Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 78 (2016) 19 – 25

Procedia Computer Science

International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Nagpur, INDIA

Multi-layer Defense against Malware Attacks on Smartphone Wi-Fi Access Channel

Kavita Sharma, B.B.Gupta*

Department of Computer Engineering, National Institute of Technology, Kurukshetra, India

Abstract

With increase in Smartphone users, uses have also increased such as email, gaming, internet banking etc. which requires it to always remain connected with Wi-Fi, thus making it vulnerable to numerous attacks. The endeavour in this paper is to explore Smartphone malware and combat challenges associated with it. Authors have proposed a novel three layer security model which detect and defence against the malware attack in network traffic and communication access point. Fine grained channel permission system is used to grant the permission to access the Wi-Fi access point thus providing security when any communication session takes place between Smartphone user and server though SSL handshake protocol. It also helps in detection of the interval time between packets sent and received which give impetus for threshold value used by TMM-HDT algorithm.

Peer-review under responsibility of organizing committee of the ICISP2015

Keywords: Smartphone Security; SmartphoneWi-Fi; Mobile Malware attack; SSL Protocol; Smartphone Malware Threat.

1. Introduction

In the recent times, Smartphone technology has advanced compared to last few years, in both hardware and software. According to performance of hardware, it works like portable computer[1-2]. It can perform many intelligent functions like adjustment of screen brightness, battery usage description, etc. An Android based Smartphone is usually inbuilt with many intelligent features, but if user wants to access extra features or function/application then they can connect it with internet and download real time applications, most of the times, which is freeware, whereas features pertaining to other operating systems based Smartphone are mostly paid. So users access the free available

* Corresponding author. *E-mail address:gupta.brij@gmail.com*

Peer-review under responsibility of organizing committee of the ICISP2015
doi:10.1016/j.procs.2016.02.005

Wi-Fi and access the internet as depicted in fig.a 1[3-4]. To access the unknown Wi-Fi access point is dangerous for the Smartphone because wireless communication transmit through the air and is more vulnerable to external intervention than wired communication which transmits information with the help of cables of rogue access point as depicted in fig.a 1. Today, people are dependent on the Smartphone for their personal and professional work; they store their confidential information and data in the Smartphone. The intruder attacks this information through the Rogue access point or free available hotspot in public places[5].

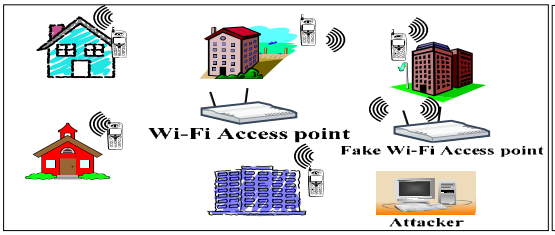

Fig.1a. Smartphone connect with fake access point

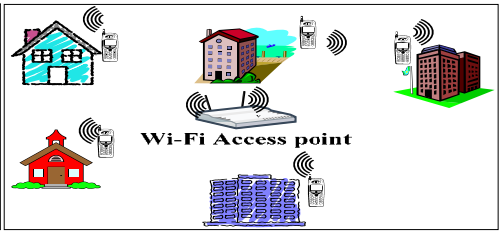

Fig. 1b. Smartphone connect with access point

1.1. Role of Malware Attack in Smartphone Wi-Fi

Attacker can easily steal network user's confidential information due to high Wi-Fi availability through Honeypot, Man in the Middle (MITM) Attack, RP Snooping, and Packet Sniffing. In Honeypot, network stores a list that is called the Preferred Network List (PNL). It will show any network availability in the range of hotspot network and attacker creates a fake access point (AP) with the same extended service set (EES) ID, and if client search the hotspot, then they get the attackers' hotspot and connect it. Another most popular technique of attack is MITM attack. In this attack, attacker place itself in the middle of online session between Smartphone and hotspot. Attacker changes the device configuration according to the fake hotspot. When user connect with this network then attacker steal all confidential information. To perform implementation, tested is composed of five devices: two Android handsets, one laptop, one desktop, and one wireless AP. The fake access points pass the message to the user and connect with the server and steal the confidential information. Many authors had successfully examined the potential of Smartphone in the UbiComp (ubiquitous computing) environments. The Smartphone has required UbiComp for context-aware computing, ubiquitous intelligence, & ambient in recording, tracking & monitoring environments. To diminish this attack, developer is required to use shared authentication process when an application communicates with external devices. So, public Wi-Fi vendor require more secure network and its broadcast. For this vendor can use the strong encryption method or VPN tunneling security method.

