Global Journal of Science Frontier Research
Mathematics and Decision Sciences
Volume 12 Issue 11 Version 1.0 Year 2012
Type : Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 2249-4626 & Print ISSN: 0975-5896

Security Issues in Wireless Local Area Networks (WLAN)

By Dr. Gurjeet Singh
Desh Bhagat Institute of Engg & Management Moga

Abstract - This paper deals with this wireless local area security technologies and aims to exhibit their potential for integrity, availability and confidentiality. It provides a thorough analysis of the most WLAN packet data services and technologies, which can reveal the data in a secure manner. The paper outlines its main technical characteristics, discusses its architectural aspects based on security and explains the access protocol, the services provided, in secured way. This paper deals with security techniques for wireless local area networks.

GJSFR-F Classification : MSC 2010: 68U01

SECURITY ISSUES IN WIRELESS LOCAL AREA NETWORKS WLAN

Strictly as per the compliance and regulations of :

Open Association of Research Society, USA
Research | Diversity | Ethics

© 2012. Dr. Gurjeet Singh. This is a research/review paper, distributed under the terms of the Creative Commons Attribution-Noncommercial 3.0 Unported License http://creativecommons.org/licenses/by-nc/3.0/), permitting all non commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

Security Issues in Wireless Local Area Networks (WLAN)

Dr. Gurjeet Singh

Abstract - This paper deals with this wireless local area security technologies and aims to exhibit their potential for integrity, availability and confidentiality. It provides a thorough analysis of the most WLAN packet data services and technologies, which can reveal the data in a secure manner. The paper outlines its main technical characteristics, discusses its architectural aspects based on security and explains the access protocol, the services provided, in secured way. This paper deals with security techniques for wireless local area networks.

I. Introduction

A wireless LAN (WLAN) is analogous to a wired LAN but radio waves being the transport medium instead of traditional wired structures. This allows the users to move around in a limited area while being still connected to the network. Thus, WLANS combine data connectivity with user mobility, and, through simplified configuration, enable movable LANs [1]. In other words WLANS provide all the functionality of wired LANs, but without the physical constraints of the wire itself.

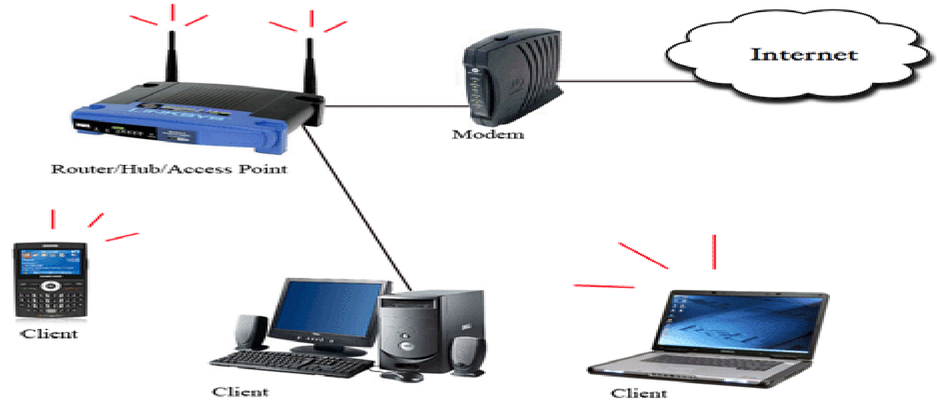

Figure 1.1 : Wireless Local Area Network

Generally a WLAN (in Infrastructure mode, see below) consists of a central connection point called the Access Point (AP). It is analogous to a hub or a switch in traditional star topology based wired local area networks. The Access Point transmits the data between different nodes of a wireless local area network and in most cases serves as the only link between the WLAN and the wired LAN. A typical Access Point can handle

Author : *AP, Deptt of CSE/IT, Desh Bhagat Institute of Engg & Management, Moga. E-mail : hi_gurjeet@rediffmail.com*

© 2012 Global Journals Inc. (US)

a handsome amount of users within a radius of about 300 feet. The wireless nodes, also called clients of a WLAN usually consist of Desktop PCs, Laptops or PDAs equipped with wireless interface cards.

