Asian Journal of Applied Science and Technology (AJAST)
Volume 1, Issue 5, Pages 69-72, June 2017

Smartphone's Hotspot Security Issues and Challenges

Sandeep Kumar[1] and Roney Z Augustine[2]

[1]*Assistant Professor, Department of ECE, MVJ College of Engineering, Bangalore, India. Email: sandeep.kumar@mvjce.edu.in*
[2]*UG Student, Department of ECE, MVJ College of Engineering, Bangalore, India. Email: roneyaustin@gmail.com*

Article Received: 14 May 2017 *Article Accepted: 03 June 2017* *Article Published: 05 June 2017*

ABSTRACT

Abstract- Smartphone becomes the most typical and popular mobile device in recent years. It combines the functionality of mobile phone and PDA. Besides, it provides many computer's functionality, such as processing, communication, data storage and etc. It also provides many computer's service, such as web browser, portable media player, video call, GPS, Wi-Fi and etc. This paper analyzes and compares the feature and security issue among three popular brands of smartphones aiming to help customers choose suitable mobile device based on their specific needs. Ad hoc network is a networking concept, which emerged in the beginning of the 1990's. Also known as Peer to Peer network, these types of networks have facilitated connections among computers. Currently, smartphones are connected to each other wirelessly to share information through hotspot ad hoc feature. These types of connections have led to many threats and attacks. There have been limited research efforts in threat detection mechanisms for smartphone hotspot connections. This paper will propose a smartphone hotspot Intrusion Detection system (IDS) which simulates the detection of the attacks (especially DOS attacks), on smartphone hotspot connections.

Keywords**: S**mart phones, IDS architecture, Hotspot, Attacks and Framework.

1. INTRODUCTION

Smartphone are increasingly becoming a target of security threats. First, the quantity of aggressor performing program assault is expanding late year, whose objectives are a wide range of sorts of cell phone's applications. There is one sort of Trojan that can contaminate clients' web seeking motor and change site pages or exchanges. Some methodologies can be utilized to shield clients from this sort of assault, for example, exchange approval, site to customer confirmation, security code advancement and so forth. The suppliers of cell phone's applications ought to assume greater liability to shield their clients from these assaults [1-4].

The Mobile Ad-Hoc network (MANET) is about multi devices, which are connected to each other without interface node infrastructure. The last few years have witnessed exponential growth of ad hoc connections, due to increased used of mobile devices especially smartphones. Smartphones have the ability to connect to each other wirelessly to share information. The smartphone hotspot works over short distances in low transmission rate conditions.

The one hand, the smartphone ad-hoc makes sharing of the data faster and less expensive, on the other hand, this new type of ad-hoc means new types of security challenges and threats such as loss of data confidentiality and data privacy. Additionally, the MANET security structure plays an important role in enhancing the MANET experience. Therefore, this paper will cover three important aspects: smartphone hotspot security challenges, application of proper data collection methodology and recommendation of best practices to minimize security threats [5,6].

2. SMARTPHONE HOTSPOT SECURITY CHALLENGES

Continuous changes in networking paradigm have led to a constant battle of maintaining security is such an environment. The main characteristics of the mobile ad-hoc/hotspots network depend on the user's environment and behavior. Therefore, controlling the ad-hoc environment is considered as a huge challenge, especially considering the lack of effectiveness detection mechanisms and prevention techniques such as mobile anti malwares. Additionally, traffic monitoring and data ownership is hard to follow. Maintaining the policies through smartphones are possible but it poses management challenges. These challenges give a rise in malicious attacks and misbehaviors. Moreover, changes in smartphone features in each version leads to enhancement in the ad-hoc connections and it also increases the risk and threat levels. That's why they are considered new generation threats. Thus security techniques and countermeasures are unable to keep pace with mobile ad-hocing connection challenges which lead to failure in data protection and attack preventions. Moreover, through smartphones hotspots channel there are clear breaches to providers' privacy. The privacy breaches which is highlighted over the hotspots are refer to breach provider device through detection of the provider location, using GPS, ability to consume the internet bytes and access the share folders. Moreover, along with user privacy breaches there are other security challenges such as controlling the connection sessions and managing the user's privileges. These challenges have been categorized under weak policy appliance within this type of MANET.