2. Defence Technique of Malware Attack on Smartphone Wi-Fi

i. Secure Sockets Layer (SSL) Network Protocol[6]

This uses SSL connection authentication and explain how diverse the application as well as the library use on iOS validate SSL certificate. For determined vulnerability in logic through SSL to connect with attack to utilize black and white box technique and take gain in user Smartphone. The SSL library generates vulnerable certificate between client and server with SSL connection7.

ii. Trained Mean Matching (TMM) Algorithm[8]

This is used to one-hop & two-hop wireless hop channel to collect data, then compute the mean & standard deviation of server Inter-packet Arrival Time collected in the hop which represents as μ1 dap and π1 dap.

- To filter the server IAT between the range [μ1dap –π1dap, μ1 dap +π1dap].

- Now we calculate the second mean of residual server IAT which is denoted by μ2 dap and evil twin server the two HOP denoted as μ2 dap. Compute the average as T_θ
- To calculate the average between one- hop and two- hop server IAT use sequential probability ratio test (SPRT) technique which calculate the probability of two server IAT and calculate the exceeding trained threshold value which is denoted by e1 and e2 which computes the percentage of collected server IAT.
- In next phase , compute the sequence of IAT observation server represent by $\{\partial\}_{i=1}^{n}$ and use binary random variable which is shown by βi to denote the i[th] server IAT avail to evil twin Access point system or not. This phase is known as detection phase.
- If €i >Tθ then βi=1 then show the Evil Access point Server otherwise βi=0 means normal access point. Then find out the sequence represent by $\{\beta\}_{i=1}^{n}$

➢ Two hypotheses H1 represent to the Evil access point and H0 represent the normal Access point. We represent P (βi=1/H1)= θ1 and P (βi=1/H0)= θ0.

➢ According to training data set assume θ0=P1 and θ1=P2.

➢ Now, calculate the hypothesis ratio π with assumption that the server IAT are IID (Independent and identically distributed) represent as .

$$\pi = \frac{In(\alpha_{1.....}\alpha n / H_1)}{In(\alpha_{1.....}\alpha n / H_0)} = \sum_{i=1}^{n} \frac{pr(\alpha_i / H_1)}{pr(\alpha_i / H_0)}$$

➢ A threshold random walk to compute the log probability ratio the walk starts from zero. If βi=1 then it start up with length as In (θ1)-In (θ0),

➢ If βi=0 the start-up with length In (1-θ_1)-In (1-θ_0).

➢ All the results decide in one line for every random walk. Let ρ and σ are user selected false +ve and false -ve rate.

➢ The random walk is shown as upper bound and lower bound. It is represented as a normal AP otherwise it is not complete and next decision is tried around.

➢ IAT consume too much time.

➢ The training knowledge in one wireless network is hardly discrete applicable to a further network.

iii. HOP Differentiating Technique (HDT Algorithm)[8]

For Server-to-AP IAT Ratio (SAIR) analyses make three assumptions:

- To take more time, cost during collecting one couple of server IAT and AP IAT is in second. So in short, time interval wireless network environment does not change.
- The attackers try to attract to the victim client to connect with the evil Access point. Then attacker gives a better RSSI (received signal strength Indication) and a smaller wireless collision probability.
- If network congestion in Ethernet then user choose to surf internet through normal AP.

➢ According to some variable we can represent model. Let $\Delta\chi_a$ represent AP IAT and η represent the SAIR under authentic environment. Let represent let $\Delta\hat{x}_a$ represent AP IAT and $\hat{\eta}$ represent the SAIR under ideal environment. Then we get the equation:

$$\eta = \frac{\Delta\chi_s}{\Delta\chi_a}$$

$$\hat{\eta} = \frac{\hat{\Delta}x_s}{\hat{\Delta}xa}$$

- Now we calculate the mean of η between the normal AP & Evil twin AP then we can efficiently detect the evil twin attack.
- $$E(\hat{\eta})_{one-hop} = 2T_{DIFS} + 2T_{SIFS} + 2E(T_{BF}) + \frac{2L_{ACK(MAC)} + L_{ACK(TCP)} + L_P}{B_W}$$
- To compute SAIR threshold θ_0 for HDT algorithm, try to minimize the probability of making erroneous decision. Then represent by:

  P1 = p ($\theta_{one-hop} > \theta_0$) and P2=p($\theta_{Two-hop} > \theta_0$)
- The problem arise to transformed to compute E(θ_0) then shown by:

  $$\hat{\theta}_0 = \arg\min 1 < \sum_{i=1}^{n} \frac{pr(\alpha_i / H_1)}{pr(\alpha_i / H_0)} < 2(p1+1-p2)$$
- When θ_0 increase from 1 to 2 in fine grained step.
- If all step, increase θ_0 by 0.01 and compute P1+1-P2 if reaches 2. Then the value of $\hat{\theta}_0$ leading minimal P1+1-P2.
- According to wireless 802.11 standard:
  - If we compute the packets without any collisions then,

    The protocol 802.11b θ_0 =1.31, P1<21.8%, P2>76.9%;

    The protocol 802.11g θ_0 =1.48, P1<27.3%, P2>71.5%;
  - If we compute the packets with any collisions and collisions number are under three then,

    The protocol 802.11b θ_0 =1.34, P1<21.2%, P2>74.9%;

    The protocol 802.11g θ_0 =1.48, P1<27.3%, P2>71.2%;
- HDT approach that is more effective [8].

Table 1: Defence mechanism against attack on Smartphone Wi-Fi access point

S.No.	Year	Defence	Description	Weakness
1.	2014	To use the approach by defence in depth against the man in middle attack.	To gain access to the message.	Due to low level security awareness by the users of mobile banking services and the high level of risk.
2.	2014	Use defence approach to multiple location service technologies, multiple bands, and fingerprinting.	The attackers connect with legitimate user through fake Wi-Fi access point and steal useful information.	The complexity and cost of jamming plus impersonation attack decreasing because it is typical to do the cellular based location service. Which uses triangular to get an exact location.
3.	2013	To defence by fine grained permission system.	To trace the location and attack on the confidential information. Break the security model CIA.	The application with some sensitive permission sets are actually benign from result of static analysis, those permission sets might not be used by real-world attackers very often. In such cases, there is a good reason to remove it from the sensitive permission Database.
4.	2013	To defence with Internet validation protocol.	The attacker disable the already connection with valid access point and connect with fake Wi-Fi access point when Smartphone come in the Hotspot range.	Static identifier Validation technique is used for only particular attack. Dual technique is that it has to compromise the internet access, as random key has not prior validated through validation test.
5.	2013	To defence by using SSL	Man in middle attack, to create fake	Many user applications depute security

		protocol.	Wi-Fi access point and steal the user confidential information.	function to SSL APIs. And lot of Vulnerabilities about these applications which is not resolve.
6.	2012	To defence the using improve and secure SSL validation protocol.	To beak the SSL validation certificate protocol.	The SSL certificate validation protocol in libraries and many security critical applications is completely broken.
7.	2012	Wireless IDS.	It possible to identify the fake Access point, with a very simple approach, without any modifications at the infrastructure or the hardware.	It is work only Client Side.
8.	2011	To use Trained Mean Matching (TMM) and Hop Differentiating Technique (HDT).	To distinguish network traffic between wired and wireless nodes use round trip time (RTT).	The demerits of this technique are distance and packets Hops.
9.	2010	To use attack detection technique TMM and HDT algorithm.	The Evil Twin attack compromised the security.	TMM is time consuming, trained knowledge is difficult direct apply to another network.
10.	2006	For security purpose use public tags requirements more time, lightweight cryptographic schemes implemented.	The attacker change Wi-Fi setting up a rogue AP facilitate DNS poisoning and phishing attack. Phishing attacks performed in different way forms forged emails and spoofed websites.	The attacker attack on the weakness of the mobile environment when the medium of transmission and recipient then phishing attack performed.

3. Proposed Three Layer Detection Method against Malware Attack

We propose a three level novel technique to combat security challenges faced by Smartphone Wi-Fi Access point against malware attack. To use this approach, fine–grained permission system is needed while accessing the play store. The novel permission should be considered as sensitive permission for accessing fine-grained permission. If we find that some malicious activity is there, then detection technique HDT algorithm will be used in conjunction with secure SSL network protocol. This technique is categorized into three phases:

Layer 1:

Fine grained Permission system is used to take permission for accessing the system. This system identifies if the access point is malicious or not, collects all sensitive information about the access point. IF it is not harmful or unsuspecting then it grants the permission to access the Wi-Fi network.

Layer 2:

The SSL network protocol is to face the issues to access the network against man in middle attack. To establish connection between client and server then it provides the authentication, integrity and confidentiality. It provides end-to-end security next to an active, malware attack. The SSL connection establishment is typical part the authentication server. For authentication SSL use handshake protocol when server issues the public key certificate. The security purpose client must verify the SSL certificate that certificate issue by the valid authority, name and expired date of certificate.