II. Types of Wireless Networks

There are three types of wireless networks:

a) Wireless Personal Area Networking (WPAN)

WPAN describes an application of wireless technology that is intended to address usage scenarios that are inherently personal in nature. The emphasis is on instant connectivity between devices that manage personal data or which facilitate data sharing between small groups of individuals. An example might be synchronizing data between a PDA and a desktop computer. Or another example might be spontaneous sharing of a document between two or more individuals. The nature of these types of data sharing scenarios is that they are ad hoc and often spontaneous. Wireless communication adds value for these types of usage models by reducing complexity (i.e. eliminates the need for cables).

b) Wireless Local Area Networking (WLAN)

WLAN on the other is more focused on organizational connectivity not unlike wire based LAN connections. The intent of WLAN technologies is to provide members of workgroups access to corporate network resources be it shared data, shared applications or e-mail but do so in way that does not inhibit a user's mobility. The emphasis is on a permanence of the wireless connection within a defined region like an office building or campus. This implies that there are wireless access points that define a finite region of coverage.

c) Wireless Wide Area Networking (WWAN)

WWAN addresses the need to stay connected while traveling outside this boundary. Today, cellular technologies enable wireless computer connectivity either via a cable to a cellular telephone or through PC Card cellular modems. The need being addressed by WWAN is the need to stay in touch with business critical communications while traveling.

III. Ieee 802.11b Security Features

The security features provided in 802.11b standard [2] are as follows:

a) SSID – Service Set Identifier

SSID acts as a WLAN identifier. Thus all devices trying to connect to a particular WLAN must be configured with the same SSID. It is added to the header of each packet sent over the WLAN (i.e. a BSS) and verified by an Access Point. A client device cannot communicate with an Access Point unless it is configured with the same SSID as the Access Point.

b) WEP - Wired Equivalent Privacy

According to the 802.11 standard, Wired Equivalent Privacy (WEP) was intended to provide "confidentiality that is subjectively equivalent to the confidentiality of a wired local area network (LAN) medium that does not employ cryptographic techniques to enhance privacy" [4].

IEEE specifications for wired LANs do not include data encryption as a requirement. This is because approximately all of these LANs are secured by physical

Ref.

2. Dr. Gurjeet Singh & Dr. Jatinder Singh "Security Issues in Broadband Wireless Networks" Global Journal of Researches in Engineering Electrical and Electronics Engineering, Vol 12, Issue 5, 2012.

© 2012 Global Journals Inc. (US)

means such as walled structures and controlled entrance to building etc. However no such physical boundaries can be provided in case of WLANs thus justifying the need for an encryption mechanism.

WEP provides for Symmetric Encryption using the WEP key. Each node has to be manually configured with the same WEP key. The sending station encrypts the message using the WEP key while the receiving station decrypts the message using the same WEP key. WEP uses the RC4 stream cipher.

c) *MAC Address Filters*

In this case, the Access Point is configured to accept association and connection requests from only those nodes whose MAC addresses are registered with the Access Point. This scheme provides an additional security layer.

IV. Problem Definition

Ubiquitous network access without wires is the main attraction underlying wireless network deployment. Although this seems as enough attraction, there exists other side of the picture. Before going All-Wireless, organizations should first understand how wireless networks could be vulnerable to several types of intrusion methods.

- *Invasion & Resource Stealing:* Resources of a network can be various devices like printers and Internet access etc. First the attacker will try to determine the access parameters for that particular network. For example if network uses MAC Address based filtering of clients, all an intruder has to do is to determine MAC address and assigned IP address for a particular client. The intruder will wait till that valid client goes off the network and then he starts using the network and its resources while appearing as a valid user.
- *Traffic Redirection:* An intruder can change the route of the traffic and thus packets destined for a particular computer can be redirected to the attacking station. For example ARP tables (which contain MAC Address to IP Address Mapping) in switches of a wired network can be manipulated in such a way that packets for a particular wired station can be re-routed to the attacking station.
- *Denial of Service (DOS):* Two types of DOS attacks against a WLAN can exist. In the first case, the intruder tries to bring the network to its knees by causing excessive interference. An example could be excessive radio interference caused by 2.4 GHz cordless phones or other wireless devices operating at 2.4GHz frequency. A more focused DOS attack would be when an attacking station sends 802.11 dissociate message or an 802.1x EAPOL-logoff message (captured previously) to the target station and effectively disconnects it.
- *Rouge Access Point:* A rogue Access Point is one that is installed by an attacker (usually in public areas like shared office space, airports etc) to accept traffic from wireless clients to whom it appears as a valid Authenticator. Packets thus captured can be used to extract sensitive information or can be used for further attacks before finally being re-inserted into the proper network

These concerns relate to wireless networks in general. The security concerns raised specifically against IEEE 802.11b networks [4] are as following.

- *MAC ADDRESS AUTHENTICATION:* Such sort of authentication establishes the identity of the physical machine, not its human user. Thus an attacker who manages to steal a laptop with a registered MAC address will appear to the network as a legitimate user.

Ref.

4. WLAN Association, "Introduction to Wireless LANs", WLAN A Resource Center, 1999, http://www.wlana.com/learn/intro.pdf

© 2012 Global Journals Inc. (US)

- *ONE-WAY AUTHENTICATION:* WEP authentication is client centered or one-way only. This means that the client has to prove its identity to the Access Point but not vice versa. Thus a rogue Access Point will successfully authenticate the client station and then subsequently will be able to capture all the packets send by that station through it.
- *STATIC WEP KEYS:* There is no concept of dynamic or per-session WEP keys in 802.11b specification. Moreover the same WEP key has to be manually entered at all the stations in the WLAN.
- *SSID:* Since SSID is usually provided in the message header and is transmitted in clear text format, it provides very little security. It is more of a network identifier than a security feature.
- *WEP KEY VULNERABILITY:* WEP key based encryption was included to provide same level of data confidentiality in wireless networks as exists in typical wired networks. However a lot of concerns were raised later regarding the usefulness of WEP. The IEEE 802.11 design community blames 40-bit RC4 keys for this and recommends using 104- or 128-bit RC4 keys instead. Although using larger key size does increase the work of an intruder, it does not provide completely secure solution. Many recent research results have proved this notion [5]. According to these research publications the vulnerability of WEP roots from its initialization vector and not from its smaller key size

V. Virtual Private Network (vpn)

A Virtual Private Network (VPN) is a network technology that creates a secure network connection over a public network such as the Internet or a private network owned by a service provider. Large corporations, educational institutions, and government agencies use VPN technology to enable remote users to securely connect to a private network.

A VPN can connect multiple sites over a large distance just like a Wide Area Network (WAN). VPNs are often used to extend intranets worldwide to disseminate information and news to a wide user base. Educational institutions use VPNs to connect campuses that can be distributed across the country or around the world.

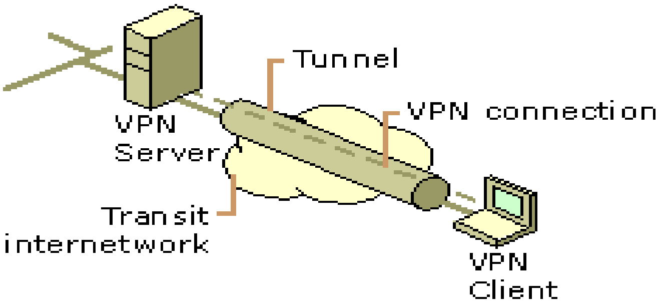

Figure 1.2 : Virtual private network

VPN technology provides three levels of security [7]:

- *Authentication:* A VPN Server should authorize every user logged on at a particular wireless station and trying to connect to WLAN using VPN Client. Thus authentication is user based instead of machine based.

Ref.

5. John Vollbrecht, David Rago, and Robert Moskowitz "Wireless LAN Access Control and Authentication", White Papers at Interlink Networks Resource Library, 2001. http://www.interlinknetworks.com/images/ resource/WLAN_Access_Control.pdf

- *Encryption:* VPN provides a secure tunnel on top of inherently un-secure medium like the Internet. To provide another level of data confidentiality, the traffic passing through the tunnel is also encrypted. Thus even if an intruder manages to get into the tunnel and intercepts the data, that intruder will have to go through a lot of effort and time decoding it (if he is able to decode it).
- *Data authentication:* It guarantees that all traffic is from authenticated devices thus implying data integrity.

Notes

Common Uses of VPNs

The next few subsections describe the more common VPN configurations in more detail.

Remote Access Over the Internet

VPNs provide remote access to corporate resources over the public Internet, while maintaining privacy of information. Figure 2 shows a VPN connection used to connect a remote user to a corporate intranet.

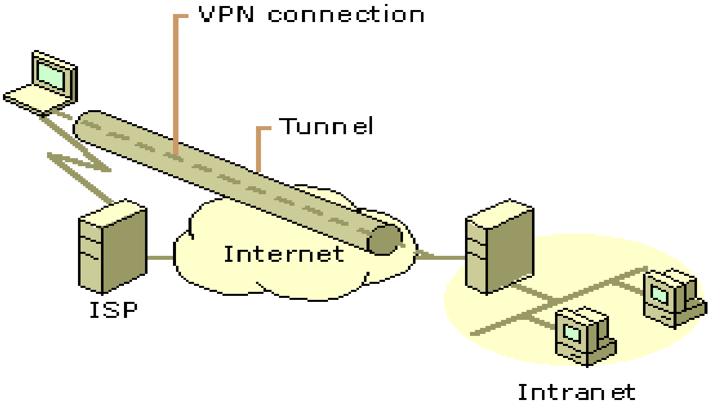

Figure 1.3 : VPN connection to connect a remote client to a private intranet

Rather than making a long distance (or 1-800) call to a corporate or outsourced network access server (NAS), the user calls a local ISP. Using the connection to the local ISP, the VPN software creates a virtual private network between the dial-up user and the corporate VPN server across the Internet.

Connecting Networks Over the Internet

There are two methods for using VPNs to connect local area networks at remote sites:

- **Using dedicated lines to connect a branch office to a corporate LAN**. Rather than using an expensive long-haul dedicated circuit between the branch office and the corporate hub, both the branch office and the corporate hub routers can use a local dedicated circuit and local ISP to connect to the Internet. The VPN software uses the local ISP connections and the Internet to create a virtual private network between the branch office router and corporate hub router.
- **Using a dial-up line to connect a branch office to a corporate LAN**. Rather than having a router at the branch office make a long distance (or 1-800) call to a corporate or outsourced NAS, the router at the branch office can call the local ISP. The VPN software uses the connection to the local ISP to create a VPN between the branch office router and the corporate hub router across the Internet.

© 2012 Global Journals Inc. (US)

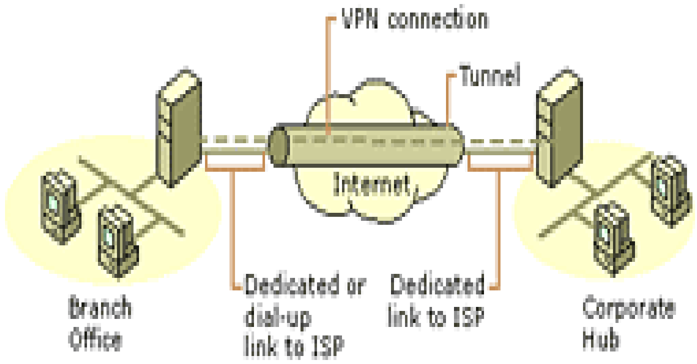

Figure 1.4 : Using a VPN connection to connect two remote sites

In both cases, the facilities that connect the branch office and corporate offices to the Internet are local. The corporate hub router that acts as a VPN server must be connected to a local ISP with a dedicated line. This VPN server must be listening 24 hours a day for incoming VPN traffic.

Connecting Computers over an Intranet

In some corporate internetworks, the departmental data is so sensitive that the department's LAN is physically disconnected from the rest of the corporate internetwork. Although this protects the department's confidential information, it creates information accessibility problems for those users not physically connected to the separate LAN.

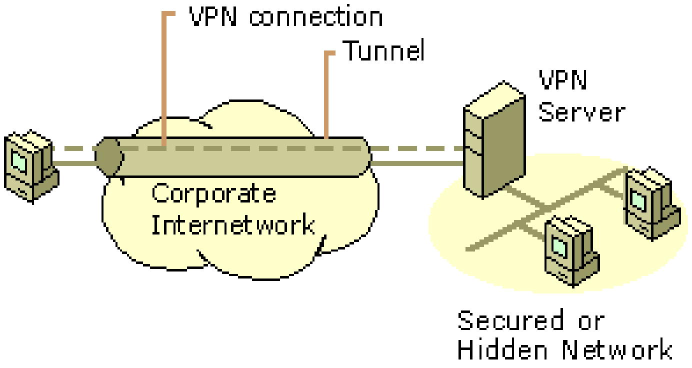

Figure 1.5 : Using a VPN connection to connect to a secured or hidden network

VPNs allow the department's LAN to be physically connected to the corporate internetwork but separated by a VPN server. The VPN server is not acting as a router between the corporate internetwork and the department LAN. A router would connect the two networks, allowing everyone access to the sensitive LAN. By using a VPN, the network administrator can ensure that only those users on the corporate internetwork who have appropriate credentials (based on a need-to-know policy within the company) can establish a VPN with the VPN server and gain access to the protected resources of the department. Additionally, all communication across the VPN can be encrypted for data confidentiality. Those users who do not have the proper credentials cannot view the department LAN.

Notes

© 2012 Global Journals Inc. (US)

VI. Cisco Leap (Light Weight Authentication Protocol)

Cisco LEAP, or EAP Cisco Wireless, is an 802.1X authentication type for wireless LANs that supports strong mutual authentication between the client and a RADIUS server. LEAP is a component of the Cisco Wireless Security Suite. Cisco introduced LEAP in December 2000 as a preliminary way to quickly improve the overall security of wireless LAN authentication. LEAP is a widely deployed, market-proven EAP authentication type.

Cisco's LEAP fills two noteworthy WLAN security holes [4]:

- Mutual Authentication between Client Station and Access Point: We described in Section 2 (Problem Definition) of Rogue Access Points. This was because of the One-Way, Client Centered Authentication between the Client and the Access Point. LEAP requires two-way authentication, i.e., a station can also verify the identity of the Access Point before completing the connection.
- Distribution of WEP Keys on a Per-session Basis: As opposed to the static WEP Keys in 802.11 specifications, LEAP protocol supports the notion of dynamic session keys. Both the Radius Server and Cisco client independently generate this key. Thus the key is not transmitted through the air where it could be intercepted.

