iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** VI **Month of publication:** June 2022

DOI: https://doi.org/10.22214/ijraset.2022.43849

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VI June 2022- Available at www.ijraset.com

Research Paper on Enhancing Mobile Security from Vulnerable Attacks

Priyansha Tiwari[1], Santosh Kumar Singh[2]
[1]*B Tech (CSE), Manav Rachna International Institute of Research and Studies, Delhi India*
[2]*Asstt Professor, Shri Shankaracharya Professional University Junwani Bhilai Chhattisgarh India*

Abstract: ***The use of Smart phones has come veritably popular around the globe in this digital period and in recent days its stoner's number has increased at indefinite position, as everyone rush to explore the digital world. The people are switching towards Smart phones in order to pierce numerous operations similar as fiscal, business, educational and social etc. Thus these bias are the main target of hackers, still on the other hand the Smart phone manufacturers are trying to design stylish security model to overcome all vulnerabilities. Then we bandy the Android Security armature and possible attacks to android OS and also punctuate the pitfalls which are associated with this particular bias. This paper describes the vulnerabilities plant in Android grounded Smart phones and also describes the attacks like honour escalation, sequestration attack and other pitfalls which are associated with these particular bias. In last section we bandy the possible countermeasure against the attacks and pitfalls due to that, the Android Smart phones come vulnerable.***
Keywords: Vulnerability, Threat, Hacking.

I. INTRODUCTION

The Android Smartphone has come truly popular because of its swiftly adding operations related to gaming, education, business, banking, and social networks. Hence the Smartphone store has different type of information in their database analogous as help, banking account and information related to businesses and the security is critical issue for Smartphone against above stated information. As the android is an open source of operations which are developing truly swiftly and because of these open source operations the hackers can easily target the Smartphone. Among those operations may be some are malware but stoners are Ignorant about that. This paper is study predicated which bat different vulnerabilities, hole falls and attacks associated with it. There are various malware are being for Android Smartphone in request which might lead to different type of attacks, some of these are mooted in this paper with three possible countermeasure. This paper is salutary for those stoners, operation formulators, security professionals and for those who are interested in mobile security. The paper is organized in different sections. The first section bandy the Android security architecture in which summaries authorization medium, sandboxing, access control and also define the Factors encapsulation and operation signing and Alternate section bandy Vulnerabilities in Android Smartphone like web view, SSL/ TLS and NFC. It also highlights vulnerability regarding social and sharing authentication excrescencies. Third section is about the security challenges where we discusses the different risks to Android due to that possible attacks compromised the security of Android smart phones just like honors escalation attach, communication attack, insulation affiliated attack. This section also describes about the malware attack, it also describes the difference between possible risks with respect to attack. In the last we recommend the possible countermeasure which describes result forthe vulnerabilities, risks and attacks that are mooted in this paper

II. .ANDROID SECURITY ARCHITECTURE

Android security Architecture consists of the following factors. How we can cover the information with different encryption. The android has limited resource, so it's veritably delicate to apply traditional security services. Thus experimenters are trying to propose different behavioural approach to guard against malware. bandied android security Armature and its issues, malware discovery and analysis through both approaches dynamic and static, and also bandied malware penetration and covert ways.

A. Sandboxing.

The Sandboxing is used to separate the application from system resource. Due to sandboxing each application has unique identifier to access its own file, and also other file whose marker as read/write / executable for other application.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VI June 2022- Available at www.ijraset.com

B. Application Signing.

The application signature is verified in an Android Smart phones through cryptographic mechanism. Due to this cryptographic signatures built the trust to developer among these applications. There is certificate which is self-signed by developer that is validated at the installation time of application. This help application to identify the originality and also share with same processes that are related with same certificate.

C. Access Control.

In access control, the mechanism of each file has particular access rule and each process assign a User ID. Each file has rule for user, group and for everyone. Each process has a particular permission to read, write or execute the file.

D. Normal Permission

Normal permission provides access on application level functionalities. It allows access data or resources outside the app's sandbox where there is only minor risk involved which does not need explicit user's approval. However, the user able to review which normal permission is grated after the application installation.

