A Present Day Android Technology Security Analysis

Neha Verma

Abstract - The important motive is to analyze the security of Android phones. Smartphone usage is increasing with a wide and unlimited variety of applications. Some applications are critical as banking and users are not known to the future risks involved with these android applications. Android adaptation percentage is increasing fast in this modern epoch. Android has also beaten windows. In this paper, Android security has been analyzed considering penetration testing. We have considered the popular tools for testing the security in the suite of TCP/IP. The paper includes a discussion about conclusion that is the android secure or not and up to what extent we can trust using its applications. This work is worthful and useful for researchers who use smartphones having android technology in a critical environment.

Index Terms— Android, Penetration testing, Smartphones, Linux, Vulnerability

I. INTRODUCTION

Smartphone conformability is emphasizing as of its versatile functionality. Recently these android phones are used for talking and also can execute the functions of devices like pager etc. and moreover includes applications of entertainment and banking etc. A compact hardware and reliable software combination with a fast operating system will be able to serve us with such advanced services without any failure. The Android is contingent on the reoriented linux kernel plus consists of video calling etc. These features help in increasing the validation of android but also open the future risks which are unanticipated. A survey was released in 2011 by a customer intelligence firm which concluded 33% individuals are not using smartphones, 34 % looking for an android in the upcoming six months or more. And out of these 21% will go for IPhone, 12% for Blackberry and 25% have not decided [1]. Hence it is showing the increasing interest of customers in smartphones having android. Android smartphones day by day growth and success makes it more eye catching for hackers as well which is quite risky for the users and technology lovers. Penetration testing is a tool which is helpful in finding out security holes for the detection of vulnerabilities. Surveillance can be evaluated by replicating an attack in distinction to malicious source like Black Hat Hacker [2, 3]. National Institute of Standards and Technology introduced methodology that how penetration evaluation can work [4]. It is a stack which consists of middleware of operating system with applications [5, 6]. The android architecture is complex [7]. Android has the core linux and guarantees that users will enjoy similar internet activities equivalent to their experience on desktop. Android uses virtual machine of java for handling of applications and does not give any support for running conventional java applications.

Manuscript Received on October 2014.

Neha Verma, M.Tech Student, University School of Information and Communication Technology, Guru Gobind Singh Indraprastha University, Delhi, India

Operating systems in phones are in use when the first creation of the mobile phone took place but those particular were meant for specific devices. With the spread of the phone with android technology, the significance of security increased as well. Latest application enlargement and speedy launch of further performance functionality is the indispensable aspect for the advancement of smartphones. For assessing the network stack security, the architecture of android, penetration test procedure depend on familiar attacks against TCP/IP (Transmission Control Protocol/ Internet Protocol) and tools which are useful to make desired penetration tests are researched.

We have additionally studied the security operations of the android. In the Android progress process many updates took place and versions got released with new advanced features and defect fixes.

II. RELATED WORK

White box testing is used to render the security interpretation. Firstly the aim system is perceived and subsequently penetration tests took place, initiating from well-established vulnerabilities to deep penetration attacks. While doing the penetration test the concern was on network connectivity of WLAN. Android has versions additionally. Therefore, our purpose was not sole individual version. Versions like 1.6 (Donut) which is the oldest, 2.1 (Éclair) and 2.2 (Froyo) has been tested who's adoption extended. We have probed the refinements which are generated in distinctive versions by testing the same. In the NIST (National Institute of Standards and Technology) forethought phase, test targets and policies are set and identified respectively, and management responsibilities are accomplished and result in reports. Penetration checking is executed in stages and it is an operation to estimate out the security vulnerabilities by appraising the system with malicious techniques. Intention of this examination is to guard crucial data from hackers who are unauthorized.

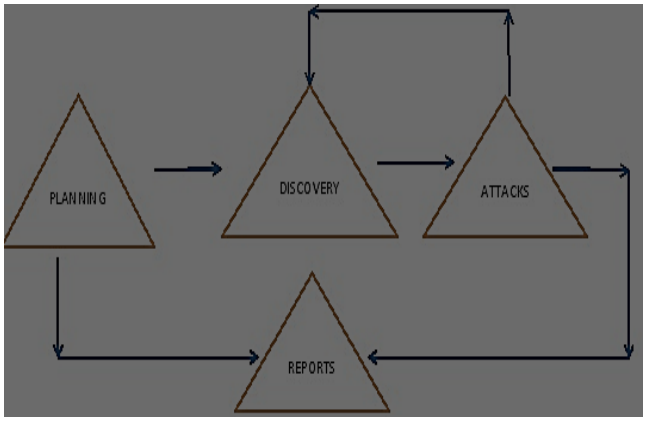

FIG 1. Penetration testing Methodology

When vulnerability is raised it is used for exploiting framework to acquire access for sensitive information. It is indispensable for an organization to uncover the issues of security present in internal network. Firms can intent for fortification against any attempt of hacking using the matching information. Seclusion and documentation security of user are the main concerns nowadays. Assume if a hacker control to retrieve the details of user of Facebook. Due to this shortcoming left in a system a firm can meet some legal issues.

