses all network components by locking down the wireless LAN's perimeter, security communication across the wireless LAN and monitoring network traffic. It provides the industry's only enterprise level security appliance for wireless LANs to discover wireless LAN vulnerabilities, enforce security policies and detect then respond to intruders. It uses a distributed architecture of remote sensors and centralized server appliance to constantly monitor all wireless activity in real time allowing enterprises to control the wireless air space and define and enforce policy compliance [30]. Using it organizations can set policies for how all wireless LAN devices should be configured and then monitor all WLAN devices to identify when any device deviates from that policy.

Other products can provide the IDS portion incorporated in their Wireless network management tools like the ones provided by Air-Wave [www.airwave.com] and AirMagnet [www.airmagnet.com]. Typically, these tools become network management tools that have the ability to provide: Wi-Fi security policy management, wireless intrusion detection, rogue AP detection, connection troubleshooting, trend analysis, reporting and capacity planning and may even assist in the site survey process.

V. The Proposed Model

Detecting unauthorized access devices is the first step to efficiently defend your WLAN. Therefore, the solution to the issue such as rogue devices always begins with detection. Security staff needs to have complete visibility of all connected access points and clients in the network with deterministic rules that identify the devices that are authorized to be network member.

The proposed model consists of two basic sub models. First, sub model basic functions are WLAN detection and prevention of unauthorized AP. Second, sub model basic functions are protecting and preventing data leakage of ad hoc client's.

5.1 Unauthorized AP Detection and Prevention

The more specific the wireless policy, the easier unauthorized access detection becomes. For example, if you know the MAC address of your devices, you can then easily identify rogues based on MAC address. In the same way, Rogues can also be identified based on other factors such as the hardware vendor, Channel, or SSID. All of this requires the ability to scan the airwaves and identify every device based on a variety of criteria, again illustrating the need for comprehensive wireless monitoring. As a closing note, it is important to think of rogue detection as part of the larger security policy and not the security policy itself. The response process of rogue device threat should ideally be broken to two steps: First step is suppression where the rogue device is immediately quarantined from the network. Second step is a removal where the rouge device is physically located by staff and potentially removed from the network.

WLAN unauthorized access detection and prevention is a continuous process. Fig. 7 presents the required process components. These components are:

1) Sensors are used to capture the wireless traffic and network behavior. Sensors we are used here RF scanning and AP scanning. RF scanning sensors will be quick to detect any wireless device operating in the area. However, the drawback of these sensors is the possibility of dead zones, which are not covered by the sensors. If unauthorized AP such as rogue AP finds its place in any of these dead zones, it will be unnoticed. AP scanning automatically discovers APs operating in the nearby area and exposes the data through its interface. Though it is a very useful, the ability of the AP to scan neighboring devices is limited to a very short range. Unauthorized APs operating outside this coverage area will go unnoticed.
2) A central monitoring and response engine to collect its inputs from available sensors.
3) A management component to identify the connection to unauthorized access according to authorized list database and take appropriate actions. The attack prevention here it means taking the appropriate action in order to avoid attacks such as blocking attack connection.

These actions are taken according to predefined organization policy and authorized access list as shown in Table 5. The objective from authorized access list is to find unique device characteristics that cannot be fabricated. Any newly detected AP that falls outside the authorized list would be flag as unauthorized or rogue AP. Management component use different authorized attributes values to populate the authorized list like SSID, MAC, BSSID, Media Type, Channel, and AP Vendor in addition to WLAN location used as comment attribute as shown in Table 5. Organizations would in most probably standardize on the authorized SSIDs and sometimes may want their APs to operate on select channels. The MAC you see in insider is the BSSID of the access point, a unique value per SSID that is being advertised by the AP. Generally for low cost access points that allow only a single SSID to be broadcast, it is common to see that the BSSID address is the Ethernet port +/- 1, i.e. 00-04-01-ad-cf-45 for Ethernet and 00-04-01-ad-cf-46 for BSSID. Sometimes we use certain standard on 802.11 a,b,g, or bg in our WLAN APs. This enables our toll to compare with our access list and to alert WLAN administrators whenever AP with different radio media type is detected.

Sometimes WLAN administrator wants his APs to operate on authorized select channels. This enables the proposed tool of our model to send alert whenever AP operating in a different authorized channel is detected.

