A Tailored Approach to Enhance Wireless LAN Security

Ankur Kumar Shrivastava, Ishan Ranjan, Abhinav Kumar, Anant Kumar Rai, Ramander Singh, Archit Rastogi, Nitisha Payal, Amod Tiwari

Abstract: ***In the current business scenario world most organizations are moving from wire-connected networks to wireless networks. Thus there is a large growing market for Wireless LANS globally but there are various black holes, which is associated with such types of networks. This paper will provide an overview of the major risk threats and vulnerabilities in WLAN systems and finally we will present a holistic approach of securing Wireless Network.***

Keywords: - IEEE 802.11, SSID (Service Set Identifier), WEP (Wired Equivalent Privacy), Wi-Fi (Wireless Fidelity), WPA (Wi-Fi Protected Access).

I. INTRODUCTION

We can classify network into two broad parts: -

- Wired Network (LAN)
- Wireless Network

In the wired network connections, assume it as a jack in which we plug our network cable for network connection and hence a wired connection is established. The jacks in wired network connections are almost similar to the phone jacks; they can differentiate based on the size of the jacks and the color of network jacks is yellow and orange. Wired network is popular for the quick and easy access for worldwide network (1).

Wireless networks are the most challenging and growing part of information technology. Due to wireless networks flexibility, businesses, educational institutions establishments and households are increasingly adapting this technology, which makes wireless network an integral part of today life. The dissimilarity between wireless and wired networks is the way they transmit information and connect to network. As per the security threats, the main dissimilarity between wired and wireless networks is how hard to acquire access to the data when transmitted.

In the wired networks, this is only possible by tapping the media cable that is used for the network communication. In wireless networks, air is used as a media for communication. The information/ data transmitted via the radio frequency can be tapped or accessed by low cost easy to use gadget that is readily available in the market.The network is the spinal cord of any organization. Nearly all establishments use wired network as a central network for their communication. But as technology enhanced, the wireless LAN comes into existence. Dissimilarity among wireless LANs and wired is the process in which they send and receive the data packet. For the organizations, it is very much important that how their users can retrieve the information residing in the data packet. The innovation of new technologies always comes with a byproduct, which is the abuse for the technology. Thus the secure usages of Wi-Fi of networks have become a wide area of study.

In wired network, if any intruder wants to access the data illegally, he needs to tap the media cable off the wired network. On the other side, in case of wireless networks, the medium used for transmit the data is air. There are various types of equipment’s that are easily available in the open market at a chipper price, which will help the intruders to easily get access to the confidential data. For example, in any organization if users are transmitting some confidential information using a wireless LAN, an intruder can easily captured and shared the confidential information with equipment available in the market.

After identifying the major weaknesses of first generation Wireless-LAN security, organizations are confused regarding implementation of wireless network for their communication. But on the other hand, after discovering the weaknesses of Wireless networks, standard bodies like IFTF, IEEE, and Wi-Fi Alliance are start developing the next generation of wireless LAN security solution.

II. RELATED WORK

A. Classification of wireless network: -

- Wi-Fi is the corporate term for the wireless LAN (WLAN) communication technology refers to IEEE 802.11 family of wireless networking standards. The term Wi-Fi is synonymous with 802.11b, as it is the first standard in the family to enjoy worldwide popularity.

Revised Manuscript Received on 30 August 2012
*****Correspondence Author(s)

Ankur Kumar Shrivastava*, CMJ University, Shillong, Meghalaya,India **Ishan Ranjan**, Department of Computer Science MIET, Meerut, India
Abhinav Kumar, Mahindra SSG, Mumbai, India
Anant Kumar Rai, NII Consulting, Mumbai, India
Ramander Singh, Department of Information Technology MIET, Meerut, India
Archit Rastogi, Department of Computer Science MIT, Meerut, India
Nitisha Payal, Department of Computer Science MIET, Meerut, India
Amod Tiwari, Department of Computer Science, PSIT, Kanpur, India

In now days, however, Wi-Fi can refer to any of the known standards: 802.11a, 802.11b, 802.11g and 802.11n. (2)

□ The Wi-Fi Alliance (see sidebar) certifies the vendor products to ensure 802.11 products detailed 802.11 specifications should be followed on the market. Sadly, 802.11a technology is not at all compatible with 802.11b/g/n, that's why Wi-Fi product lines have been somewhat fragmented (3).

