Global Information Assurance Certification Paper

The Effect of WLAN Security Evolution on Home, Enterprise and Hotspots Market

Weng Khong Tang

GIAC Security Essentials Certification (GSEC)

Practical Assignment
Version 1.4b
Option 1

September 4, 2003

Table of Contents

Abstract 3

1.0 Introduction to Wi-Fi Security Evolution 3

1.1 WEP 4

1.2 WPA 4

1.3 802.11i or WPA2 5

2.0 Market Opportunity for Wireless LAN Worldwide 6

2.1 Enterprise Market 6

2.1.1 WEP the Quick Fix 6

2.1.2 The Promise of WPA 7

2.1.3 Is VPN the Solution 8

2.2 Home Market 10

2.2.1 Activate WEP at a very least 10

2.2.2 What is PSK 11

2.3 Hotspots Market 11

2.3.1 What is Hotspot 12

2.3.2 Components and Operation 12

2.3.3 Security and Roaming 13

3.0 Conclusion 14

References 16

Abstract

Wireless LAN (WLAN) is no longer a new term nowadays. The popularity and usage of Wi-Fi networking has grown spectacularly for the past few years. Compared to wired LANs, wireless systems can be faster to deploy and much lower cost to operate. In fact, WLAN technology has been the fastest growing segment in the communications market. According to Gartner Research, "Worldwide shipments of wireless LAN equipment equaled 9 million units in 2001. We forecast that shipments will continue to grow through 2007, at a compound annual growth rate of 42 percents" [1].

This paper begins with an overview of the Wi-Fi security evolution then followed by a brief discussion on Wired Equivalent privacy (WEP), Wi-Fi Protected Access (WPA), and 802.11i, tentatively known as WPA2. It then reveals how this evolution plays an important role on wireless security enhancement on the three major markets: Enterprise, Home and Hotspots. The discussion of Enterprise market section will then provide a glimpse into Bluesocket Wireless Gateway (WG), which gives better and ideal wireless network solution to replace VPN in the enterprise environment. The discussion continues by examining the cool feature, WPA Pre-Shared Key (WPA-PSK) which is designed to run in special home mode for Home market. Looking at an increase demand in the Hotspots market, this paper will explain the operation of a typical WLAN Hotspots and its components. The topic of Hotspots continues by discussing its security and roaming issue faced by the wireless users, Hotspot providers and Wireless Internet Service Providers (WISPs). This paper then concludes with the discussion of wireless security on the three major market places and its evolution. The discussion of WLAN is very broad so some knowledge of wireless LAN concept and networking are assumed of the reader.

1.0 Introduction to Wi-Fi Security Evolution

Security awareness is very important in WLAN nowadays. Having said that, WLAN security becomes a constant challenge and in fact many other security technologies have been developed and continue to be developed to bring strongly enhanced, accepted and adopted Wi-Fi security solution to market.

WEP, the native security protocol which has been well known and used in the Wi-Fi networking has posed a far less secure mechanism than it could be. In fact WEP has been now widely recognized as flaw. According to an article "Weakness in the Key Scheduling Algorithm of RC4" [2] has proven that intruders can easily crack WEP with the proper equipment and tools. Because of its cryptographic weaknesses, a lot of efforts have been done by the Wi-Fi Alliance and IEEE members to come out with a stronger security technology.

The result of this effort is WPA. Wi-Fi Protected Access (WPA) which is a subset of the current 802.11i draft was designed to address all known WEP vulnerabilities especially on the two primary security enhancements: data encryption and user authentication [3]. WPA provides users a high level of assurance with data protection while allowing only authorized users to have access to the network resources. Since no security solution can ever claim to be absolutely secure, an ongoing research has been started to produce an even better and longer term WLAN security solution, the IEEE 802.11i standard. In fact, the 802.11i specification is still under development and expected to be due out in May 2004 [4]. The 802.11i security mechanism will provide even better security enhancement with stronger encryption and authentication algorithms. The following subsections will briefly explain this evolution.