These attribute values in Table 5 enable the proposed model to detection unauthorized AP and alert WLAN administrators whenever AP operating with a different value outside authorized list such as whenever AP operating in a different channel is detected. For example, when WLAN administrator staff detects rogue AP they can use the sensor to launch a network disassociation flooding attack of numerous packets against rogue AP. In addition, if the hacked AP linked to wired network a management component can identify the connected switch port and shutdown it. This would normally disconnect clients of the AP without dropping the connection and clients get associated to the nearest AP.

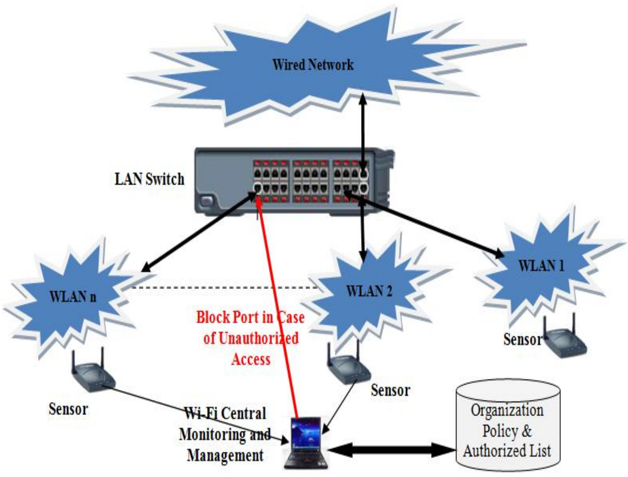

Wired Network
LAN Switch
WLAN n
WLAN 2
WLAN 1
Block Port in Case of Unauthorized Access
Sensor
Sensor
Sensor
Wi-Fi Central Monitoring and Management
Organization Policy & Authorized List

Figure 7: Wireless protection and prevention against unauthorized access

Authorized access list in Tables 5 shows AP of WLAN n not authorized due to unauthorized MAC then a management component will block its port in the LAN switch as shown in Fig. 7. However, today attackers can easily spoof MAC address and device driver characteristics are difficult to separate multiple devices with same device driver. Kohno et al. [30] used clock skew as a device fingerprint. In this work, we used clock skew too as a fingerprint to AP device in addition to attributes list in Table 5. We implemented clock skew like Jana et al. [31] did but the details of this part outside the scope of this paper (see [30, 31, 32]).

Table 5: Authorized Access List

SSID	MAC	BSSID	Type	Ch	Vender	Location
WLAN1	00230fc45b		802.11b\g	6	Proxim	Finance Office Buldin g1
WLAN2	00230fc47b			1	Cisco	Account Buldin g2
	00230fc43b			11		
	00230fc44b					
WLANn	00230fc46c					Mgr Office Buldin g3

5.2 Secure Wi-Fi Ad Hoc Client

While the focus thus far has been on access points, the same principles also apply to clients. A rogue client could indicate an unknown user trying to get unauthorized access to the network. On the other hand, it could be an unconfigured employee device searching randomly for any available connection. In either case, it represents an issue that requires immediate attention from technical staff. Fig. 8 provides the proposed wireless protection of ad-hoc client against the unauthorized access attack and data leakage as well.

The proposed model in Fig. 8 is consists of four main modules, Traffic Sniffer Module (TSM), Ad-Hoc Client Manager Module (ACMM), Traffic Filter Module (TFM), and Traffic Analysis Module (TAM).

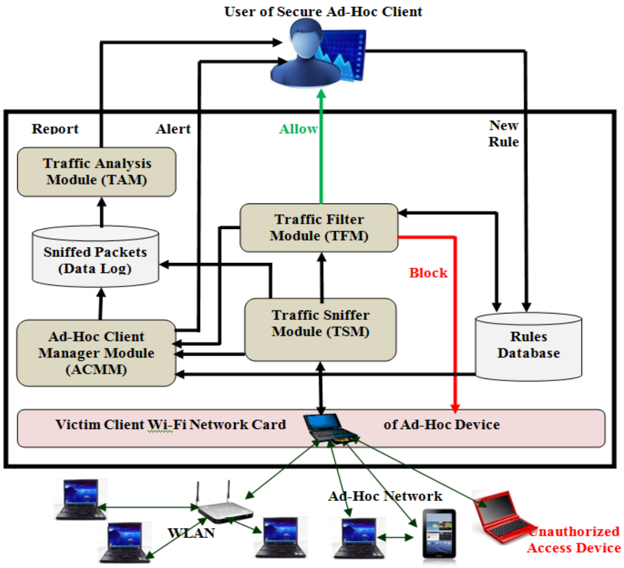
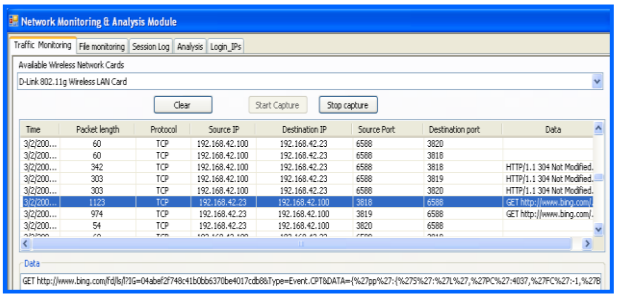