B. How wireless work?

□ *SSID:* Using SSID in association with an AP, network access control can be implemented by the administrator. The SSID partitioned a wireless network into several networks serviced by APs. Each AP is mapped with an SSID corresponding to a wireless network. To access this network and data over network, client terminals must be configured with the correct SSID. A building might be segmented into multiple numbers of networks by the number of floors and departments. So, for users who want to access network from a multiple locations, a client terminal must be configured with multiple SSIDs.

➢ *MAC address filtering:* Each client computer can be identified using a unique MAC address of its 802.11 Network Interface Card, while each AP can be identified by an SSID. To expand the security of an 802.11 wireless network, every available AP must be programmed with a list of MAC addresses associated with the various client computers allowed to access the AP. That is, a client is not allowable to ally with APs, if client's MAC address of NIC is not available in the list. Enhanced security is offered by MAC address filtering along with SSIDs. However, it is optimum suitable to small-scale business networks in which the MAC address catalogue can be efficiently managed manually or by an automated system. Each AP must be programmed manually with a list of MAC addresses, and the list must be kept up-to-date for secure access.

➢ *WEP:* Each client and AP on a wireless LAN uses symmetric key cryptography i.e. the single key to encrypt and decrypt data under WEP. The key use for encryption and decryption process resides in the client computer and in each AP over the network. The 802.11 Wi-Fi standard does not specify any key management protocol, so all WEP keys over a network can be managed manually. Support for wired equivalent Privacy is almost standard on most current available 802.11 cards and AP.

➢ *WPA & WPA2:* WPA and WPA2 are standards based security certification from the Wi- Fi Alliance for organizations, enterprises, SMB's, and small office/home office wireless networks that provides mutual authentication process to verify individual users and advanced encryption. WPA provides enterprise-class encryption techniques and WPA2.These are the next generation of Wi-Fi of a network security, which supports government grade encryption techniques.

C. Security Standard related to Wireless: -

➢ 802.11
➢ 802.11a
➢ 802.11b
➢ 802.11g
➢ 802.11n
➢ Bluetooth

Protocol	*Author*	*Frequency*	*Modulation*	*Data Rate*
802.11	IEEE	900 MHz	FHSS	300kbps
802.11a	IEEE	5GHz	OFDM	54 mbps
802.11b	IEEE	2.4 GHz	DSSS- FHSS	1-11 mbps
802.11g	IEEE	2.4 GHz	OFDM	54 mbps
802.11n	IEEE	2.4GHz - 5GHz	OFDM	54 mbps
Bluetooth	Blue tooth consortium	2.4 GHz	FHSS	1 mbps

Table. 1

III. RISK, THREAT AND VULNERABILITY

A. In this section we are discussing some well-known risks associated with wireless network: -

➢ *Bandwidth Stealing:* When an outsider entity or intruder connect to wireless network Aps by using Internet connections to download files, software, music's or movie, games to reduce employee productivity. It is known as bandwidth stealing.

➢ *Criminal Activity:* When an unauthorized access taken to perform any malicious activity that is come under this section.

➢ *Clear Text:* Some packets are travel unencrypted inside your organization network when intruder enter into your network he can easily install network sniffers onto your network and capture the information.

➢ *Denial of Service:* When an intruder wants to render a particular network so that server cannot full fill the legitimate user request, known as DOS attack.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

- *Evil Twins:* When an employee want to connect to his organization network by using his / her laptop and accidently connect to fake network. This is known as evil twins; because employee thinks he/she connects to authenticated network but accidently connected to fake one and that network will steal password, id and other sensitive and private information.

- *Eavesdropping:* As we all aware that wireless network will be facilitated on radio frequency, so any intruder listen these frequency can easily pick unencrypted message and disclose the crucial information of any organization into market, this is known as eavesdropping.

- *Litigation Risks:* When an intruder performing illegal activity such as distributing child pornography and if such activity discovered and investigated the origin of such illegal attack will be traced back to an organization.

- *Masquerade:* When an intruder hide himself under protective cover using internet lines and appear on to your network as a part of your organization, its is known as masquerade.

