Vol. 4, No. 10 October 2013 ISSN 2079-8407
Journal of Emerging Trends in Computing and Information Sciences

http://www.cisjournal.org

A Practical Approach for Evaluation of Security Methods of Wireless Network

[1] Mohd Izhar, [2] Mohd Shahid, [3] V.R. Singh

[1] HMR Inst. of Tech. & Mgt, GGSIP University, Delhi, Ph.D. Scholar of Mewar University, NH-79, Gangrar, Chittorgarh (Rajasthan) India

[2] Ph.D. Scholar of Mewar University, NH-79, Gangrar, Chittorgarh (Rajasthan) India

[3] Ph.D. recognized Supervisor of Mewar University, NH-79, Gangrar, Chittorgarh (Rajasthan) India

shahidpdmce@gmail.com, [3] vrsingh@teee.org

ABSTRACT

MAC filtering, WEP key encryption, WPA2 and firewalls are the Security Modes used for securing our wireless network. These Security Methods are standardized by IEEE as well as by WECA Alliance. IEEE 802.11-2007 Standard for wireless network classifies security algorithms into: RSNA and Pre-RSNA. Pre-RSNA algorithms are the algorithms used before RSNA. Pre-RSNA security comprises the algorithms; WEP (Wired Equivalent Privacy) and IEEE 802.11 entity authentication. RSNA security comprises the algorithms like TKIP, CCMP, RSNA establishment and termination procedures, including use of IEEE 802. 1X authentication, key management procedures and providing mechanisms for protecting management frames. WECA is a group of software and hardware vendors who is responsible for developing and standardizing equipments related to Wifi networks. Both IEEE and WECA work together for security and efficiency of wireless Network. All Pre-RSNA Methods fail to meet their security goals than RSNA with WPA2 Methods come in the picture, which have its own weakness and Problems. This paper, after reviewing certain papers as referenced, checks the security of wireless network theoretically and practically in order to know how these security methods fail for providing security to wireless Networks. The evaluation is done by creating and developing a Practical Scenario and examining it. The developed scenario has a server with internet facility, the server is connected with various access points at different wings and these access points are accessed, as and when required, by various moving / stationery nodes. The equipments used for this scenario is fully compatible with IEEE and WPA2 standards and methods. Latest web browser capabilities and OS firewall Competence with these advanced modes of RSNA methods has also been taken into account in order to develop secure network model.

Keywords: *RSNA, CSMA/CA, CCMP, MAC and PHY.*

1. INTRODUCTION

In IEEE 802.11-2007, Revision of IEEE Std 802.11-1999 was approved on 08.03.2007 and published on 12 June 2007 by IEEE. This revision gives the IEEE 802.11 standard for wireless local area networks (WLANS) with all the amendments that have been published to date i.e.08.03.2007. The original standard was published in 1999 and reaffirmed in 2003. IEEE 802.11i, an IEEE standard ratified June 24, 2004, is designed to provide enhanced security in the Medium Access Control (MAC) layer for 802.11 networks [3]. The 802.11i specification defines two classes of security algorithms: Robust Security Network Association (RSNA), and Pre-RSNA. Pre-RSNA security consists of Wired Equivalent Privacy (WEP) and 802.11 entity authentication. RSNA provides two data confidentiality protocols, called the Temporal Key Integrity Protocol (TKIP) and the Counter-mode/CBC-MAC Protocol (CCMP), and the RSNA establishment procedure, including 802.1X authentication and key management protocols.

This paper analyzes these Pre-RSNA and RSNA methods in order to migrate from pre-RSNA to RSNA methods and to conclude that how these security modes fail in the real scenario as there are a lot of hackers, ethical hackers and crackers who breach the so called securities in minutes. The ultimate goal is to develop a secure wireless network model with these RSNA methods, web browser capabilities and OS firewall capabilities. Securities modes one by one such as MAC filtering, WEP Key and WPA2 Key encryptions are deployed and breaching of it is shown through our developed practical scenario.

