International Journal of Recent Engineering Research and Development (IJRERD)
Volume No. 01 – Issue No. 08, ISSN: 2455-8761
www.ijrerd.com, PP. 35-37

Secured Wireless Communications

DVSS. Subrahmanyam
Dept. of CSE , Swami Vivekananda Institute of Technology (SVIT), Mehaboob College Campus , Secunderabad – 500 003 , Teangana State , India

Abstract: Now-a-days almost all Internet users are converting their wired internet connections to wireless internet connections. These conversions created a huge demand for Wi-Fi devices in the market to access internet. Every year millions of Wi-Fi devices are sold in the market. Wi-Fi devices are associated with different levels of security measures. Most of the wireless devices are vulnerable to various security threats as wireless devices are vulnerable in their default configuration mode. Users are not fully aware of various security measures available on wireless devices that differ from device to device. This drawback has been a boon for various anti-social elements such as terrorists and hackers who attack on these wireless devices without users knowledge. So users should know about all these security threats and they should go for secured wireless communications.

Keywords: Wireless communications, Wi-Fi devices, security threats **,** vulnerability

I. INTRODUCTION

Wireless communications occupied a major role in day-to-day activities of human lives. All wired internet connections have been transforming into wireless internet connections[2]. Various advantages and features of wireless communications are making users to go for wireless internet. This has created a big boom in the market for wireless communication devices which are based on Wi-Fi technology. Wi-Fi stands for Wireless Fidelity. It refers to wireless networking technology that allows computers, laptops and other electronic devices to communicate with each other over a wireless signal environment[2][3]. Many mobile devices , video game systems and other electronic devices have Wi-Fi capability, which has been an in-built feature of these devices, which enables all these devices to connect to the internet without employing any cables. In general, users always look at the advantages and special features they are getting from wireless communications but most of the users are not aware of the security threats on the other side of the coin. Users are purchasing millions of Wi-Fi devices in the market every year. This figure is being increased year by year, as statistical figures are concerned. But unfortunately most of these wireless devices are vulnerable in their default configurations. Users are not aware of various security levels that are to be set up on these Wi-Fi devices[2][1]. One important thing to be noted is that most of the users do not want to pay much attention to these underlined cautions. This drawback has been a boon for anti-social elements such as hawkers , terrorists and other cyber crime criminals. Users should not give any chance to allow these elements into our systems. It is known to everyone that prevention is better than cure. The entire wireless communication security is based on Wi-Fi security features[3][4][2]. So users are always advised to be aware of Wi-Fi security features. Otherwise users will be prone to security threats because of their unawareness of things.

II. Wi-Fi SECURITY MEASURES

Anti-social elements always use unsecured Wi-Fi networks for their anti-social activities. So users should make their Wi-Fi networks more secured. As per the statistics of Government of India, approximately 83% of home users of internet experienced at least one security threat during the year 2014[2]. So users should consider this as a serious problem to our society and nation . Only primary measures are discussed here in this paper which have been fundamental security measures , to avoid major security threats, that all users should follow basically. If users are able to follow these cautions, they will be in a position to avoid nearly 85% - 90% of major security threats[1][3][4] .

II. i . STRONG PASSWORD IS NEEDED

Users should always use strong passwords. A password can be a strong password if it contains a minimum of 15 characters[2][3] . Computer key board provides 26 English alphabets from A,B,C, ---------- Z (both lower case and upper case) , ten decimal numbers from 0 ,1,2,3 ---------- 9 and 32 special characters such as * , # , @, & etc., Users are advised to take at least two or three characters , on an average, from each of the above said groups. It is always advised not to leave any of the groups as said above. Out of 15 character password , take 4 characters from upper case alphabets, 4 characters from lower case alphabets , 4 characters from digits and the remaining 4 characters from special characters[2]. This is only a case for understanding

