International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 04 | Apr-2018 www.irjet.net p-ISSN: 2395-0072

A Survey on Wi-Fi Security Techniques

Radhi S Nair[1], Prof. Ashok Babu[2], Dr. Vinodh P Vijayan[3]

[1]M.Tech Student, School of Computer Sciences, MG University, Kottayam, Kerala, India
[2]Assistant Professor, School of Computer Sciences, MG University, Kottayam, Kerala, India
[3]Associate Professor & Head of the Department, Department of Computer science &Engineering, Mangalam College of Engineering, Ettumanoor, Kerala, India

---

Abstract – *The Wi-Fi network access is highly important, and it is a easy way to get internet freely. Billions of people over the world browsing Wi-Fi in their homes and business, for net browsing, CCTV, embedded systems etc. But also we can share our personal information through Wi-Fi. So that Security is an important factor in Wi-Fi consumption. There is few existing tool for protection. But these are not effective. So there is a urgent need for light weight solution. In this paper, the specified survey on several Wi-Fi Security methods makes a introduction of new solution for Wi-Fi security*.

Key words: Wi-Fi, rogue AP, Sniffing, fog computing

I. INTRODUCTION

Technology is making rapid progress and is making many things easier to do. As the innovative thinking of person is increasing day-by-day. Wi-Fi technology continuous to develop, the potential to improve ourselves and our society steadily increases. Wireless fidelity enabled computers send and receive data indoors and outdoors anywhere within the range of the base station. People use Wi-Fi with all different electronic devises. This causes a wide network in a small area. This will lure attacker attention. There are many devices uses Wi-Fi that communicate virtually .Our society has its control over things easily, and helps people get answers online quickly. Wi-Fi is alternative network to wired network which is commonly used for connecting devices in wireless mode. Wi-Fi simple and cost effective way to connect to internet without need of wires. I t is growing in popularity because of decreasing costs and the freedom it gives to users

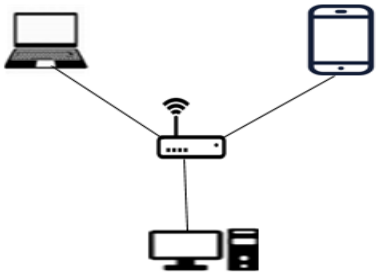

Fig. 1 Wi- Fi model

Our personal information's can be transferring through the Wi-Fi, like banking details with password, organization information's etc. Hackers can easily intercept wireless network traffic over open air connections and extract information like passwords and credit card numbers. Now a day's security is most complicated in Wi-Fi. There are lots of software can be downloaded online, these technique can be using attackers for hacking. There are mainly three types of Wi-Fi attack: Rogue access points, Sniffing and Deauth attack. Currently, there is few existing tool for protecting all procedure while users using Wi-Fi. But these are not effective. Wired equivalent privacy (WEP), Wi-Fi Protected Access (WAP) these are security mechanism for Wireless Lan. WEP and WPA use easy way to encrypt the data, which can be hack in a very short time. [5] In this case here we would like to introduce new Wi-Fi security software system known as "ultimate Wi-Fi security software system". It consist mainly three modules, to protect user from security threats during before connection, connection, after connection.

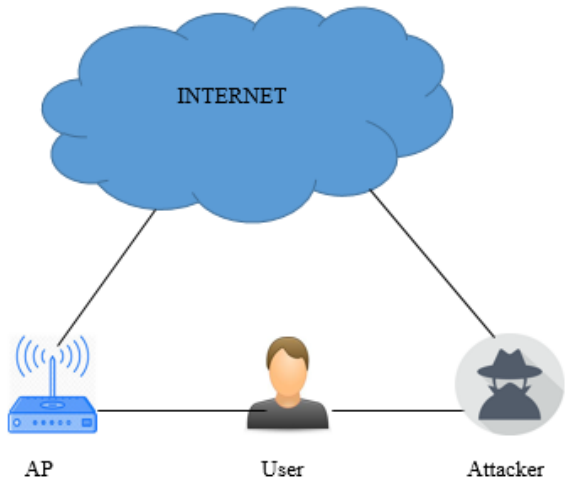

Fig. 2: Wi- Fi attack model using AP

The Wi-Fi security is most important one. There are lots of researches based on Wi-Fi security issues. So we are preparing a survey on Wi-Fi security techniques

III. LITERATURE SURVEY

Linsong Cheng and Jillang Wang introduce an automatic user identification approach using signals on Wi-Fi APs. Wi-Fi APs can be used by any user who wants our personal information such as bank detail, credit card numbers, and other privacy information's. It leads to leaking of personal information and may slow down network speed and make many problems in case of authorized peoples. Generally we used passwords for APs securities. But these password can be easily cracked. This happen mainly Because of many cracking software are available and automatic password sharing software are available. So automatic user identification becomes more important. [1] In this case introduce Ni-Fi (Non-intrusive User Identification for Mobile Devices Using Wi-Fi Signals). It will find legitimate users and undesired users. It uses physical signal information from users, which will difficult to attackers. The Aps require user to set a white and black list based on MAC address. Ni-Fi can be deployed on most COTS Wi-Fi routers. I t will provide secure AP environment .This method have some issues, users localization difficult to obtain .Now a days high level cracking software's generated by data thief's for AP's cracking.