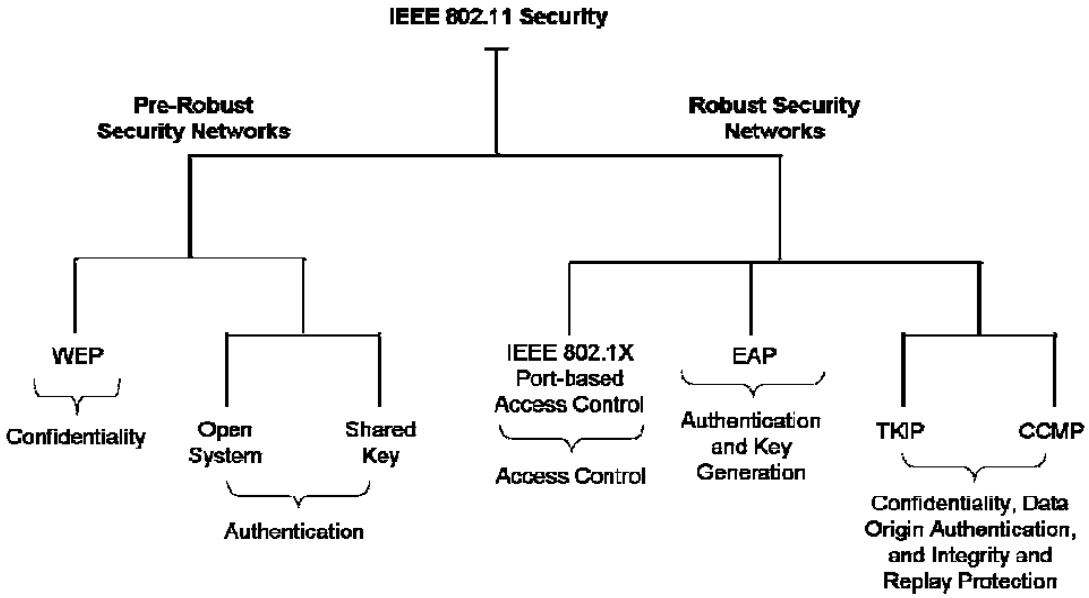

Fig 1 : Broad Classificaiton of Security Protocol

2. BACKGROUND

2.1 Wired equivalent Privacy

WEP-40(40-bit key) is defined as a means of protecting the confidentiality of data exchanged among authorized users of a WLAN from casual eavesdropping. The same algorithms have been widely used with a 104-bit key instead of a 40-bit key; this is called WEP-104. WEP security involves two parts, Authentication and Encryption. Authentication in WEP involves authenticating a device when it first joins the LAN. The authentication process in the wireless networks using WEP is to prevent devices/stations joining the network unless they know the WEP key [4].

Many Papers have been published relating to security methods of Pre-RSNA discussing the Wireless LAN 802.11 network security including the comparisons of SSIDs, MAC address filtering and the WEP key encryption. Various simulative platforms of software and hardware is designed to crack WEP key based on these authentication methods and analyzing the weaknesses of WEP and RC4, It has been shown that WEP Key can be cracked including SSID enumeration, MAC address spoofing and WEP key cracking by FMS(Fluhrer, Mantin, Shamir) Attack[5].

2.2 Temporal Key Integrity Protocol

Wired Equivalent Privacy (WEP) was developed in order to secure wireless networks and provide security equivalent to the one that could be expected from a wired network. When WEP failed miserably to deliver the required security, the Temporal Key Integrity Protocol (TKIP) was built around WEP to fix its flaws and provide backwards compatibility with older equipment. Much resources and money were invested into upgrading old WEP networks to TKIP[7]. The TKIP is a cipher suite enhancing the WEP protocol on pre-RSNA hardware. TKIP modifies WEP.

2.3 Counter Mode with Cipher Block Chaining (CBC) Message Authentication Code(MAC) Protocol (CCMP)

Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) is an encryption protocol that forms part of the 802.11i standard for wireless local area networks (WLANs), particularly those using WiMax technology. CCMP was the second security protocol introduced as a replacement for WEP in the 802.11i amendment CCMP made from scratch using the modern AES block cipher. CCMP is based on the CCM of the AES encryption algorithm. CCM combines CTR for confidentiality and CBC-MAC for authentication and integrity. CCM protects the integrity of both the MPDU Data field and selected portions of the IEEE 802.11 MPDU header.