purpose. Then the following out puts can be observed. Four characters from 26 upper case Alphabets can be selected in C (26 , 4) ways. i.e., in 14,950 ways. Four characters from 26 lower case Alphabets can be selected in C (26 , 4) ways. i.e., in 14,950 ways. Four characters from 10 decimal numbers in C (10 , 4) ways. i.e., in 210 ways. Four characters from 32 special characters in C (32 , 4) ways. i.e., in 35,960 ways. Thus the above said 16 character password can be selected from 14,950 X 14,950 X 210 X 35,960 ways, which is a very big number. If a 20 character password is used, it can easily imagined how much bigger number it is[3][4]. So users are always advised to make utilization of maximum characters given for that purpose. It is very difficult for hackers to crack passwords which are having more characters and utilizing all available choice of characters. Encryption key of lengthy passwords can't be easily broken by hackers.

Suggestions : 1. Choose passwords of length minimum 15 character length , always better to have 20 character password for more security reasons.
2. Frequent change of passwords is also needed, which provides maximum protection from hackers.
3. Hackers can't make any attempts on lengthy and frequently changing passwords[2][3][4].

II.ii . WEP / WPA / WPA2

All these are encryption standards. WEP stands for wired equivalent privacy and WPA / WPA2 stand for Wi-Fi protected access[2][3][4]. Almost all wireless access points follow these encryption standards. Wi-Fi security algorithms have undergone many modifications and upgrades which led to new algorithms. The most widely used Wi-Fi security algorithm in the world is WEP. It appears on all router control panels. But it has many drawbacks. As it is having many flaws and weaknesses it is officially retired from this domain. But many router control panels are still using WEP. It is advisable not to use WEP. It attracts hackers ' eye very easily. It is vulnerable to security threats. More security attacks are possible with WEP. So it is strictly advised not to use WEP. To overcome all deficiencies of WEP, Wi-Fi protected access (WPA) is introduced. At the beginning stage it shown good performance . It introduced new concepts such as pre-shared key (PSK), Temporal Key Integrity Protocol (TKIP). But it attracted more intrusions[2]. These are not direct attacks but attacks on supplementary systems. But ultimately it gave chance to security attacks comparatively very few than WEP. To overcome the deficiencies raised by WPA, another encryption standard is introduced called WPA2[2]. This encryption supersedes all of its previous encryption standards. It provides maximum protection to security threats. It is widely used encryption now-a-days for protection from security threats. So it is advisable not to use WEP but to use WPA2. It has become a common standard for IEEE standard 802.11i[2].

III.iii . ISOLATE WIRELESS NETWORK FROM WIRED NETWORK

A little bit care is needed for wired networks. They are not to be connected to the access point directly. If it is connected, there is a chance of wireless client to enter into wired network. So it is always advisable not to connect access point directly to wired network[2][3]. Some cautions are to be considered between wired network and access points. A firewall and an anti-virus are to be installed between these two ends. If these are not installed, hackers can easily enter into wired network to attack data and other important information. So it is always safe to isolate the wireless network from wired network with a firewall and anti-virus gateway. Pay more attention on connecting points such as access points. Thus it restricts access to all other . This is an important thing that is to be considered in case of wired networks[3][4].

III. iv . ALLOW ACCESS ON THE BASIS OF MAC ADDRESS

It is always suggested to restrict access to only authorized users but not to all. If any user wants to connect to the access point that user should be authorized on the basis of Media Access Control (MAC) address, which is available on the back side of the modem. If it is done , then access to point is restricted to only authorized users which has always been a safe mode for all users[2][3][4]. Thus accesses can be regarded as MAC-based accesses. It is always safe to make it mandatory. This is known as MAC address filtering. At this stage almost all unwanted or unauthorized users are automatically filtered. It prevents the access point from most of the users who enter into the access pint without any authorization[2][4].

III. v . DON'T KEEP ACCESS POINT ALWAYS OPEN

Whenever computers are not in use, it is advisable to shutdown the systems. If systems are always kept open even though they are not in use, then hackers always try to enter into the system by breaking the password. They will make their own efforts to break the existing password. That is why access points are not to open every time when they are not in use. Shutdown the system is a good practice in all aspects[2][4]. Access points have default names and passwords. Unfortunately most of the users do not change default names and passwords of their access points. It is needed to change the default names of the access points. Because

default names are known to all other users on the network as these names are provided by manufacturers. It can be very easy for hackers to crack the system. It is also an important thing to be taken care of[2][3][1].

III. vi . SSID INFORMATION

SSID stands for Service Set Identifier. It is used to identify an access point on the network. Users can connect to the access point through this SSID. This information should not be made public in order to allow authorized users only[2][3]. This information not to be open. SSID is linked with name of the network. So name of the network not to be broadcasted. Any wireless user can connect to the access point if the name of the network is known. SSID information not to be leaked for all these security reasons.

Firmware is to support access points. A strong and up-dated firmware is needed from time to time to support access points [3]. Always use up-dated firmware for access points otherwise it opens loop holes of security which attracts wireless users to enter into the system very easily. So up-dated firmware is to be maintained every time. It is designed mainly for business organizations but not for home users so it is strictly advised not to public SSID information to all [3][4].

III. vii . PROTECTION FROM SNIFFERS

Sniffer is a software program that is used to find loop holes, bottlenecks and problems in the network. Its main function is only to detect flaws vulnerabilities in the network. This problem mainly occurs when a wireless network user sends information to a wired network user. In this case wired network receiver finds it difficult to receive the information properly[2]. These are all the places where sniffers use to theft information from users. In order to protect information from sniffers it is advisable to use Virtual Private Network(VPN), which is used to construct a network by using public wires usually internet, or Internet Protocol Security (IPSEC), which provides a set of protocols for internet security, based communication [2][4].

III. viii . DEACTIVATE DHCP SERVICE

DHCP stands for Dynamic Host Configuration Protocol, which enables a server to provide an IP address to a computer in the network [2][3][4]. Getting an IP address is easy with DHCP protocol over a network. When the number of users accessing a particular access point is minimum then it is always good to disable the DHCP service. Hackers always try to enter into access points which are not busy as they can make any number of attempts to enter into the access point and it is difficult for them to do the same thing at busy points. Internet security protocols are designed to care of all these pre-cautions. Some measures are to be taken on users side too. More care is concentrated on the access point where the system is connected to the network [2].

IV. CONCLUSION

These are all the most common things that all users should know before they are using wireless networks. Now a days every activity of business organizations and day to day life is linked with communications. It is inevitable to depend on communications and especially on wireless communications which can simply called as mobile communications too. Here in this paper basic measures that can be taken by users are discussed in order to avoid major security threats. These are very much needed not only for business organizations but also for home users too. It is known that prevention is always better than cure. Major security threats can be avoided by taking all these simple pre-cautions.

V. REFERENCES

[1]. Chris Anley, The Shell Coder's Handbook, John Wiley & Sons page no. 18 – 65, 2011
[2]. Information Security Education & Awareness , Department of Electronics & Information Technology, Ministry of Communications & Information Technology, Government of India
[3]. Jon Ericson, Hacking The Art of Exploitation, Starch Press , 2 nd edition page no. 98-126 , 2008
[4]. Kevin D Mitrick, The art of Intrusion , Computer Security Books, page no. 86-125 , 2005

VI. ABOUT THE AUTHOR

Dr. D.V.S.S.Subrahmanyam is a Professor at Dept. of Computer Science & Engineering at Swami Vivekananda Institute of Technology (SVIT), Secunderabad. He did his graduation AMIETE, M.Tech and Ph.D in Computer Science & Engineering, Also did M.Sc in Industrial Mathematics and another M.Sc in Mathematics and M.Phil in Mathematics. Areas of interest include Software Engineering, Software Quality Analysis, Cyber Security and Big Data Analysis.