For experimental purpose we used Smartphone application testbed on a Nexus with Android based Smartphone and running iOS4.2.1. We use DNS cache poising which disturbs and divert client connection to stimulate attack server and execute on a dell laptop which represent the access point.

Layer 3:

We propose to utilize the RTT (round trip time) of network traffic to discriminate between wired & wireless nodes. Here the basic communication configuration & properties of such evil twin attack in wireless networks as well as create novel algorithm is discussed to identify peak recognition during preserving a tremendously small rate of false positive.

The web browser communicates through distant web server via an evil twin AP as well as usual AP. The attacker place AP with the help of his laptop and readily available software. This AP has SSID as authenticated AP and created confusion of user which AP has connected. Most of the time user gets connected to evil twin access point as it shows high RSSI (received signal strength). Most of the operating system considers the different AP bearing same name (SSID) belongs to same organization.

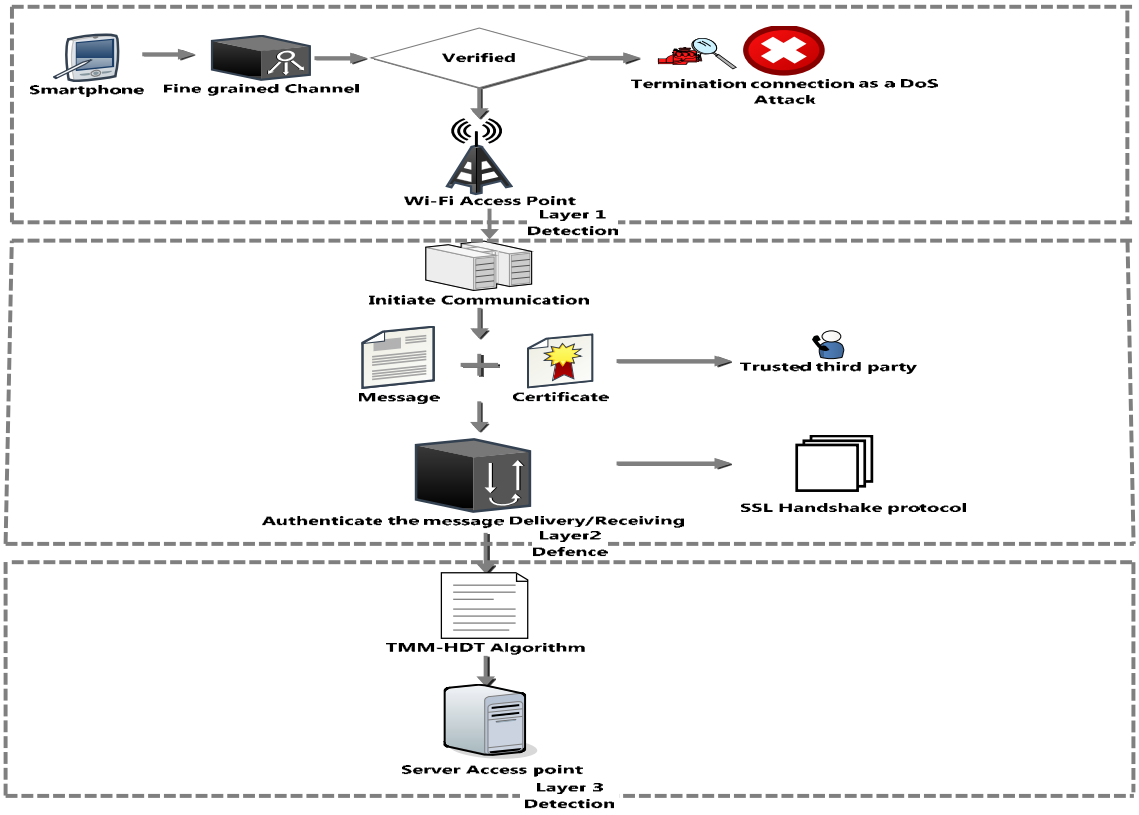

Fig.2. Proposed an Approach to More Secure Three Layer Wi-Fi Channel

The HDT Algorithm improves TMM by eliminating the training requirement. HDT is defiant to the environment change like network saturation and RSSI fluctuation.