A. Ilustration of Free Tools

Nmap, Nessus, Metasploit, Wireshark, OpenSSL, Cain & Abel, THC Hydra [8].

Constraints of tools: At intervals tools can show erroneous positive output which finally results in spending additional time of developer by investigating these vulnerabilities which are not there [8].

B. Port Scanning

The succeeding measure of penetration checking was to accomplish port scanning so to uncover devices which are active, open ports along with running services. A network executive plus hacker can retrieve what kinds of assistance are running and which are accessible to public. The TCP/IP stack comprises of vulnerabilities and ports are classified into following ranges as mentioned [9]:

- Well Known (0-1023)
- Registered (1024-49151)
- Dynamic (49152-65535).

First category of ports is for web servers (ascribed by IANA- Internet Assigned Numbers Authority) and system services. Normal programs use registered ports. Third party programs use dynamic ports. Port scanning is exercised through different strategies described in "Port scanning strategies and the fortification against them" [10].Nmap tool for port scanning is selected as an upshot of its admiration. Mechanism of TCP network formation and stoppage is important as many scans may violate the process. For initiating an association link using TCP/IP between consumer and assistant, a handshake process has to be done before any normal communication gets begin.

C. TCP connection and termination is done in the underneath steps [11].

(i) If a consumer likes to be disconnected it will redirect a segment having FIN message including a sequence number received at last.
(ii) After receiving segment, ACK is send from server to the consumer for acknowledging the request of termination.
(iii) Server creates its FIN packet therefore then redirects it once finished with the transmission.
(iv) Last FIN packet was accepted by the consumer and finally connection has to be closed.

D. Test Scenario

Smartphones have utilities which are running i.e. a web and FTP as http-proxy plus ccproxy-ftp over the mentioned ports 8080 plus 2121.

D-Link access point works as the central wireless service provider for communicating. Two computers were used: one for generating forms of attacks plus other one for analyzing traffic which took place during an attack. Ubuntu is used on both machines. Wireshark which is a traffic analyzer is installed on both systems for analyzing the data. Many complimentary command line equipments are unoccupied for checking and exploiting the vulnerabilities, and some comprehensive tools are selected by us: Nmap and Linux command tools Hping3, Dsniff along with packit for attacks. The particular tools are established on one system of Ubuntu for precipitating the attacks. Nmap can run on categories of operating systems as u- nix and windows. Packets were seized from scans and analyzed to deeply grasp the documentation being exchanged. Wireshark is rendering on sole machine of Ubuntu to catch and explore the wireless traffic through our tests. Port scanning is used to postulate data about target systems. Data that was collected in this step will be helpful for further enhancing the penetrating tests. It is necessary to mention that android is not parallel to Nmap 5.0 rather it imparts a set of versions of kernels of linux for 1.6 and 2.1 but no data regarding 2.1. After testing with Nmap 5.5, same results obtained for 1.6 and 2.1 and for 2.2, we found the accurate match of operating system with also the exact match of linux kernel which is 2.6.32.15 [13]. Many results of port scanning are similar to linux with android 1.6 plus 2.1 with linux kernel 2.6.29 in addition to android 2.2 with linux kernel 2.6.32 [13].

The risk corresponding with scan results is low as per the documentation of CAPEC-300 [12]. As we traced this documentation for the same to be complete, a bit of other scans were tried also but no useful knowledge was obtained.

E. Tools Used

A widespread tool nmap including guide of network scanning. Host discovery plus OS detection are its attributes.

F. Attacks on the framework stack of android

Attacks fall in to these sets:

Eavesdropping: After stopping of a packet, a hacker is capable to grab data.

Man in middle: Contents can be modified by a hacker and by intercepting communication session is taking over linking duo devices with the help of network packet sniffer.

DOS attack: To discontinue the permitted user from acquiring data and is caused by traffic flooding.

Android 1.6's has been lowered because of affected user interface while attack and the response time are enlarged. The observation was that Android 2.1 response time is not influenced by the flooding attacks, but a remarkable increase in interval time of Android 2.2 was there and it is unexpected for the reason that it is reliant on kernel and it was presumed to be at lower menace of attacks. Android is unguarded to ARP (Address Resolution Protocol) attacks like gratuitous ARP flooding. This attack is used to reroute traffic or for denying any service to the loser. Even if ARP reply is unicast or broadcast android smartphone moves in the accepted forgery IP-MAC (Media Access Control) binding in theirs ARP cache. No

methodology is there to restrain analogous form of attacks. Android is present day operating system and is mature system as it is reliant on linux kernel. Land attack and teardrop attacks were unsuccessful. Flooding attack against a port which is closed is successful and the system cannot communicate with any other device during this attack and potential is even unsatisfactory than the performance during flooding of an open port.