E. Shared User ID

Shared user ID enables Android system to share data between application components. Both applications need to be signed with same digital certificate in order to be assigned a shared user ID as shown in image. Developers will able to pass through the restriction on isolation model & both applications will gain access to run in the same process.

F. Signature Permission

Signature permission has to be granted for the application to sign with the same certificate as the application asked for permission. Signature permission works like shared user ID, nonetheless, it provides more control between applications when sharing same digital certificate. Android system will grant for permission before installation.

G. Components Encapsulation.

The components are declared as private as well as public. Within same application, private components are accessible for each other. The public components are accessible by other application which is not in the same sandboxing, having full accessible permission, it also restricted through with customized permission.

III. POSSIBLE ATTACKS

There is much vulnerability in android smart phones that use public network to access many services like financial, connected to public network might be vulnerable to Attackers. Some of Android vulnerabilities are discussed below.

A. Android SSL/TLS

This vulnerability is found by German researcher, it's found due to poor SSL/TLS implementation, these implementation come by way of customized SSL code that as more permissive than default Android setting. During analysis of Google Play marketplace there are 41 applications are credential for bank account, e-mail account, social media account and remote out of 100. Due to poor SSL implementation in third party application, there are 185 million users could be affected.

B. Android NFC

Charlie Miller found this vulnerability; it shows that how Android Smartphone could allow for exploitation through NFC to take over device by using hardware or device within distance of few centimetres to attack a phone. NFC vulnerability are very critical due to that attacker has full control over the Smartphone so he/she may do any operation on it.

C. Social and Sharing Authentication Flaws

The Smartphone (Android) in which social application such as Face book, LinkedIn, twitter, and other applications which saved authentication password in unencrypted plaintext so it is vulnerable. Attacker might be installed in any malware on Smartphone which may be transferred to these unencrypted plaintext to remote side command-and-control server. So all social application might have threat because of this vulnerability.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VI June 2022- Available at www.ijraset.com

D. Zygote Socket (Android)

There is vulnerability in Zygote socket so there are many Zygote process built and flooding, so that consume the all resource of Android Smartphone due that DOS attack can happen and it reboot the phone.

E. Dirty USSD (Unstructured Supplementary Service Data)

This vulnerability is disclosed in September 2012, it allows hacker remotely reset and wipe the android smart phone (Android 4.1 Jelly bean). Attacker to find the vulnerability in the dialler, which is mostly used by operator to send command to phone operator, it uses the USSD code to perform above attack. The attacker might be using NFC, malicious URL or QR code to exploit the vulnerability of Android remotely without user permission. This vulnerability seen in Samsung, after that researcher also find in Android OS. Its countermeasure will be presented in the next section.

F. Repackaging

This susceptibility is observed mostly in business applications which run on Android Smartphone. Anyone could register himself/herself as android application developer, as these applications are open way. Android application easily decompiled so application modified and can be repacked. This vulnerability is caused due to structural characteristics of byte code. The Android application is written in Java in byte code so that code modified and repackaged with Attacker private key, then publish with self-signed on Android market or third-party market.

IV. PROBLEM IDENTIFICATION

This section we show attacks through attacker compromise the Android Smartphone application. The malicious user can publish malware which is distinguished as normal app at app store. Smartphone development increase day-by-day, it uses open space for communication which arisen many security challenges.

A. Privilege escalation Attack

This attack is actually happened due to vulnerabilities in android transitive privilege that allow application to bypass the restriction imposed by the sandbox. There is a weakness in its authorization mechanism so that it may result into privilege escalation attack. In this attack the applications which bypass the restriction of sandbox due to its compromise at run-time and non privilege. It can happen due to an application which has less permission (non-privilege) which is not restricted to access the component of an application which has more privilege (privileged).

B. Cross-Side Scripting Attack

The mobile applications are encoded with web language and native languages, due to web technologies the hybrid application introduce the security risk as compare to other traditional web application. Find out XSS vulnerability on hybrid applications which create possibility for an attacker to bypass access control policies of web View and web kit to run malicious code into victim's Web view.

C. Tap jacking Attack.

In this attack, the attacker hijack the what user tap on his Smart phone. Attacker exploits the vulnerabilities in android UI (User Interaction) component. This is program which is used to intercept and inspect touch events that delivered to foreground activity. This attack can be mitigated through set the Filter touch For Security property to true or override the method.