Salvatore J. Stolfo [2] introduce new method for cloud computing security. Cloud computing rises the performance and also have some disadvantages like data theft & various attacks. It will enables confirming whether data access is genuine when anomalous information access is detected. It will confusing the attacker with fake information and generate decoy file. When unauthorized user is detected it provide OTP system at the user level. This method can be considered fully differentiable, if a real user will always secured at this task. Monitor data access in the cloud and detect abnormal data access pattern. Prevent real sensitive customer data from fake worthless data.

In [3] introduce traditional wireless security method such as WEP and WPA. IEE 802.11 introduce wired equivalency privacy .It is the original wireless security standard for Wi-Fi and is still commonly used on home computer networks. WEP key used for authentication and encryption. This WEP key can be cracked in short period of time. WEP key stored on device. This is a problem if the device is stolen or otherwise accessed without permission. It is stands for Wi-Fi Protected Access .This standard was developed to replace WEP. It uses temporary key integrity protocol and advanced encryption standard. Once a device connects to a WPA network, key are generated via a four–way handshake that takes places with the access point and device. [6] WPA 2 offer a higher level of security than WPA because AES offers stronger encryption Temporary key integrity protocol .WPA2 uses CBC-MAC .each client has their own key and each packet is encrypted with a unique key. But these are not effective, there are lots of software can be downloaded online which can be hack in a very short time.

Chrishtoph Neumann [4] proposed device fingerprinting for intrusion detection and provide prevention of medium access control address spoofing .In case of open wireless networks like hotspots often implement MAC address based access control in order to guarantee that only trusted client station connect. The attacker can be cracke mac address and also prevent rogue access points, it will stop fake AP connection. The attacker open his Wi-Fi in public place or somewhere. There is actually available a public Wi-Fi. The attacker put his Wi-F name same as available public Wi-Fi's. The people connect more chances to attackers Wi-Fi because it have may be full range, so in this case the people cheated. This technique stop the rouge APs attacks. This method takes five network parameters can be captured with a standard wireless card. Using a generic method to calculate a signature of a device.

Wi-Fi based gesture recognition system proposed by Heba Abdelnasser. This Wi-Fi based system are based on analyzing the changes in characteristics of wireless signals. It doesn't need additional sensors. Thus eliminate the requirement of calibration and special hardware .This method uses Wi-Fi RSSI to detect human hand motions around user devices

III. CONCLUSION

In this survey paper describes many methods of security technique in Wi-Fi and specifies advantages of these methods. We have done a survey on methods such as AP security for Wi-Fi, Fog computing, traditional Wi-Fi security methods. Wi-Fi security is most important in our global. Because we need to secure our personal information's transferring through Wi-Fi. So we need a light weight solution for Wi-Fi security.

REFERENCES

[1] Linsong Cheng, Jiliang Wang , "How can I guard my AP?: nonintrusive user identification for mobile devices using WiFi signals", Proceedings of the 17th ACM International Symposium on Mobile Ad Hoc Networking and Computing, Paderborn, Germany , July 05 08, 2016. P91-10

[2] Salvatore J. Stolfo, Malek Ben Salem, Angelos D. Keromytis." Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud." EE Symposium on Security and Privacy Wo.2012.

[3] Rob Flickenger, Roger Weeks," wireless hacks wireless hacks: 1100 Industry Most Sharp Tips and Tools", Tsinghua University Press, 2007

[4] Christoph Neumann, Olivier Heen, St'ephane Onno, "An empirical study of passive 802.11 Device Fingerprinting", in 2012 32nd International Conference on Distributed Computing Systems Workshops.

[5] Heqing Huang Department of Computing Imperial College London, SW7 2AZ London, UK, Y an Ja, Shiliang Ao Xidian University Xian, China "A Whole-Process WiFi Security Perception Software System", 2017 International Conference on Circuits, System and Simulation.

[6] Johnny Cache, Joshua Wright, Vincent Liu, Hackers Big Exposure: "Wireless Network Security," Machinery Industry Press, 2012.