International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 05 | May -2017 www.irjet.net p-ISSN: 2395-0072

DENIAL OF CONVENIENCE ATTACK TARGETED TO SMART PHONES

Pavan M, Jasmine j

Department of Information Science and Engineering, BMS College of Engineering Bengaluru, Karnataka, India

---

Abstract - ***A denial-of-service attack targeted at popular smart phones that are used by normal users who are not technology savvy. This type of attack, which we call a denial-of-convenience attack, prevents non-technical savvy victims from utilizing data services by exploiting the connectivity management protocol of smart phones when encountered with a Wi-Fi access point. It is very easy for an attacker, to attack smart phones by establishing an invalid or fake Wi-Fi access points which does not have internet connection. This type of attack prevents the mobile user from accessing internet unless he gets to know the attack and disables the Wi-Fi features. Implementing a solution to overcome such attacks can be done by establishing the validation to check whether it is a valid Wi-Fi access point.***

If the fake access point is introduced while there is an ongoing connection with another valid Wi-Fi access point, the existing connection will not be interrupted. However, if the smart phone is put to sleep by the user or after a period of inactivity, it reconsiders all Wi-Fi access points in the area when awaken. As a result, the smart phone connects to the fake access point when it perceives that the fake access point has the strongest signal. In this project, we have proposed the Wi-Fi awareness system, which provides the awareness of public Wi-Fi access points.

Keywords—Denial of service attack, Wi-Fi, Smart phones, Accesspoint

1.INTRODUCTION

The android telephones are rapidly assuming control over the market. As of now, half of all U.S. portable supporters claim a cell phone .This quick development in cell phone appropriation is expected in allow part to the different administrations these gadgets can give. Checking email, utilizing GPS route, gushing video and numerous different administrations rely on upon Internet availability. We have found that the larger part of cell phones can be effectively denied of their Internet administrations, and consequently, of the vast majority of their usefulness through a particular type of a dissent of-administration assault exhibited in this paper, Wi-Fi Internet association which does not uses the constrained portable broadband information plan of the client. Neither of these stages checks regardless of whether the Wi-Fi get to point (AP) has an Internet association. An assailant can abuse this shortcoming to prevent the Internet access from claiming these cell phones

2. LITERATURE SURVEY

• **Porter Felt, A., Chin, E., Hanna, S., Song, D., and Wagner, D.** [1] proposed a framework about **Android Permissions Demystified**. Android's unhindered application market and open source have made it a famous stage for outsider applications. Starting at 2011, the Android Market incorporates a bigger number of utilizations than the Apple App Store. Android underpins outsider advancement with a broad API that furnishes applications with access to telephone equipment, WiFi and cell systems, client information, and telephone settings.

• **Nauman, M., Khan, S., and Zhang, X**. [2] proposed a framework about **Extending Android Permission Model and Enforcement with User-characterized Runtime Constraints**. Android is the primary mass-delivered buyer showcase open source portable stage that enables engineers to effortlessly make applications and clients to promptly introduce them. Giving clients the capacity to introduce outsider applications causes genuine security concerns. Current security instrument in Android enables a cell phone client to see which assets an application requires, human must choose the option to enable access to all the asked for authorizations in the event that she wishes to utilize the applications. It additionally depict the bundle installer that enables the client to set these limitations through a simple to-utilize interface.

• **Song, Y., Yang, C**. what's more, Gu, G.[3] proposed a framework about **Who Is Peeping at Your Passwords at Starbucks? – To Catch an Evil Twin Access Point**. Wi-fi systems are ending up noticeably exceptionally prevalent with the progress of remote LAN procedures and the wide organization of Wi-Fi gear. Clients can without much of a stretch get to the Wi-Fi organize when they are at home, at work, or notwithstanding voyaging. In any case, there is a rising danger that can bargain the security of remote clients – insidious twin assaults. A detestable twin in a remote LAN is basically a phishing (maverick) Wi-Fi get to point (AP) that resembles a honest to goodness one (with the same SSID name), however really has set up by a foe, who can listen in on remote correspondences of clients' Internet get to. A detestable twin assault is anything but difficult to dispatch. In the first place, by utilizing particular promptly accessible programming, an aggressor can just design a portable PC to be a get to point in a remote system. At that point, the

assailant can make sense of the SSID and the radio recurrence that the honest to goodness AP is utilizing.

