An Analysis Of Wireless Security

Salendra Prasad

Abstract: The WLAN security includes Wired Equivalent Primary (WEP) and WI-FI protected Access (WPA). Today WEP is regarded as very poor security standard. WEP was regarded as very old security standard and has many security issues which users need to be addressed. In this Paper we will discuss Wireless Security and ways to improve on wireless security.

1 INTRODUCTION

In this day and age we as a global community are growing at a super-fast rate. Communication is a vital tool which aids us in breaking the distance barrier. Over the past decades there has been a monopoly in the telecommunications business, but now with the power of the internet, and super-fast data transfer rates people can communicate across the globe and only pay local rates. *Wireless mediums*: are connections that do not use any physical wires/cables, instead it uses radio Frequency, microwave, satellite and infrared to transmit data over the air. Radio frequency (RF) uses radio signals to communicate between wireless devices. The radio frequency standards are known as Bluetooth, Wi-Fi and WiMax. Bluetooth is a short range RF communication that can transmit data in any direction within ten meters. Remote system security basically shields a remote system from unapproved and noxious get to endeavors. Normally, remote system security is conveyed through remote gadgets (more often than not a remote switch/switch) that encodes and secures all remote correspondence as a matter of course. Regardless of the possibility that the remote system security is traded off, the programmer is not ready to see the substance of the movement/bundle in travel. Additionally, remote interruption identification and counteractive action frameworks likewise empower assurance of a remote system by cautioning the remote system executive if there should arise an occurrence of a security rupture. A portion of the normal calculations and measures to guarantee remote system security are Wired Equivalent Policy (WEP) and Wireless Protected Access (WPA). Generally speaking, tried and true way of thinking holds that remote systems are presently sufficiently secure to use in by far most of homes, and numerous organizations. Security highlights like WPA2 can scramble or encode organize activity with the goal that its substance cannot effectively be deciphered by snoopers. In like manner, remote system switches and remote get to focuses (APs) fuse get to control elements, for example, MAC address separating that deny demands from undesirable customers. Clearly every home or business must decide for themselves the level of hazard they are agreeable in taking while executing a remote system. Today WEP is regarded as very poor security standard. WEP was regarded as very old security standard and has many security issues which users need to be addressed. The better a remote system is regulated, the more secure it progresses toward becoming. In any case, the main really secure system is the one never fabricated! [1].

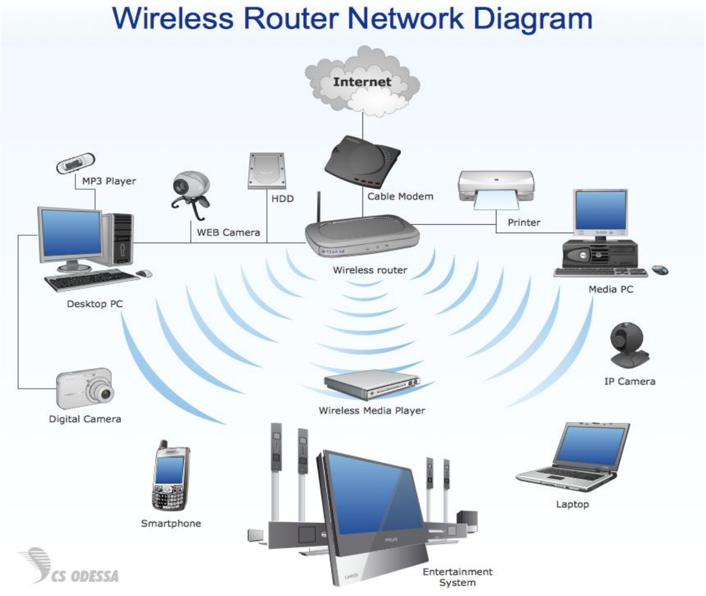
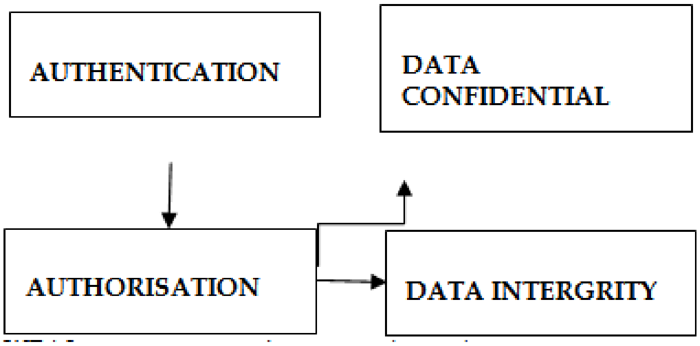