1.1 WEP [5]

WEP is an acronym for Wired Equivalent Privacy has been part of the 802.11 Wireless LAN encryption standards for the past few years. WEP is quite a simple security mechanism whereby it only encrypts and decrypts data between 802.11 wireless clients and Access Point (AP). This means that once frame exists beyond the wireless network, WEP is no longer applied. Throughout the whole data encryption process, the payload of each frame will be encrypted and transmitted using RC4 stream cipher algorithm and decrypted at the receiving end with the same 40 bits key. However, WEP is vulnerable to a variety of attacks because it is lack of dynamic key distribution and relatively short Initialization Vectors (IVs). WEP also provides no protection on forgery and replays. This leads to hackers easily decrypt any of the 802.11 frames with any sniffing tools and easily to derive information about the encryption key.

1.2 WPA [6] [7] [8]

WPA (Wi-Fi Protected Access) is a standard based security mechanism based on the IEEE 802.11 standard. Compared to WEP, WPA is an enhanced and more complicated wireless security version in term of data encryption and user authentication. WPA has been designed as a software upgrade to run on existing Wi-Fi Certified products, no hardware will need to be replaced. It is also designed to secure all versions of 802.11 devices, including 802.11a, 802.11b and 802.11g.

Wi-Fi Protected Access (WPA) consists of two main components, Temporal Key Integrity Protocol (TKIP) and 802.1x mechanisms. These two combinations will form a stronger wireless network security mechanism by preventing most sophisticated attacks on wireless network. In addition, WPA is designed to meet different requirements for Enterprise, Hotspots and Home environments.

WPA was designed to address the vulnerabilities inherent with WEP. To reduce

the decipherability of the key stream used in WEP, TKIP is used as an interim solution. Because of the static nature of the encryption key in WEP, TKIP generates new keys for every 10k of data transmitted over the wireless network. TKIP has changed the way keys are derived and rotates keys more often for security. Another area of improvement would be that of the user authentication mechanism. To obviate the authentication weakness of WEP, WPA has implemented 802.1X together with one of the standard Extensible Authentication Protocol (EAP) types to provide a stronger user authentication mechanism. Though WPA can provide excellent security to a certain extent, the demand for a better security mechanism for WLAN has never ended.

1.3 802.11i or WPA2 [9] [10]

802.11i or tentatively named as WPA2 will be the IEEE 802.11 standard for Wireless LAN network when it becomes available. In fact, the 802.11i specification has not been finalized yet and is still under development. 802.11 use dynamic negotiation of authentication and encryption algorithm between access points and mobile clients. The authentication schemes are based on 802.1x and EAP and eventually TKIP will be replaced by a new encryption algorithm, Advanced Encryption Standard (AES), which will be implemented at the hardware level. AES is the standard approved by National Institute of Standards and Technology (NIST). This standard specifies the Rijndael algorithm, a symmetric block cipher that can generate keys length of 128, 192 and 256 bits to process data blocks of 128 bits. AES protocol will provide enhanced encryption algorithm which will replace 802.11's RC4 based encryption. In addition, 802.11i will require new hardware change in Access Points (APs) for higher performing processors. The up coming 802.11i will provide replacement technology for WEP security. Figure 1 below illustrates the evolution of WLAN security

Figure 1: Evolution of WLAN security [11]

Evolution of wireless LAN security
WEP goes the way of the dodo bird, WPA emerges as missing link to 802.11i

Name
Wired Equivalent Privacy
Wi-Fi Protected Access
802.11i or Wi-Fi Protected Access Version 2

Acronym
WEP
WPA
WPA2

A.K.A.
Won't Even Protect
Will Protect Alright
Will prove airtight

Features

Weak encryption keys based on RC4 algorithm (typically 40-bit keys).

Static keys that make easy targets for hackers

Same underlying RC4-based encryption as WEP

TKIP (temporal key integrity protocol) added so that keys are rotated and encryption is strengthened.

Strong AES encryption based on Rijndael algorithm (128, 192 or 256 bit key sizes).

Adds two strong authentication features: wireless robust authentication protocol or WRAP; counter with cipher block chaining message authentication code protocol or CCMP.

Life span
1997-2003
2003-2004
2004-??????

2.0 Market Opportunity for Wireless LAN Worldwide

The rapid growth of Wireless LANs on marketplaces has well been taken place recently. This growth is mainly attributed to the maturing of WLAN technology. The key markets that collectively form the WLAN marketplace are Enterprise market, Home market and Public or Hotspots market.