B. Some well-known threats associated with wireless network: -

- *Bluetooth Attacks:* Bluetooth technology is rapidly growing and being adopted worldwide very fast. For this we need increased security from intruder or hacker who had uncovered significant security vulnerability and risk such as unauthorized access, eavesdropping.

- *Hidden Rouge APs:* Any unknown, unmanaged un sanctioned device with in an organization is known as rouge access point and they will open the back door entry for intruder within a wireless network.

- *Mobile Device Weaknesses:* Devices such as, smart-phones, communicators such as the Nokia 800, PDAs and even point-of-sale devices, all of them require wireless connectivity. However, these embedded device platforms are much behind to the modern security practices and facility for wireless networks, with operating systems, which do not regularly updates patches for application flaws. Due to this devices are vulnerable to attacks for an extended period of time

- *PEAP and TTLS Configuration Weaknesses:* A wide range of organizations has turned their security to stronger authentication protocols such as PEAP and TTLS to authenticate wireless users and provide authorized access to the wireless network. While installing PEAP and TTLS protocols, the configuration of user machine is a crucial component for the wireless security of the network. Repeatedly, PEAP and TTLS networks are poorly installed on user machine and expose them to network impersonation attacks.

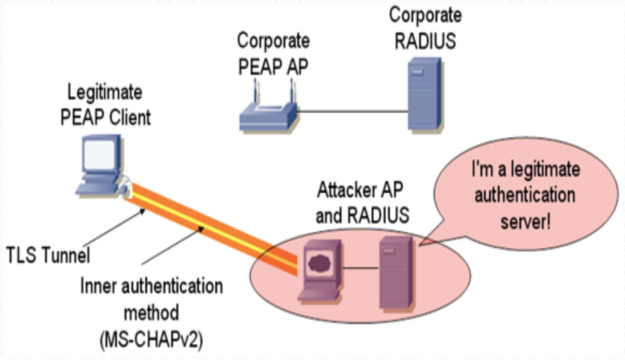


Fig. 1. Intruder impersonate a legitimate AP and RADIUS Server

C. Some well-known vulnerability associated with wireless network: -

- *Accidental Associations:* Such type of incidents takes places when a wireless network is install using the same SSID as other network and within the range of other Wi-Fi device. Peoples may accidentally associate with other network without there knowledge.

- *Insecure Network Configurations:* there is a miss conception in people and organization minds that if they are implementing and using firewall or virtual private network technique they are absolutely secure. But unfortunately this is not true all big or small security holes are exploitable and vulnerable if the routers, firewall or VPNs are not configured properly. *Social Engineering*

- *Social Engineering:* It is one of the most common, effective and dangerous types of attacks perform by intruders or hackers. This type of attack really panics us and can be perform for many other purposes instead of compromising security of a wireless networks.

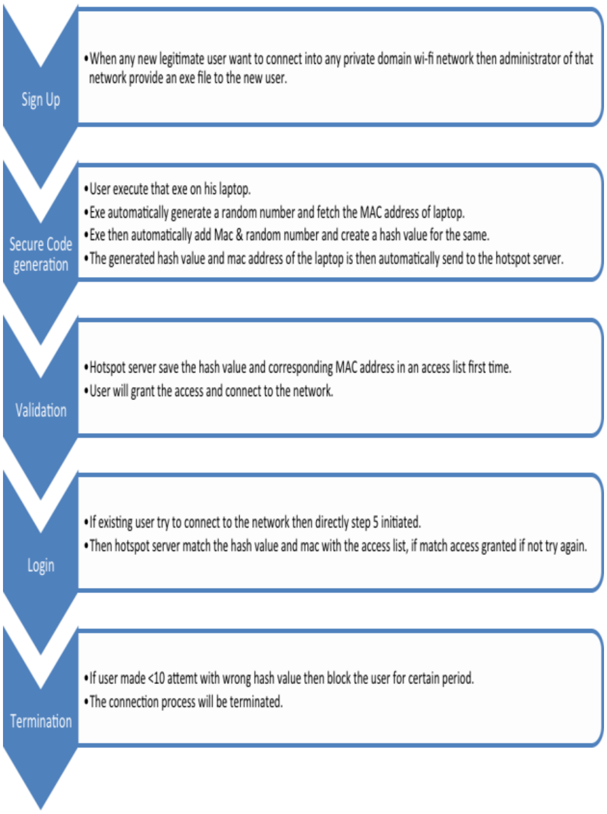
- *Wireless Driver Attacks:* This is the next generation attack to expose targeted system directly. In almost all big wireless card manufacturer devices some exploitable vulnerabilities are identified. Which can be exposed through automated tools even then when they are not connected to the wireless network.