***FIGURE 1**: SHOWS THE WIRELESS CLIENTS.*

How Wireless Security Works

Nowadays we have the comfort of having wireless networks but we tend to ignore the way that they are extremely unsecure. For instance, with a wired system, you must be specifically associated with the system. In any case, with a remote system—where the association is made conceivable by a radio flag—anybody inside the communicate separation may have admittance to the system. For confidentiality trust and Integrity the wireless platform has developed WEP which is wireless equivalent privacy a security protocol developed by IEE. Most people thought WEP wasn't stronger so later WEP 2 developed and then WPA and WPA 2. **802**.1**X** a wireless protocol for large business. [2]



- *Salendra Prasad is a Post Graduate student in Information Technology in University of Fiji.Eemial: salen_prasad@yahoo.com*

WPA2 is more secured compared to other encryptions stated above.it uses counter mode with cipher block chaining message authentication code protocol (CCMP. It has encryption with counter mode. It has capability negotiation that is: (1) confidentiality and integrity: WEP, TKIP, CCMP, and vendor specific. (2) Authentication used is 802.1x, pre-shared key and vendor specific.80211i has five phases of operations. (1) Discovery, (2) Authentication, (3) Key Management (4) Protected Data transfer (5) Connection termination.

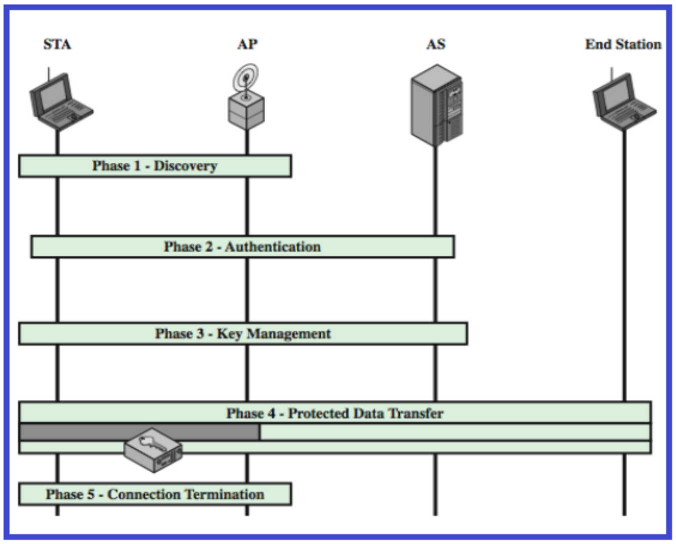
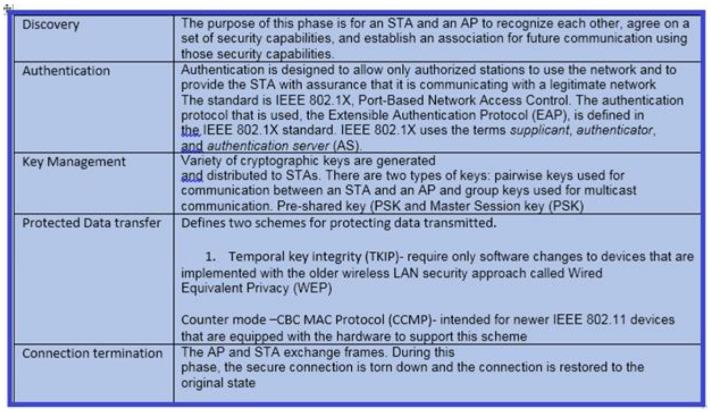