2.4 Review

Various attacks have been shown at WEP. When WEP failed to deliver the Security, the Temporal Key Integrity Protocol (TKIP) was built around WEP to fix its flaws and provide backwards compatibility with older equipment. On November 8, 2008, German researchers released a paper demonstrating a practical attack against the Temporal Key Integrity Protocol (TKIP) encryption algorithm used to secure Wi-Fi networks that are certified for Wi-Fi Protected Access (WPA). Motoral inc 2008 analyzed and recommends that enterprises must use AES-CCMP encryption with their WPA or WPA2 deployments. Motorola WLAN infrastructure is fully certified for AES-CCMP. [16] Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) is an encryption protocol that forms part of the 802.11i standard for wireless local area networks (WLANs), particularly those using WiMax technology.

Various Papers has been published for analyzing CCMP.

3. TOOSL, SERVICES AND METHODS

3.1 Practical Scenario

A Practical Scenario, as shown in the following figure, has been developed in order to configure the devices as per the IEEE and WPA2 Modes and in order to check the security threats. Figure shows that ISP provides the internet facility which is at the server, the server acts as a default gateway and is connected with different access points through switches. Different wireless nodes are then connected at these access points.

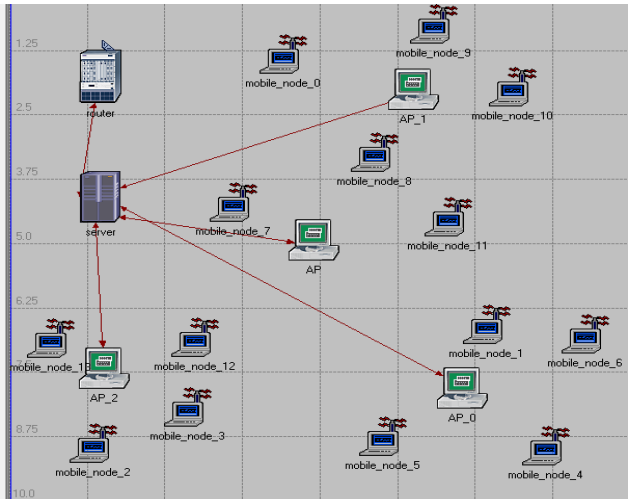

Fig 2: Typical WLAN Scenario

3.2 MAC Filtering and for MAC Spoofing

MAC filtering allows only some MAC address to be part of wireless network but there are various ways by which one can easily change the MAC address as desired. Typically following 3 ways are common:

a. One can change the MAC address through device manager of the System.
b. One can also change the MAC address through editing the Registry of the System.
c. The MAC address can be changed through the MAC address Changer such as TMAC and SMAC software.

There are several scanning tools by which one can come to know the physical address of any node in the network. These IP Scanners are free, fast and easy-to-use network scannera. IP Scanner is able to locate all the computers on wired or wireless local network and conduct a scan of their ports. It can detect all the IP addresses on any Wi-Fi network. Even advanced IP Scanner, can wake up and shut down remote groups of Windows machines. The list is as follows: Advanced IP Scanner 2.2.224, Colasoft MAC Scanner Pro 2.2, Angry IP Scanner 2.x, IPScan-II. The tool which has been used for scanning the network is free open source Angry IP scanner.