IV. TAILORED APPROACH

For protecting our wireless network from above stated risks, threats, and vulnerability we are suggested a new approach for wireless LAN security that will prevent wireless network from such risk and vulnerability to a remarkable extend. In our approach we have divided our entire approach in 5 steps, those are as follows: -

- Sign Up
- Secure Code Generation
- Validation
- Login
- Termination

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)



- When any new legitimate user want to connect into any private domain wi-fi network then administrator of that network provide an exe file to the new user.
- User execute that exe on his laptop.
- Exe automatically generate a random number and fetch the MAC address of laptop.
- Exe then automatically add Mac & random number and create a hash value for the same.
- The generated hash value and mac address of the laptop is then automatically send to the hotspot server.
- Hotspot server save the hash value and corresponding MAC address in an access list first time.
- User will grant the access and connect to the network.
- If existing user try to connect to the network then directly step 5 initiated.
- Then hotspot server match the hash value and mac with the access list, if match access granted if not try again.
- If user made <10 attemt with wrong hash value then block the user for certain period.
- The connection process will be terminated.

Fig. 2. Tailored Approach

A. Concept was: -

1. When any new legitimate user wants to connect into particular private domain Wi-Fi of a network then administrator of that network provides an exe file to the new user.

2. User executes that exe on his laptop. 3.

Exe automatically generates a random number and obtains the MAC address.

4. Exe then automatically adds MAC & random number and computes a hash value for the same.

5. The generated hash value and mac address of the laptop is then automatically sent to the hotspot server.

6. Hotspot server save the hash value and corresponding MAC address in an access list first time.

7. User will grant the access and connect to the network.

8. If existing user try to connect to the network then directly step 5 initiated.

9. Then hotspot server matches the hash value and mac with the access list, if match access granted if not try again.

10. If user made <10 attempt with wrong hash value then block the user for certain period.

11. The connection process will be terminated.

B. Flow Chart of the Process: -

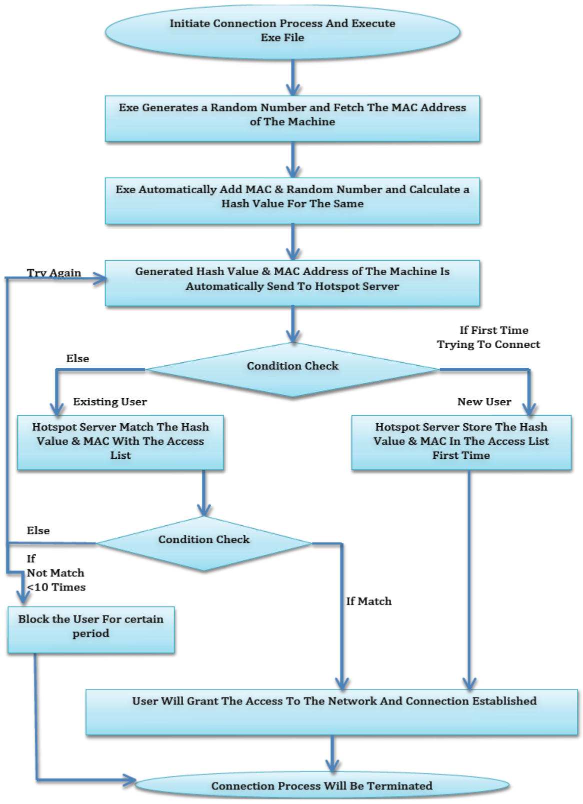

Initiate Connection Process And Execute Exe File
Exe Generates a Random Number and Fetch The MAC Address of The Machine
Exe Automatically Add MAC & Random Number and Calculate a Hash Value For The Same
Try Again
Generated Hash Value & MAC Address of The Machine Is Automatically Send To Hotspot Server
If First Time Trying To Connect
Else
Condition Check
Existing User
New User
Hotspot Server Match The Hash Value & MAC With The Access List
Hotspot Server Store The Hash Value & MAC In The Access List First Time
Else
Condition Check
If Not Match <10 Times
If Match
Block the User For certain period
User Will Grant The Access To The Network And Connection Established
Connection Process Will Be Terminated

