Research Inventy: International Journal Of Engineering And Science
Vol.3, Issue 7 (August 2013), PP 01-05
Issn(e): 2278-4721, Issn(p):2319-6483, Www.Researchinventy.Com

Securing Wi-Fi Network Via Proxy Servers

Surbhi Gupta[1], Puneet Bhalla[1]
[1.] *Department of Computer Science , Dronacharaya college of engg., Gurgaon*

ABSTRACT : *"Unsecured wi-fi network (genetically known as Wireless Local Area Network or WLAN) has become a national celebrity in vamp category due to it's misuse by terrorists, in the recent past.Even otherwise, any open and unsecured node, especially wireless,is an extremely serious security hazard for any network, whether it is corporate, personal, home or small office user. Wi-fi networks are in the news in the recent past due to effective misuse of these by terror organisations. They have been misused asthese wireless (wi-fi) networks have been installed unsecured. Withthe misuse by terrorists, unsecured wi-fi misuse has become national celebrity in villain and vamp categories."*

KEYWORDS: *AES, DAIR, MAC, Proxy server, TKIP, WEP, WPA*

I. INTRODUCTION

Wi-Fi is the name of a popular wireless networking technology that uses radio waves to provide wireless high-speed Internet and network connections. The Wi-Fi Alliance, the organization that owns the Wi-Fi (registered trademark) term specifically ***definesWi-Fi as any "wireless local area network (WLAN)*** products that are based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards."Initially, Wi-Fi was used in place of the 2.4 GHz 802.11b standardonly, however the Wi-Fi Al liance has expanded the generic use of the Wi-Fi term to include any type of network or WLAN product based on any of the 802.11 standards, including 802.11b,802.11a, dual-band, and so on, in an attempt tostop confusion\about wireless LAN interoperability.Wi-Fi works with no physical wiredconnection between sender andreceiver by using radio frequency (RF) technology, afrequency within the electromagnetic spectrum associated with radio wavepropagation. When an RF current is supplied to an antenna, an electromagnetic field is created that then is able to propagate through air or space. The cornerstone of any wireless network is an access point (AP). The primary job of an access point is to broadcast a wireless signal that computers can detect and "tune" into. In order to connect to an access point and join a wireless network, computers and devices must be equipped with wirelessnetwork adapters.*Wi-Fi is supported by many appl ications and devices including video game consoles, home networks, PDAs, mobile phones, major operating systems, and other types of consumer electronics.* Anyproducts that are tested and approved as "Wi-Fi Certified" (aregistered trademark) by the Wi-Fi Alliance are certified asinteroperable with each other, even if they are from differentmanufacturers. For example, a user with a Wi-Fi Certified productcan use any brand of access point with any other brand of clienthardware that also is also "Wi-Fi Certified". Products that pass thiscertification are required to carry an identifying seal on theirpackaging that states "Wi-Fi Certified" and indicates the radiofrequency band used (2.4 GHz for 802.11b, 802.11g, or 802.11n,and 5GHz for 802.11a).[1]

1.1.How to secure wi-fi and protect ourselves –

The question arises – what a person must do to take care that the wireless network (wi-fi) is not misused by any anti-social, antinational or criminal element or anyone else, may be insider, who is not authorised to access / use the network. The question is: how to secure your wireless network or wi-fi network connection or access point (AP) .There are three important aspects of wireless (or any) security –

A. Wireless network must be technically reasonably secured.
B. User must be educated in security.
C. Security must be monitored for weaknesses and breaches.

1.2.Checklist to protect your wireless (wi-fi) network

1.2.1.Mandatory Controls –

1. Change Default Administrator Passwords and Usernames
2. Turn on (Compatible) WPA / WEP Encryption
3. Enable Firewalls On Each Computer and the Router
4. Disable Auto-connect feature
5. Position the Router or Access Point (AP) Safely

6. Turn Off the power switch of Router/AP, when not in use
7. Assign Static IP Addresses to Devices

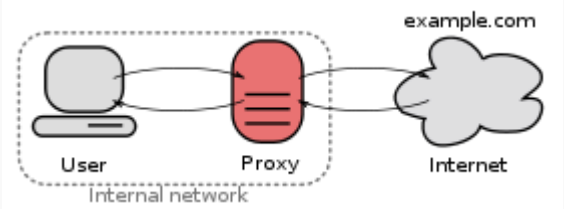
1.2.2.Desirable Controls -
8. Change the Default SSID
9. Disable SSID Broadcast
10. Enable MAC Address Filtering

II. SCOPE OF STUDY

Proxy server is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different server and the proxy server evaluates the request as a way to simplify and control its complexity.[2]A proxy server may run right on the user's local computer, or at various points between the user's computer and destination servers on the Internet.

- A proxy server that passes requests and responses unmodified is usually called a gateway or sometimes a *tunneling proxy*.
- A forward proxy is an Internet-facing proxy used to retrieve from a wide range of sources (in most cases anywhere on the Internet).
- A reverse proxy is usually an Internet-facing proxy used as a front-end to control and protect access to a server on a private network, commonly also performing tasks such as load-balancing, authentication, decryption or caching.[3]

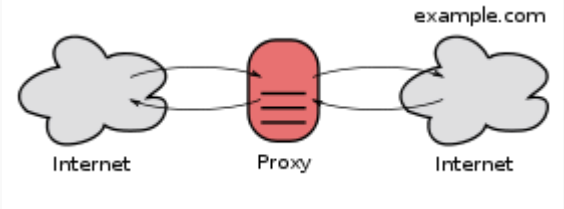
2.1.Forward proxies



A forward proxy taking requests from an internal network and forwarding them to Internet.

Forward proxies are proxies where the client server names the target server to connect to.[3] Forward proxies are able to retrieve from a wide range of sources (in most cases anywhere on the Internet).The terms "forward proxy" and "forwarding proxy" are a general description of behavior (forwarding traffic) and thus ambiguous. Except for Reverse proxy, the types of proxies described in this article are more specialized sub-types of the general forward proxy concept.

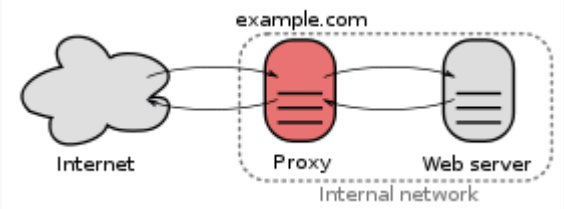
2.2.Open proxies



An open proxy forwarding requests from and to anywhere on the Internet.

An open proxy is a forwarding proxy server that is accessible by any Internet user. Gordon Lyon estimates there are "hundreds of thousands" of open proxies on the Internet.[4] An*anonymous open proxy* allows users to conceal their IP address while browsing the Web or using other Internet services. There are varying degrees of anonymity however, as well as a number of methods of 'tricking' the client into revealing itself regardless of the proxy being used.

2.3.Reverse proxies



A reverse proxy taking requests from the Internet and forwarding them to servers in an internal network.Those making requests connect to the proxy and may not be aware of the internal network.

A **reverse proxy** (or surrogate) is a proxy server that appears to clients to be an ordinary server. Requests are forwarded to one or more origin servers which handle the request. The response is returned as if it came directly from the web server.[3]Reverse proxies are installed in the neighborhood of one or more web servers. All traffic coming from the Internet and with a destination of one of the neighborhood's web servers goes through the proxy server. The use of "reverse" originates in its counterpart "forward proxy" since the reverse proxy sits closer to the web server and serves only a restricted set of websites.

III. RELATED WORK

3.1.A very rudimentary test to verify your wireless network iscompletely unsecured –

In the MS Windows environment, drag your mouse over the wireless icon in the bottom right corner (this corner is called the "system tray") of your computer screen. This wil l display the name of your wireless network. If it shows the default name of the wireless network, as provided by the manufacturer, you have high probability of having an unsecured network. In unsecured network, this may be the make or model of your wireless router and you may seesomething like, "Linksys" or "D-Link" or "Default (Unsecured)". [Linksys, 3Com, Netgear, D-Link, Microsoft Broadband are brand names of some wireless (wi-fi) routers]. This test is like a Thermometer test, which measures the body temperature only. Higher body temperature means some abnormality but cannot diagnose it. At the same time, normal temperature does not mean that all is normal.

3.2.Encryption schemes

There are many methos available for the wi-fi security, many encryption schemes such as EAP,TKIP, AES, WEP, WPA,WPA2 etc and many security tips are develeped.

3.2.1.AES:- Advanced Encryption Standard is gaining acceptance as appropriate replacement for RC4 algorithm in WEP. AES uses the Rijandale Algorithm and supports the following key lengths-128 bit, 192 bit, 256 bit. AES is considered to be un-crack able by most Cryptographers. NIST has chosen AES for Federal Information Processing Standard (FIPS). In order to improve wireless LAN security the 802.11i is considering inclusion of AES in WEPv2.

3.2.2.TKIP:- The temporal key integrity protocol (TKIP), initially referred to as WEP2, is an interim solution that fixes the key reuse problem of WEP, that is, periodically using the same key to encrypt data. The TKIP process begins with a 128-bit "temporal key" shared among clients and access points. TKIP combines the temporal key with the client's MAC address andthen adds a relatively large 16-octet initialization vector to produce the key that will encrypt the data. This procedure ensuresthat each station uses different key streams to encrypt the data [5].

3.2.3.WEP: - The industry's solution: WEP (Wired Equivalent Privacy) [7], [5], [8], [9], [10]

- Share a single cryptographic key among all devices
- Encrypt all packets sent over the air, using the shared key
- Use a checksum to prevent injection of spoofed packets [6].

Some devices support the various versions of WEP-

- WEP-64-bit key (sometimes called WEP-40)
- WEP 128-bit key (sometimes called WEP-104)
- WEP 256-bit key.

3.2.4.WAP:-WAP stands for Wi-Fi Protected Access [7], [5], [8], [9], [10]. This standard was developed to replace WEP. Wi-Fi devices typically support multiple variations of WPA technology. Traditional WPA, also known as WPA-Personal and sometimes also called WPA-PSK (for pre-shared key), is designed for home networking while another version, WPAEnterprise, is designed for corporate networks.WAP2 is an improved version of Wi-Fi Protected Access supported by all newer Wi-Fi equipment. Like WPA, WPA2 alsoexists in Personal/PSK and Enterprise forms [8].

3.3.Protocol stack

The protocol stack for WLANs was designed such that existing applications can use them with minor modifications. The three layers are same to other networks:-application, transport and network layers are same. Proxy server works on upper three layers but mostly on the application layer.Proxy server plays very important role in LAN network , in the same way if we add the proxy server to WLAN than in the same way with the help of proxy server can protect the WLAN network also .Proxy server in between the clients and server.Proxy server is also known as"application level gateway".proxy server provides increased performance and security. In the proxy server the data enters through one port and is forwarded to another port or the rest of the network. Basically proxy server plays the two important role:-

3.3.1. Performance impovement:-Proxy servers saves the requests for a certain time period. Hence the performance increases dramatically for a group of users.for example if a person p request for a web page ,after some time another person q requests the same site than the proxy server returns the same web page for person q that it already fetched for the person p,instead of forwarding the request to the server. Hence the time will be saved .

3.3.2. Filteration:-Proxy severs can also povides the facility of the filtering. Porxy server povides the content filteringapplication i.e. they control the content that may be relayed either in one direction or in the both directions.Proxyserver can filter the requests.for example in school or in colleges certain web sites are blocked or we can not open some web sites this can also be done with the help of the proxy servers.