D. Malware Attack.

These attacks are done through a program which is installed on Smartphone by user to click on any application, Advertise or any way user just click for trustable application but in back end it installs a malicious code on phone which affects it.

E. Privacy Attack.

These types of attacks are related with privacy which leaks the user confidential data, bank account, user contact, meeting schedule, and other social account information to attacker. Back hat, Scroogled ad and other attacker related android privacy.

F. Repackaging attack.

The Hackers use the Reverse Engineering process in which attacker decompiles the DEX file and then it is decompiled into different source code like java. There are many tools are in market which are used to obtain Java code like undx and dex2jar. The decompiling technique is used during repackaging attack; following steps are used in reverse engineering process.

• Modification Point search,
• Recompilation
• Code injection & modification,
• Manifest change
• Self-signing

This attack was found in South Korea in banking application, user perform few steps to transfer money by using Android banking application.

G. Communication Attack

Communication related attack are mostly found in signal transmission, such like GSM network user A5 , A5/2 algorithm to encrypt transmitted signal sending between phone and tower, so attacker might be cracked the A5 algorithm in space or to compromise the Android OS affects the signal. Android based smart phones access internet through Wi-Fi so attacker may perform passive or active attack to crack encryption key of Wi-Fi communication.

H. NFC Attack

Android and Nokia Smartphone also vulnerable through NFC attack, NFC tags built-in antennas and card reader are used to transfer the data from NFC reader to specific phone number or web site and may to specific Smartphone. But it may very dangerous to send malicious web site to Smart phone through Android Bean, and hide from user by using medium of NFC.

I. Smudge Attacks

The mostly Android Smartphone use touch screen for phone lock and unlock, in Android pattern are used for password which are just graphical contact point, user traverse these Point for successful Pattern Match. Attacker use different way to recognize the password pattern such like lighting and camera with different angle as well as different style of light. To recognize the pattern there are different techniques are used to take photograph with different lighting and angle, and also perform some experiment on these photograph to find the correct pattern.

V. METHODOLOGY

Mobile security, which refers to the protection of mobile devices against cyber security threats, is a top-of-mind concern for today's companies due to the growing use of mobile devices for business purposes. As remote workers access corporate data and applications using no trusted mobile devices, companies require an easy-to-use solution that protects their data without negatively impacting employee productivity.

Mobile security is complex because of the large number of potential attack vectors – devices can be targeted at multiple levels:

- *Applications:* Malware can be developed and deployed as malicious apps that users unwittingly install on their devices. Mobile security solutions should be able to detect and block downloads of these malicious apps.
- *Network:* Mobile devices and the legitimate apps that run on them can be targeted at the network level. Man-in-the-Middle, phishing, and other attacks take advantage of network connectivity to steal data or deliver malicious content. Mobile security involves blocking these network-level attacks.
- *OS:* Both iOS and Android operating systems can contain exploitable vulnerabilities, which are used for jail breaking/rooting devices either by users or by malware. This provides an attacker with advanced permissions on the device, breaking its security model. Mobile security incorporates real-time risk assessments, configuration monitoring, and other tools to detect exploitation of device vulnerabilities.

Secure Mobile Access is an important component of an enterprise cyber security strategy. As mobile devices become a more widely-used option for remote work, the data, applications, and systems that they access are at increased risk of compromise by infected devices.

At the same time, mobile security needs to prioritize the needs of the device users, including privacy and usability. Achieving this while providing effective mobile threat defence requires a mobile security solution that implements these core principles of optimal mobile threat defence:

- *Covering All Attack Vectors:* Mobile devices can be attacked via multiple vectors, including at the application, network, and operating system levels. A mobile security solution should provide protection at all of these levels.
- *Full Risk Visibility into Mobile Risk:* Risk visibility is an essential component of enterprise risk management strategies. Mobile security solutions must be capable of providing security teams with an accurate accounting of the risk level of the remote workforce.
- *Enterprise-Level Scalability:* Enterprises may have thousands of devices to manage and secure. Mobile security solutions should be capable of supporting a large and diverse (including both Android and iOS devices) set of devices used for business.
- *Optimized User Experience:* Mobile devices are popular because they increase employee productivity. Mobile security solutions must be designed to have minimal impact on the user experience.
- *Privacy by Design:* Mobile devices used for work may be BYOD and dual-use devices. These devices must be secured in a way that does not compromise the privacy of the devices' users.

