An Overview of Security of Wireless Networks

Qazi Ahmad Faraz, Zeeshan Hayat, Waqas Ahmad, Amir Shehzad, Farid ud Din, Iqtidar Shah and Fayyaz Gul
Gandhara University of Sciences, Peshawar, Pakistan

Abstract– **A lots of organizations are adopting wireless technologies at a hasty rate. Utilization of wireless applications vary from extending large commercial services, schools and employees using hand-held devices to organizations rethinking their exploitation strategies for using or extending hard-wired networks. Unfortunately, the leading parts of today's deployments are not sufficiently secured and expose organizations to unnecessary and unexpected menaces that could pilot to a major security failure. In this paper we outlined the basics of a wireless networks, from the beginning to new technologies available for secured wireless networks.**

Keywords– Security, Issues, QoS, Solution and Performance

I. INTRODUCTION

In times gone by, communications between computer systems have been tethered mutually with cables and wires, but that is hurriedly changing. Wireless networks put forwards communication between computer devices around anywhere, unhindered by the physical boundaries of a wired network. WLANs can be used to substitute wired LANs, or as an expansion of a wired infrastructure. It costs outlying less to set up a wireless Local Area Network as compared to arrange a wired network/infrastructure. A foremost expense of inaugurating and amending a wired network is the outlay to sprint network and power cables, each and every one in harmony with confined building codes. Wireless LANs give you more mobility and elasticity by consenting you to keep on linked to the Internet and to that particular network on which you do roaming.

A. IEEE Standard 802.11

The 802.11 standard is a cluster of stipulation/specifications for WLANS formed by the Institute of Electrical and Electronics Engineers Inc. (IEEE). The first WLAN standard was espoused in 1997. The Unique 802.11 standard was brought out in 1999 and make available for data rates/speed up to 2 Mbps at 2.4 GHz, utilizing either DSSS or FHSS [1]. In view of the fact that several task groups have been twisted to craft appendage and augmentations to the inventive 802.11 standard. Wireless Ethernet Compatibility Alliance (WECA) is the diligence organization that endorses 802.11 products that are reckoned to assemble a foundation standard of compatibility/interoperability. The earliest folks/family of products to be licensed by WECA is that all about or based on the unique 802.11b standard and offers data rates/speed up to 11 Mbps at 2.4 Ghz. In addition other standards subsist such as 802.11g and 802.11a [2]. Wired networks send traffic over a dedicated stripe/line that is bodily/physically confidential; WLANs fling or transmit their traffic over public space, airwaves. This commences intrusion from additional traffic and the call for further security. Moreover intrusion from some other wireless Local Area Network devices, the 2.4 GHz is as well used by microwaves and cordless phones. Any WLAN client within the service area of an access point can access data being transmitted to or from the access point. Radio waves are not stopped by obstructions such as walls, ceilings or floors, thus the transmitted data may reach unintended recipients even outside the building where the access point is installed. The wireless signal at present can be detected up to 1500 ft. away, and at even greater distances with specialized equipment [3].

B. Wireless Approaches Types

Within ad-hoc approach/mode, stations are in touch unswervingly with each other. An ad-hoc network is formed on the fly, when mobile devices within propinquity of each other have a need to communicate and no pre-existing network infrastructure is in place next to their location. An ad-hoc has no link to the outside world. In infrastructure mode/approach, the stations communicate only with a central access point. The access point take steps as an Ethernet bridge between the wireless media and wired network the access point is connected to [4].

II. FUNDAMENTAL SECURITY

Fundamental security embraces the use of Service Set Identifiers (SSIDs), open or shared-key authentication, static WEP keys, and optional Media Access Control (MAC) authentication. This mingle offers a straightforward level of access control and privacy, but each element can be compromised. Wireless Equivalent Privacy (WEP), which is the encryption service for data transmitted on the WLAN. WEP offers the capability to encrypt data employing either 40-bit or 128-bit encryption algorithms. A resultant function of WEP is to thwart unauthorized access to a wireless network. The current WEP implementation utilizes a shared-key method, in which a 'password' is created and installed on every wireless device and wireless Access Point.

Data communications are encrypted and decrypted with this key. Attackers cannot by far get hold of this key through packet capturing techniques. The 802.11 standard does not assert how the shared key is established. In practice, nearly all installations use a key that is shared between all stations and access points [5]. The 802.11 standard chains two means of client authentication: open and shared-key authentication. Open system authentication is the default authentication protocol for 802.11. Open system authentication substantiates everybody who asks for authentication. The authentication management frames utilized by this protocol are sent in obvious text even when WEP is enabled. Open authentication engross slight more than supplying the correct Service Set Identifiers (SSID). A Network Name, or SSID, may possibly be assigned to a wireless network, and programmed into every wireless client. This Network Name is first verified when a wireless client endeavors to connect to a wireless Access Point. If the name does not match, connectivity is rejected. Some administration responsibilities are mandatory to program the Network Name into each wireless client upon the initial installation, and every time the Network Name is changed. Since this Network Name is able to be viewed in the client's network properties, and is transmitted over the wireless network in unencrypted form, an attacker can get hold of it with little effort [6].

