International Journal of Combined Research & Development (IJCRD)
eISSN:2321-225X;pISSN:2321-2241 Volume: 12; Issue: 6; June 2023

WI-FI Attacker using IOT Device

AISHWARYA.S [1] , SANTOSH.S.G [2]

[1], MCA Final Year , [2] Associate Professor

[1,2] Dept. of MCA,JNNCE, Shivamogga, Karnataka , India

Email [1] aishwaryaachar888@gmail.com

Abstract : As technological developments, novel risks appear, creating true hazards to users. In recognition of their predisposition connected devices have become a popular target for thieves on the internet. Even enabled the dynamic nature of IoT networks, advancement is tough Protection mechanisms based on norms. This research effort examines denial of service (DoS) in a network using Wi-Fi. The venue is a dwelling with various IoT objects hooked up to the internet through the 802.11 Wi-Fi protocol. The potentially hazardous scenario is a deauthentication threat. Deauth (DoS) tactics directed towards wireless networks based on the 802.11 standard. Whenever an end-user wants to disconnect from a wireless access point, it conveys deauthentication or alienation frames. Recognising that these frames have been secured, no licensed user is required. As a result, a malicious user might generate those structures and distribute them to the access point in such a way that the access point perceives they are from the victim rather than the assailant.

Keywords : Deauth, Beacon, Cybersecurity, Penetration.

1.Introduction

Due to the fact that a staggeringly huge number of gadgets, including smartphones, laptops, tablets, IoT devices, etc., support IEEE 802.11 wireless networks, they have become among the most popular networks. Wireless networks are susceptible to unauthorised access and probable assaults unless specific precautions are taken, in contrast to cable networks where intercepting sent information requires physical access and is not conceivable. For wireless networks, the passive access comes naturally. Attackers can readily target wireless devices since the Wi-Fi network cannot stop users

from "listening" to traffic being broadcast and offers the chance to capture and examine packets. Consequently, a hacker has complete freedom to access the system and intercept information.

Long-term research has been conducted on IEEE 802.11 security techniques and Wi-Fi vulnerabilities. However, the need of security has not diminished, and continued investigation into the IEEE 802.11 standard's flaws is required to stop more violations.

This article discusses a deauthentication assault, one of the many attacks that Wi-Fi networks are vulnerable to because of flaws in the IEEE 802.11 standards. Deauthentication attacks are Management frame attacks, which are denial-of-service (DoS) attacks against one or more users. The Administrative frameworks are significant system data packets that are used to regulate how stations and access points communicate with one another.

2. System Framework

There are three types of frameworks:

1. Administrative frameworks
2. Managing frameworks
3. Information frameworks

The Administrative frameworks are used to control and monitor the operation of a wireless network. They include frames that are used for authentication, association, disassociation and deauthentication. It is responsible for ensuring the interaction Control frames are used to manage the flow of data between wireless devices. They include frames that are used for requesting data, acknowledging data and controlling the transmission of data.

Information frameworks are used to carry user data over a wireless network. They include frames that are used to transmit information such as emails, files and web pages between devices.it contain actual data received from the network layer.

Information frameworks are transmitted over the network in encrypted form but management frames are not transmitted in an encrypted form.

because of 802.11 Administrative frameworks posed to lack of encryption they are vulnerable to various threat like deauthentication attacks. By this an attacker could take advantage of this vulnerability and mislead the MAC address of devices, mimic a client or access point and starts to send deauthentication requests. The frames are accepted as coming from new device and connection that is established prior is broken.

Therefore, a dos attack is a one of the censorious attack that disturbs the client’s transaction.

After a successful attack, the client station disconnects from the wireless network and cannot reconnect until attack stops.

A specific channel can also be targeted by performing a DoS attack on multiple users simultaneously.

3.Problem statement

In the area of wireless communication, the deauthentication assault is regarded as one of the most potent DoS attacks, but it is also one of the trickiest to precisely diagnose. The purpose of the work is to conduct a realistic investigation of the client-AP interaction during frame exchange under normal circumstances and during a DoS attack.

The following assignments have been made in order to fix the issue.

1. Use of a deauthentication attack in practise.
2. Frame analysis to look for irregularities during the attack.
3. Creating an algorithm to identify deauthentication attempts.

4.related work

This topic addresses the literature review that addresses the resources that support the topic chosen for the construction of the research project. Following a brief discussion of WiFi networks, the Internet of Things, information security, and security policies, a description of the terminology of Denial of Service (DoS) Attacks is provided.

4.1 Information Security

The definition of computer security has evolved over time, but according to Guttman and Roback (1995), it is a set of guidelines, procedures, and tools used to protect a system's resources, including its hardware, software, firmware, data, and communications, as well as its integrity, availability, and confidentiality.According to Landwehr (1981), security is violated when confidentiality, availability, and integrity are not verified.According to De Moraes (2010), the following rules regulate the foundations of information security:

- Integrity is the guarantee that the data has not been altered during transmission or storage and has therefore stayed unaltered.
- The method by which the communication is kept secure so that unauthorised users cannot access it is known as confidentiality. The message's contents are only known to the sender and receiver.

- Availability is the guarantee that security measures are in place to keep the system accessible and that users can access it at all times.

4.2 Dos(denial-of-service)

- Initial Internet denial-of-service assaults were recorded in the first few years of the 1990s. It is attempting to prevent legitimate users from obtaining specific features on an equipment or the system, even when the machine, system, or network makes those assets or amenities available (denial-of-service, or DoS) (Kumar & Selvakumar, 2011).
- Denial of service is an example of a wireless network vulnerability used by Kuncheva (2004) because it makes it simple for an attacker to bombard an access point with specially designed protocol messages intended to use up system resources.

  Because they interfere with network function by utilising a variety of techniques in an effort to prevent the network from being able to supply services, denial of service attacks are conceptualised as a common destructive attack technology (Augusto Filho, 2021).

  Distributed assaults pose a serious risk to the service, even when the targets are major multinational conglomerates. Denial of service attacks on certain well-known websites, including CNN.com, Yahoo, eBay, Amazon.com, and Amazon.com, have been successfully carried out (Garber, 2000). While attempting to handle the traffic created by the attack, the victim simply stops providing services to real clients.

4.3 Iot(Internet of things)

The Internet of Things (IoT), which allows common objects or "elements" to interact with one another and react to instructions regardless of time as they remain linked, is increasingly viewed as an extension of the internet (Santos et al., 2016).

These devices not only gather but also distribute information. The widespread availability of internet connectivity and low-cost CPUs has permitted the transformation of many physical objects into IoT devices. Their fundamental pillars are personality, which includes the distinctive recognition of objects in order to connect them to the network; indicators, which collect and store pertinent information about included objects; connections, which include technologies to join intelligent objects; processing data, which involves computing units; amenities, which constitute the Internet of Things and can differ depending on the amenities offered; and linguistics, and these refers to the language used for dealing with the objects.

Leading IT firms and governments around the world are now paying close attention to the IoT as a serious security issue. Figueira (2016) contends that IoT privacy is a concern that has to be handled

carefully. It's critical to match functionality and privacy needs at various points in the creation and operation of IoT products since lots of these individuals are intended to gather environmental information obtained from a smart device interconnection. Local storage or cloud storage will be used for this data. As a result, it is important to secure any personal or sensitive data that may be at risk.

4.4wifi-network

One of the most popular network technologies for Internet access is a Wireless Local Area Network (WLAN). Present in areas including businesses, residences, universities, hotels, and airports, it is anticipated that, like the mobile phone network, it will soon be accessible everywhere.

Numerous wireless network technologies were created in the 1990s, but IEEE 802.11, often known as Wi-Fi, unquestionably gained the most popularity (Kurose and Ross, 2005).

A simple local home network often comprises of PCs or other mobile devices that may access the internet and a router that receives the signal from a broadband modem (Jobstraibizer, 2010). It can serve as an extension since it is flexible.

Risks are conceptualised depending on the harm they create when a vulnerability is exploited (Stoneburner et al., 2001). They may be located and diminished, but they cannot be entirely done away with.

According to and Geus and Nakamura(2007), flaws in an infrastructure or network manifest as as a consequence of poor design or delivery of a product, norms, or piece of application. These software will continue to have faults even after they have been patched.

Some types of assaults are more prevalent than others, as pointed out by Landwerhr (2001).

• Denial of service attacks (DoS): overwhelm the machine with repeated requests, preventing the system from responding to any queries.

•.Port scanning: its goal is to find network amenities that are out there, programming versions, software systems, while there's is a barrier in the way, as well as additional information.

• Deception sites gather financial information from clients by impersonating legitimate websites.

According to Wadlow (2000), acquiring a piece of hardware or software that would completely safeguard a network is challenging since security is contrasted to a path where the objective is stability itself. Risk management is essential as a neutralising method because the expedition has no result.

Because criminals use cutting-edge methods to hide their identities and avoid being caught, digital crimes are only increasing in quantity and in the manner in which they are structured (Nakamura and

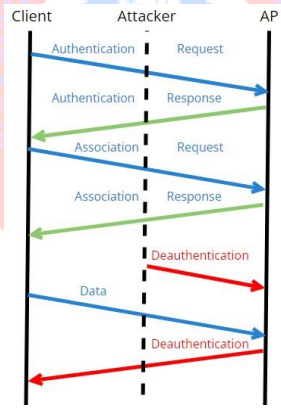
Geus, 2007).

A set of specified guidelines known as a "security policy" is developed in order to maintain the security attributes of the system (Landwerhr, 2001). The aforementioned serves as a foundation for determining what is and isn't permitted (Bishop, 2003).

Spafford et al. (2003) distinguish between two alternative security policy implementation models: A pattern of denial seeks to identify only what is permitted and denies everything else, whereas a pattern of permission seeks to identify only what is prohibited and permits everything else.

Physical security, management security, and logical security are the three categories into which security policies are broken. Physical security advocates preventing unauthorised access to the system's physical resources. While the management security policy is in charge of outlining the procedures for developing and maintaining security policies inside an organisation, The description of users with access rights to the system and the nature of those rights are elaborated in the logical security policy (Landwerhr, 1981).

5.Working of deauthentication attack



1.Sniffing network traffic or recording handshakes: To get the essential details about the target client device, the attacker first records the four-way handshake between a client and the access point (AP).

2. Forging deauthentication frames: The attacker creates and sends deauthentication frames with the MAC address of the AP or the targeted client device using specialised tools or software. These frames are delivered using the AP's machine address or a forged Ethernet address to make it appear as though they come from the AP, and they appear to be authentic.

3. Flooding the network: The assailant fills the network by sending a substantial amount of deauthentication packets repeatedly or quickly. The target client device is overloaded by this influx of

deauthentication frames, which causes it to lose connection to the Wi-Fi network.

4. Effect on the target device: When the forged deauthentication frames are received by the target client device, it interprets them as authentic disconnect requests. The device disconnects from the network as a result, and it can then try to reconnect. However, the device can find it difficult to maintain a steady connection because of the continuing deluge of deauthentication frames.

5.Using the flaw: The deauthentication attack makes use of a flaw in the 802.11 protocol, notably the absence of authentication or encryption for deauthentication packets. Due to the lack of authentication in these frames, any nearby device is able to send them, making it simple for an attacker to create fake deauthentication frames and send them.

It's crucial to remember that deauthentication assaults might be used maliciously to facilitate other attacks, interrupt network connectivity, or carry out unauthorised monitoring. Network administrators can put countermeasures in place to defend against deauthentication attacks, such as installing wireless intrusion detection systems (WIDS), turning on encryption technologies like WPA2 or WPA3, and keeping an eye on network traffic for odd patterns or high numbers of deauthentication frames.

6.Research method

6.1 penetration test phase

a)strategy and investigation

• establishing the scope and goals of the experiment, covering the systems to be tested and the procedures to be used;

• Harvesting data to understand concerning a desires processes and potential flaws (e.g., system and web addresses, smtp server)

b)inspection

The following step is to define how the envisaged programme will respond to specific violations. Typically, this is done by:

• Fixed inspection: Analysing a program's source code to determine how it will operate when implemented. These instruments are capable of examining the entire code in just one pass.

• Runtime inspection: Examining a program's code while it is running. This sort of monitoring is more helpful because it records an application's behaviour in real time.

c)attaining entry

Using web application attacks such as cross-domain scripting, query injection, and backdoors, this approach determines a The recipient's vulnerabilities. To understand the possible harm that these weaknesses may create, researchers attempt to exploit them, usually by increasing their authority, collecting data, recording conversations, and so on.

d)retaining privilege

The purpose of this stage is to evaluate if the flaw can be utilised to generate a persistent footprint that is operable for an adequate amount of time for a hostile actor to get comprehensively access. To extract the most sensitive information from a company, sophisticated continuous assaults are employed, which may get stuck in a system for months.

e)scrutiny

The results of the penetration test are then put into a paper that includes a variety of data. • The specific flaws that were disclosed; • Obtaining proprietary data; and • the duration in which that the pen tester was able to remain concealed in the network.

2.penetration test tools

a) Software for network analysis and intercepting packets:

A device that sniffs packet is an object of software or physical equipment that examines network data transfer. It is sometimes referred to as a protocol analyzer, network analyzer, or packet analyzer. These devices examine data packet streams that go between connected computers as well as between linked machines and the larger Internet.

b) intruder tactics

Employing the ESP8266 module, NodeMCU tools, and Lua programming, It is a connected device deauthentication demonstration device.

c)router:

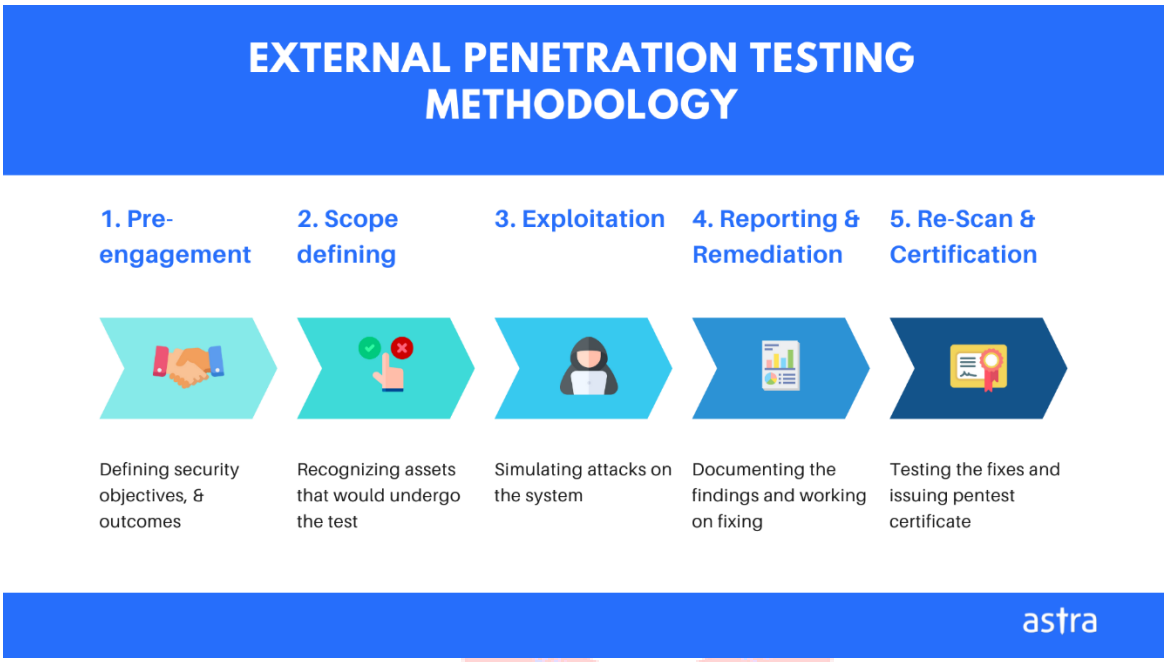
It is a communication device with a transponder and an antenna that broadcasts and receives

signals from distant clients through an 802.11 standard wireless network while also giving internet access to consumers.

d) target :the device used in IP.

3.external penetration test:

A definition of the scope and depth of external penetration testing must be established. It is necessary to make the necessary informational and practical preparations.



7.conclusion

Although there are various advantages to using the context of wireless networks, one must not overlook the negatives, one of which is protection. As a result, although we have to take actions to keep personally secure, we must all work together to sufficiently protect the technology on which we trust.

This paper examined basic wireless network ideas along with IoT devices used in conjunction with the Wi-Fi network, and illustrated the susceptible components via a deauthentication operation. Because wireless networks have benefits over wired networks in terms of portability and ease of equipment deployment, they are more vulnerable to assaults since the signal's range cannot be totally controlled.

8.References

[1] "Impact of metric selection on wireless deauthentication DoS attack performance," IEEE Wireless Communications Letters, vol. 2, no. 5, pp. 571–574, 2013. J. Milliken, V. Selis, K. M. Yap, and A. Marshall.

[2]M. Bogdanoski, P. Latkoski, and A. Risteski, "Analysis of the Impact of AuthRF and AssRF Attacks on IEEE 802.11e-Based Access Points," Mobile Networks and Applications, vol. 22, no. 5, pages 834–843, 2017.

[3] T. Khalil, "IoT security against DDoS attacks using machine learning algorithms," International Journal of Scientific and Research Publications, vol. 7, no. 6, 2017, pp. 739–741.

[4]E. Oriwoh and G. Williams, "Internet of Things: The Argument for Smart Forensics," Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance 2015; USA: IGI Global; p. 407–423.

[5]P. Thornycroft [4] (2016) Internet of Things Wi-Fi connections might be challenging. [Online]. accessible at bit.ly/3cv2UqI.

[6]"Smart security of IoT against DDOS attacks," International Journal of Innovative Engineering Applications, vol. 2, no. 2, pp. 35–43, 2018. A. Efe, E. Aksoz, N. Hanecio, and S. N. Yalman.

[7]"Security issues in the Internet of Things (IoT): A comprehensive study," International Journal of Advanced Computer Science and Applications (IJACSA), vol. 8, no. 6, pp. 383–388; M. A. Razzaq, S. H. Gill, M. A. Qureshi, and S. Ullah.

[8] "A comprehensive IoT attacks survey based on a building-blocked reference model," International Journal of Advanced Computer Science and Applications, vol. 9, no. 3, pp. 355–373, 2018. H. A. Abdul-Ghani, D. Konstantas, and M. Mahyoub

[9] "Performance study of 802.11 w for preventing DoS attacks on wireless local area networks," in Wireless Personal Communications, vol. 95, no. 2, pp. 1031–1053, 2017.

[10]What changes from ubiquitous computing to the Internet of Things in interaction evaluation? R. M. Andrade, R. M. Carvalho, I. L. de Araujo, K. M. Oliveira, and M. E. Maia, International Conference on Distributed, Ambient, and Pervasive Interactions, 2011. Springer, Vancouver, BC, Canada, July 9–14, 2017, pp. 3–21.