Government College of Engineering Jalgaon

(An Autonomous Institute of Govt. of Maharashtra)

Department of Computer Engineering

A
Report
On

Wireless Networking & Security

Submitted By: Ajinkya Bhausaheb Borate

Submitted To: Prof. S. D. Cheke

Abstract

I intend to survey Wireless Network Security since wireless networks are very common, both for organizations and individuals. Many laptop computers have wireless cards pre-installed. The ability to enter a wireless network has great benefits. However, wireless networking has many security issues. Hackers have found wireless networks relatively easy to break into, and even use wireless technology to crack into wired networks. As a result, enterprises must define effective wireless security policies that guard against unauthorized access to important resources.

My survey research may involve the following aspects: wireless network architecture, data security in wireless networks, secure data storage in wireless networks.

Table of Contents:

1. Introduction:

Nowadays, the Internet becomes the basic need of human life and is used not only for entertainment purposes, but it helps in doing routine activities like fund transfer, paying bills, ticket reservations, educational research, learning perspectives, business trade, media coverage, etc. If we define the Internet in a single line then it should be, “network of networks known as internet”. If we talk about just a network, then what exactly the definition of a network is? Where it came from? So, the answer is: two or more than two nodes (sometimes known as system or computer systems) are connecting to share crucial information or resource. In 1961, Leonard Kleinrock proposed an idea named ARPANET (Advanced Research Project Agency Network) in his research titled “Information Flow in Large Communication Nets” [1]. The term ‘packet’ came in 1965, and it aims to send data from one node to another. In the era of 1969, ARPANET was one of the first packet-switching networks; this was first used for sharing research from Stratford Research Institute at UCLA (University of California, Los Angeles). Bob Kahn invented TCP/IP in 1978; the aim was to route data from one form to another [2]. The first version of the 802.11 standards for WIFI has a transmission speed up to 2Mbps [3]. In 2018, WAP3 introduced WIFI encryption; more security means more protection [4]. The main objective of computer networks is to exchange resources; there are two main types of networks: (1) wired network and (2) wireless network. In computer networks, data exchange through a connection called data link between nodes, establish a link with the help of cable like coaxial, fiber-optics, and twisted pair. In a Wireless network (WLN), the network is set up by frequency signals, and it means accessing the network without a cable connection [5]. It means accessing internet services without a physical connection but in a particular domain (range) for example WIFI (stands for wireless fidelity).

2.Wireless Network Architecture:

The wireless network is the combination of diferent networks, which allow one computer to access another without means of wired connection physically [10]. The authors recommended an energy managing technique named RadioHub for saving energy consumption in Wireless NetworkOn-Chip (WiNOC) architecture. In this type of environment, the physical wired connections are not used; however, in some complex architecture wired cables can also be used. These days the most common wireless communication channels are radio signals in the form of the frequency range. Wi-Fi connections are the most common example of such networks.

Wireless networks are implemented in the physical layer, which is layer 1 of the OSI reference model [11]. Access points are used to establish a network connection in a wireless environment. This access point is a type of hardware device, which detects and permits the network to access remotely. The next hardware device considered as the most essential part of wireless networks is the router device, which provides a physical way to communicate different networks [12].

There are two main types of wireless network architecture, which discussed below: Standalone Architecture (also known as Ad-hoc mode): In Ad-hoc architecture, all devices are directly connected for communication just like peer-to-peer connection [14]. For setting up on Ad-hoc mode, manual confguration is required instead of an automated process, and no access point such as a router/switch is required for communication. Such type of architecture is used in a small environment e.g. a centralized business domain [15]. Ad hoc wireless network architecture illustration is given in Fig. 1 [15]. Centrally Coordinated Architecture (also known as Infrastructure mode): Devices are connected with the help of an access point means a router/switcher is required for communication. Automatically confgure instead of manually handling. Such type of architecture is used in a large environment, e.g. distributed business domain [15]. Centrally Coordinated wireless network architecture, illustration is given in Fig. 2 [15].

3.Wireless Protocols and Standards:

The term wireless refers to the transmission of information through electromagnetic waves rather than a wire. The frst wireless transmitters were used in the early twentieth century by the use of radiotelegraphy in Morse code [16]. Technology keeps evolving and is becoming a very important part of the life of many people. It has caused many people to become reliant on technology for almost all kinds of work. Types of wireless access technologies.

