The Impact of Using Security Issues in Wireless Local Area Networks

Ajay Kumar Verma[1]
Deptt: Computer Science
(Shobhit University)
Meerut, India
ajayncv@gmail.com

Dr.Manoj Kapil[2]
Principal
(SITE,Subharti University)
Meerut, India
manoj.kapil@gmail.com

Dr. Amit Asthana[3]
Associate Professor
Deptt: Computer Science
(SGT University) Gurgaon,India
drasthanaamit@gmail.com

Abstract—
Wireless LANs (WLANs) are quickly gaining popularity due to their ease of installation and higher employee mobility. Constant increase in use of wireless infrastructure networks for business purposes created a need for strong safety mechanisms. This paper describe the various security issues in Wireless LAN implemented using Virtual Private Networking with an attempt to suggest a model of security implementation. The paper also gives a summary of security improvements of WEP protocol that can lead to a higher level of wireless network infrastructure protection. Comparative analysis shows the advantages of the new 802.11i standard in comparison to the previous security solutions.

Keywords: *authentication, confidentiality, integrity, WEP protocol, deficiencies of WEP, security threats to 802.11, TKIP, 802.1x, WLAN safety improvements, RC4, AES*

DOINumber:10.48047/nq.2022.20.22.NQ10349 **NeuroQuantology2022;20(22):3503-3508**

I. INTRODUCTION

Wireless networks are becoming more popular today. Big corporations are using them more and more often due to their advantages. Wireless LANs must adhere to the many of the same rules as traditional wired LANs, including full connectivity to stations, the ability to broadcast, high capacity, etc. In addition, wireless LANs has some special requirements unique to their forms of communication Popularity of local wireless networks owes much to their advantages, such as: user mobility, fast and simple installation, flexibility, scalability and relatively low price. WLAN (Wireless Local Area Network) enables users to access resources no matter of the place they occupy. By using mobile computers, users can have the access to the resources no matter of their location within the wireless network. All the above mentioned advantages come from the medium that transfers the data – with the wireless networks, it is the air. Data are transferred via radio waves spreading throughout the space and thus the information reaches anyone with the appropriate radio receiver. Therefore, there is a problem of the protection of information. Traditional mechanisms for the physical protection of wired networks (firewalls and shields) cannot be applied to the protection of wireless networks. It was necessary to create mechanisms.

II. RELATED WORKS & IEEE 802.11 VULNERABILITIES

A lot of research has been done in exploring threats, vulnerabilities, attacks and a variety of counter measures to overcome the same has been proposed .To protect the wormhole, each node shares a secret key with every other node and maintains an updated list of its neighbors. Neighbor list are built in a secure manner by using the direction in which a signal is

heard from a neighbor with the assumption that the antennas on all the nodes are aligned. To provide the security to WLANs, it requires five main security requirements to be achieved which are data integrity, confidentiality, authentication, access control & non repudiation.

The above stated concerns relate to wireless networks in general. Some of the security concerns raised specifically against IEEE 802.11 networks are as follow.

i) MAC Address Authentication: Such sort of authentication establishes the identity of the physical machine, not its human user. Thus an attacker who manages to steal a laptop with a registered MAC address will appear to the network as a legitimate user. [7]

***ii) One-way Authentication*:** WEP authentication is client-centered or one-way only. This means that the client has to prove its identity to the AP but not vice versa. Thus a rogue AP may successfully authenticate the client station and then subsequently will be able to capture all the packets sent by that station through it.

iii) Static WEP Keys*:** There is no concept of dynamic or per-session WEP keys in 802.11 specifications. Moreover the same WEP key has to be manually entered at all the stations in the WLAN, causing key management issues.iv) SSID:*** Since SSID is usually provided in the message header and transmitted as clear texts, it provides little security.

***v) WEP Key Vulnerability*:** Many concerns have been raised regarding the usefulness of WEP in securing 802.11 WLANs. Some of them are as follow:

vi) Manual Key Management - Keys need to be entered manually on all the clients and access points. Such overhead may result in infrequently changed WEP keys.

vii) Key Size - The IEEE 802.11 design community blames 40-bit RC4 keys for the WEP vulnerability, and recommends using 104 or 128-bit RC4 keys instead. Although using larger key size does increase the work of an intruder, it does not provide completely secure solution.

viii) Decryption Dictionaries - Infrequent re-keying and frames with same IV result in large collection of frames encrypted with same key streams. These are called *decryption dictionaries* [1] [2]. Therefore, even if the secret key is not known, more information is gathered about the unencrypted frames and may eventually lead to the exposure of the secret key.

With vulnerabilities outlined above, it is reasonable to assume that an 802.11 WLAN protected by WEP alone can be easily cracked by using readily available tools such as *Air Snort* and *WEP Crack*. Alternative security solutions are apparently needed.

III. WIRELESS LANS

Wireless LANs must adhere to the many of the same rules as traditional wired LANs, including full connectivity to stations, the ability to broadcast, high capacity, etc. In addition, wireless LANs has some special requirements unique to their forms of communication. A few of these follow:

a) **Throughput** - Due to the decreased bandwidth of radio and IR channels, the Medium Access Control (MAC) protocol should make as efficient use of this available bandwidth as possible.

b) **Backbone Connectivity** - In most cases, wireless LANs connect to some sort of internal (wired) network. Therefore, facilities must be provided to make this connection. This is usually one station that serves as the Access Point (AP) to the wired LAN for all stations.

c) **Power Considerations -** Often times, wireless stations are small battery powered units. Algorithms that require the station to constantly check the medium or perform other tasks frequently may be inappropriate.

d) **Roaming -** Wireless stations should be able to move freely about their service area.

e) **Dynamic** - The addition, deletion, or relocation of wireless stations should not affect other users.

f) **Licensing** - In order to gain widespread popularity, it is preferred that FCC licenses not be required to operate wireless LAN's.Wi-Fi® is a system of wirelessly connecting devices that use radio waves, allowing for connection between devices without the expense of cumbersome cables or without needing them to be facing one another. Wi-Fi stands for Wireless Fidelity® and is used to define the wireless technology in the IEEE 802.11b standard. It operates in the unlicensed 2.4 GHz radio spectrum, uses direct-sequence spread spectrum (DSSS) for modulation, supports variable data rates up to 11 Mbps, and has a range of about 50 meters.

Wi-Fi allows users to gain convenient wireless internet access, though without the sufficient security precautions it can also let outsiders or intruders to do the same without anyone noticing. As “hot-spots” are becoming increasingly popular and cities working towards becoming entirely wireless, users is becoming

more vulnerable to cyber crime. Techno-criminal can attack a user's wireless network in order to gain free internet usage or obtain personal and valuable information.

The threat of intrusion into the home wireless network has forced users to adopt a range of security. Security measures have improved since the release of the first system called Wired Equivalent Privacy (WEP). The majority of new Wi-Fi products use a system called Wi-Fi Protected Access, created by the Wi-Fi Alliance. It not only provides a 128-bit encryption of data that is being transmitted but locks on to individual computers and changes the access key every 10000 packets. It is more complicated than WEP, though it is more secure with improved authentication, authorization and encryption capabilities

Keywords: 802.11, Network Management, Network Security, Protocols, Performance

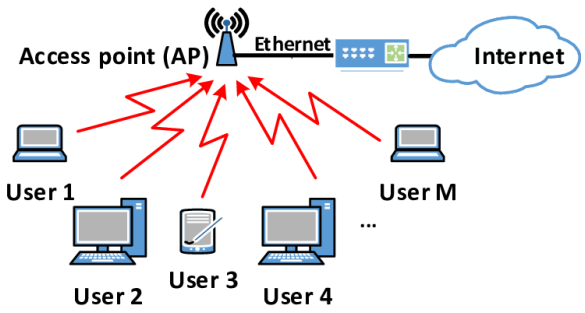

Figure 1: A typical 802.11 wireless Network

IV. WLANs Security Technologies

There are three basic security technologies introduced by IEEE 802.11 to validate right to use the WLANs and to reserve confidentiality of data transmitted. The technologies were WEP, Open System and Shared Key Authentication. The usage of security mechanism to discover and fix security holes has to be compatible with that of the policies,

which are being supplied by organization's management so as to accomplish greatest results. This strategy describes who the legitimate users, their responsibilities are and also what should be done in case of violations to the general guidelines