FIGURE 4: *SHOWS FIVE PHASES OF OPERATION OF 802.11 [2]*

THE FIVE PHASES ARE FURTHER EXPLAINED BELOW



Discovery	The purpose of this phase is for an STA and an AP to recognize each other, agree on a set of security capabilities, and establish an association for future communication using those security capabilities.
Authentication	Authentication is designed to allow only authorized stations to use the network and to provide the STA with assurance that it is communicating with a legitimate network The standard is IEEE 802.1X, Port-Based Network Access Control. The authentication protocol that is used, the Extensible Authentication Protocol (EAP), is defined in the IEEE 802.1X standard. IEEE 802.1X uses the terms *supplicant*, *authenticator*, and *authentication server* (AS).
Key Management	Variety of cryptographic keys are generated and distributed to STAs. There are two types of keys: pairwise keys used for communication between an STA and an AP and group keys used for multicast communication. Pre-shared key (PSK and Master Session key (PSK)
Protected Data transfer	Defines two schemes for protecting data transmitted. 1. Temporal key integrity (TKIP)- require only software changes to devices that are implemented with the older wireless LAN security approach called Wired Equivalent Privacy (WEP) Counter mode –CBC MAC Protocol (CCMP)- intended for newer IEEE 802.11 devices that are equipped with the hardware to support this scheme
Connection termination	The AP and STA exchange frames. During this phase, the secure connection is torn down and the connection is restored to the original state

SOME NOVEL SOLUTIONS

Attack on WEP protected network

One of the most common problem with this encryption is that the attacker can easily hunt down the Mac address of the user and perform the attack with this address. The attacker will use passive scanner to list down the addresses of the users connected on web. After the user ends the session the attacker can connect with the same address. The second type of attack on WEP is dictionary attack where the attacker uses cracking utility to check the words in a dictionary with a backup file. The third of attack in WEP is cryptographic attack. The attacker can easily perform this attack when through the WEP key selection is random. The attacker can break the WEP when the client is not attached in seven steps stated below.

SOME NOVEL SOLUTION

Network security need to be increased. Users need to be educated by running PD sessions. Better security standards should be explained. There are different wireless standards used. And users need to when to use which options. WEP standard should not be used since its very week. WPA is better than WEP. It eliminates 802.11 security issues and it is easy to setup. It is bested recommend to use in home networks. WPA2 is more secured compared to WPA. It takes time to setup but it is best option and is recommended to use in corporate environments. The solution for future use of wireless technologies is very challenging for the designers. Today due to competitions among different companies requires sufficient and timely information to be transmitted for productivity and organization growth. These organizations will require the best solutions for their company's secured data not be revealed. They will require better security for their wireless solutions and they may adopt to new routers which should not have old security features which have loop holes. These features need to be eliminated from new router and the designers should design routers with most best security features including WPA2- PSk and AES. While configuring this router users should not be given opportunity to select any other security feature. The router should have **Biometric Login System** which will work together with the biometric App in wireless device. A **Biometric Device** allows fingerprint and retina login systems. So if users want to login in router a Biometric device should be present in the router and so if other users want to connect to wireless connection a biometric app should be downloaded that will allow retina or fingerprint scan to login.

CONCLUSION

Wireless networking provide numerous opportunities to increase productivity and costs. It also alters an organization overall computer security risk profile. Although it is impossible to totally eliminate all risks associated with wireless networking, it is possible and reasonable level security by adopting a systematic approach to assessing and managing risk. My write-up discussed threats and vulnerabilities associated with each of the three basic technology components of wireless networks (clients,access points, and the transmission medium) and described various commonly available counter measures that could be used to mitigate those risks. It also stressed the importance of training wireless security. [6]

References

[1]. B. Mitchell, "lifewire," 2016. [Online]. Available: https://www.lifewire.com/securing-a-wireless-computer-network-816537. [Accessed 20 April 2017].

[2]. ben, "whatismyipaddress," 2015. [Online]. Available: http://whatismyipaddress.com/wireless-security. [Accessed 2 April 2017].

[3]. T. Mangir, "Wireless Security," 2016. [Online]. Available: temangir@csulb.edu. [Accessed 2 April 2017].

[4]. Marco, "Blog," 2015. [Online]. Available: https://blog.marconet.com/blog/5-wireless-security-solutions-to-ease-your-mind. [Accessed 5 April 2017].

[5]. C. Ostlund, "Network Security," 2016. [Online]. Available: https://blog.marconet.com/blog/network-security-measures-protect-before-during-and-after-an-attack. [Accessed 2 April 2017].

[6]. Graham, "Wireless Security," 2006. [Online]. Available: http://rgjournals.com/index.php/ijwwc/article/view/329/154. [Accessed 6 April 2017].