Fig. 3. Concept flow chart

V. CONCLUSION & FUTURE WORK

In this research paper we tried to understand the wireless network as well as the security risks, threats and vulnerabilities associated with the wireless. We also developed a tailored approach to enhance the wireless security across the globe and also ensure that the security incident associated with wireless security will be decreased to considerable numbers. As of now we are not implement the suggested process for enhancing the wireless security but in future we will try to develop this framework and then will measure the effectiveness and efficiency of the suggested process.

REFERENCES

1. http://cybersecurity.my/data/content_files/11/649.pdf (Wierless LAN Security Guied Line By Noor Aida Idris and Mohamad Nizam Kasim).
2. http://www.freewimaxinfo.com/wired-network-connections.html (31st May, 2012. 12:50 PM).
3. http://en.wikipedia.org/wiki/Wireless_network (31st May, 2012. 12:50 PM).
4. http://compnetworking.about.com/cs/wireless80211/g/bldef_wifi.htm (31st May, 2012. 12:57 PM).
5. http://www.windowsnetworking.com/articles_tutorials/overview-wireless-network-security.html.
6. http://www.lanarchitect.net/Articles/Wireless/SecurityRating/.

7. http://www.zdnet.com/blog/ou/the-six-dumbest-ways-to-secure-a-wireless-lan/43.
8. http://www.computerworld.com/s/article/97178/Five_Steps_To_WLAN_Security_A_Layered_Approach.
9. http://www.iss.net/documents/whitepapers/wireless_LAN_security.pdf.
10. http://www.sans.org/reading_room/whitepapers/wireless/wireless-lan-security-issues-solutions_1009.

AUTHOR PROFILE

Ankur Kumar Shrivastava: Born in 1981 in Ghazipur distict (Uttar Pradesh). Phone Number +919335092777 & E- Mail Id: ankurshrivastava16@gmail.com. He completed his B.Tech. (Information Technology) from Allahabd Agriculture Institute Deemed University,Allahabad, M.B.A. (Marketing) from Sikkim Manipal University, Sikkim, M.S. (Information Security & Cyber Law) from Indian Institute of Information Technology,Allahabad, and currently pursuing Ph.D (Information Security) from CMJ Shillong,Meghalaya.He had 2 years Industry Experince from Reliance (RIPL,DAKC),Mumbai.He had more than 1 year Teaching Experience fromMeerut Institute of Engineering & Technology, Meerut. He published one Paper in Springer International Conference (ICIP-Banglore)in August 2011,his another paper was published in National Conference at IIT-BHU(AIATA-BHU) in December 2011. His major field of Study Areas are Information Security, Forensic Science, Cryptography, Network Security, Vullnerability Assesment and Penteration Testing, ISO 27001 and Software Engineering.

Ishan Ranjan: Born in 1963 in Rorkee Phone Number +917500244244 & E-mail Id: iranjan.miet@gmail.com. He completed his B.E.(Electrical Engg.) from University of Roorkee, in 1985,M.E. (Measurement & Instrumentation)from University of Roorkee, Roorkee in 1988. M.A.Sc. (Electrical & Computer Engineering.), Concordia University from Montreal, CANADA in 1990. Ph.D(IT Outsourcing) from Birla Institute of Management &Technology, Greater Noida in 2006. He had more than 12 years of Teaching Experience and 11 years of industrial experience. Currently he is working as Director – special projects in MIET, Meerut. Ishan ranjan has more than 11 international and 28 national Publications in his credit.