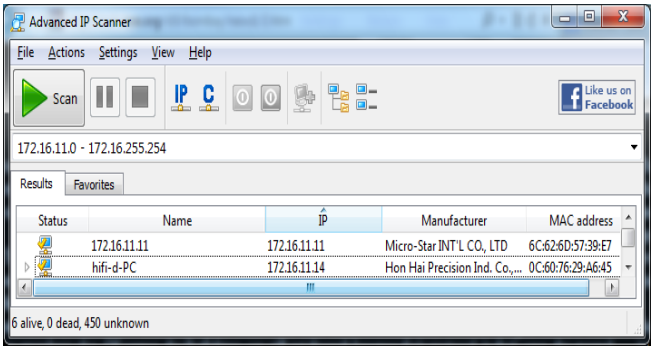

Fig 3: Scanning Result of Angry IP Scanner

SMAC is a powerful MAC Address Spoofer for Windows 7, VISTA, 2008, 2003, XP, 2000 systems. SMAC is developed by Certified Professionals (CISSP, CISA, CIPP, and MCSE SMAC capabilities are: 1. Automatically Activate new MAC Address right after changing it. 2. Show the manufacturer of the MAC Address. 3. Randomly generate any New MAC Address or based on a selected manufacturer. 4. Pre-load MAC Addresses List and choose the new MAC address from the list.

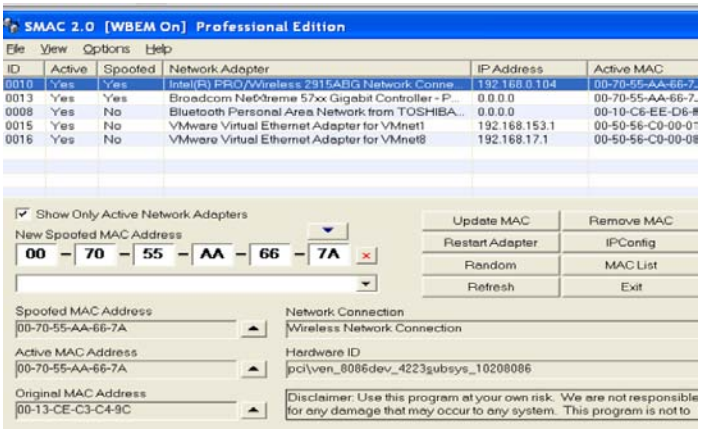

Fig 4: SMAC Address Changer

Technetium MAC Address Changer or TMAC can change (spoof) Media Access Control (MAC) Address of Network Interface Card (NIC) or Wireless Network Card (Wi-Fi), irrespective of the NIC's drivers or its manufacturer [10]. It has many new features which can to change IP Address, Gateway, DNS Servers, IPv6 support, enable/disable DHCP in one click, network configuration presets and also many other features.

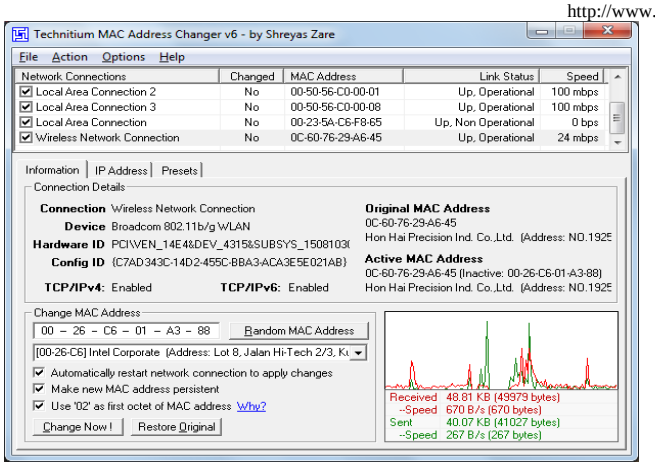

Fig 5: TMAC Address Changer

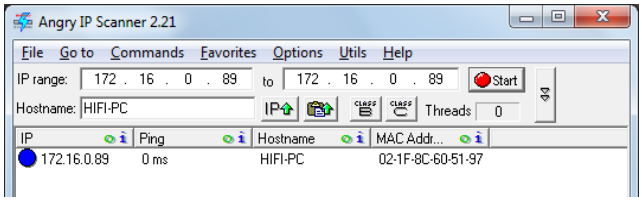

Fig 6: Spoofed MAC Address at WLAN

3.3 Cryptography Services

Cryptography has several applications in network security. Cryptography can provide five services. Four of these are related to the message exchange. The fifth is related to the entity trying to access a system for using its resources. IEEE Std 802.11 provides the ability to protect the contents of messages. This functionality is provided by the data confidentiality service. IEEE Std 802.11 provides three cryptographic algorithms to protect data traffic: WEP, TKIP, and CCMP. That means one can use the devices conforming this IEEE standard or WPA2 devices for security evaluation purpose.

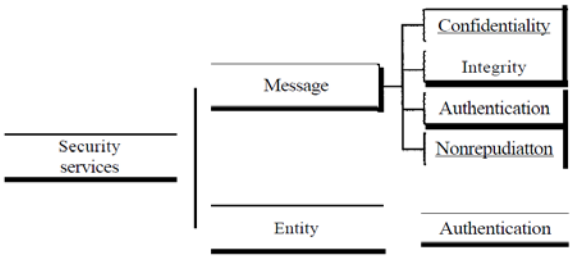

Fig 7: Cryptography Services

3.4 Security Services

Cisco, net gear devices are available for such conformity one can create scenario and can check the security practically as per requirement. Besides the security methods may include the simulation through simulator such as NS2, Matlab, Qualnet and/or Opnet for evaluation purpose. Cracking WEP and its Protection.

3.5 WEP Key and its Cracking

Various papers have been published showing how to crack WEP, and a practical is also done for cracking the wep. This is very simple procedure and one need only a Bootable DVD of Backtrack which contains various utilities used for cracking, Wireless card and the WEP network which needs to be active that means other users are connected already and doing things on the network. Some methods of attack need not the active WEP Network [36].

Step by step procedure is:
Boot from the Backtrack DVD as shown in the fig,

In command mode type startx to load graphical interface. Type iwconfig to list the entire network interface.

The Command airmon-ng start wlan0 is used to device to keep on monitor mode.

The command airodump-ng mon0 provides information about wireless network and its client.

Now type the command airodump-ng -c <channel> -w <output filename> - -bssid <bssid including :'s> mon0.

This command is used for recording the data in a file. One need around 10,000 – 30,000 packets of date to crack the password.

Now open a new terminal type the command aireplay-ng --arpreplay -b <bssid> -h <client STATION address> mon0, it will increase the nos. of packets and stop it at about 5000 packets.

Open a 3rd terminal window to crack the packets, type aircrack-ng -z -b <bssid> <output filename from earlier>*.cap and within some minutes and around some 5000 to 30000 packets it will show the message the key found in hexadecimal form.

Long password is used to protect the network and it reduces the chance of a brute-force attack. One can check up his/her security and can try to break password with your own Nodes. Aircrack is the most popular tool for this purpose which is used to attack WEP and WPA encryption.

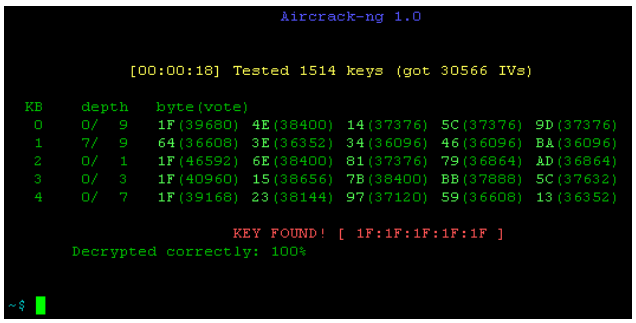

Fig 8: Showing WEP Crack Key Found

3.6 WPA2 Weakness

WPA encryption is understood stronger than wep and it was designed specifically to replace wep. WPA uses TKIP for security, which stands for Temporal Key Integrity Protocol. In the TKIP mode, the encryption keys are changed at set intervals. That means it takes long time to intercept the keys by the hackers as these are dynamic and if somebody able to find the key, these keys might get changed, and becomes useless for the hackers. WPA2 can also be used for wireless encryption and is known as 802.11i standard/AES. WPA2 can be implemented in two versions Personal and Enterprise. WPA2 Personal protects unauthorized network access by utilizing a set-up password. WPA2 Enterprise verifies network users through a server. The Problem by using WPA2 is that the entire device on network must use WPA2 or compatible. If any of the device on the network that only supports WPA, this device will not be able to join the network unless router supports WPA/WPA2 mixed mode. Also WPA2 and advanced encryption such as CCMP-AES is understood secure way for home and small offices but the problem is that many AP still in use are good enough for security purposes but they are lacking Wireless-N or other advanced encryption of WPA2.