A. Authentication techniques:

Authentications Techniques are categorized in to two types, which are being used to access WLANs. They are shared key authentication methods and Open System authentication methods, which are defined by IEEE 802.11. In the open system authentication method, communications between node and AP are visible. This method does not bother if WEP key used to access WLANs is not correct, i.e. though key is incorrect; the AP allows access to WLANs it only checks for network SSID. AP broadcasts SSID by default hence it is not safe. In shared key authentication method AP transmit challenge text to the stations. Now by the use of WEP keys challenge text can be encrypted and then it is returned back to the AP. The AP decrypts the cipher text and compares it with original text. If decrypted text and original text are identical then it is ensured that both AP and STA are using the same key. Hence the station is authenticated. Authentication of station is mandatory here but AP authentication is not required, hence it may be even possible that station can be connected to an attacker AP. The

second problem in the shared key authentication method that intruder. [3]

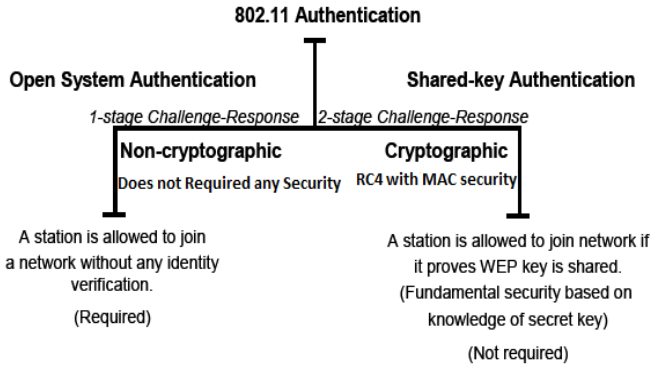

Figure 2: A typical 802.11 Authentication

V. VPN (Virtual Private Network) Security Solution

A VPN model is an enhancement of a venture's private Internet within a public network, for instance, the Internet, constructing a protected private relation, fundamentally by means of a private channel. VPNs firmly transmit relevant data across the Internet hence connecting isolated users, different offices, along with business associates into an extensive corporate network. The VPN model is virtual, and this denotes that the physical form of the network should be clear to whichever VPN connection. [4]

VPN can protect users from the attacks that directly influence the confidentiality of application data, but it cannot prevent attacks that indirectly ruin confidentiality. Man in the middle, high jacking and replay attacks is the best examples of these kinds of attacks.

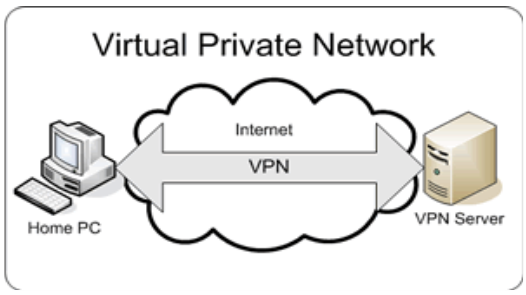

Figure 3: VPN Security

Virtual private networks are mainly used in company infrastructures with strong authentication levels. Virtual private networks are based the different protocol strategies like TCP/IP. It mainly concentrates on how the encryption technology works and support to the virtual environment? Encryption is nothing but the conversion of original message to desired message which is called decryption. Decryption is just reverse of encryption technology.)