Our methodology is to implement SSL code by writing a code in android studio for protection of our mobile from outside attacks. We have developed the system which will protect our mobile device and try to throw back a warning message to attacker system. This concept can be implemented in every mobile for protecting data and sensitive information. The way which will be used in our method is here in the form of block diagram:

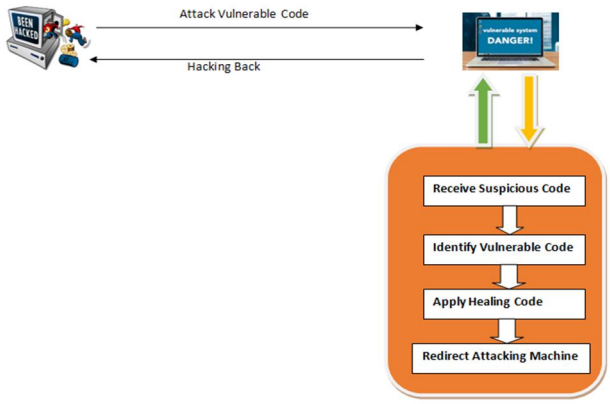


Figure 1: Block Diagram of Security Layer in Mobile Device

VI. RESULT ANALYSIS

After developing the system we can protect mobile from unauthorised access and send a warning message to attacker system. The table explains attack probability before and after SSL security:

SNo	Attack	Before Implementation	After Implementation
1	SQL Injection	80%	30%
2	XSS	90%	35%
3	Mail ware	78%	30%
4	Private	70%	25%

Table 2: Attack Probability

System shows the security enhancement after implementing the techniques.

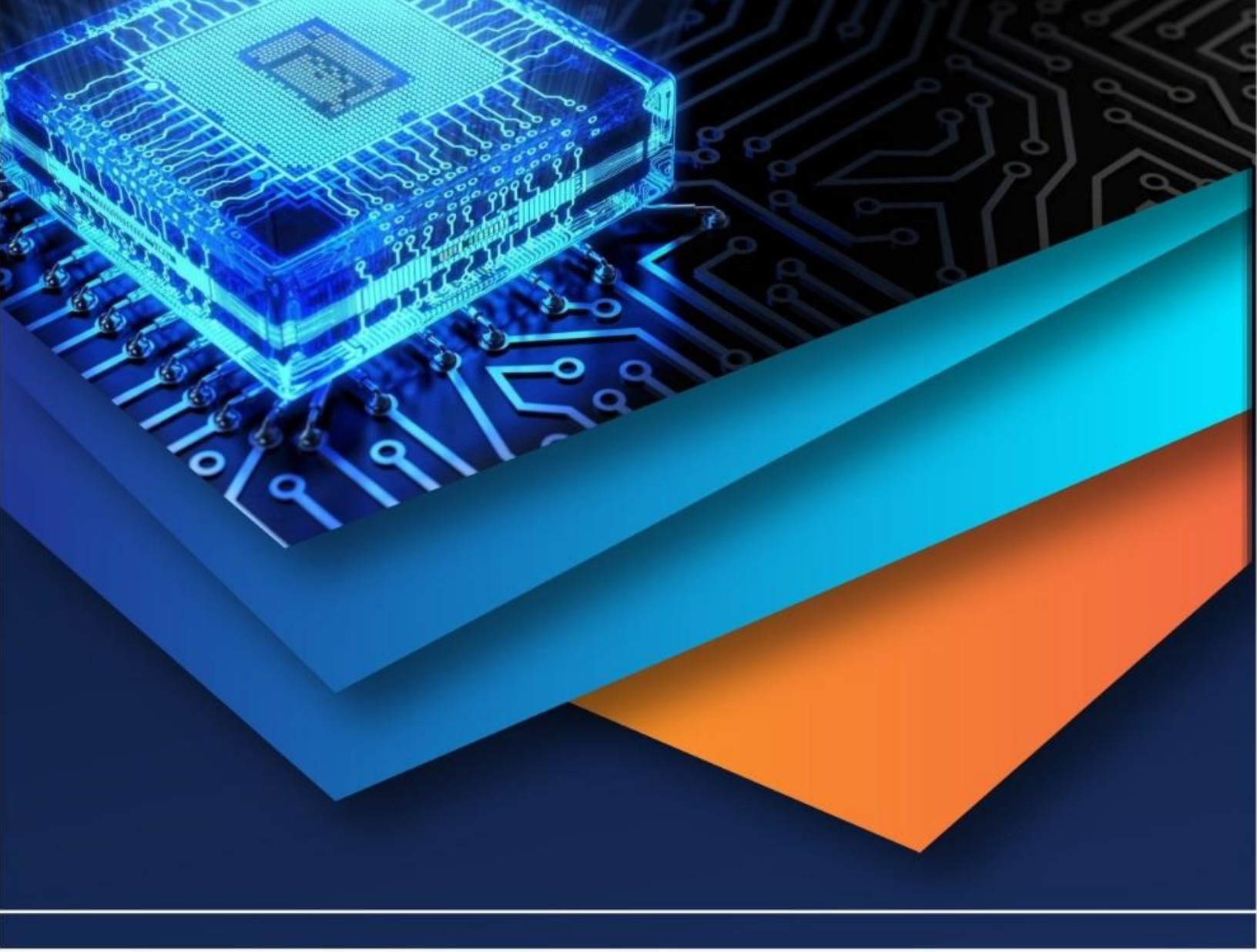
The percentage of companies admitting to suffering a mobile-related compromise has grown, despite a higher percentage of organizations deciding not to sacrifice the security of mobile devices to meet business targets. Mobile security trends create new challenges and opportunities, which require a redefinition of security for personal computing devices. System fulfils the requirements.