III. CONCLUSIONS

This research is done on penetration evaluation. It is exceedingly compelling that android technology has increased over some last years. Android provides many attributes for developers. Attacker can position malwares which can affect system functionality which is permanently a venture. Vulnerability test was performed. Security of android is crucial for the reason that of its high rise usage in smartphones market. We have probed penetration evaluation of smartphones which is joined to a WLAN network. The paramount part of work was to gather data about the android as of its version details, its architecture nd security mechanism. Firstly, we analyzed many scans to spot out vulnerabilities in threesome android versions.

While doing it we were accomplished to accumulate documentation regarding the desired host as whether it is active or not and the status of some ports and services running on it. It is shown that it is probable to execute fingerprinting of android so the sort of the android can be ascertained by an attacker and then security flaws can be spotted in the joined device. Secondly, forms of attacks were accomplished against network stack of android. Initiating with flooding attacks which are rendered in multifarious ways SYN, UDP (User Datagram Protocol) flooding etc. Such attacks can engender to denial of service by consuming resources like bandwidth etc. A little about ping of death, land attack etc. has been explored. While manipulating with massive ICMP datagram's the android system is assured and the massive packets are ignored. Over the android many link layer attacks were victorious. ARP poisoning was executed by sending forgery updates of ARP to the desired host and it remain successful. So traffic was switched to a terminus which was adopted by the hacker. By sending fallacious MAC addresses, denial of service and session hijacking etc. were successful at link layer. The reason of this exploration was to execute penetration evaluation of android installed smartphones. Hardware encryption, security keys and data recovery facilities are not a segment of android system, just mentioning few shortcomings of the android system. Some surveillance operations have been used in the android which can control the security risk.

Consequently we can extrapolate that it is a trusted operating system plus our results and findings of this exploration must motivate these operating system vendors regarding the security shortfalls which we have probed and system functionality can be ameliorated when the devices are flooded with numerous types of traffic.

IV. FUTURE WORK

By reason of the widening count of malware, SQL injection and buffer overflow attacks, underneath exploration is expected:

- Surveillance exploration of android libraries.
- Exploration of surveillance in application layer protocols of android smartphones.

There are java libraries in android just as the media etc. Their run-time framework is distinctive than usual applications in the smartphone and accordingly, supplementary intention should be spent to evaluate the security pitfalls in this part.

REFERENCES

1. Consumers Now More Likely to Buy Androids Than iPhones,http://www.marketforce.com/2011/02/consumers-now-more-likely-to-buy-androids-than-iphones/,Accessed on February, 2011.
2. Gold, S., "Get your head around hacker psychology [Information Technology cyber-security]," Engineering & Technology, vol.9, no.1,pp.76,80, Feb. 2014
3. Shanmugam, J.; Ponnavaikko, M., "Risk mitigation for cross site scripting attacks using signature based modelon the server side," Computer and Computational Sciences, 2007. IMSCCS 2007. Second International Multi- Symposiums on , vol., no., pp.398,405, 13-15 Aug. 2007
4. Special Publication 800-115, Technical Guide to Information Security Testing and Assessment, September 200 (replaces SP800-42), Accessed on March, 2011.
5. [5] Kuzmanovic, N.; Maruna, T.; Savic, M.; Miljkovic, G.; Isailovic,D.,"Google's android as an application environment for DTV decoder system," Consumer Electronics (ISCE), 2010 IEEE 14th International Symposium on, vol., no., pp.1,5, 7-10 June 2010
6. Yong-Hua Cheng; Wen-Kuang Kuo; Szu-Lin Su, "An Android system design and implementation for Telematics services," Intelligent Computing and Intelligent Systems (ICIS), 2010 IEEE International Conference on , vol.2, no., pp.206,210, 29-31 Oct. 2010
7. Xueliang Zhao; Dan Tian, "The architecture design of streaming media applications for Android OS," Software Engineering and Service Science (ICSESS), 2012 IEEE 3rd International Conference on, vol., no., pp.280,283, 22-24 June 2012
8. [8] Wei Pan; Weihua Li, "A Penetration Testing Method for E-Commerce Authentication System Security," Management of e-Commerce and e-Government, 2009. ICMECG '09. International Conference on, vol.,no., pp.449,453, 16-19 Sept. 2009
9. Information about TCP/IP port assignments, http://support.microsoft.com/kb/174904, Accessed on February 2011.
10. www.sans.org/reading-room/whitepapers/auditing/port-scanning-techniquesdefense-70
11. http://condor.depaul.edu/jkristof/technotes/tcp.html
12. Jinhua Liu; Wenbo Pan; Jiahui Hu; Xianwei Zhou;Jianwei An,"Research of secure ecosystem based on Android platform," Cyberspace Technology (CCT2013), International Conference on , vol., no., pp.375,379, 23-23 Nov. 2013
13. https://gupea.ub.gu.se/bitstream/2077/27864/1/gupea_2077_27864_1 pdf