With shared-key authentication, the access point drives the client device a challenge-text packet that the client has to encrypt with the correct WEP key and revisit to the access point. Exclusive of the correct key, authentication will fall short and the client will not be allowed to associate with the access point. The solitude of transmitted WLAN data is well thought-out sheltered when that data is encrypted with a key that be able to used only by the intended beneficiary/receiver of the data. Encrypting data helps ensure that it remains unaltered all the way through sending-and-receiving transmission process. Media Access Control Layer (MAC) imparts trustworthy data liberation from the physical wireless media to the higher/top layers of the OSI reference model.

By using an illicit access method from the upper layers to the wireless media. A technique used to manage access from the upper layers to the wireless media is called Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA). Improved security is recommended for those consumers requiring enterprise-class security. The Cisco Wireless Security Suite is an enhanced security solution that endows with full support for WPA and its building blocks of 802.1X, which be full of strong, mutual authentication and energetic per-user, per-session encryption keys and TKIP for enhancements to RC4-based encryption such as key hashing (per-packet keying), message integrity check (MIC), initialization vector (IV) changes, and broadcast key rotation.

III. GUIDLINES AND DECEPTION

Whilst establishing wireless network or infrastructure and access points there are a small number of swift steps that can be in use to instantaneously secure the network, Nevertheless it do not craft it secure. Some of these ways include:

- Default SSID ought to be amended: every router or access point arrives/comes with a default SSID. By altering this it can acquire longer for an attacker to identify what type of device he is demanding or trying to hack.
- Default password ought to be amended: generic default passwords are allocated to entrée or access points and routers. Occasionally the password is admin. By altering this password, the attacker cannot change the settings on your router as effortlessly.
- Immobilize distribution/broadcasting SSID: By default AP's transmit their SSIDs, if you shutoff this setting then it is so difficult for outsiders to locate your AP [7].
- MAC must authorize for filtering: WARNING: this can only toil in minor environments where a centralized access or entree list does not require to be sustained. You can facilitate only explicit wireless cards to contact the AP by only permitting those MAC addresses.
- Shares ought to be turnoff: If safety is imperative, scanning for shares and turning off the shares on the network can lend a hand. In addition encrypting sensitive data can thwart hackers from way in to the data.
- Set your wireless entrée or access points in a stiff to locate and attain spot.
- Maintain your drivers on every wireless apparatus or equipments updated. This assists patch obtainable security vulnerabilities.
- Examine current press releases about emerging wireless news

IV. RISING STANDARDS

IEEE has recognized dilemmas with each of the currently available wireless security mechanism. It has been functioning on documents to alleviate the hazards and management overhead allied with each technique, whereas guarantying operability with the mainstream of Wireless clients. These documents are the 802.11x and 802.11e standards. These documents discuss the ability to provide user-level authentication not in favor of popular authentication mechanisms utilized for Remote Access methods. Public-key infrastructure (PKI) is the blend of software, encryption/encoding technologies, and all other services that facilitates enterprises to guard the safety and security of their communications and commerce, business, trade, companies transactions on the Internet.

Digital certificates issued as component of your PKI allow individual users, organizations, and web site operators to confidently validate the identity of each party in an Internet transaction. A digital certificate guarantees that the message or document the certificate sign has not been changed or corrupted in transit online. Digital certificates shelter information from interception during Internet transmission. PKI digital certificates replace easily guessed and habitually lost user IDs and passwords to streamline intranet [8].

Importance of Using WLAN Security is increasing and one must bear in mind that safety and security fortification or guard is dynamic and ongoing—not stagnant and static. Network managers and Wireless Local Area Networks producers or manufacturers have to to stay one step further on of the hacker.

V. CONCLUSION

In this work, we have outlined the basics of a wireless networks, from the beginning to new technologies available for secured wireless networks, and discussed the different issues related to QoS, security, performance and applications.

REFERENCES

[1] The security risks and ways to decrease vulnerabilities in a 802.11b wireless environment. (2012). Retrieved Jan 30 from the World Wide Web: http://www.securitydocs.com/thread/296

[2] WLAN Technologies and Security Mechanisms. (2011). Retrieved Nov 25 from the World Wide Web: http://www.sans.org/rr/papers/68/1301.pdf

[3] [3] Wireless is not the Problem. (2011). Retrieved Feb 20 from the World Wide Web: http://www.sans.org/rr/papers/68/175.pdf

[4] An Overview Of Wireless Security Issues. (2010). Retrieved April 25 from the World Wide Web: http://www.sans.org/rr/papers/68/943.pdf

[5] The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards. (2011). Retrieved March 25 from the World Wide Web: http://www.sans.org/rr/papers/68/1109.pdf

[6] Security to Keep Intruders Out. (2012). Retrieved March 26 from the World Wide Web:http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/a350w_ov.htm#wp1002373

[7] Penetration Testing on 802.11b Networks. (2010). Retrieved May 4 from the World Wide Web: http://rr.sans.org/wireless/test_80211b.php

[8] What is PKI? (2012). Retrieved Feb 01 from the World Wide Web:http://verisign.netscape.com/security/pki/understanding.html