VII. Secure Socket Layer (SSL)

Stands for "Secure Sockets Layer." SSL is a secure protocol developed for sending information securely over the Internet. Many websites use SSL for secure areas of their sites, such as user account pages and online checkout. Usually, when you are asked to "log in" on a website, the resulting page is secured by SSL. SSL encrypts the data being transmitted so that a third party cannot "eavesdrop" on the transmission and view the data being transmitted. Only the user's computer and the secure server are able to recognize the data. SSL keeps your name, address, and credit card information between you and merchant to which you are providing it. Without this kind of encryption, online shopping would be far too insecure to be practical. When you visit a Web address starting with "https," the "s" after the "http" indicates the website is secure. These websites often use SSL certificates to verify their authenticity. The below figure 1.6 shows the high level protocols

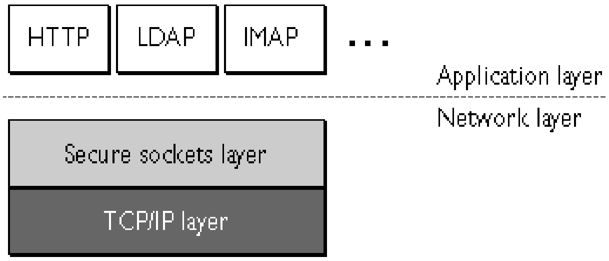

Figure 1.6 : SSL runs above TCP and below High Level Protocols

VIII. Access Point

Wireless **access points** (APs or WAPs) are specially configured nodes on wireless local area networks (WLANs). Access points act as a central transmitter and receiver of WLAN radio signals. Access points used in home or small business networks are generally

Ref.

4. WLAN Association, "Introduction to Wireless LANs", WLAN A Resource Center, 1999, http://www.wlana.com/learn/intro.pdf

© 2012 Global Journals Inc. (US)

small, dedicated hardware devices featuring a built-in network adapter, antenna, and radio transmitter. Access points support Wi-Fi wireless communication standards. Although very small WLANs can function without access points in so-called ”ad hoc” or peer-to-peer mode, access points support ”infrastructure” mode. This mode bridges WLANs with a wired Ethernet LAN and also scales the network to support more clients. Older and base model access points allowed a maximum of only 10 or 20 clients; many newer access points support up to 255 clients.

- Model Setup: Cisco Aironet 350 Series
- Data Rates: 1, 2, 5.5, 11 Mbps
- Network Standard: IEEE 802.11b
- Uplink:Auto-Sensing 0/100BaseT Ethernet
- Frequency Band: 2.4 to 2.497 GHz
- Network Architecture: Infrastructure
- Wireless Medium: Direct Sequence Spread Spectrum (DSSS)

IX. Experimental Results

There were four solutions suggested in response to the WEP vulnerability problems. Among those, IEEE 802.1x (i.e. EAP based) and Cisco LEAP will be treated as similar solutions for analysis and testing purposes and thus our test setup will only include Cisco LEAP solution for both cases. WEP based configuration will be implemented in order to emphasize and practically demonstrate the vulnerability in WEP based security. Various test results are discussed and illustrated as follows:

Legends:

------ Represents security control; .... Represents data flow

⟶ Represents interception

SP Represents a Java program that exchanges sample data with the client

a) WEP Based Approach

In this approach, WEP keys will be manually configured in both desktops and Access Point to enable WEP Key based encryption. SP will generate sample data. Then the Laptop armed with hacking software would try to break the WEP key.

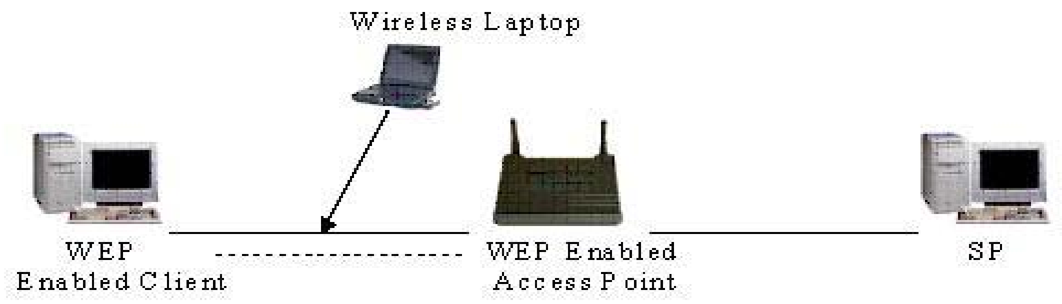

Figure 1.7 : WEP-enabled Set-up

© 2012 Global Journals Inc. (US)