A. Smart phone hotspot threats and attacks

Smartphone users are connected more to hotspots these days than normal modems. The percentage of smart phone access to hotspots is as high as 90% of the phone connections. As mentioned previously, the types of the risks and threats have increased with the increase in the usage of this ad- hocing mechanism. A number of threats have been recognized through multi studies. The following sections will review these threats and risks.

B. Malicious node

Through hotspot communication channel an open connection treated as trust. Therefore, sometimes the provider node seems to be passing the traffic but actually it is a malicious

© 2017 AJAST All rights reserved.

node and it performs a back hole attack by holding all data and traffic from other nodes.

C. DoS attack

The weak authentication mechanism leads to an increase in the probability of DoS. Strong Wi-Fi standards such as 802.11 TGi or 802.1X cannot stop the DoS on wireless hotspot connections. Therefore, it was also noticed that the intrusion detection methods for hotspots are not mature enough to detect the DoS attack or unauthorized access.

D. Session hijacking

Generally, the connection and the open session between all the nodes through a single hotspot are not encrypted. Therefore, the attacker can eavesdrop on the data and traffic. Additionally, the attacker can use malicious applications which may affect data integrity and confidentiality middle attack is a perfect example of session hijacking. Through the smartphone hotspot connections the attacker enters an open session and steals traffic through that connection.

E. MiMA: Man in Middle Attack

Man in Middle attack is a traditional way to eavesdrop or steal data in the middle of the network connection. In smartphone hotspot the MiMA are demonstrated through a fake hotspot provider who pretend himself as connector or provider to steal data and will be in the middle of the connection as an unauthorized user in the hotspot connections. The MiMA attacker can use multi attack methods such as session hijacking, traffic injection and eavesdropping.

Fig. 1 shows simulation of sniffing attack. The packets come from smartphones to access points and within the network the sniffer can intercept the packets and inspect it.

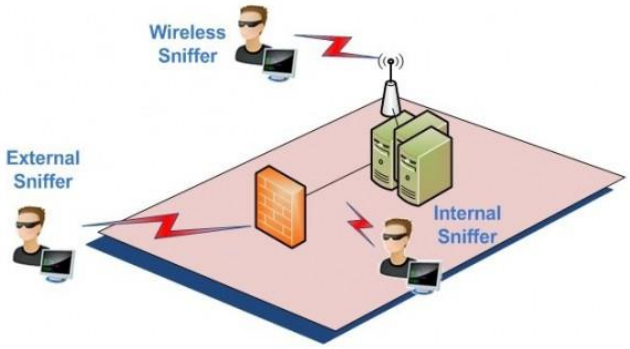
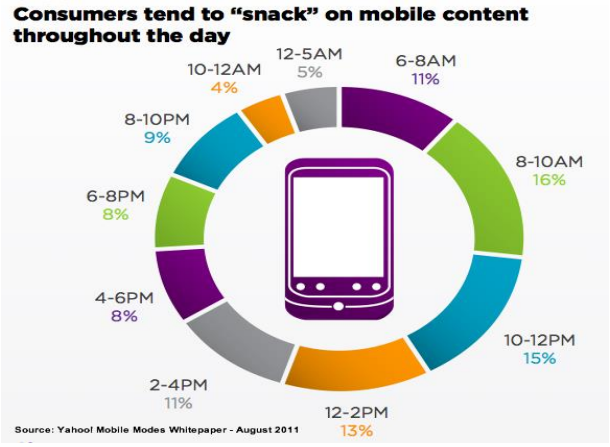