4. RESULTS AND DISCUSSIONS

Wireless LAN deployments should be made as secure as possible. Standard 802.11 securities are weak and vulnerable to numerous network attacks. CERT-In Monthly Security Bulletin- February 2012 reports that 95 security incidents were reported to CERT-In from various National/ International agencies. As shown in the figure 7, 44% incidents related to Phishing were reported in this month. Other reported incidents include 22 % Virus/Malicious Code ,03 % unauthorized scanning , 31 % incidents related to technical help under the others category. 2460 Indian websites were defaced during February 2012[24].

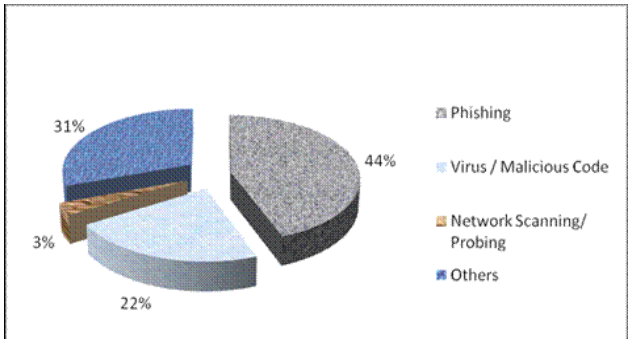

Fig 9: Security Threats shown by CERT-In

CERT-In Website Intrusion and Malware Propagation: is tracking malicious URLs on regular basis. In the month, February 2012, CERT-In tracked 475 websites infected with malicious contents. A user visiting these URLs is redirected to malicious sites which downloading malicious code such as virus, worm, Trojan. Keylogger, rootkit on to the user's computer[24].

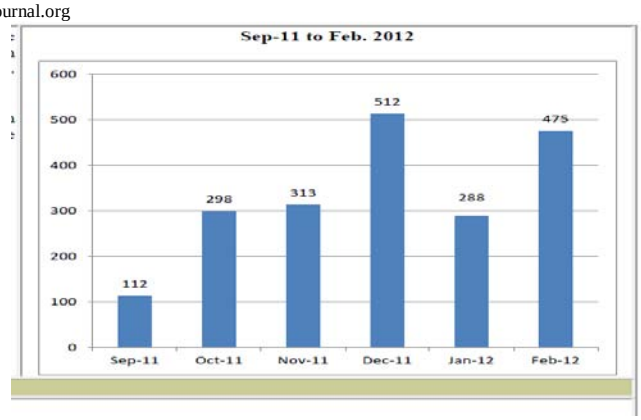

Fig 10: CERT-In shows WIMP attack Tracking Sep-11 to Feb-12

The Phishing attack can be minimized by using the latest browser capabilities such as SmartScreen Filter. Microsoft SmartScreen Filter is a feature in Windows Internet Explorer that helps in detecting the phishing and Malware websites. Such websites fraudulently got to reveal personal and financial information from the users. SmartScreen Filter runs in the background and as per the users' consent sends the web addresses of the sites that a user visits to the Microsoft SmartScreen service in order to get in checked as lists of known phishing and malware sites. If SmartScreen Filter discovers that a website visited is on the list of known malware or phishing sites, Internet Explorer displays a blocking webpage and the Address bar appears in red. Malware websites distribute software that can attack the computer. Information that is submitted to the SmartScreen web service is transmitted in encrypted format over HTTPS and can not be used for any advertising purpose.

Internet Explorer 9 allows to use ActiveX Filtering to block ActiveX controls, the 3rd party software which are not trustworthy one and are used for web rich experiences such as audio video players plug in. IE9 can block all these activex control and is turned them back on for only the sites which are trustworthy. InPrivate filtering prevents websites from collecting information of a user who uses the browser as InPrivate filtering , cookies and temporary internet files are kept in memory and cleared as the browser is closed. Even temporary information is encrypted and stored to show web pages correctly. It is secured to an extent but it can not prevent hackers from seeing and recording which websites you visited.