VII. CONCLUSION

The security issues in Android based Smartphone have become even more severe because of vulnerabilities in Android design. In this paper, we show the possible vulnerability, threats which make Android Smartphone targeted for attackers. There are some attacks are highlighted by this paper, but still remain many to open research. We also investigated the countermeasures to address the issues, vulnerabilities and attacks. The motivation of this paper was to address issues of poorly designed application, and protect application from threats.

REFERENCES

[1] S. M. Metev and V. P. Veiko, Laser Assisted Microtechnology, 2nd ed., R. M. Osgood, Jr., Ed. Berlin, Germany: Springer-Verlag, 1998.
[2] J. Breckling, Ed., The Analysis of Directional Time Series: Applications to Wind Speed and Direction, ser. Lecture Notes in Statistics. Berlin, Germany: Springer, 1989, vol. 61.
[3] S. Zhang, C. Zhu, J. K. O. Sin, and P. K. T. Mok, "A novel ultrathin elevated channel low-temperature poly-Si TFT," IEEE Electron Device Lett., vol. 20, pp. 569–571, Nov. 1999.
[4] M. Wegmuller, J. P. von der Weid, P. Oberson, and N. Gisin, "High resolution fiber distributed measurements with coherent OFDR," in Proc. ECOC'00, 2000, paper 11.3.4, p. 109.
[5] R. E. Sorace, V. S. Reinhardt, and S. A. Vaughn, "High-speed digital-to-RF converter," U.S. Patent 5 668 842, Sept. 16, 1997. (2002) The IEEE website. [Online]. Available: http://www.ieee.org/
[6] M. Shell. (2002) IEEEtran homepage on CTAN. [Online]. Available: http://www.ctan.org/tex-archive/macros/latex/contrib/supported/IEEEtran/ FLEXChip Signal Processor (MC68175/D), Motorola, 1996. "PDCA12-70 data sheet," Opto Speed SA, Mezzovico, Switzerland.
[7] Karnik, "Performance of TCP congestion control with rate feedback: TCP/ABR and rate adaptive TCP/IP," M. Eng. thesis, Indian Institute of Science, Bangalore, India, Jan. 1011
[8] J. Padhye, V. Firoiu, and D. Towsley, "A stochastic model of TCP Reno congestion avoidance and control," Univ. of Massachusetts, Amherst, MA, CMPSCI Tech. Rep. 99-02, 1999.
[9] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification, IEEE Std. 802.11, 2018.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY