Research Article Impact Factor: 0.621 ISSN: 2319-507X
Uma Patil, IJPRET, 2014; Volume 2 (9): 59-67 IJPRET

INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

WIRELESS NETWORK SECURITY: OVERVIEW

PROF. UMA R. PATIL

Department Science, Shri Shivaji College Of Computer Arts, Commerce & Science, Akola

Accepted Date: 27/02/2014 ; Published Date: 01/05/2014

Abstract: Wireless technologies have become increasingly popular in our everyday business and personal lives. Personal digital assistants (PDA) allow individuals to access calendars, e-mail, address and phone number lists, and the Internet. Some technologies even offer global positioning system (GPS) capabilities that can pinpoint the location of the device anywhere in the world. Wireless technologies promise to offer even more features and functions in the next few years. The goal of this article is to provide an overview of what is required to provide a secure communication channel in a wireless environment. The focus is on the security techniques available for Wireless Local Area Networks (WLAN) and for wireless devices (e.g. cell phones, and PDA's) used to access the Internet.

Keywords: WLAN Security, WAP, WEP, VPN, 802.11b

PAPER-QR CODE

Corresponding Author: PROF. UMA R. PATIL

Access Online On:

www.ijpret.com

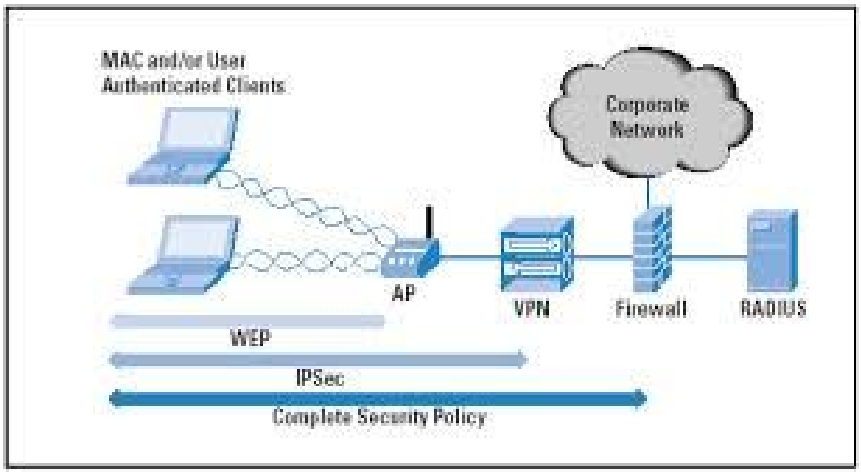
How to Cite This Article:

Uma Patil, IJPRET, 2014; Volume 2 (9): 59-67

INTRODUCTION

Wireless security is the prevention of unauthorized access or damage to computers using wireless networks. The most common types of wireless security are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WEP is a notoriously weak security standard. The password it uses can often be cracked in a few minutes with a basic laptop computer and widely available software tools. WEP is an old IEEE 802.11 standard from 1999 which was outdated in 2003 by WPA or Wi-Fi Protected Access. WPA was a quick alternative to improve security over WEP. The current standard is WPA2; some hardware cannot support WPA2 without firmware upgrade or replacement. WPA2 uses an encryption device which encrypts the network with a 256 bit key; the longer key length improves security over WEP.

A Wireless Local Area Network (WLAN) is a type of local area network that uses high frequency radio waves rather than wires to communicate between network-enabled devices. WLANs are best suited for home users, small networks, or networks with low security requirements. With the deployment of wireless networks in business environments, organizations are working to implement security mechanisms that are equivalent to those of wire-based LANs. An additional component of this security requirement is the need to restrict access to the wireless network only to valid users. Physical access to the WLAN is different than access to a wired LAN. Existing wired network have access points, typically RJ45 connectors, located inside buildings which may be secured from unauthorized access through the use of such devices as keys and/or badges. A user must gain physical access to the building to plug a client computer into a network jack. Once the device is authenticated then the user of the device can be authenticated. At this point the user may desire a secure channel for communication.



After entering the wired network, wireless traffic should be segregated so that different policies can be applied. Intranet servers, edge routers and bandwidth managers can be updated to filter on subnet(s) assigned to your WLAN. Even when addresses are hidden behind Network Address Translation (NAT), Virtual LAN (VLAN) tags can be used to avoid broadcasting wireless traffic throughout your Intranet. Leverage existing security. In addition to firewalls and VPNs, the WLAN will be required to fit within your existing security infrastructure. Consider these points in making it all work together:

- Access control lists on intranet servers and routers can block connections from the WLAN--or may need to be extended to allow the WLAN connections.

- DHCP servers can be reused to supply WLAN addresses. Since WLANs aren't inherently trustworthy, reservations can bind IPs to known MAC addresses. This isn't foolproof or highly scalable, so be selective. For example, reserve AP and server addresses.

- Creating a new user list for your WLAN--even a small one--introduces yet another database to maintain. Seek solutions that leverage existing user/device credentials and authentication databases. Make sure your WLAN authentication scheme doesn't put existing authentication credentials at risk.

- Wireless adapters create new avenues of attack. Reuse desktop security measures like personal firewalls, AV scanners and file encryption to harden stations. PDAs may require different software but shouldn't be overlooked.

Integrate wireless networks and devices with existing management infrastructure. Determine if APs, stations and WLAN software should be inventoried, configured and monitored by solutions already in place and if new wireless management tools feed your existing supervisory systems.

Enterprise-grade APs and wireless gateways can often be remotely provisioned by SNMP network managers. Some AP vendors such as Cisco, Proxim and Symbol supply wireless network managers or network management system plug-ins. Third-party wireless policy management systems are starting to emerge (more on these later).

Wireless APs and gateways may generate SNMP traps or send Syslog messages, feeding log servers and analysis tools that already monitor wired networks. But WLANs have their own reporting needs, too. Enterprises may need to audit user activity; hot spot providers must record sessions to feed billing systems and generate revenue.

RADIUS access requests sent by 802.1X, VPNs and SSL portals can help. Devices sold to the ISP market are more likely to generate RADIUS accounting records.

WEP Security

WEP stands **wired equivalent privacy** and it is the implementation of security in 802.11 wireless networks. Besides the mechanism of WEP, recent announcement of a new scheme named **Wi-Fi protected access** (**WPA**) by Wi-Fi alliance, which is intended to enforce the security of WEP, would be another topic of this paper. It is the author's intention to address the mechanism of WPA in more detail, describe its implementation in current network structure, and investigate how much security it provides. 802.11 wireless LAN protocols (also knows as Wi-Fi protocol) have become the most popular protocol for wireless networking. Current implementation of security protocol in 802.11 networks is WEP (wired equivalent privacy). WEP is an optional encryption standard for Wi-Fi network implemented in the **MAC layer** and it is supported by most wireless device venders. If WEP is activated, the Network Interface Card (NIC) encrypts each 802.11 frame before transmission using an **RC4 cipher**. The receiving station, such as an access point performs decryption when the frame arrives.

WEP uses a secret 40 or 64-bit key to encrypt and decrypt datagram. Some wireless device manufacturers also include 128 bit keys (also known as WEP2) in their products. In infrastructure mode, if WEP is activated, the receiving point must use the same key for decryption. This have to be done in the wireless access point (i.e. the wireless network hardware). In Ad Hoc mode, each NIC must be manually configured with the same key. Some vulnerabilities of WEP have been reported such as too short IVs and using of static keys.

The IV of WEP protocol is only 24 bits, therefore if the network traffic is too busy, same IV will be used within hours. If attacker could collect enough number of frames, he/she could determine the shared key by observing packets with same IV. On the other hand, 802.11 does not provide key exchange among stations, therefore the same key is used unless user make change of it. The key may remain unchanged for weeks, months or years. Hackers would have enough time to derive the key been used in the network. The shared key can be used for client authentication. This requires a four step process between

Compromised WEP Encryption

WEP encryption is vulnerable to attack1. Scripting tools exist that can be used to take advantage of weaknesses in the WEP key algorithm to attack a network successfully and discover the WEP key2 Currently the industry and IEEE are working on solutions to this

problem. The Advanced Encryption Standard (AES) is identified as a possible replacement encryption technology for WEP. In addition, revised 802.11 standards (802.11i.and 802.1x) may be adopted which address the security weaknesses of the current standard [Kapp 2002].

Wi-Fi Protected Access (WPA) :

Wi-Fi is the brand given to 802.11 products certified by the Wi-Fi Alliance, a consortium organized to promote 802.11 products and interoperability among them. Wi-Fi Protected Access (WPA) is a security enhancement for current-generation WLAN hardware. WPA incorporates just the stable parts of the 802.11i advanced security standard, which is still a work in progress. WPA products can interoperate with the older WEP products.WPA defines TKIP, which derives keys by mixing a base key with the transmitter's MAC address. An initialization vector is mixed with that key to generate per-packet keys. This stops WEP-crackers from comparing frames encrypted with the same key. WPA also includes a Message Integrity Check (MIC) to prevent data forgery. Enterprises should use WPA with 802.1X for key delivery and refresh. Organizations using WEP should apply certified WPA firmware as soon as upgrades become available. The final 802.11i standard will add AES for more robust security using next-generation hardware, but that will be a forklift rather than firmware upgrade.

IEEE 802.11b

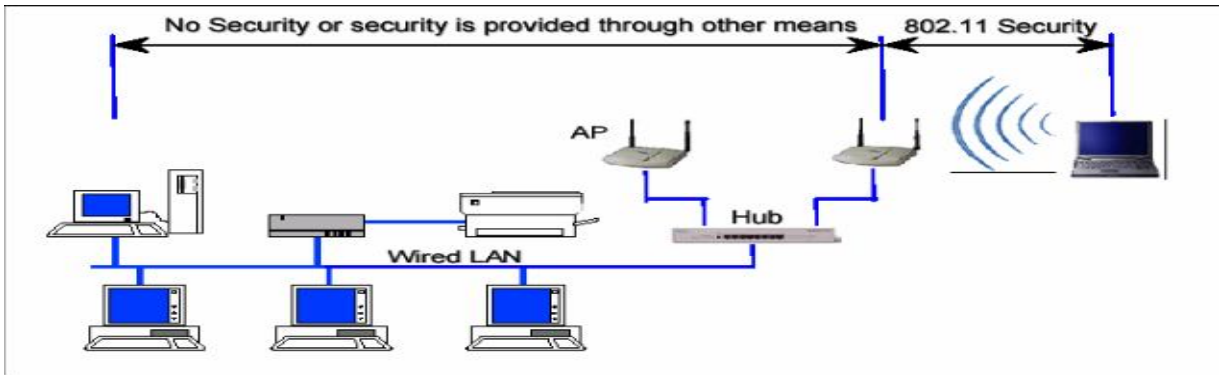
Wireless technologies enable one or more devices to communicate without physical connections – without requiring network cabling. Wireless technology aims to provide users access to information anywhere – it allows mobility. Wireless Local Area Networks (WLAN) are often implemented as an extension to wired LANs within a building and can provide the final few meters of connectivity between a wired network and the mobile user. WLANs are based on the IEEE 802.11 standard. The IEEE designed 802.11 to support medium-range, higher data rate applications, such as Ethernet networks, and to address mobile and portable stations. 802.11 is the original WLAN standard, designed for 1Mbps to 2Mbps wireless transmissions (table 1 shows comparison of 802.11 standards). The 802.11b standard is currently the dominant standard for WLANs, providing sufficient speeds for most of today's applications.