User of Secure Ad-Hoc Client
Report
Alert
Allow
New Rule
Traffic Analysis Module (TAM)
Traffic Filter Module (TFM)
Sniffed Packets (Data Log)
Block
Rules Database
Traffic Sniffer Module (TSM)
Ad-Hoc Client Manager Module (ACMM)
Victim Client Wi-Fi Network Card of Ad-Hoc Device
Ad-Hoc Network
WLAN
Unauthorized Access Device

Figure 8: Ad-hoc client defense against unauthorized access

5.2.1 Traffic Sniffer Module (TSM)

In Fig. 9, the ad-hoc client device traffics are captured by the TSM. TSM captures all the arrival Wi-Fi packets to the ad-hoc client and provides total information about it. At first user of ad-hoc client has to choose a network card then press start capture to begin sniffing the packets. Then user can choose to stop sniffing and drop the sniffed logged data packets into a “PCAP” file format as shown in Fig. 10. TSM identifies: Packet arrival time; Length; Source IP; Destination IP, used Protocol and Payload. It provides multi panes so that the user can select a specific packet in one pane to display its data content in another pane view.



Available Wireless Network Cards

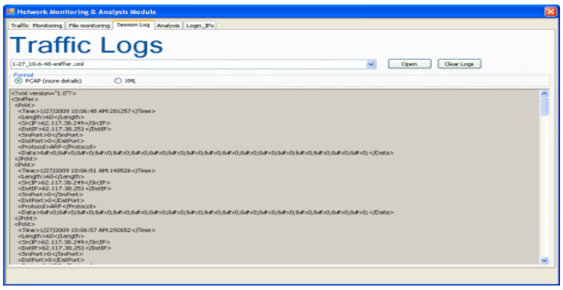
D-Link 802.11g Wireless LAN Card

Time	Packet length	Protocol	Source IP	Destination IP	Source Port	Destination port	Data
3/2/200...	60	TCP	192.168.42.100	192.168.42.23	6588	3820	
3/2/200...	60	TCP	192.168.42.100	192.168.42.23	6588	3818	
3/2/200...	342	TCP	192.168.42.100	192.168.42.23	6588	3818	HTTP/1.1 304 Not Modified.
3/2/200...	303	TCP	192.168.42.100	192.168.42.23	6588	3819	HTTP/1.1 304 Not Modified.
3/2/200...	303	TCP	192.168.42.100	192.168.42.23	6588	3820	HTTP/1.1 304 Not Modified.
3/2/200...	1123	TCP	192.168.42.23	192.168.42.100	3818	6588	GET http://www.bing.com/
3/2/200...	974	TCP	192.168.42.23	192.168.42.100	3819	6588	GET http://www.bing.com/.
3/2/200...	54	TCP	192.168.42.23	192.168.42.100	3820	6588	

Data

```
GET http://www.bing.com/fd/ls/l?IG=04abef2f748c41b0bb6370be4017cdb8&Type=Event.CPT&DATA={%27pp%27:{%27S%27:%27L%27,%27PC%27:4037,%27FC%27:-1,%27B
```