2.1 Enterprise Market

WLAN offers many significant benefits like simplicity, flexibility, mobility and cost effectiveness; it has been shown that the home users adopt WLAN at a much faster pace compared to that of the enterprises or corporations. One of the main reasons that inhibit this progress in the enterprise environment is the security concern. Enterprises are fortifying their wireless LANs with a layered approach to security that mirrors the security of wired networks. Some have been implementing propriety solutions offered by vendors to address the WEP problems. Until recently, WPA was introduced more and more enterprises are expected to start implementing WLAN using this enhanced security mechanism. In fact, WPA has effectively addressed most of the WLAN security requirements which are largely missing in WEP. Although it has not been a significant increase in the figures, there is a trend that the corporations are moving to that direction.

2.1.1 WEP the Quick Fix

WEP, the native security mechanism has not proven to be the solution to enterprise market for the past few years. WEP which runs on the physical layer in the wireless network use only a single key for all Access Points (APs) and radio clients. Nevertheless, it is lack of automated key management and this poses a much easier way for hacker to crack the static key. Another challenge of WEP is that there is no user authentication mechanism that the physical layer security alone can provide. Most APs do not offer any means to authenticate users before they are granted network access other than MAC address which can be easily spoofed. Until there is a new security technology to replace WEP, a complementary technology such as VPN has been implemented to strengthen the wireless network security. However, standalone network layer security such as VPN is still not sufficient for securing Wireless network. This is because VPN only encrypts data between endpoints over a shared IP based network, leaving the wireless network vulnerable to lower level attack on MAC and IP header. This leads to unauthenticated connections to the AP and provide an opportunity for denial of service [12].

2.1.2 The Promise of WPA

In response to the need for stronger authentication and stronger encryption algorithm, the Wi-Fi Alliance and the IEEE have come out with a new standard called WPA. WPA combines two components to provide stronger security for wireless networks, TKIP and 802.1x [6]. TKIP increases the size of the key from 40 to 128 bits and provides data encryption enhancements and improvements to fix the flaws of WEP.

These include dynamically changing the encryption key on per session and per packet basic and ensure that the message has not been tampered with during transmission with MIC (Message Integrity Code) or sometime called Michael. This can be done by comparing the computed MIC results at the sender and receiver ends. If they do not match, the packet is dropped. Longer 48 bits IV hashing is used to avoid the weaknesses of the shorter 24 bits WEP RC4 key and protect against replay [13]. 802.1x, the second component of WPA deals with mutual authentication for mobile clients. 802.1x is a standard for "Port Based Access Control" for both wired and wireless networking. 802.1x by itself does not offer any wireless security but with Extensible Authentication Protocol (EAP) these two combinations can offer mutual authentication for the wireless clients [21]. This is to ensure that users who access the network are the ones who are supposed to be there.

For enterprise networks, an authentication server such as RADIUS is required to implement 802.1x security. Before any radio clients can get access to the wireless network, 802.1x uses one of the Extensible Authentication Protocol (EAP) type and an authentication server to verify that the client credentials are authentic. Once verified, a unique master key is produced for that computing session. TKIP will then distribute this master key to both the Access Point and the radio client and sets up a key hierarchy system. The master key will then be used to dynamically generate unique data encryption keys to securely and uniquely encrypt every data packet that is wirelessly communicated during that user's session [8]. Apart from that, the authentication server also validates the Access Point to make sure that the Access Point is part of the wireless network and not a rogue AP. The 802.1x also eliminates the static key management issue by ensuring that new encryption keys are generated and distributed frequently [14]. A comparison table between WEP and WPA is illustrated in figure 2.

WEP v. WPA

	WEP	WPA
Encryption	Flawed, cracked by scientists and hackers	Fixes all WEP flaws
	40-bit keys	128-bit keys
	Static – same key used by everyone on the network	Dynamic session keys. Per user, per session, per packet keys
	Manual distribution of keys – hand typed into each device	Automatic distribution of keys
Authentication	Flawed, used WEP key itself for authentication	Strong user authentication, utilizing 802.1X and EAP

Figure 2: WEP v. WPA [8]

As mentioned earlier, VPN by itself is not a complete security solution. However, VPN can be used as a complementary technology to add security enhancement to wireless network if it is properly configured. This means that having VPN implemented on top of WPA can provide another layer of security and is likely to meet the security needs of most organizations. Though VPN may solve some problems associated with WLAN security, is VPN designed specifically for WLAN environment or is there a better technology that can replace VPN - a topic worthy of discussion.