b) LEAP Based Approach

In this approach one of the desktops will act as RADIUS server, while the client will be configured to use LEAP.

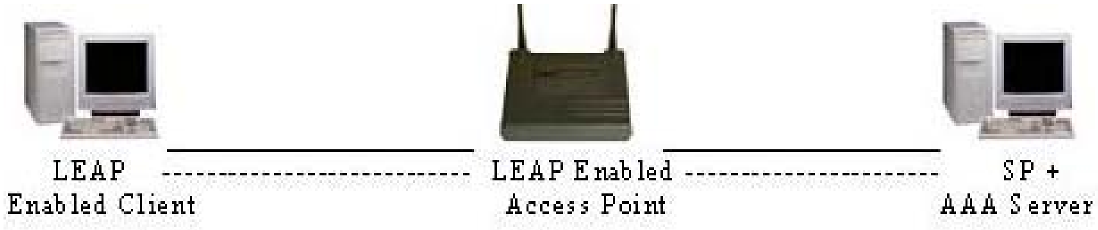

Figure 1.8 : LEAP-enabled Set-up

c) VPN Based Approach

In the VPN approach, the Access Point will be VPN aware; i.e. it will only accept and forward VPN traffic to a desktop computer configured as VPN server (and an optional AAA server). The second desktop computer will be installed with VPN client software.

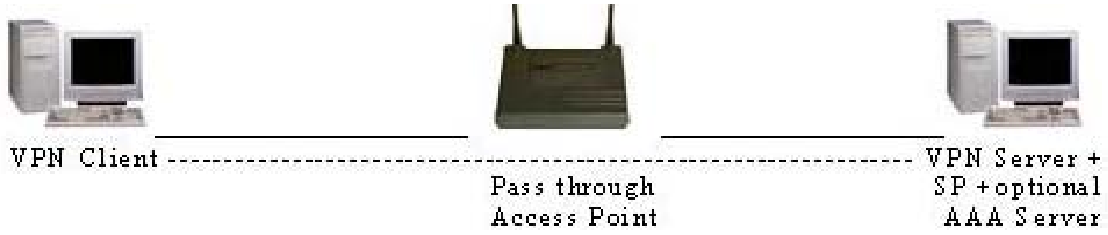

Figure 1.9 : VPN-enabled Set-up

An alternate approach would be to have the access point act as a VPN server. However this is not the approach most widely used primarily because of performance considerations.

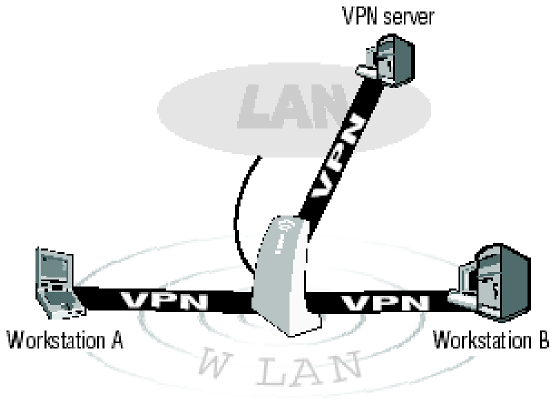

Figure 1.10 : VPN Server

d) SSL Based Approach

One of the desktops will be configured as a server (most probably a web server) implementing SSL. The second desktop will act as a SSL client. Again all traffic has to pass through Access Point.