Figure 9: Ad Hoc Device Traffic Sniffer Log


Network Monitoring & Analysis Module

Traffic Logs

1-27_10-6-48-sniffer.xml

Format
● PCAP (more details) ○ XML

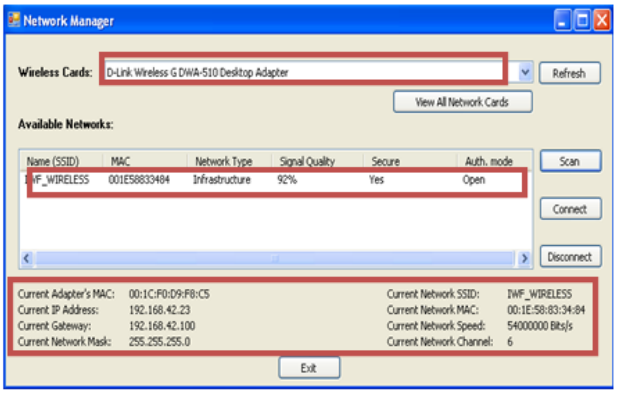
```
<?xml version="1.0"?>
<Sniffer>
 <Pckt>
  <Time>1/27/2009 10:06:48 AM:281257</Time>
  <Length>60</Length>
  <SrcIP>62.117.38.249</SrcIP>
  <DstIP>62.117.38.251</DstIP>
  <SrcPort>0</SrcPort>
  <DstPort>0</DstPort>
  <Protocol>ARP</Protocol>
  <Data>&#x0;&#x0;&#x0;&#x0;&#x0;&#x0;&#x0;&#x0;&#x0;&#x0;&#x0;&#x0;&#x0;&#x0;&#x0;&#x0;&#x0;&#x0; </Data>
 </Pckt>
 <Pckt>
  <Time>1/27/2009 10:06:51 AM:148526</Time>
  <Length>60</Length>
  <SrcIP>62.117.38.249</SrcIP>
  <DstIP>62.117.38.251</DstIP>
  <SrcPort>0</SrcPort>
  <DstPort>0</DstPort>
  <Protocol>ARP</Protocol>
  <Data>&#x0;&#x0;&#x0;&#x0;&#x0;&#x0;&#x0;&#x0;&#x0;&#x0;&#x0;&#x0;&#x0;&#x0;&#x0;&#x0;&#x0;&#x0; </Data>
 </Pckt>
 <Pckt>
  <Time>1/27/2009 10:06:57 AM:292652</Time>
  <Length>60</Length>
  <SrcIP>62.117.38.249</SrcIP>
  <DstIP>62.117.38.251</DstIP>
  <SrcPort>0</SrcPort>
  <DstPort>0</DstPort>
```

Figure 10.Traffic Data Log in “PCAP” File Format

5.2.2 Ad-Hoc Client Manager Module (ACMM)

ACMM provides information about the available wireless networks. Fig. 11 shows the available (given wireless card) details of specific ad-hoc device near to you to connect. The output will be displayed after scanning process with the following details: Network card type, Network name, MAC address, Signal quality, Security and Authentication. User can do “scan process” at any time to be informed with the available wireless networks and their data.

As shown in the Fig. 11, the SSID name called "HMF_WIRELESS" is displayed and its corresponding MAC address. Also, the signal quality for this detected network is displayed and secured WLAN status (see Fig. 11). The “Scan” option can be selected more and more to detect the additional Wi-Fi networks. In addition, ACMM arise alerts when policy violation detected. Such as a file/directory on the host machine is required to be illegal accessed by a network user.


Network Manager

Wireless Cards: D-Link Wireless G DWA-510 Desktop Adapter

Available Networks:

Name (SSID)	MAC	Network Type	Signal Quality	Secure	Auth. mode
IWF_WIRELESS	001E58833484	Infrastructure	92%	Yes	Open

Current Adapter's MAC:	00:1C:F0:D9:F8:C5	Current Network SSID:	IWF_WIRELESS
Current IP Address:	192.168.42.23	Current Network MAC:	00:1E:58:83:34:84
Current Gateway:	192.168.42.100	Current Network Speed:	54000000 Bits/s
Current Network Mask:	255.255.255.0	Current Network Channel:	6

Figure 11: Available Details of Specific Device

5.2.3 Traffic Filter Module (TFM)

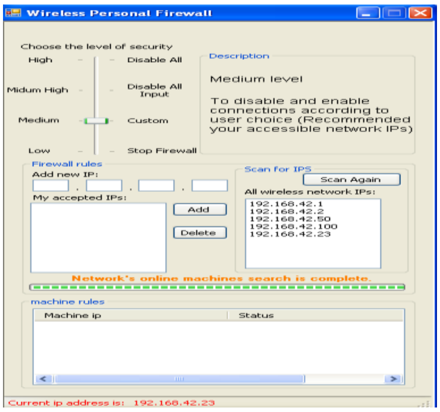
TFM is ad-hoc client filter to allow/deny the connections to the ad-hoc client. It is different from windows firewall as it is designed to provide more options, which allow user to prevent the connections by all other network nodes on the same network from, connect to the user host. In addition, the user has an option to identify some legible machine IP(s) to allow them to connect to his secure ad-hoc client. So that, the user has the ability to connect to the network, while all other network nodes will be denied. TFM takes its decision to allow or block specific connection based on sniffing data from TSM and available rules in the database. TFM send its decision to both ACMM and user of secure ad-hoc client with alert message. Finally, TFM may update existing rule or add addition rule into rules database. Sometimes TFM leave this filtering decision to the user of secure ad-hoc client.