(1) Wireless Personal Area Network (WPAN): These are designed for a range of 10 m. Examples of such include IrDA and Bluetooth. More technologies that are currently on the rise for this system are 802.15.4a—Zigbee and 802.15.3c—UWB [17].

(2) Wireless Local Area Network (WLAN): This system has a range of 100 m and a speed that can cater to up to 200 Mbps. Wi-Fi (802.11a/b/g) is one of the most widely used WLAN technologies [18].

(3) Wireless Metropolitan Area Network (WMAN): This technology can deliver to 75 Mbps. Several iterations of 802.16 have been certifed under a brand called WiMAX [19].

(4) Wireless Wide Area Network (WWAN): This system has a range of a few hundred Kbps and extends services to larger areas such as cities, regions, and even countries. Commonly used technologies are GSM/GPR/EDGE [20]. Third-generation technologies consist of HSUPA and EV-DO Rec C [21].

4.Categorization of Security Issues:

Security categorization is the classifcation of vulnerabilities or threats that the system of information might face in real-time processes. These categories are based on diferent factors such as the potential impact of any event or it could likely be a result of any malpractice of manipulation. It depends on the overall management system of an organization that deals with such issues. There are several risks involved in the categorization of security issues like potential loss or damage or misuse of information.

The important part of security categorization is identifying the various forms of information that the organization process, store and retrieve. In every situation, it is essential to avoid the expected risk and minimize discrepancies. Several standards followed to enlist the threats. These threats sometimes damage the confdentiality of data or its integrity as well. The companies classify their security issues as per their perceived models or sometimes by their functional practices. This can be multiple forms of security weaknesses, amongst all the most common are misinformation, falsifying the statistical information, theft or damage of data, web-based hacking, and internal employee manipulation.

4.1 Threat Classifcations Principles

4.2 Threat intent

- 4.2.1 Intentional Threats
- 4.2.1.1 Intentional Threat in Cloud Environment
- 4.2.1.2 Data Leakage or
- 4.2.1.3 Malpractice of Cloud Resources
- 4.2.1.4 Malicious Insider Threa

4.3 Effects of Threats

There can be plenty of damage happen with information or data.

The common two effects would be the corruption or misuse of data and disclosure of information. The money launderers and smugglers normally do this. The data can be manipulated by mixing it with scripting viruses stored on tapes, hard disks, and other forms of electronic media so that it is completely unreadable and cannot be accessed or used for unauthorized purposes. These threat actions can cause unauthorized use of leakage of perusal or sensitive data.

- 4.3.1 Theft of Service

  Theft of services is the legal term for a crime that is committed when a person obtains valuable services (as opposed to goods) by deception, force, threat, or other unlawful means, i.e., without lawfully compensating the provider for these services [62]. Cloud computing is best for providing fast and reliable services to end-users
- 4.3.2 DOS A denial-of-service (DoS) attack occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor [67]. The authors in their study have followed the systematic methodology to identify the problem, gather information, and conduct a test to validate the performance.

4.4 Elevation of Privilege

Use some illegal means or the use of loopholes in the system to get permission to access, which otherwise was not allowed. Maintaining security is the leading risk in wireless application networks. Access privilege is rendered for normal activities, but it can spot away from exploitation by the attacker.

4.6 Threats by Social Messaging Apps

Major threats that whatsApp and other messaging and social media applications pose for mobiles are:

- Web Malware
- Unencrypted Backups
- Data Sharing with other Apps
- Encryption Vulnerabilities
- Malicious Code

4.7 Social Media Security Risks

Phishing emails, scams, web-based frauds and human manipulation through social networks are the most common security risk that provides fnancial and social damages to society. • Privacy concerns • Information about you that you post.

• Information about you that others post.

• Information about you the social networking sites collect and share with others.

• Leakage of Personal and Professional Information shared with family, colleagues and trusted resources.

• The information may be used for social engineering and committing frauds and forgeries.

5. Wireless Networks Security Challenges:

Security is the primary concern specially when data is transmitting from end to end, it must be secured, and protected.

5.1 Security Requirements or Ethics in Network

5.1.1 Confdentiality Only a receiver must read the transmitted data, and if data is hacked, the hacker cannot read it. The encryption of data is applied for confdentiality purposes [90].