• **Kumar, N., and UlHaq, M**.[4] proposed a framework about **Penetration Testing of Android-based Smart telephones**. Ace's Thesis. The reason for this work has been to play out a security investigation of Android-based Smart telephones. Advanced mobile phone utilization and adjustment are expanding step by step with an assortment of uses. The applications can be exceptionally basic in nature, for example, portable managing an account, and versatile installment frameworks and clients are regularly unconscious about the security dangers required in such applications. Android working framework, is expanding in the Smartphone business. It has officially beaten the most famous versatile working frameworks. In this examination the design of the Android working framework and tried its security through entrance testing. pickingthe most well known and prescribed instruments to test the security in the TCP/IP suite and diverse assaults have been performed on three distinctive Android adaptations.

• **Vidas, T., Votipka, D., and Christin, N**.[5] proposed a framework about **All Your Droid Are Belong To Us**: A Survey of Current Android Attacks. Indeed, even with the incorporation of security as a feature of the first outline, the new security highlights make new open doors for assault, and the development of the stage gives impetus. Much like a client that will introduce an application unreliably downloaded from the Internet regardless of any working framework notices, a client may effortlessly introduce applications that demand many Android consents without even batting an eye.

3. Existing System

A smart phone being targeted by DOC attack would display an optimal network connection status. When the smart phone user notices that her phone has no Internet connection, she can manually disable the Wi-Fi function of her phone, and then her phone would automatically return back to the mobile broadband, and hence, regain Internet access. For this reason, it is known as "denial-of-convenience" attack because it is not a hard denial-of-service to smart phone users.

Problem:

The smartphones are quickly taking over the mobile phone market. Android and iPhone are by far the most popular smartphones among consumers. Both of these platforms are designed to automatically switch from a mobile broadband connection to a Wi-Fi connection whenever possible.

However, neither of these platforms verifies whether or not the Wi-Fi access point (AP) has an Internet connection. An attacker can exploit this weakness to deny the Internet access of these smartphones. It is very easy for an attacker to launch such a DOC attack

Majority of users is able to diagnose this attack and successfully navigate through the solution above. As a result developing an automated solution to resolve this type of attack is highly desired.

Microsoft's Windows, for instance, uses the Network Connectivity Status Indicator feature to verify the validity of an Internet connection. NCSI achieves this by sending a validation challenge to a predetermined service and comparing its response against the expected result.

3.PROPOSED SYSTEM

Denial of convenience attack: It is simple for an assailant to dispatch such a DOC assault. All it requires is setting up a Wi-Fi get to point that does not have an Internet association. This can be effectively accomplished through a tablet phone with a shabby versatile Wi-Fi connector. At the point when inside the scope zone of this fake get to point, cell phones will naturally disengage from their versatile broadband and associate with this hotspot. The fake get to point does not give Internet association; these advanced mobile phones will be denied of any type of Internet get to. Larger part of clients has the capacity to analyze this assault and effectively explore through the arrangement above. Consequently, it is trusted this DOC assault still forces critical danger to numerous cell phone

Here we initially scan for different get to focuses, in the wake of finding a substantial get to point we give a secret key or key for login. At that point the approval server checks the watchword or key, on the off chance that it is legitimate then it naturally associates with the get to point.

The client can login to the fake get to point .since it's a fake get to point and it can't create the mystery key and it is not associated with the web. Subsequently the approval server does not acknowledge the key and the assault is recognized.

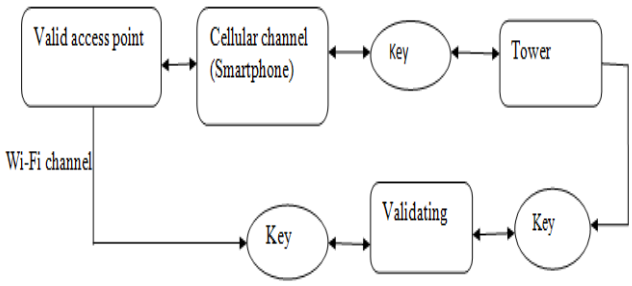

Figure . Real Access Point

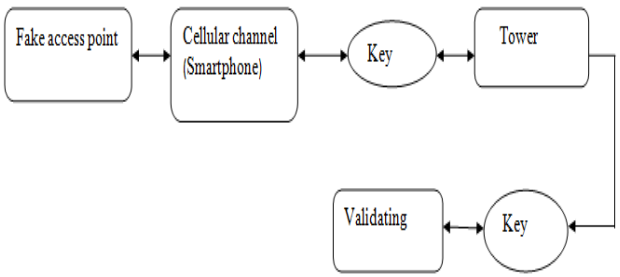

Figure. Fake Access Point

In the below chart it demonstrates that the client ought to first enroll to login and get to the association, and all the action of the client is put away in information base.