Once the user or TFM allowed this access, this allowed device can access the files in the secure ad-hoc client. With every try from the guest user to access a new file in the secure ad-hoc client the pop-up alert window will appear to the user with details about this new access and options to allow or block this access regardless previous decision.

If the user or TFM blocked this connection then TFM will drop all packets from blocked device (IP) to prevent this IP to access any files in the secure ad-hoc client. This IP will be added to a filtering rules database to prevent this IP from accessing or dealing with the user's machine. In all cases, the user can change the status of any IP from trusted IP to blocked IP and from blocked IP to allowed IP or the user can add a new IP to the trusted list or to the blocked list.

There are four level levels of security available in TFM as shown in Fig. 12:

- High: This level disables all packets to / from our secure ad-hoc client.
- Medium High: This level disables all input packet to our secure ad-hoc client, but you can send (connect to) other devices in your ad-hoc network.
- Medium: This level is custom level which allow you to connect with other devices in your ad-hoc network (send & receive packet) and reject the rest of devices in your ad-hoc network, this is level is preferable in case of using proxy on our secure ad-hoc client.
- Low: This level stops filtering operation of TFM and it is not recommended.


Wireless Personal Firewall

Choose the level of security

High	Disable All
Midum High	Disable All Input
Medium	Custom
Low	Stop Firewall

Description

Medium level

To disable and enable connections according to user choice (Recommended your accessible network IPs)

Firewall rules

Add new IP: . . .

My accepted IPs:

Scan for IPS

All wireless network IPs:
192.168.42.1
192.168.42.2
192.168.42.50
192.168.42.100
192.168.42.23

Network's online machines search is complete.

machine rules

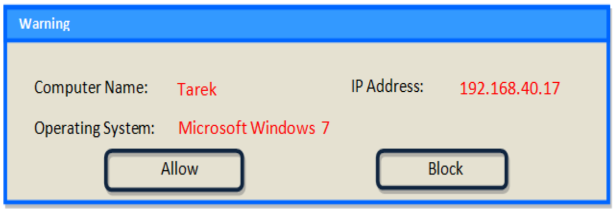
Machine ip	Status

Current ip address is: 192.168.42.23

Figure 12: Wireless Packet Filtering in TFM

When discovering a new ad-hoc connect device appeared in the network an appropriate alert should be raised to our underlying secure ad-hoc client user. This alert should has some details appeared about the new device connects to the ad-hoc network; these details are device IP, device Mac address and the device name. The idea is that when a new device connects to the ad-hoc network it broadcasts ARP packets to all devices in the ad-hoc network because ARP is used as a simple announcement protocol. This is useful for updating other devices mapping of a hardware address when the sender's IP address or MAC address needs to be updated in all ad-hoc network devices. By detecting ARP packets according to ARP packet structure, we can reach to the user's client.

If the details of this device already exist in the user's database, it means it's already known device. If not it means it's a new device joined the ad-hoc network. The system will alert the user about this new connected device. System gives the following information about connected device: IP address, Mac address and device name then the user can know if this new connected device is trusted or it's not trusted and he/she has to take action against it. The ACMM raised the alert message to user of our secure ad-hoc device client contains computer name, IP address, operating system and message say "This computer trying to access your machine", when policy violation detected as shown in Fig. 13. Without this alert, the user of secure ad-hoc client could not know that a new network device trying to access his machine. Now, the user of secure ad-hoc client should to decide whether to allow or deny this new connection through TFM.



Computer Name: Tarek

IP Address: 192.168.40.17

Operating System: Microsoft Windows 7

Figure 13: The Alert Message on Illegal Access Trial

This proposed model is a client-side filter to allow/deny the connections to our secure ad-hoc client. The secure ad-hoc client user can select either allow or block option as shown in Fig. 13. The secure ad-hoc client user reaction should be logged to be used by TAM.

5.2.4 Traffic Analysis Module (TAM)

TAM allows the user of secure ad-hoc client to get a reports, statistics, and analysis charts of network activities captured by the system. These charts can give the user information about the most active IPs with the user's machine in the last session, the most active source and destination ports, and the most active IPs through a specific period of time determined by the user as well.

The statistical analysis of the machine activities can be viewed by charts representing the most frequent used IPs. Fig. 14 shows an example of the machines traffic within a period of time (3 hours). Graph shows IPs 192.168.40.12 and 192.168.40.17 that have accessed the secured ad-hoc client machine in this period of time.

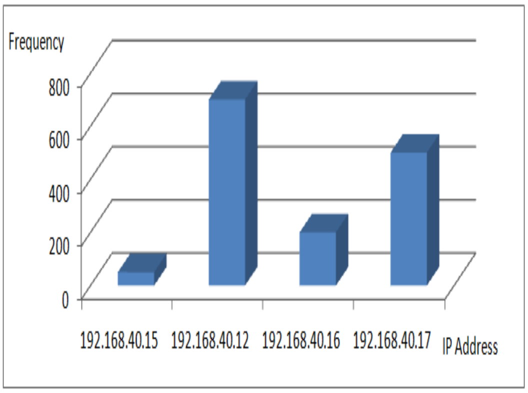
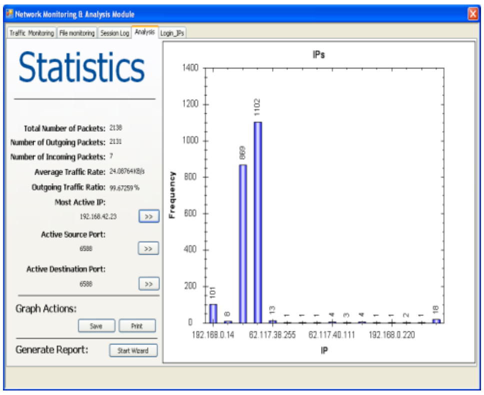


Figure 14: The frequency of the IP usage within 3 hours

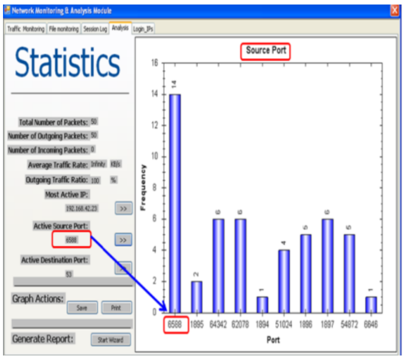
Fig. 15 displays the output from traffic analysis module. It shows that 192.168.40.23 is the most active IP device connected to our ad-hoc device client.



Total Number of Packets: 2138
Number of Outgoing Packets: 2131
Number of Incoming Packets: 7
Average Traffic Rate: 24.08764KB/s
Outgoing Traffic Ratio: 99.67259 %
Most Active IP: 192.168.42.23
Active Source Port: 6588
Active Destination Port: 6588

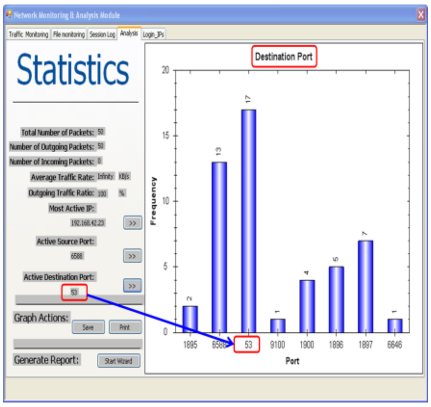
Figure 15: Most Active IP Connected Device

Fig. 16a and 16b is statistic result from analysis module. It displays both most active source port and destination port respectively.



Total Number of Packets: 50
Number of Outgoing Packets: 50
Number of Incoming Packets: 0
Average Traffic Rate: Infinity KB/s
Outgoing Traffic Ratio: 100 %
Most Active IP: 192.168.42.23
Active Source Port: 6588
Active Destination Port: 53

Figure 16a: Most Active Source Port



Total Number of Packets: 50
Number of Outgoing Packets: 50
Number of Incoming Packets: 0
Average Traffic Rate: Infinity KB/s
Outgoing Traffic Ratio: 100 %
Most Active IP: 192.168.42.23
Active Source Port: 6588
Active Destination Port: 53

Figure 16b: Most Active Destination Port

6. Conclusions and Future Directions

Wireless connectivity is simple access to the network compared to traditional wired connectivity such as Ethernet. Wireless standards provided a comprehensive solution to the WLAN security but wireless security will have to continually evolve to keep up with the newest attacks. Current researches looking for authentication and encryption algorithms to ensure that defenses capabilities are in place to provide a complete security solution. Detecting unauthorized access devices is the first step to defend your AP and ad-hoc client.

