Journal Of Harmonized Research (JOHR)

Journal Of Harmonized Research in Engineering
7(3), 2019, 23-29

ISSN 2347 – 7393

Review Article

A REVIEW ON NEED, IMPORTANCE AND PREVENTIVE MEASURES FOR INFORMATION SECURITY IN WIRELESS NETWORKS

Nikita Bahaley

Dept. of Computer Science and Information Technology, St. Wilfred's College of Arts, Commerce and Science, New Mumbai, Maharashtra, India.

Abstract*:* This paper provides a study on the fact that how important is to maintain the privacy, authenticity of data while it goes through network or stored on the server along with some measures that should be taken to prevent it from malicious use. In today's era whatever may be the age group of people in the society, everybody uses electronic devices and internet for sending personal/official data or files, for educational purpose, for doing bank transactions, downloading data from the internet etc. so it is very crucial to keep the information safe from unauthorized access that is sent, received, downloaded i.e. goes through internet or stored on some server. The basic security requirement of any network is its confidentiality, integrity and authentication. Whether it is a physical layer or application layer or any layer; the information must be secured at all the levels while it goes from source to destination as well as during its storage in wired as well as wireless networks.

Keywords- information security, data security, security, network, authentication, information tampering, confidentiality, integrity, availability

Introduction*:* The radio propagation has the broadcast nature and hence the wireless air interface is open as well as accessible to both authorized as well as unauthorized users. Due to this reason, wireless networks are more vulnerable to the malicious activities which can involve active as well as passive attacks [1].Whereas in case of wired networks; each and every system in the network is connected to each other with cables. So in case of wired networks, the information is somewhat more secure as compared to the wireless networks and hence there are less chances of an attacker's success that he will attack on the network and will get access to it and can tamper the information.

For Correspondence:
nikitabahaley@gmail.com.
Received on: March 2019
Accepted after revision: September 2019
Downloaded from: www.johronline.com

Day by day the users of web application are increasing and hence the amount of data that is stored on servers has increased. Many financial services, online payments and lot applications are based on web where the attacker targets user's passwords, credit card numbers and other crucial information. The leakage or tampering of private data occurs on large scale and it causes a serious impact. Individual person's private information stored on servers and generally it is accessed by them by using their usernames and passwords. Password leakage is one of primary reasons for disclosure of user's sensitive data. This happens due to the fact that most of the internet users use same passwords for all of their web application accounts. Attacker can use any of way to get sensitive information like network sniffing, injecting malicious client side code or by compromising web application server[2].

During the past decades, wireless communications infrastructure and services have been proliferating with the goal of meeting rapidly increasing demands [3][4]. According to the latest statistics released by the International Telecommunications Union in 2013 [5], the number of mobile subscribers has reached 6.8 billion worldwide and almost 40% of the world's population is now using the Internet. Meanwhile, it has been reported in [6] that an increasing number of wireless devices are abused for illicit cybercriminal activities, including malicious attacks, computer hacking, data forging, financial information theft, online bullying/stalking, and so on. So it has become very important to improve wireless communication security to fight against cyber-crimes because more and more people are using wireless networks for bank transactions, accessing personal e-mails due to widespread use of smartphones.

One of the best ways to protect sensitive information is to owner encrypt it and be the only one who can decrypt it. By using this way that is giving the full control of information to the users, the risk that can be caused by compromising online server can be reduced. But the main challenge with this is key management. Some of the existing methods uses same computer to store the keys, but the problem occurs when the same computer has to be used by the other person. Some other method chooses to store the key on online server. Till now the password is the key component of most of the online authentication systems and hence the leakage of password directly threatens the users. To increase the security in such cases, users are always guided to choose the strong passwords, but generally they end up in using same passwords for all their online accounts to reduce memory burden.

Like wireless networks, mobile phones/devices are mostly used by the people to perform any online transactions, sending some sensitive data over internet etc. Mobile phones/devices have a particular set of risks and vulnerabilities associated with them, especially risk factors related to youth populations. The mainstream media has highlighted the concern about young people being targeted by bullies and paedophiles through mobile phones and other media technologies [2] [7][8]. For example, Valentine and Holloway who explored young people's use of cyberspace noted parental concerns about young people's vulnerability [25].

A wireless network generally uses the OSI protocol architecture which consists of application layer, transport layer, network layer, MAC layer and physical layer. To meet the security requirements like authenticity, confidentiality, integrity and availability, security threats and vulnerabilities associated with these protocol layers are typically protected separately at each layer. For example, cryptography is widely used for maintaining privacy of data transmission by preventing information disclosure to unauthorized users in the network.