1. Table: Comparison of 802.11 standards

	802.11b	802.11a	802.11g
Frequency	2.4GHz	5GHz	2.4GHz
Speed	11Mbps	54Mbps	54Mbps
Accessibility	Worldwide	US	Worldwide

Security of 802.11 Wireless LANS

The 802.11 standard's security is composed of authentication and encryption. When shared-key authentication is enabled, stations can associate with the AP only if they have a 40- or 128-bit key known to both parties. When Wired Equivalent Privacy (WEP) is enabled, the same key is fed into the RC4 cipher to encrypt data frames. Only stations that possess the shared key can join the WLAN, but the same key decrypts frames transmitted by other stations. If your policy requires authentication of individual stations, or confidentiality beyond the air link, you must adopt other measures. The IEEE 802.11b specification identified to provide a secure operating environment. The security services are provided largely by the WEP (Wired Equivalent Privacy) protocol to protect link-level data during wireless transmission between clients and access points. That is WEP does not provide end-to-end security but only for the wireless portion of the connection. Security for the radio path is depicted in Figure 1.



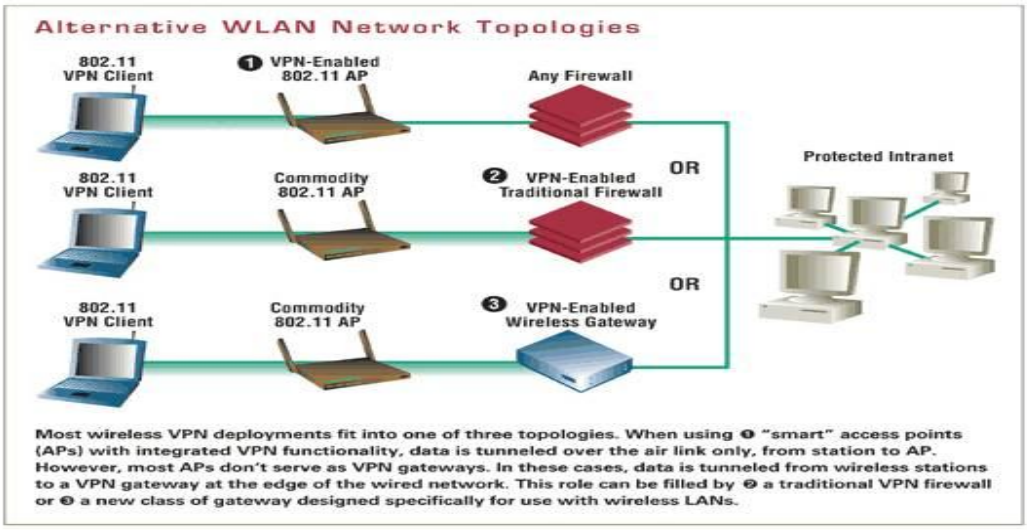
Configuring a hard-to-guess SSID makes neighbors less likely to mistake your WLAN for their own. Stations running Windows XP automatically join any discovered network by default. Enabling shared-key authentication prevents this. Using WEP is like locking your office desk. Motivated intruders can jimmy a low-grade lock. Given enough data, a persistent attacker can use freeware tools to crack WEP. Nevertheless, these can be your first line of defense. Small business and home networks should always use them; enterprises may opt for higher-level measures. The 802.1X standard addresses the need for more robust authentication and the 802.11i standard's Temporal Key Integrity Protocol (TKIP) provides for more robust encryption.

VPNs: VPNs are a great way to secure offsite wireless traffic. Requiring teleworkers to VPN into a company network lets that employer ignore whether or not the worker's home network is secured. Requiring hotspot visitors to VPN into a company network makes even more sense, since employers clearly have no control over the security used in public Wi-Fi hotspots, or lack thereof. And, as I mentioned earlier, mobile VPNs excel at not just encrypting over-the-air wireless traffic, but making network connectivity more usable for devices that roam between coverage areas. On the other hand, using VPNs to secure onsite corporate wireless traffic is now declining. When wireless networks were limited to WEP, VPNs were the only way to reliably encrypt over-the-air traffic. But every Wi-Fi access point shipped in the past four years supports more robust wireless security. VPNs are no longer the easiest or cheapest way to do so.