2.1.3 Is VPN the Solution

Traditional most enterprise VPN are basically being deployed to secure WAN connectivity such as remote internet access to the corporate, site to site VPN and provide connectivity to external business partners for accessing specific resources. Though VPN can provide necessary security through encryption, tunneling and firewall capabilities, they are not designed to provide WLAN's additional needs.

Base on an article, the Bluesocket Wireless Gateway (WG) is designed to secure and manage the evolving uses of WLAN access [15]. Bluesocket WG provides the security, mobility, easy to manage and cost effective manner for WLAN environment. Figure 3 below shows the mobility is the key driver for Wireless LANs. Like a traditional VPN, Bluesocket Wireless Gateways can provide a secure IPSEC tunnel and do stateful packet inspection and filtering. Furthermore, Bluesocket WG does provide roaming capability when a user roams to another Access Point that is on a different subnet, no interruption in the session and no re-

authentication process is required. However, VPN was not designed for this purpose as it provides a secure wireless connection only through one subnet per session. In addition, WG does things that VPN traditionally don't such as reduce user and device management overhead and supporting an open standard based wireless security solution compared to the proprietary VPN clients which are not an ideal solution for WLAN environment [15]. Bluesocket Wireless Gateway has a simple solution that brings all the WLAN benefits without the need to deploy a VPN. A summary of the key differences between VPN switch and WLAN Gateway is illustrated in Figure 4. With the emergence of WPA and Bluesocket Wireless Gateway will definitely provide a better and ideal solution for Enterprise market.

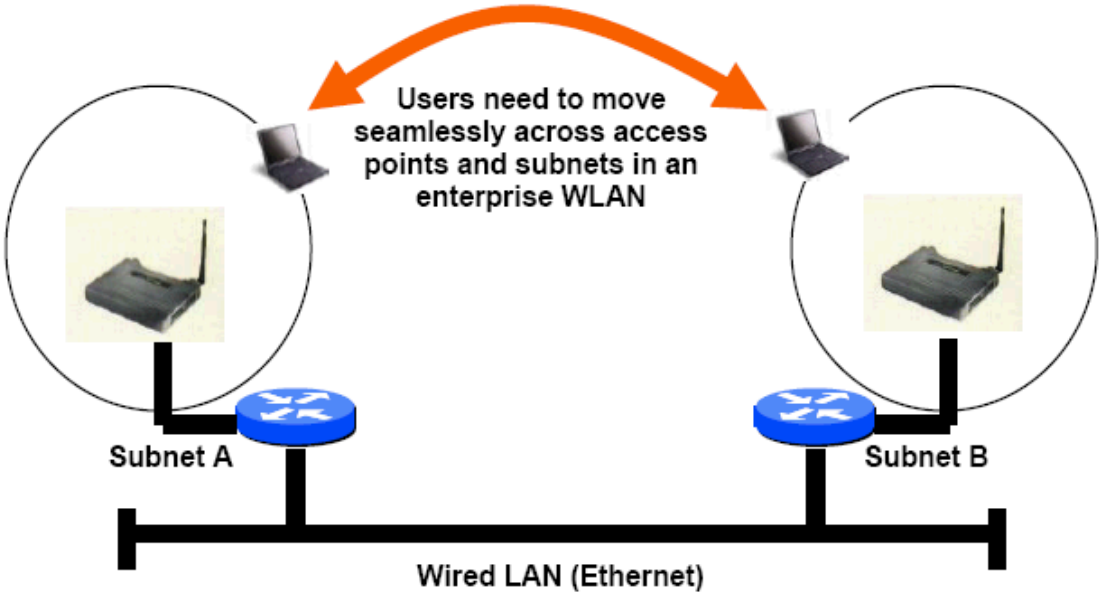

Figure 3: Mobility is the key driver for Wireless LANs [15]