When someone visits a website, some content are provided by a different website. That content could be used to gather information. Tracking Protection list is a new feature introduced in web browser Internet Explorer 9. It prevents the websites for collecting information. Users can create their own custom lists or install lists directly from an official Microsoft website to allow to get information by these websites. One can turn off Tracking Protection or ActiveX Filtering to show content on specific websites that is trusted one. A firewall is like a

gatekeeper that checks information coming from outside and decide to block or allows it. Firewall is a software or hardware that checks information coming from the Internet or a network. Windows Firewall with Advanced Security is a Microsoft Management Console (MMC) snap-in that provides more advanced options for IT professionals. With this firewall, one can set up and view detailed inbound and outbound rules and integrate with Internet Protocol security.

Windows Defender is antispyware software that's included with Windows and runs automatically when it's turned on. It can help protect the computer against spyware and other potentially unwanted software. Spyware is installed on computer without knowledge at any time one connect to the Internet, and it infects the computer when one install some programs using a CD, DVD, or other removable media. Spyware is mostly programmed to run at later point of times, not just when it's installed. Windows Defender has two ways to keep secure from spyware from infecting the computer:

Real-time protection: Windows Defender alerts, when spyware attempts to install itself or to run on computer. It also alerts when programs attempt to change important Windows settings.

Scanning options: Windows Defender can also be used to scan for spyware that might be installed on the computer, to schedule scans on a regular basis, and to automatically remove anything that's detected during a scan.

5. CONCLUSION

MAC address filtering is not a good solution for wireless Network security as Mac address, besides other disadvantages of MAC address filtering, can easily be spoofed as above shown. WEP key is also not advisable as it is cracked within minutes. WPA2 key encryption is understood best, however, sometimes organizations having advanced 802.11n and AES securities but the systems being used are loaded with windows XP or Vista and WPA2 does not qualify as strong security. That means the organization must use latest software and hardware for network securities and also APs with a built-in firewall.

On the other hand, some security features used at the connecting nodes can solve the problem of misuse such as windows Firewall, Windows Defender, Smart Screen Filter, InPrivate filtering and activex Control. Others protection measures are windows update as patches are provided time to time by Microsoft and are used to fix the bugs, antivirus and/or antispyware programs for protections from spyware and malicious software/malware. One must have password protected administrator account, Sometimes working with limited user accounts helps in securing the System, window 7 requires the confirmation from the administrator while program attempt to make changes to the system.

To conclude it is possible to break WPA2 but it will take a long time to break into such WPA2 enabled network. However there are software available freely for mapping and cracking networks and also hackers/ethical hackers keep them busy for breaking the security. Even then WPA2 security is understood best compared to other security mode to an extent. Use of Hardware security modules can be a complete solution for wireless network securities but they are costly to its users. Filtering through OS and web browser built in securities can stop security threat to an extent.

6. ACKNOWLEDGMENT

Our sincerely thanks to the management of HMR Institute of Technology and management, GGSIP University, Hamidpur, Delhi, PDM College of Engineering, M.D. University, 3A, Sarai Aurangabad, Bahadurgarh Haryana and Mewar University, NH-79, Gangrar, Chittorgarh Rajasthan who supported the most in preparing this document.

REFERENCES

[1] IEEE Std 802.11-2007, Revision of IEEE Std 802.11-1999,IEEE 3 Park Avenue New York, NY 10016-5997, USA 12 June 2007.

[2] IEEE Std. 2009 Revision of IEEE Std 802.11-2007, 30 sept. 2009.

[3] Changhua He & John C Mitchell “Security Analysis and Improvements for IEEE 802.11i”, Network and Distributed System Security Symposium, San Diego, California, 3-4 February 2005.