Although cryptography improves the achievable communications confidentiality, it requires additional computational power and it imposes latency, because a certain amount of time is required for both the processes; data encryption and decryption. Wireless networks are prone to various malicious attacks, like DoS attack, eavesdropping, sniffing, spoofing, MITM attack, phishing etc.

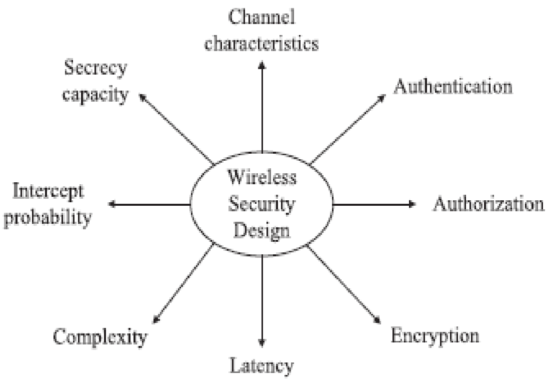

Fig 1: wireless security methodologies and security factors [1]

The Requirement of Security in Wireless Network: Maintaining privacy of data is a typical security requirement, which refers to the capability of restricting data access to authorized users only, while preventing eavesdroppers from intercepting the information. Generally speaking, secure wireless communications should satisfy the requirements of authenticity, confidentiality, integrity, and availability [10], as detailed in the following.

- **Authenticity:** Authenticity means confirming the identity of a network node to distinguish authorized users from unauthorized users. In wireless networks, a pair of communicating devices should first perform mutual authentication process before establishing a communication channel for data transmission [11]. Typically, a network node is equipped with a wireless network interface card and has a unique MAC address, whichcan be used for authentication purposes.
- **Confidentiality:** The confidentiality means limiting access of information to intended users only and preventing the disclosure of the information to unauthorized users in the network [48]. In symmetric key encryption technique, the sender first encrypts the original data which is called as plain text, using an encryption algorithm with the help of a secret key that is shared with the intended receiver only. Next, the encrypted plaintext which is called as cipher text is transmitted to the destination that then decrypts its received cipher text using the secret key. Since the eavesdropper has no knowledge of the secret key, it is unable to interpret the plaintext based on the overheard cipher text. Traditionally, the classic Diffie–Hellman key agreement protocol is used to achieve the key exchange between the source and destination and requires at rusted key management center[12].
- **Integrity:** Maintaining integrity of data means though out the life cycle of data, it should be accessed and modified by authorized users only. The data integrity may be violated by insider attacks.
- **Availability:** The principle of availability states that information going through network or stored on server should be available all the time to authorized users only, upon request. The violation of availability, referred to as denial of service, will result in the authorized users to become unable to access the wireless network, which in turn results in unsatisfactory user experience [13], [14].

Security Weakness in Wireless Networks: Apart from the differences, wired and wireless networks have some similarities. Both the networks uses OSI model for the communication which consists of different layers like physical layer, MAC layer, Network layer, Transport layer and application layer. Along with this, there are some types of attacks that are carried by attackers, which are similar between wired and wireless networks. Every OSI layer has its own unique security challenges and issues, since different layers rely on different protocols, hence exhibiting different security vulnerabilities.

The various protocols that are used at different layers of OSI model are:

1. Application Layer: FTP, TELNET, SMTP, HTTP.
2. Transport Layer: TCP, UDP.
3. Network Layer: IP, ICMP
4. Mac Layer: CSMA/CA, ALOHA, CDMA, OFDMA
5. Physical Layer: it is used as a transmission medium where various techniques like coding, modulation etc. are used before sending the data towards receiver.

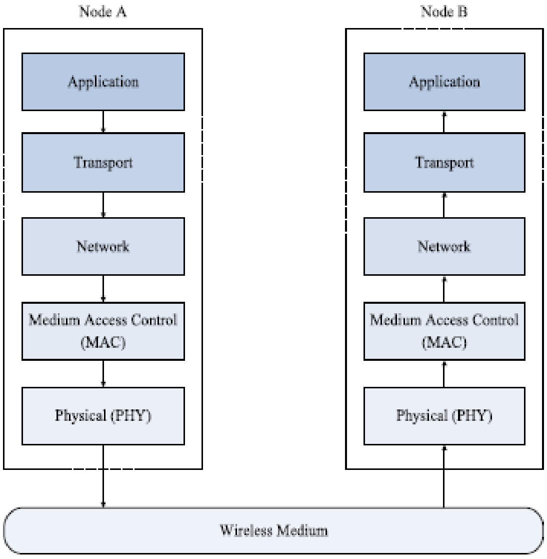

Fig2: Protocol architecture of generic wireless OSI layers

The main types of attacks that can be launched on physical layer of OSI model are: Eavesdropping and Jamming[1].

- **Eavesdropping** means here attacker tries to intercept the communication that is taking place between authorized network users.
- **Jamming** refers to interruption of legitimate transmission that is here attacker restricts authorized user from sending the data.

The various types of attacks that can be launched on MAC layer by the attacker are: MAC spoofing, identity theft, MITM attack and the network injection[1].

- **MAC spoofing** is nothing but the falsification of MAC address.
- **Identity theft** means stealing the identity of authorized network user.
- **MITM attack** refers to the attack where attacker captures the data going through the network, modifies it and sends it to receiver, by impersonation of pair of communicating nodes.
- **Network injection** means injecting forged network commands and packets.

Main types of attacks that take place at network layer are:IP spoofing, IP hijacking, smurf attack[1].

- In **IP spoofing** attacker falsifies the IP address to perform malicious activities in the network.
- In case of **IP hijacking attack**, attacker impersonalises the IP address of authorized user in the network to launch the attack.
- **Smurf attack** refers to the paralysation of network by launching huge number of ICMP requests in the network.

Types of attacks in transport layer are: TCP flooding, UDP flooding, TCP sequence predictionattacks [1].

- Sending a huge number of ping requests to the server to make it busy is nothing but **TCP flooding**.
- In **UDP flooding**, attacker sends an overwhelming number of UDP packets.
- Fabrication of legitimate user's data packets using predicted TCP sequence index takes place in **TCP sequence prediction attack.**

Main types of attacks that take place at application layer are: malware attack, SQL injection, cross-site scripting, FTP bounce, and SMTP attack[1].

- Malware is nothing but malicious software. In **malware attack**, attackers program the software in the form of code, scripts and active content.
- **SQL injection** means inserting rouge SQL statements attempting to gain unauthorized access to legitimate websites.
- Attacker injects client side scripts into web pages for by passing some of the access control measures to get unauthorized access in **cross site scripting attack.**
- In **FTPbounce** attacker impersonates a legitimate user to get unauthorized access.
- **SMTP attack** refers to malicious attack in e-mail transferring between SMTP client and server.

Defence Protocols For Information Security: The various security protocols used in the aforementioned wireless standards are:

1. **Bluetooth:** Bluetooth is a short-range and low-power wireless networking standard, which has been widely implemented in computing and communications devices as well as in peripherals, such as cell phones, keyboards, audio headsets, etc. However, Bluetooth devices are subject to a large number of wireless security threats and may

easily become compromised. As a protection, Bluetooth introduces diverse security features and protocols for guaranteeing its transmissions against potentially serious attacks [15]. For security reasons, each Bluetooth device has four entities [16], including the Bluetooth device address (BD_ADDR), private authentication key, private encryption key and a random number (RAND), which are used for authentication, authorization and encryption, respectively. More specifically, the BD_ADDR contains 48 b, which is unique for each Bluetooth device. The 128-b private authentication key is used for authentication and the private encryption key that varies from 8 to 128 b in length is used for encryption. In addition, RAND is a frequently changing 128-b pseudorandom number generated by the Bluetooth device itself.

2. **Wi-Fi:** The family of Wi-Fi networks mainly based on the IEEE 802.11 b/g standards has been explosively expanding. The most common security protocols in Wi-Fi are referred to as WEP and WPA [18]. WEP was proposed in 1999 as a security measure for Wi-Fi networks to make wireless data transmissions as secure as in traditional wired networks. However, WEP has been shown to be relatively weak security protocol, having numerous flaws. Hence, it can be "cracked" in a few minutes using a basic laptop computer. As an alternative, WPA was put forward in 2003 for replacing WEP, while theimproved WPA2 constitutes an upgraded version of the WPA standard. Typically, WPA and WPA2 are more secure than WEP and thus they are widely used in modern Wi-Fi networks. The WEP protocol consists of two main parts, namely the authentication part and encryption part, aiming for establishing access control by preventing unauthorized access without an appropriate WEP key and hence they achieve data privacy by encrypting the data streams with the aid of the WEP key.
3. **The WEP** authentication uses a four-step "challenge–response" handshake between a Wi-Fi client and an access point operating with the aid of a shared WEP key. To be specific, the client first sends an authentication request to the access point, which then replies with a plaintext challenge. After that, the client encrypts it's received "challenge text" using a pre-shared WEP key and sends the encrypted text to the access point. It then decrypts the received encrypted text with the aid of the pre-shared WEP key and attempts to compare the decrypted text to the original plaintext. If a match is found, the access point sends a successful authentication indicator to the client. Otherwise, the authentication is considered assailed. Following the authentication, WEP activates the process of encrypting data streams using the simple Rivest Cipher 4 Algorithm operating with the aid of the pre-shared WEP key [17].
4. **WiMax:** The protocol stack of a WiMAX system defines two main layers, namely the physical layer and the MAC layer. Moreover, the MAC layer consists of three sub layers, namely the service specific convergence sub layer, the common part sub layer, and the security sub layer. All the security issues and risks are considered and addressed in the security sub layer. The WiMAX security sub layer is responsible for authentication, authorization, and encryption in WiMAX networks. The security sub layer defines a so-called PKM protocol, which considers the employment of the X.509 digital certificate along with the RSA public-key algorithm and the AES algorithm for both user authentications as well as for key management and secure transmissions. Authentication in WiMAX is achieved by the PKM protocol, which supports two basic authentication approaches, namely the RSA-based authentication and the EAP-based authentication [19].
5. **LTE:** Long Term Evolution is the most recent standard developed by the 3G partnership project for next-generation