WLAN Application Description	VPN Switch	WLAN Gateway
Design Philosophy	General purpose security solution	High Performance, best-of-breed solution designed for Wireless LANs
Typical Deployment Scenario	Remote Access; Site-to-site WANs	LAN oriented solution; supports high bandwidth "islands" of users
Mobility	No	Yes; across access points and subnets
Client support	Proprietary VPN client recommended	Proprietary client not required; but can work with several clients
Device Support	Limited number of 802.11 devices—closed solution	Wide range of mobile devices—open solution
Support for Guests, Visitors; Public WLANs	No (with some exceptions)	Yes (e.g., Browser-based log-in using SSL, Transparent Windows log-in)
Traffic Type	Encrypted traffic	Choice of Encrypted and Un-encrypted traffic
Investment Protection/ Future WLAN developments	WLANs are a niche segment for VPN vendors; emerging protocols and features may or may not be supported in future	Focus on WLANs ensures support for emerging technologies and protocols (802.1x, WPA, 802.11i, AP detection and management, 802.11e, 802.11f)
Ease of configuration and management	Complex multi-function deployment of security solution	Simple, elegant solution focused on WLAN security and management

Figure 4: Difference between a VPN switch and WLAN Gateway [15]

2.2 Home Market

Since WLAN network was first introduced to the communications market, wireless adoption within home environment has been the fastest growing segment. WLAN network can easily be set up by plugging an Access Point into an Ethernet port together with wireless stations equipped with wireless network adapter cards. It also takes advantage of the fact that the wireless equipments by default are shipped with security features disable and no extra configurations are needed. Perhaps, these make wireless networks so popular and common in Home market.

2.2.1 Activate WEP at a very least

Depending on the amount of network traffic and the information being exchanged over the air, it is all up to the wireless clients to decide whether to enable the security features on their wireless devices. With WEP enabled, it provides the basic level of protection against the drive by

unintentional visitors. Another way of securing the wireless network would be the Media Access Control (MAC) filtering whereby Access Points are manually configured with a list of accepted MAC addresses [14]. While this is not a foolproof, MAC address filtering only provide basic control of which wireless stations are allowed to communicate with the assigned APs. Due to the WEP nature of the reused static encryption key and easily spoofed MAC address, wireless network is vulnerable for attack. Despites the deficiencies of WEP, it does provide some margin of security compared with no security at all.

2.2.2. What is PSK [16] [19]

Though the home users are less aware and concern about the security implications associated with wireless networks, a better wireless security solution, WPA, is available and ready to be deployed. WPA has been designed to run in a special home mode called Pre-Shared Key (PSK). This mode has given a better wireless security solution to suit the home environments with no authentication server. Under WPA, the pre-shared key is used only in the initial setup of the dynamic TKIP key exchange. PSK allows the use of manually-entered keys or password to start the encryption process. To get it started, a unique password (also called a master key) is required to be set on the Access Points and wireless stations that are on the WLAN network. Then, WPA automatically takes over from that point. All wireless devices only with the same matching password can join the network and then automatically kicks off the TKIP encryption process. Throughout the encryption process, TKIP takes the original master key as a starting point and derives its encryptions keys mathematically from the master key. Those generated keys are then regularly rotated (called rekey interval) and changed (called rekeying) to ensure that no same encryption key is used twice. These features make WPA a far stronger security solution than WEP.

2.3 Hotspots Market

Nowadays Wireless LANs have emerged as a popular and effective way of accessing the internet, not only in the home and at work but have spread into the public arena as well. These public access locations also known as hotspots have been added every day in a very fast pace. According to Techworld.com [17]:

> The report forecasts there will be 71,079 hot spots worldwide this year, up from just 14,752 in 2002 and 1,214 in 2001 and the number of hot spots will grow to 151,768 in 2005. There were 9.3 million visitors to hot spots in 2003, up from 2.5 million in 2002. North America, with 4.7 million users, will top both Europe and Asia-Pacific this year. The report projects 2.7 million users in Asia Pacific and 1.7 million in Europe this year.

2.3.1 What is Hotspot

A hotspot is a specific geographic location in which an Access Point provides public wireless broadband network services to mobile visitors through a WLAN. Hotspots are often located in heavily populated places such as airports, train stations, coffee shops, conventions centers and hotels. To access internet based services offered in the hotspots, notebook or PDA device must be configured with Wi-Fi certified technology in order to communicate with the wireless Access Point installed in the public facility.

2.3.2 Components and Operation

There are some basic components being involved in the operation of a typical WLAN hotspot [18]. These components are client wireless adapter card, Access point, Billing system, Authentication server, Access Controller and optional VPN gateway.