This work presents two models. First model consists of these components: Sensors to capture the wireless traffic and network behavior, central monitoring and response engine to collect its inputs from available sensors, and a management component to identify the connection to unauthorized access according to authorized list database and take appropriate actions. In this model, we used the access list table in addition to clock skews for detecting unauthorized AP in WLAN. Second model presents a solution to protect ad-hoc clients. This model consists of four main modules, traffic sniffer, ad-hoc client manager, traffic filter, and traffic analysis.

The proposed solution faced the problem of detecting unauthorized APs and/or ad-hoc client, but the general problem of finding encryption-free method to detect spoofed MAC by any wireless client still remains open area of research.

References

[1] LaRoche, P. and Zincir-Heywood, A.N., “Genetic Programming Based Wi-Fi Data Link Layer Attack Detection”, “In Proceedings of the 4th Annual Communication Networks and Services Research Conference (CNSR 2006)”, IEEE Press, May 24–25, 2006, pp. 8–15.

[2] Securing Wi-Fi Wireless Networks with today’s Technologies, Wi-Fi Alliance. Available at: http://www.Wi-Fi.org/files/wp_4_Securing%20Wireless%20Networks_2-6-03.pdf [Accessed Nov. 2009].

[3] Balachandran, S., Dasgupta, D. and Wang, L., “A Hybrid Approach for Misbehavior Detection in Wireless Ad-Hoc Networks”, “In Symposium on Information Assurance”, New York, USA, June 14–15, 2006.

[4] M. E. Elhamahmy and Tarek S. Sobh, "Preventing Information Leakage Caused by War Driving Attacks in Wi-Fi Networks", Proceedings of the 14th International Conference on AEROSPACE SCIENCES & AVIATION TECHNOLOGY, ASAT–14, pp 09, May 24 – 26, 2011, Military Technical College, Kobry Elkobbah, Cairo, Egypt, 2011.

[5] S. Zanero, "Wireless malware propagation: A reality check," IEEE Security and Privacy, vol. 7, no. 5, pp. 70{74, September-October 2009.

[6] Tom Rowan, “Negotiating Wi-Fi security”, Network Security, February 2010, pp: 8-12, 2010.

[7] Huajian Mao, Nong Xiao, Weisong Shi, and Yutong Lu, “Wukong: A cloud-oriented file service for mobile Internet devices”, Journal of Parallel Distributed Computing, Vol. 72 (2012), pp: 171–184, 2012.

[8] Yung-Wei Kao, ChiaFeng Lin, Kuei-An Yang, and Shyan-Ming Yuan, “A Web-based, Offline-able, and Personalized Runtime Environment for executing applications on mobile devices”, Computer Standards & Interfaces, Vol. 34 (2012), pp: 212–224, 2012.

[9] Reed M., P. Syverson and D. Goldschlag, Protocols using Anonymous Connections: Mobile Applications, 1997 Security Protocols Workshop.

[10] G. Perrucci, F. Fitzek, G. Sasso, W. Kellerer, J. Widmer, "On the impact of 2G and 3G network usage for mobile phones battery life", European Wireless, 2009.

[11] Lee Barken and Eric Bermel, "Wireless Hacking: Projects for Wi-Fi Enthusiasts", Chapter 10: Wireless 802.11 Hacks, Appendix A, pp 299-323, Published by Syngress

[12] A. Muthitacharoen, B. Chen, D. Mazieres, A low-bandwidth network file system, in: Proceedings of the eighteenth ACM symposium on Operating systems principles, ACM, 2001, pp. 174–187.

[13] Martin Beck and Eric Tews, “Practical Attacks against WPA, November 8 2008, http://dl.aircrack-ng.org/breakingwepandwpa.pdf

[14] T. Raman, "Cloud computing and equal access for all", in: Proceedings of the 2008 International Cross-disciplinary Conference on Web Accessibility (W4A), ACM, 2008, pp. 1–4.

[15] WPA™ Deployment Guidelines for Public Access Wi-Fi® Networks, Wi-Fi Alliance. Available at: http://www.Wi-Fi.org/files/wp_6_WPA%20Deployment%20for%20Public%20Access_10-28-04.pdf [Accessed 27 Nov. 2009].