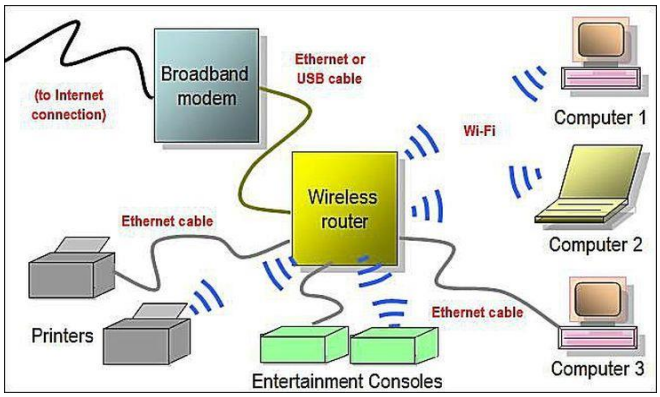
Figure 1. Sniffing attack simulation

3. RESEARCH METHOD

This research uses both qualitative and quantitative approaches. The primary data collection method which has been used is a questionnaire which was administered to measure and evaluate the security issue that networks are facing with increased used of smartphone ad-hoc (hotspot) connections within the domain network. The survey was distributed to 37 participants from different security and IT professions such as Network Administrators, Security Managers, Cyber Specialists and IT Technicians. These participants have been chosen based on their field experience and security knowledge. Additionally, they were chosen to represent small, medium and large-sized organizations. The interesting revelation of the response was that the concept of Bring Your Own Device (BYOD) is currently well-known in more than 83% of the organizations which allow smartphone connections to their business work.



This answer leads to many questions including the capabilities of their network to handle the traffic and its ability to secure both business and personal information. Therefore, it was necessary to know the Wi-Fi standard currently used in their network to measure and evaluate the performance.



Allowing smartphones through the company network means allowing hundreds and thousands of unknown devices to consume the bandwidth. Additionally, using the standard and normal Wi-Fi connections with huge data and traffic load may not be sufficient. Therefore, more than 50% of the participants state that current wireless connections are not performing well with increase in the data sizes. Therefore, this affects the required performance. Moreover, handling the big data transmission over the wireless connections have led to increased security concerns as well. The smartphones are able to connect to each other and share the interne t services through the hotspot point. The participants pointed out that this type of connection has huge security issues, based on different attacks types that have been generated and becomes a root for mobile malware and backdoor attacks. Therefore, assessing these risks is considered a challenging task for security managers. However, it was surprising that more than 35% of the participants never checked the impact of allowing smartphones to connect to their network or through personal hotspot. This highlights a serious issue that there are

© 2017 AJAST All rights reserved.

possibilities of security vulnerabilities over their network especially considering that they never update their security methods and control mechanisms

4. PROPOSED INTRUSION DETECTION SYSTEM (IDS)

Intrusion detection system (IDS) is a well-known countermeasure in standard network security. The IDS works to monitor the internal activity and detect any abnormal events and raise the alarm to the administrator.

Cell phone innovation is increasingly turning into the overwhelming specialized device for individuals over the world. Individuals utilize their cell phones to keep their contact information, to peruse the web, to trade messages, to keep notes, convey their own records and reports, and so forth. Clients while perusing are additionally equipped for shopping on the web, subsequently inciting a need to sort their charge card numbers and security codes. As the cell phones are getting to be noticeably across the board so do the security dangers and vulnerabilities confronting this innovation. Late news and articles show colossal increment in malware and infections for working frameworks utilized on cell phones (principally Android and iOS). Significant constraints of cell phone innovation are its handling force and its rare vitality source since cell phones depend on battery use. Since cell phones are gadgets which change their system area as the client moves between better places, interruption recognition frameworks for cell phone innovation are frequently delegated IDSs intended for portable specially appointed systems. The point of this exploration is to give a short outline of IDS innovation, give a review of significant machine learning and example acknowledgment calculations utilized as a part of IDS advances, give a diagram of security models of iOS and Android and propose another host-based IDS show for cell phones and make verification of-idea application for Android platform for the newly proposed model.

The proposed IDS acts as an app, which runs automatically with the hotspot connections in the smartphones. The IDS contains a counter which works by matching the two important parameters for securing the hotspot connections which are the traffic filtering and the bandwidth consumption as shown in below. The IDS contain alarm logs which work in making access decisions for other devices to the hotspot connection.

A. Traffic count

As mentioned above, the most common attacks through the hotspots are DoS and sniffing attacks. Therefore, the proposed IDS considers traffic filtering and counting of the packets to detect any unusual traffic load. The traffic matching is a component of proposed IDS and contains the following features and functionality of multi parts, which are traffic filtering and header filtering. The traffic filtering works by matching the normal traffic load which is settled by the users into the real traffic load which is usable. The proposed IDS aims to detect any high traffic load, which can be DoS attacks. Additionally, it detects the specific phone which causes the attack on the IDS employs header filtering to identify the attacker generating high traffic.

B. Bandwidth consumption

The bandwidth consumption has been considered as measurement parameter of proposed IDS. Normally the smartphones has low bandwidth range, hence, the bandwidth utilization considers critical issues of the smartphones, because of originality of less traffic range which any consumption normally the small capacity. Therefore, if the traffic matching detects high traffic it reports to bandwidth consumption part which monitors the traffic and disconnects any high traffic devices which are reported from any client.

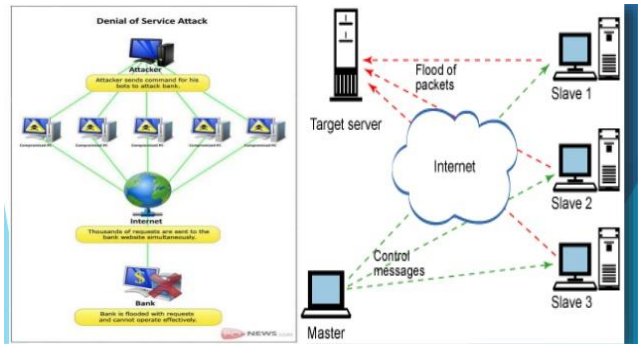
C. Detection log

To maintain security and avoid repeated threats are the main concern of any risk management plan. Hence, the proposed IDS will contain detection log, which stores all history alarms. These logs notify the provider (hotspot provider) in future if the detected attacker tries to connect again. Therefore, the IDS contains logs with small memory which store historical logs, saves time of the connection and blocks untrusted connection according to attack source list.

D. Simulation

This part of the research will introduce effective control methods for smartphones access and hotspot threats. This research reports the development of the simulation based on different parameters which are the number of packets and bandwidth utilizations over the hotspot connections. E. Routing and Roaming.

One of the security and management challenges within the smartphones or mobile ad hoc is the routing mechanisms. The mobile devices change their locations much faster and roam very often. Therefore, it is hard to apply a policy to these types of connection. Moreover, the ability to detect the attacker over the hotspot connections considered as a high level security challenge in current networks. In this paper we simulate the given attack which has been identified over the survey. The simulation has been done over the matlab to demonstrate the ability of performing the DoS attack and sniffing attack over smartphones hotspot connections as showed in Figure.



The purpose of applying these simulations is to demonstrate the ability to hack over the hotspot as shown in fig. The following figure demonstrates the attacker trying to flood other clients by sending large volumes of packets.

The simulation clearly demonstrates the possibility of hotspot connection attacks through high traffic and bandwidth

© 2017 AJAST All rights reserved.

utilizations. Therefore the proposed IDS will work by tracing back the attack through filtering the traffic and history log.

5. CONCLUSION

This research focuses on smartphone ad-hoc hotspot security issues and challenges. Hence it reports the results of simulating DoS attacks, the most frequent type of attack happening these days over the hotspots. The SIDS contain logs that require a small memory to store history logs, saves time of the connection and it blocks untrusted connections according to the attack source list.

REFERENCES

[I] P. Garcia-L6pez, R.T.aJ.A. (2010) 'Moving routing protocols to the user space in MANET middleware', *Journal of Network and Computer Applications,* vol. 33, no. 5, September, pp. 14.

[2] Conti, M. and Giordano, S. (2014) 'Mobile ad hoc networking: milestones, challenges, and new research directions', Communications Magazine, *IEEE, vol. 52, no. I, January, pp. 12. google.com (2013) 123, [Online], Available: Hyperlinks "google.com" google.com [5 Nov 2015].*

[3] Atallah, E., Bonnefoi, P.F., Burgod, C. and Sauveron, D. (2006) 'Mobile ad hoc network with embedded secure system', *Seventh edition of e-Smart conference, Nice, France.*

[4] Zhang, H., Liu, B., Susanto, H. and Xue, G. (2015) 'Auction-based Incentive Mechanisms for Dynamic Mobile Ad-Hoc Crowd Service', *ArXiv preprint arXiv: 1503.06819,1 2.*

[5] Chung, E., Joy, J. and Gerla, M. (2015) 'Discover Friends: Secure Social Network Communication in Mobile Ad Hoc Networks', A*rXiv preprint ArXiv, pp. 7.*

[6] Mohammed, M.A., Al-Chateau, B. and Ibrahim, D.A., 2016. Case based Reasoning Shell Framework as Decision Support Tool. *Indian Journal of Science and Technology, 9 (42).*

© 2017 AJAST All rights reserved.