5.1.2 Integrity The transmitted data must be received by the receiver as same as sent by the transmitter without any alteration or modifcation in data.

5.1.3 Availability Network should remain operational at all the time.

5.1.4 Non-Repudiation The sender must accept the transmitted data at all times. For this, Digital Signature should be implemented to achieve Non-Repudiation [91].

5.2 Attack/Threat Types

5.2.1 Active In this type, the hacker tries to modify or delete or append in transmitting data in between the transmission, and impacting on authenticity, integrity, and confdentially of data [92].

5.2.2 Passive In this type, in this type, the hacker can view the data without updating it, and it is impacting confdentiality.

5.2.3 Insider When any point is compromised, and from this point, data is captured and execute the malicious program/script.

5.2.4 Outsider In this type, there is no access, it is just captured the data, which is transmitted.

6.Security Solutions of Wireless Networks:

In the previous section, we have addressed some security issues, and the main threats to produce, change, and intercept. Many safety measures that resolve security threats are below.

6.1 Encryption The organization can use various encryption methods. It is one of the safest ways to protect the information transmitted over the network. For regulatory organizations, symmetric key encryption and asymmetrical key encryption methods are important [102].

6.2 Securing Wireless Access Point In violating network security, unauthorized installed wireless connections play an important role. By taking the following countermeasures, the organization can reduce the risk of these types of access points:

(1) Remove rogue access points

(2) Default confguration must be updated i.e. the permitted access must be done safely.

6.3 Minimize the Risk of Denial-of-Service Attacks The problem areas may be detected through routine wireless networking audits; removal of ofending devices may reduce the risk of DOS attacks [103].

6.4 Techniques of Signal Hiding Attacks need wireless networks to be located and identifed. The SSID is an identifcation number broadcast by APs. The SSID is a network identifer. If he/she knows the SSID code, STAs cannot access the network. Therefore, we should turn the SSID transmission of when, not in use and allocate cryptic names to SSIDs to prevent the network [104].
6.5 The Secure use of the Wireless Network

(1) Firewall Technology

(2) Encryption and Decryption Technique

(3) Don't Access Public Hot Spots

6.6 Soft Computing Techniques Soft computing and its related methodologies are new; therefore, they can extend in various felds.

6.6.1 Artifcial Neural Network ANNs are non-algorithmic neuron systems inspired techniques used in non-linear wireless applications. It makes the system efcient and reliable than traditional linear procedures by its ANN communication. [105].

6.6.2 Fuzzy Logic It is a rules-based system to address a variety of wireless network problems. We stress the need to control confusion and ambiguity when working with wireless networks. Fuzzy logic thus ofers an uncertain device structure that is hard to examine [106].

6.6.3 Genetic Algorithm This soft computing approach is genetically engineered and natural. A genetic algorithm is a very effective tool to deal with multifaceted wireless network optimization needs

7. Conclusion:

In this paper, we surveyed and reviewed security issues and threats, which are used to hack the data of the client and make the network untrustworthy. We review different protocols, security issues, and their solutions, proposed through research to overcome the security issues of WLAN. WLAN protection is a system that is constantly changing when running on OTA and exposed quickly to a group of hackers we have raised different wireless network security issues. These security approaches in an organization are fairly good and easy to implement. Soft Computing is an emerging field and a forum for the detection and prevention of intrusion into networks and other attacks. We have discussed open research issues, which led the researcher to the development of a better security mechanism for WLAN.

8. References

1. Bay M (2019) Hot potatoes and postmen: how packet switching became ARPANET's greatest legacy. Internet Hist 3(1):15–30

2. Cerf VG, Abbas AE (2019) Internet, technology, and the future: an interview with vint Cerf. Next-generation ethics: engineering a better society. Cambridge University Press, Cambridge, p 54

3. Yalda E, Obraczka K, Amiri B (2018) A machine learning approach for dynamic control of RTS/CTS in WLANs. In Proceedings of the 15th EAI international conference on mobile and ubiquitous systems: computing, networking and services, pp 432–442

4. Al-Mejibli IS, Alharbe NR (2020) Analyzing and evaluating the security standards in the wireless network: a review study. Iraqi J Comput Inform 46(1):32–39

5.Google, ChatGPT