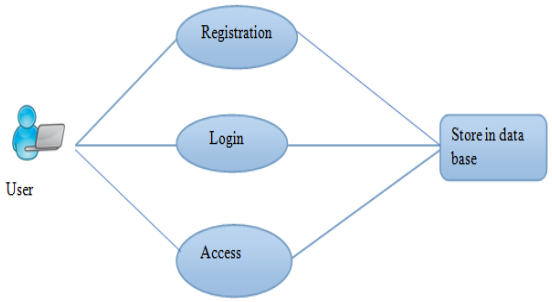

Figure. Registration

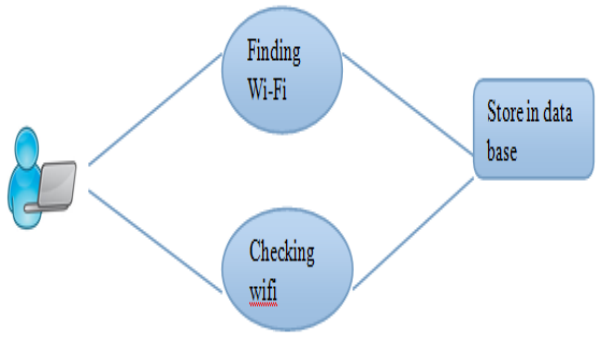

Figure. Checking Wi-Fi

In the above outline the client initially finds the Wi-Fi get to focuses and checks whether it is substantial or not. In the event that the get to point is legitimate then it is put away in information base.

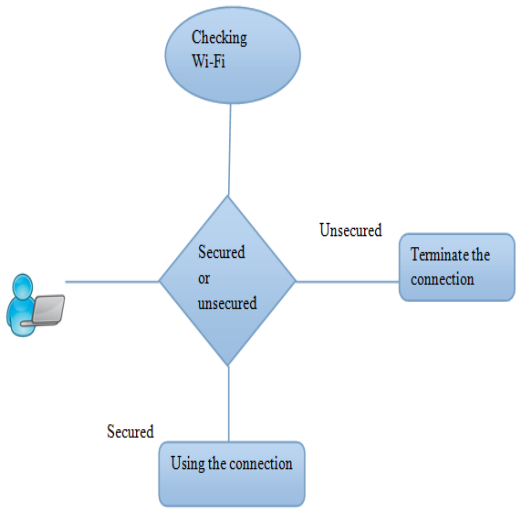

Figure . Validating

The above diagram shows the validation of network by client can secured or unsecured access, on the off chance that is secured and association id built up and on off chance that is unsecure.

4.METHODOLOGY

Methodology is a process of analysis of methods. At first the user should register to login and access the connection, and all the activity of the user is stored in data base. Then it checks the available access points, then the Wi-Fi coverage broad connection will be shown to check the available access points are secured or unsecured, if it is secured then the connection is established, and if it is unsecure then it simply terminates the connection of Wi-Fi and connects to a mobile data. Detecting whether the available Wi-Fi access points genuine or fake, in the background of Wi-Fi Sniffer application the Google url path will be accessed. In particular time out period, if Wi-Fi sniffer able to fetch or access the path of Google then the available Wi-Fi access point is genuine. Or else the available Wi-Fi access point is fake

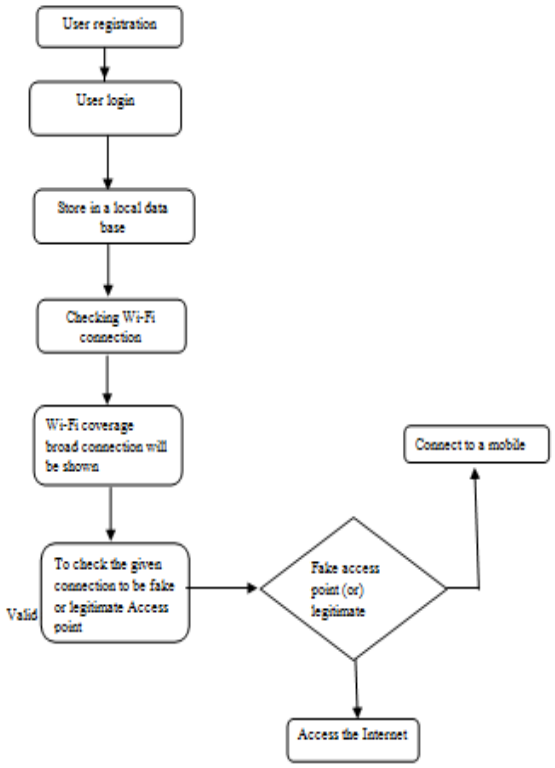

Figure. Legitimate access point

Wi-Fi commander: It is a client side application, in this application the client made to register or connect for the server Wi-Fi access point by entering the server IP address and the server port address. Once the client enters the server IP address and port address, then the next option is to get connected to the server by clicking on connect button. Once the client gets connected to the server, then request from the client side is sent to the customer.

