Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 04, April-2021

Public Wi-Fi: The Untold Story

Serin F
Department of Computer Science
Al Azhar College of Arts and Sciences
Thodupuzha, Kerala, India

***Abstract*—While living in this well-advanced world, it is pretty much necessary to know how much secure we are and how can we make ourselves more secure. Almost everyone can see a physical attack done by someone and it can be prevented or we can escape from that attack somehow, using not much effort. But in the case of a cyber-attack, it is very difficult to even understand whether we are attacked or not. It is not because of the complexity of the architecture of technology, but because of the lack of knowledge. In this paper, we will be discussing about one of the most dangerous attacks, Man-In-The-Middle attack, which is a network attack. This attack is that much dangerous so that an attacker doesn't need the victim to install or click on anything, but only needs to connect in the same network.**

Keywords— MITM, ARP cache poisoning, TCP, SSL, Tunneling, Different types of spoofings and poisonings

I. INTRODUCTION

Almost everyone in this world is using internet and almost 75% of youths and officials are using wi-fi networks to connect to internet. So many are using the free public wi-fis and they are also even ready to connect with any freely available wi-fi. This is just because of the lack of knowledge about the traps that are hidden behind these glittering papers. An attacker can almost fully compromise a system connected in his network, without much effort. He just need the victim to be in the same network. It is almost 35% of the total cyber-attacks done around the world[1]. MITM attack is also a type of eavesdropping attack. Eavesdropping is stealing information that are communicated in a network[2].

III. TYPES OF MITM ATTACKS

Most commonly there are 3 types of MITM attacks that are done by an attacker in a network They are listed and explained below:

A. ARP CACHE POISONING

ARP CACHE POISIONING is a type of man in the middle attack in which the ARP cache is controlled using false packets to the router. Address Resolution Protocol (ARP) is a protocol used in networking for connecting basic identification of MAC address and other device details to identify the user[4]. In ARP poisoning, the attacker sends altered ARP packets through the LAN and it will sync the MAC address of the attacker with another host. An illustration on the process of ARP CACHE POISONING is shown in figure 1.

II. HISTORICAL BACKGROUND

Man-in-the-middle attack is considered to be noted in 1984, by the Royal British Intelligence (also known as MI-6) during the World war II by intercepting the German militaries radio communication system. The first talk regarding MITM was made by Mr. Leslie Lamport in the year of 1981. It is understandable from the sentences given above, the attack done during the WW II in 1984 by the Royal British Intelligence, was the result of the researches done over the talk given by Mr. Lamport[3]. But he may not have thought that this attack could be one of the main attacks done by hackers to do notorious things. MITM is considered to be the second most common attack, just after phishing attacks.

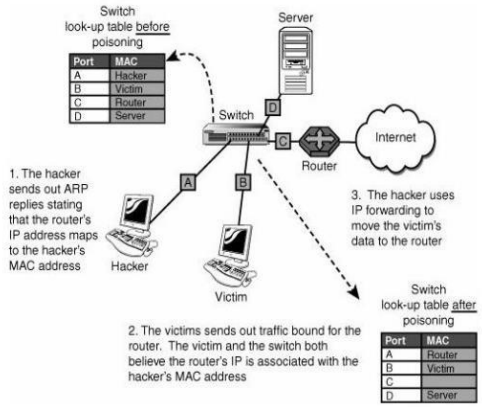


Figure. 1: Process of ARP CACHE POISONING

The process of ARP CACHE POISONING is so much sophisticated and it pretty much difficult to identify since the attacker successfully compromises the router and fakes the router that the router ip is associated with the attacker's MAC address.

B. DNS SPOOFING

Domain Name System (DNS) is a conventional naming system and a method used for converting a hostname into computer friendly ip-address. DNS actually converts domain names into ip addresses. DNS cache can be considered as a temporary database, in which the list and details of the recently visited websites are stored. The router has DNS server address stored, so that it asks the DNS server for the ip address of that hostname. The DNS server finds the ip address that belongs to the hostname you searched and then is able to understand what website you are asking for, after which your browser can then load the appropriate page.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 04, April-2021

DNS spoofing is done by injecting a forged DNS entry into the DNS server. All the users in the network will be using this forged DNS instead of the original DNS. This will be continued until the cache expires. An illustration of the DNS spoofing attack is shown in Fig 2.

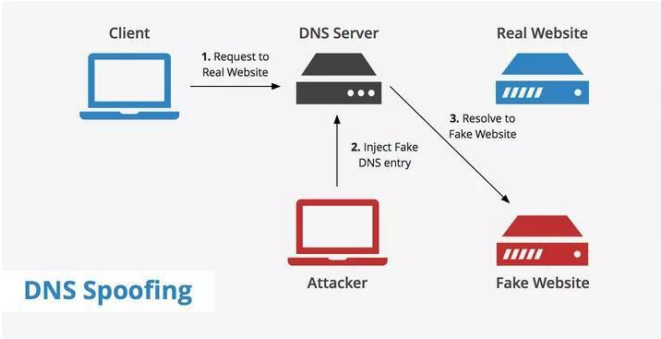


Fig 2: Process of DNS spoofing[5]

In the DNS spoofing process, the attacker creates a fake website and the DNS server cache is poisoned so that every hostname that is requested to search by the client is resolved to the fake website hostname and thereby, attacker gains the supreme authority over the data communicated by the client over the network.

C. *SESSION HIJACKING*

Session is started when there is a connection between client and server. In TCP this can be performed by taking over the TCP session. In OSI Model this attack can be executed on two layers: application layer and network layer. On application level the attacker can get access to session ID by gaining control over http session and on network level, the attacker intercepts the connections and gains access to the packets exchanged between client and server. An illustration of the SESSION HIJACKING attack is shown in Fig 3.

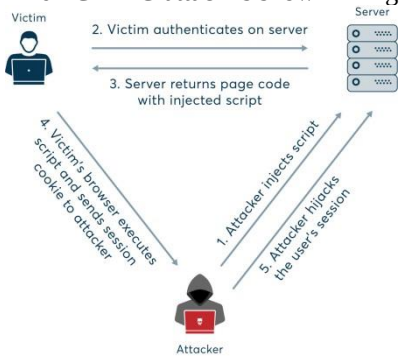


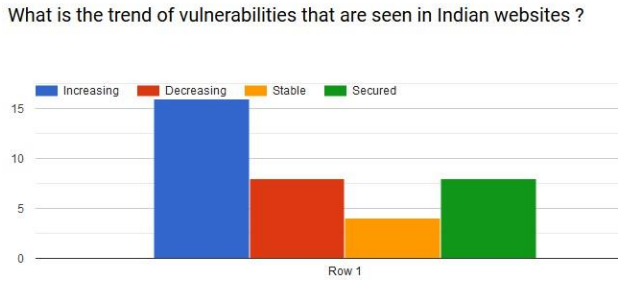
Fig. 3: Process of session Hijacking

IV. RESULTS AND DISCUSSIONS

No one can come into a conclusion without making perfect surveys on the research topic. Therefore, a survey was done among 100 students from different colleges and the results are mentioned. Another survey was also conducted among 50 cyber security professionals around the world and the inferences made from the survey are also included.

For collecting samples, a questionnaire of about 10 questions were prepared and distributed. The survey lasted for two days.

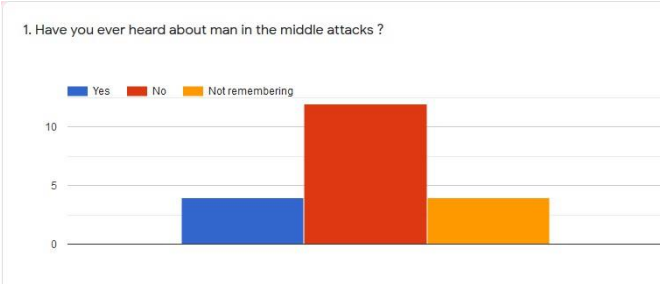
In order to know the present condition of the Indian websites, we also asked a question on the trend of vulnerability found in Indian website. The graph of the result is given below.