[16] IEEE Std 802.11-1997 Information Technology-telecommunications And Information exchange Between Systems-Local and Metropolitan Area

Networks specific Requirements-part 11: Wireless LAN Medium Access Control (MAC) And Physical Layer (PHY) Specifications, IEEE, 1997. http://ieeexplore.ieee.org/search/freesrchabstract.jsp?arnumber=654749&isnumber=14251&punumber=5258&k2dockey=654749@ieeestds&query=%28802.11+1997%29%3Cin%3Emetadata&pos=0

[17] Gopinath K. N. and Hemant Chaskar, "A quick reference to Rogue AP security threat, Rogue AP detection and mitigation", AirTight Networks, 2009, www.AirTightNetworks.com

[18] Ter Kah Leng, “Wireless Internet regulation: Wireless Internet access and potential liabilities”, Computer law & Security Report, Vol. 23 (2007), pp: 550 – 554.

[19] Reiter M. K. and Aviel D. Rubin. Crowds: Anonymity for Web Transactions. ACM Transactions on Information and Systems Security, (1)1, 66-92, June 1998.

[20] Mishra, A. and Arbaugh, W. A., “An Initial Security Analysis of the IEEE 802.1x Standard”, University of Maryland, Tech. Rep. CS-TR-4328, 802.11, IEEE 802.11 Standard, 2005. Available at: http://grouper.ieee.org/groups/802/11/ [accessed 24 Mar, 2010]

[21] Borisov, N., Goldberg, I. and Wagner, D., “Intercepting Mobile Communications: the Insecurity of 802.11”, “In 7th Annual International Conference on Mobile Computing and Networking”, 2001.

[22] Fluhrer, S., Mantin, I. and Shamir, A. “Weaknesses in the Key Scheduling Algorithm of RC4”, “In 8th Annual International Workshop on Selected Areas in Cryptography”, 2001.

[23] Wireless LAN solution engine (WLSE), http://www.cisco.com.

[24] Siemens Enterprise Communications, "WLAN Security Today: Wireless more Secure than Wired", White Paper, July 2008.

[25] ManageEngine UK Distributor: Networks Unlimited, "Wireless Network Rogue Access Point Detection & Blocking", www.manageengine.co.uk [accessed 2005]

[26] Tarek S. Sobh, “Wired and Wireless Intrusion Detection System: Classifications, Good Characteristics and State-of-the-art”, Computer Standards & Interfaces, volume 28/6, pp. 670-694, 2006,

[27] Yin, H., Chen, G., and wang, J., “Detecting protected layer-3 rogue APs,” in IEEE BROADNETS ’07: Fourth Annual International Conference on Broadband Networks, 2007.

[28] Liran Ma, Amin Y. Teymorian, and Xiuzhen Cheng, "A Hybrid Rogue Access Point Protection Framework for Commodity Wi-Fi Networks", IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM 2008 proceedings, 2008.

[29] W. Wei, K. Suh, B. Wang, Y. Gu, J. Kurose, and D. Towsley, “Passive online rogue access point detection using sequential hypothesis testing with tcp ack-pairs,” in IMC ’07: Proceedings of the 7th ACM SIGCOMM conference on Internet measurement. New York, NY, USA: ACM, 2007, pp. 365–378.

[30] T. Kohno, A. Broido, and K. C. Claffy, "Remote physical device fingerprinting", IEEE Transaction on Dependable and Secure Computing, 2(2):93–108, 2005.

[31] Suman Jana and Sneha K. Kasera, " On Fast and Accurate Detection of Unauthorized Wireless Access Points Using Clock Skews", Proceedings of the MobiCom’08, September 14–19, 2008, San Francisco, California, USA.

[32] Kumari, L., Debbarma, S. and Shyam R., “Security Problems in Campus Network and Its Solutions”, “International Journal of Advanced Engineering & Application”, Vol. 1, Issue 1, pp. 98-101, Jan 2011.

Tarek Salah Sobh received his B.Sc. degree in computer engineering from Military Technical College, Cairo, Egypt in 1987. Both M.Sc. and Ph.D. degrees from Computer and System Engineering Department, Faculty of Engineering, Al-Azhar University, Cairo, Egypt. He has managed, designed and developed several packages for business applications and security systems. He has authored/co-authored of many refereed journal/conference papers and booklet. Some of the articles are available in the ScienceDirect Top 25 hottest articles. His research of interest includes distributed systems, knowledge discovery, database system design and development, data mining, information fusion, software engineering, intelligent systems, networks and computer security, and network management.