Chat Server: Chat server acts as server side application, the IP address is generated by the server application. The user of the client is made to enter the IP address generated by the server, and also the port number to connect the server.

The connected client's mobile IMEI number is obtained in the text form from client side application to the above specified server application.

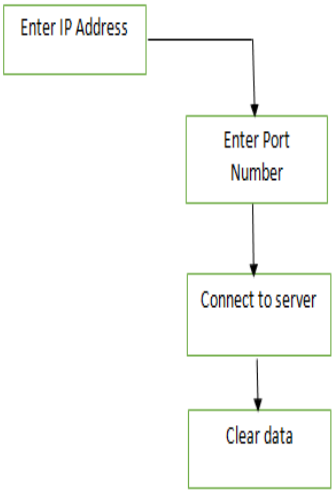

Figure . Wi-Fi commander

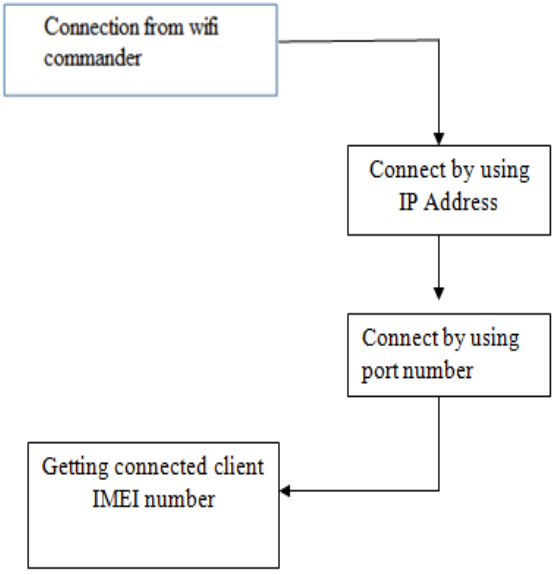

Figure. Chat Server

5. IMPLEMENTION

The principle objective or point of this venture is to discover that the associated wifi get to point is fake or honest to goodness. The proposed framework comprises of an Android application that executes a comparable system mindfulness component.

This module gives the outline of the application; UI is the main consideration for an application to get an effective consideration among all conceivable application .It ought to be easy to use to cover the consideration.

1.Verification

Verification is a capacity where a client introduces a few certifications to the Mobile. The client should be approved to demand administrations from the framework. The New client, he needs to get enlisted with a framework and after that validated before he can ask for Services. In an essential verification prepare, a client shows a few certifications like client name and some more data to demonstrate that the client is the genuine proprietor of the client name. A case of this sort of confirmation process is the utilization of client name and secret word.

2. Finding and Connecting with Wi-Fi get to point

Versatile naturally change from a portable broadband association with a Wi-Fi association at whatever point conceivable. This outline enables them to exploit the considerably quicker Wi-Fi Internet association which does not uses the constrained portable broadband information plan of the client. Neither of these stages checks regardless of whether the Wi-Fi get to point has an Internet association. An aggressor can misuse this shortcoming to preclude the Internet access from claiming these advanced mobile phones.

5.1 Testing

MODULE 1

Sl. No.	Input	Expected Outcome	Result
1.	1.'Register' 2. Valid input of Name/Contact/e-mail/ city/ Password.	User details validation. Storing data onto database.	Successfully Registered.
2.	1. 'Login' 2. Valid input of Name/Password	User ID validation matching.	Successfully Authenticated. Opens a new window.
3.	1. 'Login' 2. Invalid entry of name or password.	UserID should not to be accepted.	unable to login
4.	1.'Wifi Access Points' 2.'Connected Wi-Fi name'	Perform's validation in the background	Shows Wi-Fi validation

Module 2

Sl. No.	Input	Expected Outcome	Result
1.	'Server IP Address'	Valid IP Address from Server.	Entered IP address of server in client application.
2.	'Server Port'.	Port number of server.	Entered Server port number in client application.
3	'Connect'	get connected to the server application.	Successfully connected.
4	'clear'	Clear the sent request log in the application	Successfully cleared