The end user device such as laptop, PDA or handheld device must be equipped with wireless network card. This wireless card is used to communicate with the Access Points provided by the hotspot operator. The access point provides the other side of communications with the Wireless Internet Service Provider (WISP) via a broadband wired network. Whenever the Access Point receives requests from mobile devices, the requests will get forwarded to the WISP for verification. At this point, the Access controller which owned by the ISP takes control and checks for the user credential

First, it prompts for the user login account and password via the access point. Then, an authentication request is sent to the AAA provider to check against the user information from the user database resides at the RADIUS server. Once authenticated, the user's authorization information is sent back to the access controller. With this authorization information, the Access controller can decide what internet-based services are allowed for the user's requests. Finally, it captures billing record pertaining to the usage and forwards to the Billing system for further process. VPN gateway is optional and only used to form a secure VPN tunnel to the corporate network. Figure 5 illustrates the operation of a typical wireless LAN hotspot.

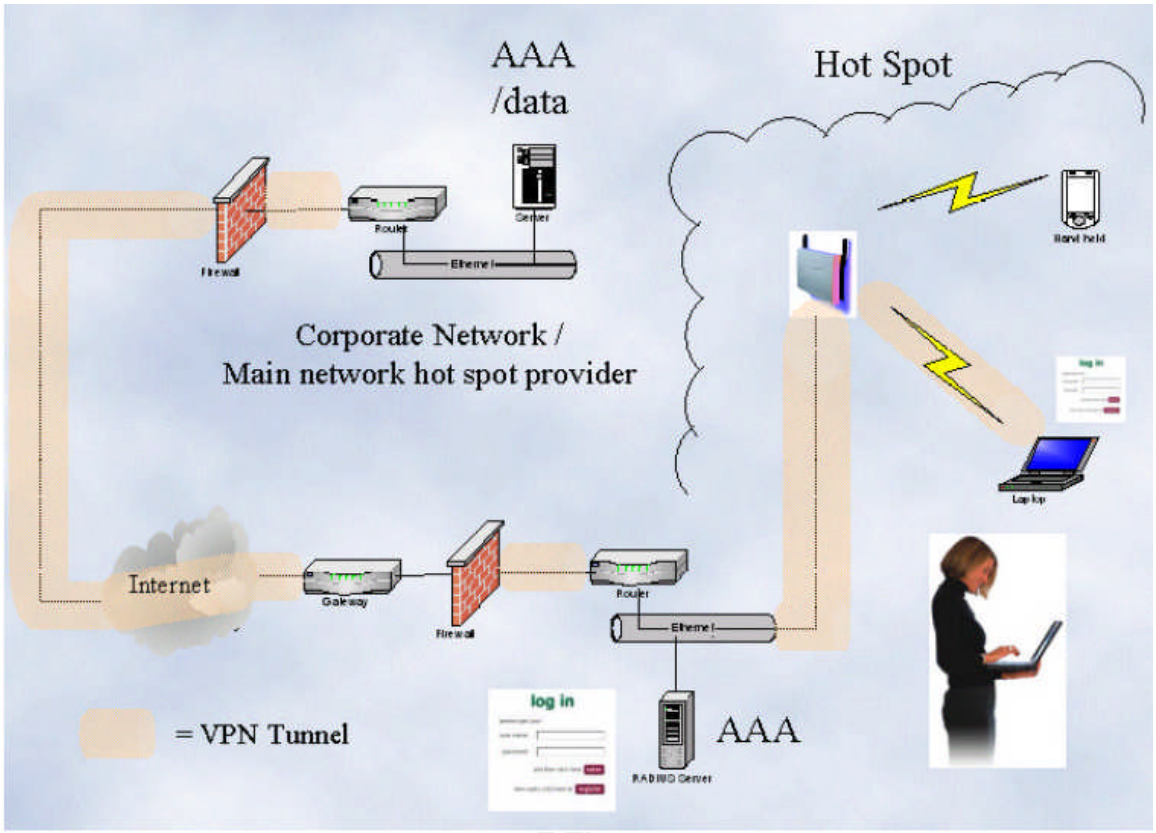

Figure 5: Wireless LANs hotspot operation [18]

2.3.3 Security and Roaming

By far, the biggest concern over WLAN has been the security. Anyone with an 802.11b wireless card can easily pickup other's broadcast in a typical Wireless LANs. Unless the information transmitted in the air is not private and confidential, this opened to hacker to easily spoof and steal the information. It is necessary to realize that the connection to the Internet via a public WLAN consists of multiple pieces that need to be secured. This includes the connection from the mobile wireless device to the nearest Access Point provided by the hotspot, the connection between hotspot to the Wireless Internet Service Provider (WISP) and the connections that involve multiple different WISPs. If the connection is to the corporate network then the connection in between the corporate network and the WISP need to be secured as well. The ideal solution is to achieve the end-to-end security. There are few roles that the carrier can be a player in the wireless market. For the scope of this paper, Wireless Internet Service provider (WISP) will be the role play in providing direct service to the hotspots.