If your company already has a remote access VPN, consider using it for WLAN security. Reuse makes the most sense when security policy is consistent for WAN and LAN access--the same credentials can be used for authentication; the same encryption algorithms can be used for confidentiality. However, WLANs present their own set of VPN issues: There is more data to encrypt on a high-speed WLAN. Additional gateways may be needed to support wireless encryption, particularly when using 802.11a/g at link speeds up to 54 Mbps.

- Tunnels are bound to IP addresses. WLAN stations roam between APs, changing IP address. Broken tunnels can be reestablished, but service disruption is often noticeable. In smaller WLANs, several APs can share the same DHCP scope. VLANs can help, up to a point. In larger WLANs, wireless gateways can provide tunnel persistence when stations roam.

- Client deployment can be costly and difficult to mandate. Reusing deployed clients is one thing, adding new clients and policies quite another.VPN tunnels, WEP/TKIP and 802.1X address different problems. Consider a business partner using a guest WLAN. A tunnel controls access to the visitor's own network; 802.1X controls access to the guest WLAN. A tunnel prevents eavesdropping from end to end; WEP/TKIP prevents eavesdropping on the air link only.



CONCLUSION:

Wireless LANs can be especially useful in training rooms as these are constantly being re-arranged for different purposes - for training in one session and then for actual work in another. This is not possible if the desks are wired as they then have to be secured to the floor. With wireless LANs this issue does not arise. Institutions which are looking at employees' ownership and use of laptop PCs and personal digital assistants (PDAs) need to find ways to provide access to the internet for employees' own machines. Wireless LANs are an easy way to manage this. There are a number of problems with wireless LANs as well. The three most significant are the security, the rapid evolution of the technical standards and the sharing of bandwidth so that the available bandwidth will be much lower than for wired networks. Wireless Security faces a number of hurdles and efforts are being put on but are relatively new and thus not fully developed. Organizations who deal with sensitive customer related data should take extra precautions when transferring data from one location to another and make sure that such transmissions are secure. Since wireless technology is new in the market but has become almost inexpensive it is gaining popularity in all sorts of businesses.

REFERENCES:

1. Tigueroa, Edgar, Wi-Fi Certified makes it Wi-Fi: An Overview of the Wi-Fi Alliance Approach to Certification,Wi-Fi alliance September 2006 .

2. Hytnen, R. and Garcia, M. 2006. An analysis of wireless security. *J. Comput. Small Coll.* 21, 4 (Apr. 2006), 210-216.

3. Loo, A. 2008. The myths and truths of wireless security. *Commun. ACM* 51, 2 (Feb. 2008), 66-71.

4. Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks, Wi-Fi Alliance ®,, April 29, 2003, 5-7

5. IEEE 802.11i Working Group, WEP2 Enhancements,2001.

6. A. Balanchandran et al., 'Wireless Hotspots: Current Challenges and Future Corrections', 2003

7. N. Borisov et al., '(In)Security of the WEP Algorithm', 2001

8. Wireless Security: An Overview by R.J. Boncella

9. Internet Security Systems. "Wireless LAN Security." 802.11b and Corporate Networks (2001): 1-10.

10. Loo, A. 2008. The myths and truths of wireless security. *Commun. ACM* 51, 2 (Feb. 2008), 66-71.

11. Barnes Ch., Bautts T., Lloyd D., Ouellette E., Posluns J., Zendzian D. M. and O'Farrell N. Hack Proofing your Wireless Network. Syngress Publishing, Inc., 2002

12. Flickenger R. Building Wireless Community Networks. O'Reily, 2002.

13. Basgall M. Experimental Break-Ins Reveal Vulnerability in Internet, UNIX Computer.

14. Guide to Wireless Network Security: John R. Vacca.