Abhinav Kumar: Born in 1986 in Ghazipur distict (UttarPradesh). Phone Number +919920423488 & E-mail Id: abhinavcool2@gmail.com. He completed his B.Tech. (Computer Science) from Rajasthan Technical University, M.S. (Information Security & Cyber Law) from Indian Institute of Information Technology, Allahabad.He had more than 2 years of Industry Experince from MG Techno Savvy Pvt. Ltd, Tryst Technologies Ltd.,NII Consulting, Mumbai.Also he had more than 6 monthsTeaching Experience fromMeerut Institute of Technology, Meerut.Currently he is working with Mahindra SSG as an Information Security Analyst. He published one Paper in Springer International Conference (ICIP-Banglore) in August 2011.his another paperwas published in National Conference at IIT-BHU(AIATA-BHU) in December 2011. He is a certified Lead Auditor of Iso27001 and ISMS. He is also certified in CCNA. His major field of work areas are ISMS, ISO 27001, VA & PT, Network Forensic Info. Sec. Auditing, COSO & Cobit frameworks.

Anant Kumar Rai: Born in 1986 in Ghazipur distict (Uttar Pradesh). Phone Number +919920423488 & E-mail Id: anantrai6feb@gmail.com. He completed his diploma (Electronics Engineering) from GovernmentPolytechnic Ghazibad, B.Tech. (Information Technology) from Uttar Pradesh Technical University, M.S. (Information Security & Cyber Law) from Indian Institute of Information Technology, Allahabad.He had more than 1 year of Industry Experince from, NII Consulting, Mumbai. Also he had more than 6 monthsTeaching Experience fromMeerut Institute of Technology, Meerut.Currently he is working with NII Consulting as an Information Security Analyst. He published one Paper in Springer International Conference (ICIP-Banglore) in August 2011.his another paperwas published in National Conference at IIT-BHU(AIATA-BHU) in December 2011. He is a certified Lead Auditor of Iso27001 and ISMS.His major field of work areas are ISMS, ISO 27001, VA & PT, Network Forensic Info. Sec. Auditing, COSO & Cobit frameworks.

Ramander Singh: Born in 1982 in Bijnor (Uttarpradesh). Phone Number +919557273811 & E-Mail Id: ramendera@gmail.com. He had done B.E (Computer Science & engineering) from Institute of Engineering & Technology Khandari Campus Agra. M.Tech (Computer Science & Engineering) From Mewar University Chittorgarh (Rajasthan**).**He has 4 year Teaching Experience from Number of Engineering Institute before his M.Tech. He published one Paper in International Conference (ICIAICT). He is IBM DB2 Certified. The major field of Study Area is Algorithm, Programming and Computer Architecture.

Archit Rastogi: Born in 1987 in Chandausi distict (Uttar Pradesh). Phone Number +918979319480 & E-mail Id. rastogiarchit26@gmail.com. He completed his B.Tech. (Computer Science) from Uttar Pradesh Technical University, and pursuing M.E. (Computer Science) from Technical Teachers Training and Research, Chandigarh .He had more than 4 year's of teaching experince with various engg. colleges. His major field of study are DAA, DBMS, C, CO, Web Tech, ITIM, ISCL.

Nitisha Payal: Born in 1987 in Meerut (Uttar Pradesh). Phone Number +917830630414 and E-mail Id: nitishapayal@gmail.com.She completed her B.Tech. (Computer Science And Engineering) with honors from Uttar Pradesh Technical University and currently pursuing M.Tech. She had 1.5 year Teaching Experience from Meerut Institute of Engineering & Technology, Meerut. The major field of Study area are Software Engineering, Software Project management, Oops, ITIM and Operating System.

Amod Tiwari: Born in 1974 in Kanauj district (UttarPradesh). Phone Number +919415539025 & E-mail Id: amodtiwari@gmail.com.He acquired his Bachelor degree in Mathematics and Science from CSJM Kanpur University Kanpur and master degree in Computer Science and Engineering from Bilaspur Central University, Bilaspur (CG) in India. His Academic excellence shines further with PhD in Computer Science and Engineering from Indian Institute of Technology Kanpur. Working for reputed firm like LML Scooter India Ltd, Kanpur, at senior level more than two years. He has been associated with Indian Institute of Technology Kanpur from 2005 to 2010. He is currently working as Associate professor and Dean Academic and Affairs in PSIT Kanpur. Amod Tiwari has more than 40 Publications in his credit.