Although some Wireless Internet Service Providers (WISPs) do provide

certain level of security with their custom software, many hotspots leave security turned off to allow wireless clients to access their wireless network easier in the first place. In fact, hotspot is the starting point that should have security enabled on the access points. Hotspot service providers should deploy WPA encryption standard to provide secure connection for wireless LAN communication. With WPA enabled, information will be encrypted securely from the user wireless adapter to the access points. To further secure the connection, AP sends the user information to an authentication server to verify the username and password before granting access to the Internet. However, the authentication process becomes more challenging when moving or roaming between WISPs. This process should be transparent to mobile users in order for them to move freely from one network to another without having to reconnect, change setting or lose connection at any point. This brings to another important challenge on wireless roaming security.

Roaming across different WISPs is crucial in public WLANs in order to maximize the coverage. In fact, the most cost effective way of expanding the network of hotspots is for the WISPs to offer roaming with other WISP networks. However, the roaming agreements between different WISPs have not yet clearly defined. The roaming agreements should include a strong authentication, authorization and accounting system to handle 802.11 usage requirements [20]. The ability to use the infrastructure of several WISPs while having a subscription with only one can be achieved with the use of digital certificate. The digital certificate represents each user credentials to a WISP. The WISP can deploy the 802.1x framework with EAP-TLS to authenticate a user's certificate and to verify the relationship between the certificate's issuing organization and the WISP [22]. A user's certificate can be forwarded from one ISP to another to request services, thereby at each hop allowing the ISP to verify the certificate and to arrange for billing according to the service level assigned to the user.

3.0 Conclusion

The benefit of wireless networks has been the driving force to bring the explosive growth in the WLAN market. However, wireless security has been the largest concern for wireless network development. To cope with this, a lot of efforts have been done by the IEEE and Wi-Fi Alliance to come out with better security solutions. This leads to the wireless security evolution from the WEP to WPA and the eventual 802.11i standard or WPA2.

Wi-Fi Protected Access (WPA) was designed to overcome the inherent flaws of WEP such as static key and short IV. With the two main components, TKIP and

802.1 x mechanisms, WPA is capable of preventing most sophisticated attacks on wireless network with better encryption process and stronger authentication algorithm. Three major market places include Enterprise, Home and Hotspots were being discussed. Enterprise market which has been the slowest growing pace in wireless network is expected to increase with the emergence of WPA as it meets the requirements of most corporate environment. Though VPN can be deployed on top of the WPA to provide a more comprehensive solution, Bluesocket Wireless Gateway (WG) is more suitable as it is designed for WLAN security and management solutions. VPN by itself only provides end to end encryption and lack of roaming capability across Access Points and subnets. Another feature that WPA can provide and specifically designed for Home market is the Pre-Shared Key (PSK). PSK is designed to run in a special home mode for home user and provide enhanced security that WEP cannot offer.

Hotspot has been the hottest topic being discussed nowadays and wireless security is the main focus faced by every party that involves. This includes the mobile user, hotspot itself and the Wireless Internet Service Provider (WISP). Early WEP implementations are vulnerable to being cracked by any tools, but the latest release of WPA can eliminate most of the known attacks and protect Wi-Fi users against interception and eavesdropping in public hotspots. The intrinsic encryption and authentication schemes defined in WPA might provide WISPs and Hotspots a better solution to secure the wireless communications. Apart from the wireless data security, roaming agreements between WISPs will be the next challenge for the service providers. In the longer run, the hotspot market is likely to converge towards a common solution.

802.11i, the new IEEE 802.11 standard for WLAN security which expected to be released in 2004 is designed to add enhanced security feature, including new encryption algorithm and dynamic key distribution. However, the implementation of 802.11i will require new hardware changed and this means new investments in the wireless devices for WLAN users.