3.4.Practical Aproach

A slew of products for securing corporate networks are available in the market. Firewalls prevent unauthorized users from gaining access to the network . IDSs detect compromised machines in the network .IPSec secures the communication channel between two authorized machines , and is frequently used byVPN software. While these techniques are effective in reducing the number of attacks from outside the corporate network, they do not secure the Wi-Fi network against the attacks. In particular, none of these can detect rogue Wi-Fi devices and DoS attacks on Wi-Fi networks. The use of VPNs and IPSec is often not sufficient, as we discussed earlier. IDS products usually detect compromised machines once the attack is launched, and most have a high false positive rate, which significantly reduces their usefulness from the perspective of a network administrator. In comparison, the DAIR security management system detects andlocates rogue Wi-Fi devices and various DoS attacks with few false positives and minimal human intervention.There are several commercial products in the area of corporate Wi-Fi security . Most use one of two approaches:they either rely on APs or they use dedicated and expensive custom hardware sensors for RF monitoring. The marketing literature of these products contains few technical details. Some commercial products rely on APs for monitoring wireless networks . Although cost effective, this approach has several limitations. First, a single-radio AP can not easily monitor multiple channels since its primary function requires it to spend most of its time on one specific channel serving associated clients. Second, the APs usually have limited CPU power and memory resources, so polling them (i.e., issuing SNMP queries) too frequently is problematic. Third, an AP only provides a view of one end of the wireless communication, so an AP-based solution can not be used to detect problems such as RF holes or excessive interference that primarily affect the client end of the communication. Finally, , monitoring the network from an AP alone does not provide comprehensive coverage. To overcome these limitations, some vendors augment the AP-based monitoring by deploying special sensor nodes throughout the organization . However, such specialized sensors are expensive, and require careful planning for an effective deployment. We are aware of only one prior research paper on detecting rogue devices . In this, mobile clients and APs monitor the network and detect rogue devices. Cisco's Wireless LAN Solution Engine uses a similar approach . The proposed scheme has a few limitations. First, it is difficult to guarantee complete coverage because the monitoring sensors are mobile. Second, the amount of RF monitoring and reporting depends on the battery of the mobile clients. Third, the algorithm proposed in Adya et al. flags any unknown AP as a rogue device, even if the AP is not plugged into the corporate network. Fourth, the proposed techniques do not detect rogue ad hoc networks, and finally, the previous work does not detect DoS attacks on Wi-Fi networks.There is some prior research on detecting greedy and malicious behavior in IEEE 802.11 networks. Bellardo et al. presenta study of

various DoS attacks in IEEE 802.11 networks. Theydemonstrate the attacks, and present simple schemes to counter them. The solution requires clients to cooperate with each other and in some cases, changes to IEEE 802.11. DAIR, on the other hand, detects these faults and reports them to the network administrator. The detection framework for DAIR is more efficient due to the presence of a larger number of sensors.DOMINO is an AP based solution for detecting greedy behavior in IEEE 802.11 hotspots . Several other researchers have proposed monitoring and characterization of wireless networks by polling the Aps.These systems have the same drawbacks as other AP based solutions discussed earlier. The benefits of dense sensor deployments were presented in Conner et al. The focus of that paper was on environmental monitoring applications such as temperature control or locating empty meeting rooms, and not Wi-Fi monitoring.

IV. CONCLUSION

WI-FI networks are growing day by day. The new challenges or we can say the security risks are also increases day to day.We can impove the performance as well as the security with the help of proxy server ,if it is implemented successfully.we can secure the WI-Fi network upto 5-10% with the help of the proxy server.

REFERENCES

[1] http://www.webopedia.com/TERM/W/Wi_Fi.html
[2] http://en.wikipedia.org/wiki/Proxy_server.
[3] Forward and Reverse Proxies". *httpd mod_proxy*. Apache. Retrieved 20 December 2010.
[4] Lyon, Gordon (2008). *Nmap network scanning*. US: Insecure. p. 270.ISBN 978-0-9799587-1-7.
[5] Wireless lan security today and tomorrow by *Sangram Goyal* and *Dr. S. A. Vetha Manickam* Center for Information and Network Security Pune University.
[6] Wireless security ppt by David Wagner.
[7] The State of Wi-Fi® Security Wi-Fi CERTIFIED™ WPA2TM Delivers Advanced Security to Homes, Enterprises and Mobile Devices by Wi-Fi Alliance.
[8] Introduction to Wi-Fi Network Security By Bradley Mitchell .
[9] Sara Nasre Wireless Lan Security Research Paper IT 6823 Information Security Instructor: Dr. Andy Ju An Wang Spring 2004.
[10] WI-FI security –WEP, WPA and WPA2 by Guillaume Lehembre.