Here we use the statistical analysis of IAT i.e. time distance between two succeeding packets received on client side. If any time high collision or from any reason time distance between some packet pair may be large. Its means this data noise and required to filter out. The two techniques improve the data pre-processing results: data filtering and data smoothing. Here we filter the noise data with a large numbers of collision networks. It clear which packets contain some error. According to IEEE 802.11 we filter out those packets AP IAT exceeds 21001 and server IAT exceed 39802.

The second approach apply in one decision round on mean of multiple input data, to smooth the input and calculate the mean if input data rather than only one input data in one decision round. We compute the mean of Server IATs instead of only one Server IAT.

3.1. Discussion

Yimin Song et al.[8] described SSL handshake protocol but face few problems that occur in accessing the critical application, crack the SSL validation certificate and not providing the security between client and server. But in the proposed model, if SSL certificate cracks, then TMM-HDT algorithm is used which detects the attack in communication channel.

According to Le Nguyen et al.[9] in the real world scenario, attackers often use permission sets that are actually present in the resultant application of static analysis. Therefore, it is better to remove such permission sets from sensitive information databases.

So, our purposed model analyse the permission set according to updated set and use SSL handshake protocol which provides more security. The performance analysis of this model can be shown by preventing the applications against malware attack that are accessed by Smartphone Wi-Fi access point.

Smartphone user send the request to Fine grained system access the *XYZ.com* website through Wi-Fi access point. Fine grained system collects the sensitive information nearest to router R1 and R2. If no malicious activity is found then request is accepted, otherwise the request is rejected. If permission is granted then user is able to access the *XYZ.com* and send the request server access point to download the abc.com application. So, apply the SSL handshake protocol which is providing the security authentication by generating the certificate with request message and servers identify these request come to legitimate user to check certificate issuer name, expired date and on which date it is generated. If it validates the certificate then Smartphone user can access the services provided by server.

Now user can access the application and download it on Smartphone. The server sends abc.com application according to user request and transfer the data packet. For security point time interval is computed between Smartphone user and server access points that send packets. If the packet transmission takes more time then collision may occur. This requires filtering the data and analysis of the packet pair by computing the threshold value through TMM-HDT algorithm. Assume Smartphone user send the request to access the application on *XYZ.com* and server respond time take with some noise to the client. This process takes 100 msec. If it take more time that means collision occur. Then TMM-HDT algorithm is required.

4. Future Work and Conclusion

A model is introduced which proposes three level technique approaches to provide the security against malware threats. This approach in future will provide more secure channel when Smartphone user access the internet facility anywhere through Wi-Fi.

Acknowledgements

This research work is being funded by DEITY, Ministry of Communication & IT, Government of India.

References

1. Erich Dondyk, Louis Rivera, Cliff C. Zou. Wi–Fi Access Denial of Service Attack to Smartphone. International Journal of Security and Networks; 2013;8:3.117 – 129.
2. Yong Wang, Kevin Streff , Sonell Raman. Smartphone Security Challenges. IEEE Computer Society Digital Library (CSDL). Computer ; 2012; 45:12. 52-58.
3. N. Leavitt. Mobile Security: Finally a Serious Problem? Computer ; 2011; 44:6. 11-14.
4. P. Traynor, W. Enck, P. McDaniel and T. La Porta. Mitigating Attacks on Open Functionality in SMS-Capable Cellular Networks. IEEE/ACM Transactions on In Networking; 2009.40-53.
5. Bo Li and Eul Gyu Im. Smartphone, promising battlefield for hackers. Journal of Security Engineering; 2011; 8:1. 89-110.
6. M. Georgiev, S. Iyengar, S. Jana, R. Anubhai, D. Boneh, and V. Shmatikov. The most dangerous code in the world: validating SSL certificates in non-browser software. Proceedings of the 2012 ACM conference on Computer and communications security; 2012.38-49.
7. Jun Liang Roy Feng, and Guang Gong. Vulnerability Analysis and Countermeasures for Wi-Fi-based Location Services and Applications; 2014.1-12.
8. Y. Song, C. Yang, and G. Gu. Who is Peeping at Your Passwords at Starbucks? – To Catch An Evil Twin Access Point. In IEEE/IFIP International Conference on Dependable Systems and Networks; 2010. 323–332.
9. Nguyen, Le, Yuan Tian, Sungho Cho, Wookjong Kwak, Sanjay Parab, Yuseung Kim, Patrick Tague, and Juyong Zhang. UnLocIn: Unauthorized location inference on Smartphones without being caught. 2013 IEEE International Conference on Privacy and Security in Mobile Systems (PRISMS); 2013.1-8.