mobile networks designed for providing seamless coverage, high data rate, and low latency [20]. It supports packet switching for seamless interworking with other wireless networks and also introduces many new elements, such as relay stations, home eNodeB (HeNB) concept, etc. An LTE network typically consists of an EPC and an E-UTRAN.

Jamming Attacks in Wireless Networks: In wireless networks, a jamming attack can be simply launched by emitting unwanted radio signals to disrupt the transmissions between a pair of legitimate nodes. The objective of a jamming attacker (also referred to as jammer) is to interfere with either the transmission or the reception (or both) of legitimate wireless communications. For example, a jammer may continuously transmit its signal over a shared wireless channel so that legitimate nodes always find the channel busy and keep deferring their data transmissions. This, however, is energy-inefficient, since the jammer has to transmit constantly.

To improve its energy efficiency, a jammer may opt for transmitting an interfering signal only when it detects that a legitimate transmitter is sending data [1]. There are many different types of wireless jammers, which maybe classified into the following five categories [21]:

1. **Constant jammer**, where a jamming signal is continuously transmitted;
2. **Intermittent jammer**, where a jamming signal is emitted from time to time;
3. **Reactive jammer**, where a jamming signal is only imposed, when the legitimate transmission is detected to be active;
4. **Adaptive jammer**, where a jamming signal is tailored to the level of received power at the legitimate receiver;
5. **Intelligent jammer**, where weaknesses of the upper-layer protocols are exploited for blocking the legitimate transmission.

Clearly, the first four types of jammers all exploit the shared nature of the wireless medium and can be regarded as wireless physical-layer jamming attacks. By contrast, the intelligent jammer attempts to capitalize on the vulnerabilities of the upper-layer protocols [22], including the MAC, network, transport, and application layers. Typically, the network, transport, and application layers are defined in the TCP/IP protocols and not specified in wireless standards (e.g., Bluetooth, WLAN, etc.), which are responsible for the PHY and MAC specifications only. The jammers targeting the network, transport and application layers essentially constitute DoS attacks (e.g., Smurf attack, TCP/UDP flooding, malware attack, etc.).

Conclusion: In this paper I have presented a survey on need, importance and some of preventive measures for information security in wireless networks i.e. protecting confidentiality, authenticity, integrity and availability of data going through network from malicious attacks. The ranges of wireless attacks that can be launched by attacker are stated here. The existing protocols for providing security against different attacks at various layers, like Bluetooth, WiMax, Wi-Fi, LTE have been reviewed. Physical layer security is also important since wireless transmissions are highly vulnerable due to its broadcast nature. Also different types of wireless jamming attacks have been summarized here in this paper.

References

[1] Yulong Zou, Jia Zhu, Xianbin Wang and LajosHanzo, “A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends”, proceedings of IEEE, vol. 104, no. 9, pp. 1727-1765, Sept. 2016.

[2] Shuang Liang, Yue Zhang, Bo Li, Xiaojie Guo, ChunfuJia, and Zheli Liu, “SecureWeb: Protecting Sensitive Information Through the Web Browser Extension with a Security Token”, Tsinghua Science And Technology, vol. 23, no. 5, pp. 526-538, Oct. 2018.

[3] O. Aliu, A. Imran, M. Imran, and B. Evans, “A survey of self organisation in future cellular networks,” IEEE Commun. Surv.Tut., vol. 15, no. 1, pp. 336–361, Feb. 2013.

[4] H. ElSawy, E. Hossain, and M. Haenggi, “Stochastic geometry for modeling, analysis, and design of multi-tier and cognitive cellular wireless networks: A survey,” IEEE Commun.

Surv.Tut., vol. 15, no. 3, pp. 996–1019, 3rd Quart. 2013.

[5] ITU, “The World in 2013: ICT facts and figures,” Jan. 2013. [Online]. Available: http://www.itu.int/en/ITU-D/Statistics/ Documents/facts/ICTFactsFigures2013.pdf

[6] Symantec Norton Department, “The 2012 Norton cybercrime report,” Sep. 2012. [Online]. Available: http://www. norton.com/2012cybercrimereport

[7] M. Whitman and H. Mattord, Principles of Information Security, 4th ed. Independence, KY, USA: Delmar Cengage Learning, 2012.

[8] Y. Xiao, H.-H. Chen, B. Sun, R. Wang, and S. Sethi, “MAC security and security overhead analysis in the IEEE 802.15.4 wireless sensor networks,” EURASIP J. Wireless Commun.Netw., 2006, doi: 10.1155/WCN/2006/93830.

[9] G. Apostolopoulos, V. Peris, P. Pradhan, and D. Saha, “Securing electroniccommerce: Reducing the SSL overhead,” IEEE Network, vol. 14, no. 4, pp. 8–16, Jul. 2000.

[10] Y. Shiu et al., “Physical layer security in wireless networks: A tutorial,” IEEE Wireless Commun., vol. 18, no. 2, pp. 66–74, Apr. 2011.

[11] Y. Jiang, C. Lin, X. Shen, and M. Shi, “Mutual authentication and key exchange protocols for roaming services in wireless mobile networks,” IEEE Trans. Wireless Commun., vol. 5, no. 9, pp. 2569–2577, Sep. 2006.

[12] Y. Wei, K. Zengy, and P. Mohapatra, “Adaptive wireless channel probing for shared key generation,” in Proc. 30th Annu. IEEE Int. Conf. Comput. Commun., Shanghai, China, Apr. 2011, pp. 2165–2173.

[13] A. D. Wood and J. A. Stankovic, “Denial of service in sensor networks,” IEEE Computer, vol. 35, no. 10, pp. 54–62, Oct. 2002.

[14] H. Huang, N. Ahmed, and P. Karthik, “On a new type of denial of service attack in wireless networks: The distributed jammer network,” IEEE Trans. Wireless Commun., vol. 10, no. 7, pp. 2316–2324, Jul. 2011.

[15] T. Muller, “Bluetooth Security Architecture,” Jul. 1999. [Online]. Available: http://www.afn.org/afn48922/downs/wireless/1c11600.pdf

[16] M. Kui and X. Cuo, “Research of Bluetooth security manager,” in Proc. IEEE Int. Conf. Neural Netw. Signal Process., Nanjing, China, Dec. 2003, pp. 1681–1684.

[17] J. Lee and C. Fan, “Efficient low-latency RC4 architecture designs for IEEE 802.11i WEP/TKIP,” in Proc. Int. Symp.Intell. Signal Process. Commun. Syst., Xiamen, China, Nov. 2007, pp. 56–59.

[18] A. Lashkari, M. Danesh, and B. Samadi, “A survey on wireless security protocols (WEP, WPA and WPA2/802.11i),” in Proc. 2nd IEEE Int. Conf. Comput. Sci. Inf. Technol., Beijing, China, Aug. 2009, pp. 48–52.

[19] D. Johnston and J. Walker, “Overview of IEEE 802.16 security,” IEEE Security Privacy, vol. 2, no. 3, pp. 40–48, Jun. 2004.

[20] D. Astely et al., “LTE: The evolution of mobile broadband,” IEEE Commun. Mag., vol. 47, no. 4, pp. 44–51, Apr. 2009.

[21] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, “Denial of service attacks in wireless networks: The case of jammers,” IEEE Commun. Surv.Tut., vol. 13, no. 2, pp. 245–257, May 2011.

[22] T. X. Brown, J. E. James, and A. Sethi, “Jamming and sensing of encrypted wireless ad hoc networks,” in Proc. 7th ACM Int. Symp.Mobile Ad Hoc Netw.Comput., Florence Italy,May 2006, pp. 120–130.

[23] Campbell, M.A., "The Impact of the Mobile Phone on Young People's Social Life", 2005,

[24]Brandtzaed, P., "Childrens Use of Communications Technologies", Mobile Media and Youth Conference, Copenhagen, 2005,

[25] Valentine, G., and Holloway, S., "Online Dangers:Geographies of Parents Fears for Childrens Safety in Cyberspace",The Professional Geographer, 53(1), 2001, pp. 71--83.