A. WEP Protocol

WEP protocol is the basic part of IEEE 802.11 (IEEE – Institute of Electrical and Electronics Engineers) standard for the protection of WLAN networks. [5] The basic function of WEP protocol is to provide data security in wireless networks in the same way as it is in the wired networks. Lack of physical connection among users and wireless networks enables all users within the network range to receive data if they have appropriate receivers. The only possible way to protect this kind of network was to create a protocol that would work on the second layer of OSI model and, in this way, provide the data protection during the transmission. In order to protect data transmitted among the communicating

B. WEP uses shared secret key of Equations

In order to provide a practical secure environment, IEEE 802.11 specification has identified and introduced several services that can be implemented. WEP originally designed to protect data at the link-level for the period of the wireless transmission between AP and clients. WEP is stand for Wired Equivalent Privacy and was originally designed as an equivalent protection to a wired network. However, there are many WEP misconceptions, for example, WEP is not an encryption algorithm, and it would never protect your data from attackers who wants to find out your data during the transmission. There is no end-to-end protection, but only for the wireless portion of the connection as depicted in the following Figure.

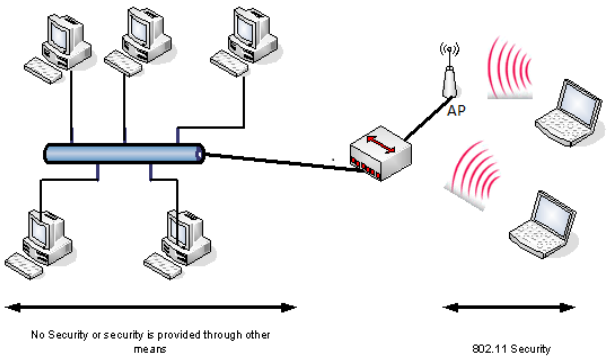

Figure 4: A typical 802.11 wireless network security

WEP was developed to create in wireless transmissions the natural security that exists in wired transmissions. It attempts to protect your data in the same way as an unencrypted wired Ethernet network. WEP can be configured in three ways:

1. 128-bit encryption.
2. 40-bit encryption.
3. No encryption mode.

WEP is an optional, negotiated, agreed-upon encryption standard that must be pre-configured by a user before connecting to a wireless AP. Once set up on both sides, all wireless communication is encrypted to ensure secure transmission. A user connecting to an AP via WEP must have WEP enabled on their PC and have a password or key shared by the end user. A simple process encrypts each packet from the access point to the client device. Each packet's data and its respective 40-bit secret number are encrypted and both pass through the RC4 encryption algorithm. Using the same 40-bit number, the RC4 algorithm is used to decrypt the received data in the opposite way, allowing the client device to transmit the data. 128-bit encryption key bits are also supported, and there are known misconceptions and errors with WEP, so we recommend using 128-bit encryption as a better solution.

VI. WEP Protocol Security

The WEP protocol is a fundamental part of the IEEE 802.11 (IEEE - Institute of Electrical and Electronics Engineers) standard for securing wireless networks. [6] The basic function of the WEP protocol is to provide data security in wireless networks as well as in wired networks. Since there is no physical connection between the user and the wireless network, data can be received by anyone within range of the network with the right receiver. The only way to secure this type of network was to create a

protocol that operates at Layer 2 of the OSI model to provide data protection in transit. To protect data sent between communicating parties,

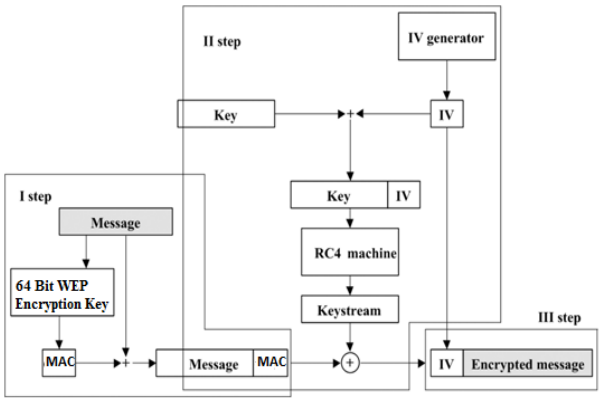

Figure 5: A typical 802.11 wireless network security

WEP uses a 40 to 140-bit shared secret key. The WEP protocol is applied in three steps [9]:

MAC Address

MAC Address is a special number on every computer
network card, switch, router, access point, or all that can
be connected with other devices in the network mechanism. It allows devices in the network to communicate with each other [1]. In an Ethernet-based
network, each header in the Ethernet frame contains
information about the MAC address of the source and
MAC addresses of the destination computer. If a computer has more than one network card, then the
computer must also have MAC Address respectively.
Each laptop currently has two MAC Address, the wired
network card (RJ-45), and wireless network card (802.11b**CONCLUSIONS**

i) A CRC (Cyclic Redundancy Code) message is calculated and added to the original message.

ii) The second step for using the WEP protocol is encryption (see Figure 1). Messages are encrypted using the RC4 algorithm. Encryption takes place in three phases. First, a 3-byte pseudo-random data sequence is generated (IV - initialization vector) and the key is expanded. The RC4 algorithm then generates a key stream based on the new key. Encryption ends with the application of an exclusive OR function (XOR) between the key stream and the message to produce the encrypted message.

iii) The final step is to send the Sequence IV and encrypted message. The reverse process applies when the message reaches its final destination. Again, an extended key is generated based on the submitted IV and shared key. Next, the RC4 algorithm generates a key stream, an XOR function is computed between the key stream and the arriving message, and as a result of the XOR function the decrypted message is received. The accuracy of the CRC sum of the decrypted message is calculated by the CRC of the decrypted message. It is then compared with the transmitted CRC. A received message matches a sent message if the CRC of the decoded message is the same as the CRC of the sent message. The WEP protocol should achieve three main security goals [10].

iv) Authentication - This is the procedure used to verify the identity of communication participants. According to the IEEE 802.11 specification, there are open system authentication and shared key authentication.

v) Open system authentication allows mobile stations to access points without verifying the identity of the station. This is a one-way authentication as the mobile station knows it is communicating with the correct access point. Open system authentication is highly vulnerable to attacks and allows unauthorized access.

vi) Shared key authentication is based on encryption techniques and question-and-answer procedures between stations and access points. Once the access point has decrypted the station's response using the shared key, the authentication process is complete and access to the workstation is granted only if the decrypted result matches the question submitted.

vii) **Confidentiality** - The 802.11 standard implements confidentiality using cryptographic techniques. The WEP protocol for protecting confidentiality uses the RC4 algorithm and symmetric keys with pseudo sequences. In general, every increase in key length provides more protection. But recent brute force

attacks on wireless local area networks have put privacy at risk. This means that unzipped logs are vulnerable to attack regardless of key length. [9].

viii) **Completeness** - The WEP protocol uses CRC technology to provide integrity of messages sent between stations and access points. Different checksums compromise the integrity of the received message. In this case, the incoming message will be rejected.

Future Scope

There is scope for improvement and future work. The possible improvements to our work can be:

i) Although it has been demonstrated that the proposed authentication approach reduces current threats, it should still be thoroughly assessed using formal evaluation methods and predicate logic.

ii) By modeling public-key cryptosystem on a computer with CPU performance equivalent to access points, it was demonstrated that it is practical in Wireless LANs. Future work should involve installing the mechanism on a real Access Point and evaluating its viability.

iii) Only rogue access points are picked up by the RAP detection system. The Rogue Access Point system can be equipped with a counterattack system to prevent further detection of RAPs. Using SNMP, this may be done to block the port used by the rogue access points.

References

[1] Jim Geirt, Implemening 802.1X Security Solutions for Wired and Wireless Networks, Wiley, 2008

[2] Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i ”National Institute of Standards and Technology, Special Publication (NIST SP) 800-97, Available at URL:http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf.

[3] K. Elissa, “Title of paper if known,” unpublished.

[4] R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.

[5] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate

[6] Institute of Electrical and Electronic Engineers (IEEE).

Part 11: Wireless LAN medium access control (MAC)

[7] physical layer (PHY) specifications. IEEE Std 802.11, 1999.interface,” IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[8] M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, 1989.

[9] White paper: Testing for Wi-Fi Protected Access(WPA) inWLAN Access Points. Net-O2 Technologies,(2004).http://whitepapers.zdnet.co.uk/0,39025942,60152756p,00.htm