References

[1] Rolfe, Andy. “Wireless LAN Equipment Market: Strong Growth Set To Continue.” October 2, 2002.
URL: http://www3.gartner.com/DisplayDocument?id=372450&ref=g_search

[2] Fluhrer, Scott, Mantin, Itsik, and Shamir, Adi. “Weakness in the key Scheduling Algorithm of RC4”
URL: http://www.cs.cornell.edu/courses\cs615\2002fa/615/rc4_ksaproc.pdf

[3] Wi-Fi Alliance. “Overview Wi-Fi Protected Access”. URL:
http://www.weca.net/OpenSection/pdf/Wi-Fi_Protected_Access_Overview.pdf

[4] Dorothy, Stanley. “802.11i: May 2004” Wi-Fi Networking News. June 26, 2003
URL: http://wifinetnews.com/archives/001829.html

[5] Geier, Jim. “802.11 WEP: Concepts and Vulnerability” 802.11 Planet June 20, 2002
URL: http://www.80211-planet.com/tutorials/article.php/1368661

[6] Interlink Networks. “WPA and 802.1x”
URL: http://www.interlinknetworks.com/resource/wa5-0-1.htm#what

[7] Mark Joseph Edwards. “Increasing Wireless Security with TKIP” Security Administrator October 23, 2002
URL: http://www.secadministrator.com/Articles/Index.cfm?ArticleID=27064

[8] Wi-Fi Alliance. “Wi-Fi Protected Access: Strong, standards-based, interoperable security for today’s Wi-Fi networks” April 29, 2003. URL:
http://www.wifialliance.com/OpenSection/pdf/Whitepaper_Wi-Fi_Security4-29-03.pdf

[9] Federal Information Processing Standards Publication 197. “Announcing the Advanced Encryption Standard (AES)” November 26, 2001
URL: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[10] Wexier, Joanie. “What’s in WPA?” NetworkWorldFusion November 13, 2002
URL: http://www.nwfusion.com/newsletters/wireless/2002/01626699.html

[11] Geier, Jim. “WPA plugs holes in WEP” Network World March 31, 2003
URL: http://www.nwfusion.com/research/2003/0331wpa.html?page=3

[12] Corbett, Cherita. “Security for 802.11 Wireless Networks”
URL: http://www.prism.gatech.edu/~gt0369c/Security_survey.pdf

[13] Dell White Paper. “Wireless Security in 802.11 (Wi-Fi) Networks” January 2003
URL: http://admin.wifi.ee/Dokumendid/WiFi-security_DELL.pdf

[14] Wi-Fi Alliance. “Securing Wi-Fi Wireless Networks With Today’s Technologies” February 6, 2003. URL:
http://www.weca.net/OpenSection/pdf/Whitepaper_Wi-Fi_Networks2-6-03.pdf

[15] Bluesocket. “Wireless Gateways: Going beyond VPNs for WLAN security and management solutions” URL:
http://www.bluesocket.com/solutions/bluesocket-vpns-bluepaper.pdf

[16] WiFi Alliance. “Overview Wi-Fi Protected Access for the Home”
http://www.wi-fi.net/OpenSection/pdf/WPA_Home_Overview.pdf

[17] Lawson, Stephen, IDG news service. “Wi-Fi hotspots set to grow” Techworld July 1, 2003. URL:
http://www.techworld.com/news/index.cfm?fuseaction=displaynews&NewsID=230

[18] Multicap. “Access on the spot: Wireless Hot spots”
URL: http://www.multicap.be/pdf/Hotspots_Eng.pdf

[19] Bowman, Barb. “WPA Wireless Security for Home Networks” July 28, 2003. URL:
http://www.microsoft.com/WindowsXP/expertzone/columns/bowman/03july28.asp

[20] Bridgewater Systems. IP Service Perspectives Volume 3, Issue 2. “How carriers Can Play in the 802.11 Market” URL:
http://monitortoday.com/IPSP_2.html

[21] Ou, George C. “Enterprise Level Wireless LAN Security”
URL: http://www.lanarchitect.net/Articles/Wireless/index.htm

[22] Verisign. “Secure Global Roaming for 802.11 Wlans”
URL: http://research.verisign.com/Papers/VeriSign-WLAN-Security.pdf