© 2012 Global Journals Inc. (US)

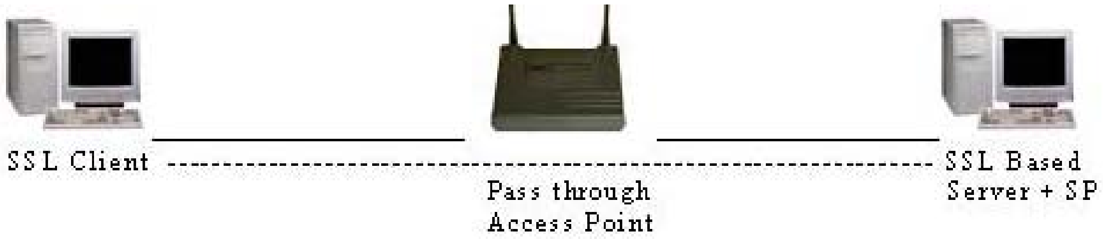

Figure 1.11 : SSL-enabled Set-up

X. Conclusion

The wireless local area network provides physical flexibility in that it does not matter where within the space the user is working they are still able to use the network. With a wired network it is necessary to decide where computers will be used and install the ports there. Often the use of space changes with time, and then either the space has to be rewired or long trailing cables are used to get from the computer to the port. With a wireless network the performance of the network will deteriorate as the usage increases but unless there is very high demand all users will be able to access the network. The network can reach places that wired networks cannot, this includes out of doors where up to several hundred metres from buildings the signal can be reached. Also, it is relatively easy to set up an access point linked back to the campus network for use in remote premises.

References Références Referencias

1. Dr. Gurjeet Singh "Performance and Effectiveness of Secure Routing Protocols in MANET" Global Journal of Computer Science & Technology" Vol 12, Issue 5, 2012.
2. Dr. Gurjeet Singh & Dr. Jatinder Singh "Security Issues in Broadband Wireless Networks" Global Journal of Researches in Engineering Electrical and Electronics Engineering, Vol 12, Issue 5, 2012.
3. Dr. Gurjeet Singh "Comparative Analysis and Security Issues in Wireless Broadband Networks" Global Journal of Researches in Engineering Electrical and Electronics Engineering Volume 12 Issue 8, 2012
4. WLAN Association, "Introduction to Wireless LANs", WLAN A Resource Center, 1999, http://www.wlana.com/learn/intro.pdf
5. John Vollbrecht, David Rago, and Robert Moskowitz "Wireless LAN Access Control and Authentication", White Papers at Interlink Networks Resource Library, 2001. http://www.interlinknetworks.com/images/ resource/WLAN_Access_Control.pdf
6. WLAN Association, "Wireless Networking Standards and Organizations", WLANA Resource Center, April 17 2002 http://www.wlana.com/pdf/wlan_standards_orgs.pdf
7. Interlink Networks, "Wireless LAN Security using Interlink Networks RAD Series AAA Server and Cisco EAP-LEAP", Application Notes at Interlink Networks Resource Library, 2002 http://interlinknetworks.com/images/resource/wireless_lan_security.pdf.
8. Jesse R.Walker, "Unsafe at any key size; An analysis of the WEP encapsulation", 802.11 Security Papers at NetSys.com, Oct 27 2000 http://www.netsys.com/library/papers/walker-2000-10-27.pdf
9. Interlink Networks, "Introduction to 802.1X for Wireless Local Area Networks", White Papers at Interlink Networks Resource Library, 2002. http://www.interlinknetworks.com/images/resource/802 1X for Wireless LAN.pdf.

© 2012 Global Journals Inc. (US)

10. Pierre Trudeau, "Building Secure Wireless Local Area Networks", White Papers at Colubris.com, 2001 http://download.colubris.com/library/ whitepapers/WP-010712-EN-01-00.pdf

Notes

© 2012 Global Journals Inc. (US)