[4] Shivaputrappa Vibhuti, “IEEE 802.11 WEP (Wired Equivalent Privacy) Concepts and Vulnerability”, San Jose State University, CA, USA, CS265 Spring 2005 (26.03.2005)

[5] NETGEAR, Inc. “Wireless Networking Basics”, October 2005.

[6] Lu Zhengqiu; Tian Si; Wang Ming; Ye Peisong; Chen Qingzhang; “Security analysis and recommendations for Wireless LAN 802.11b network”, Consumer Electronics, Communications and Networks (CECNet), 2011 International Conference on 16-18 April 2011.

[7] Finn Michael Halvorsen & Olav Haugen “Cryptanalysis of IEEE 802.11i TKIP”, Norwegian University of Science and Technology, June 2009.

[8] IEEE Std 802.11i-2004, Amendment to IEEE Std 802.11, 1999 Edition (Reaff 2003) as amended by IEEE Stds 802.11a-1999, 802.11b™-1999,802.11b™-1999/Cor 1-2001, 802.11d-2001, 802.11g-2003, and 802.11h-2003] Amendment 6: Medium Access Control (MAC) Security Enhancements, 23 July 2004.

[9] Back and Tews "Practical attacks against WEP and WPA", November 8, 2008.

[10] Paul Arana, "Benefits and Vulnerabilities of Wi-Fi Protected Access 2 (WPA2)", INFS 612 – Fall 2006

[11] Behrouz A. Forouzan "Data Communications and Networking", McGraw-Hill Forouzan Networking Series, Fourth Edition Copyright © 2007.

[12] NIST Special Publication 800-97, "Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i", February 2007.

[13] Diaa Salama Abd Elminaam1, Hatem Mohamed Abdual Kader, and Mohiy Mohamed Hadhoud, "Evaluating The Performance of Symmetric Encryption Algorithms", International Journal of Network Security, Vol.10, No.3, PP.213-219, May 2010

[14] A.K.M. Nazmus Sakib et al"Security Improvement of WPA 2 (Wi-Fi Protected Access 2)" (International Journal of Engineering Science and Technology), Vol. 3 No. 1 Jan 2011

[15] Vijay Chandramouli, "A Detailed Study on Wireless LAN Technologies", 23.10.2002

[16] "Understanding the New WPA TKIP Attack Vulnerabilities & Motorola WLAN Countermeasures", Motorola, Inc. 2008.

[17] Dajiang He, Charles. Q. Shen. "Simulation study of IEEE 802.11e EDCF" 2003

[18] ISMAHANSI BINTI ISMAIL, "Study of Enhanced DCF(EDCF) in Multimedia Application", 2005

[19] Preeti Venkateswaran, "Experiments to Develop Configurable Protocols", 2005

[20] Mark Greis, Tutorial for the Network Simulator "ns" 2008

[21] Lecture notes 2003-2004 University de Los Andes, Merida, Venezula and ESSI Sophia-Antipols, France.

[22] Guillermo Alonso Pequeño Javier Rocha Rivera, "Extension to MAC 802.11 for performance improvement in MANET", 2007

[23] Sam De Silva, Using TCP "Effectively in Mobile Ad-hoc Wireless Networks with Rate Adaptation", 2007

[24] CERT-In Monthly Security Bulletin- February 2012, website: http://www.cert-in.org.in

[25] George Ou, "Wireless LAN security guide", Jan 3, 2005.

[26] Website : http://www.technitium.com, Aug 2012

[27] Website : http://www.klcconsulting.net/smac, Aug 12.

[28] Website: http://www.softpedia.com/ get/ Network-Tools/ IP-Tools/ IPScan-II.shtml

[29] Website : http://ip-scan.qarchive.org, May 2012

[30] Website : www.radmin.com/products/ipscanner, May 12

[31] Website : http://www.angryip.org/w/Home, May 2012

[32] Website : http://www.opnet.com/itguru-academic

[33] Website : http://www.wikipedia.org. Aug 2012.

[35] Website : http://www.aircrack-ng.org. Aug 2012

[36] Website : http://www.makeuseof.com, Aug 2012

[37] Website : http://Microsoft.com/india, Aug 2012