Graph 3: Trends of Vulnerabilities

The graph says that the trend of vulnerabilities seen in Indian websites are increasing. From the graph, 44% of hackers says that the trend of vulnerabilities in Indian websites are increasing and 22% of hackers says that the trend of vulnerabilities found in Indian websites are decreasing while
11% says that the trend of vulnerabilities in Indian websites are neither increasing nor decreasing and 22% says that the Indian websites are secured.

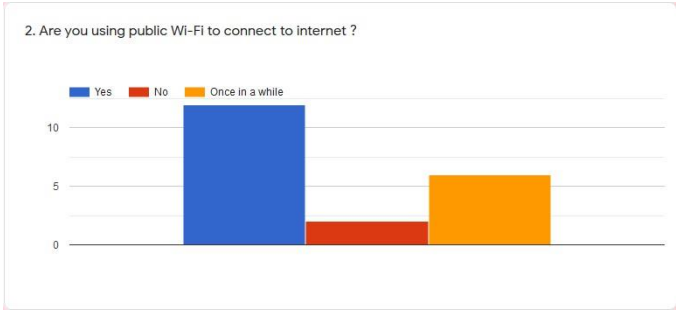
In order to know the number of youths who heard about MITM attacks, a question was asked and 20 random responses were taken. The graph of the same is given below.



Graph 4: Awareness about MITM

The graph says that almost 11 among 20 students are unaware about the dangerous sides of connecting to a public network. Which means, almost 55% not even heard about MITM attack.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 04, April-2021



Graph 5: Public wi-fi usage

The above graph shows that almost 55% of youths are relying on public wi-fi hotspots to connect to internet on a regular basis and almost 30% of users are connecting to public wi-fi hotspots, once in a while. This shows the importance of the awareness regarding network-based attacks.

The increased number of public hotspot users are favoring the attackers to steal more reliable data, without being noticed and more reliably.

CONCLUSION

From the study conducted as a part of this paper, it has been clear that almost 55% of the public wi-fi users are not aware about the dangerous sides of using the same. An attacker invaded into a network can easily monitor, steal and alter the data transferred over the network. The data packets thus captured can also be saved and reused by the attacker for malicious purposes.

Most of the universities having a computer science training syllabus or a degree course in computer science, almost all the topics related to networking are being trained and taught. But the fact is that, almost none of the universities are giving awareness about the problems that can be faced while using a public network. Even though so many defensive techniques are being taken to prevent the network-based attacks, it is to be noted that, the number of network based attacks are getting increased.

ACKNOWLEDGEMENT

As the work had come to an end, would like to thank all those who have helped me during the study period, especially my colleagues, students, friends and all those who supported and guided me. I would like to thank them all from the bottom of my heart for helping me to make this research a fine product.

REFERENCES

[1] Kapil M. Jain , Fr. Conceicao Rodrigues College of Engineering; Manoj V. Jain, Fr. Conceicao Rodrigues College of Engineering; Jay L. Borade, Fr. Conceicao Rodrigues College of Engineering
[2] https://en.wikipedia.org/wiki/Address_Resolution_Protocol
[3] Mallik, Avijit & Ahsan, Abid & Shahadat, Mhia & Tsou, Jia-Chi. (2019). Man-in-the-middle-attack: Understanding in simple words. 3. 77-92. 10.5267/j.ijdns.2019.1.001..
[4] V. Nithya,,R.Regan, J.vijayaraghavan, “A Survey on SQL Injection attacks, their Detection and Prevention Techniques”, International Journal Of Engineering And Computer Science(IJECS), Volume 2 Issue 4 Page No. 886-905, April, 2013
[5] https://www.keycdn.com/support/dns-spoofing
[6] Leo Joy, Bijimol T.K, 2019, Sqli and Indian Websites:Unmasking the Truth, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) NCACCT – 2019 (Volume 7 – Issue 05),