Module 3

Sl. No.	Input	Expected Outcome	Result
1.	'Port address of server'	Server Port Address	Generates server port address
2.	'IP address of server'.	Server IP address	Successfully generates server IP address
3.	'obtaining IP address of client'	IP address of client	Successfully gets connected device IP address

5.2 Snapshots

Figure 5.2.1 : Registration

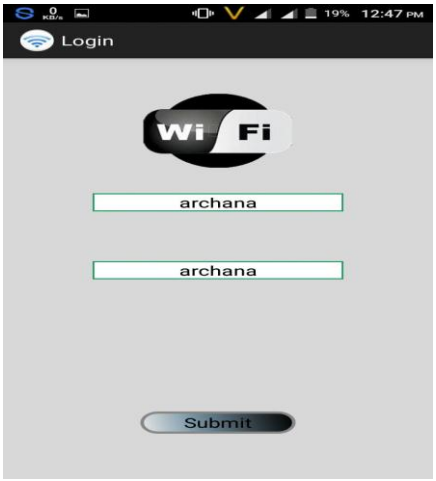

Figure 5.2.2 : Login

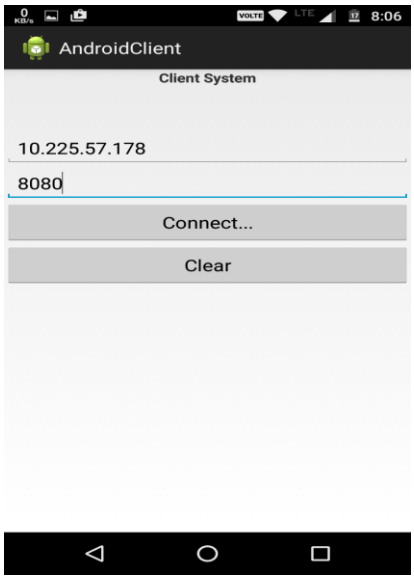

Figure 5.2.3 : Connected Sucessfully

ACKNOWLEDGEMENT

The successful completion of this project was dependent on the support and guidance we received from various sources. We would like to use this opportunity to express our heartfelt gratitude to each and every one of them.

Firstly we would like to thank the staff of the Department of Information Science and, B.M.S College of Engineering for all the support and encouragement that they generously showered upon us.

We are also extremely thankful to **Mrs.Chandrakala.G.Raju**, Assistant Professor, Department of Information science and Engineering for giving us the confidence, support and guidance in pursuing this project.

We would also like to thank the Head of Department, Information Science and Engineering, Dr. Radhika K.R. for her support and constant encouragement in meeting all challenges and giving our best to this project.

Last but not the least we would also like to express our gratitude to **Dr. Mallikharjuna Babu K**, Principal BMS College of Engineering for providing us the opportunity and the facilities in carrying out the project.

CONCLUSION

By using the wifi sniffer, one can easily obtain the information of wifi access point whether it is a valid wifi access point or a fake wifi access point. In this project, we have proposed the wifi awareness system, which provides the awareness of public wifi access points. This module provides the design of the application, It is a user friendly application.

Authentication is a function where a user presents some credentials to the Mobile. The user needs to be authorized to request services from the system. The New user, he has to get registered with a system and then authenticated before he can request Services. If the Wi-Fi access point is considered as invalid in either step, Wi-Fi Authenticator shows the connection as invalid.

REFERENCES

[1] Porter Felt, A., Chin, E., Hanna, S., Song, D., and Wagner, D. Android Permissions Demystified. In Proceedings of the eighteenth ACM Conference on Computer and Communications Security (CCS '11), Chicago, IL, October 17-21, 2011, ACM, New York, NY, 627-638, 2011.

[2] Nauman, M., Khan, S., and Zhang, X. In Proceedings of the fifth Symposium on Information, Computer and Communications Security (ASIACCS '10), Beijing, China, April 13-16, 2010, ACM, New York, NY, 328-332, 2010.

[3] Song, Y., Yang, C. what's more, Gu, G. Who Is Peeping at Your Passwords at Starbucks? – To Catch an Evil Twin Access Point. In Proceeding of the 40th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN '10), Chicago, IL, June 28-July 1, 2010, 323-332, 2010.

[4] Kumar, N., and UlHaq, M. Entrance Testing of Android-based Smartphones. Ace's Thesis. Chalmers University of Technology, Gothenburg, Sweden, 2011.

[5] Vidas, T., Votipka, D., and Christin, N. All your droid are have a place With Us: A study of current android assaults. In Proceedings of the fifth Workshop on Offensive Technology (WOOT '11), San Francisco, CA, August 8-12, 2011.