International Journal of Control Theory and Applications

ISSN : 0974-5572

Volume 10 • Number 4 • 2017

Analysis of Android Operating System Security Risks

Kashish Handa[*], Shubham Kumar Sharma[*], Kiran Khatter[**] and Rachna Bahal[*]

[*] *Manav Rachna International University, Faridabad, India*
[**] *Accendere Knowledge Management Services Pvt. Ltd., Delhi, India (corresponding author)*

Abstract: The Android based Smartphone is getting immensely popular by providing various functionalities in terms of online banking, online shopping and online learning facility in addition to its basic function to communicate each other. These devices store personal information such as address book, banking details, credit card details etc. with user friendly GUI and high speed processor. This makes the Smartphone as a valuable asset which needs to be kept secure from intruders. Since Android Operating is an open source system, it is more vulnerable to attacks and has drawn the attention of intruders who may control over the gadget and impersonate the device user to intercept the data and manipulate the services offered by the Smartphone. There are different propelled highlights in Android Working Framework through which client can undoubtedly share and download the applications from Google Play Store and unofficial market. But unofficial market attracts customers to download various applications with heavy discount on products or payback offers which may carry malwares and hijack the private data stored in the Smartphone. This paper discusses the Android architecture and presents an overview of various Android attacks and intrusion detection systems. It also discusses how a malware can propagate to Android Smartphone and what can be the possible threats. Finally, it discusses the various measures to improve the security of an Android Operating System.

Keywords: Android, Malware, Intrusion, Security Risk

1. INTRODUCTION

Android, the world's most mainstream portable stage. Android powers a huge number of cell phones in more than 190 nations around the globe. It's the biggest introduced base of any portable stage and developing quick—consistently another million clients control up their Android gadgets interestingly and begin searching for applications, diversions, and other advanced substance. Android is one of the quickest developing Smartphone working framework in the business. Android was conceived on November 5, 2007. From that point forward it has turned into an exceptionally effective working framework, information from Android Central proposes that is has now 1.4 billion gadgets under its grip. The main rendition to be propelled in the market was Android 1.5 Cupcake in spite of the fact that not being extremely well known it helped the organization to pick up enthusiasm of speculators like T-portable. In only 2 years gap a more predominant adaptation Android 1.6 Donut was propelled on October 1, 2009. This adaptation made individuals considering Android more important due its components, for example, Expanded Search Framework, Android 1.6 elements a multi-lingual discourse amalgamation motor called Pico, Battery use pointer, Android 1.6 incorporates an updated seek system that

gives a speedy, compelling, and steady path for clients to look over various sources, and so on. In any case, the adaptations that genuinely lifted the working framework were the Android 2.0 Éclair, 2.2 Froyo and 2.3 Gingerbread and contributed in making the Android business hit [1].

2. NEED FOR MOBILE SECURITY

Our Mobile devices know more about us than anyone else, Our Android devices are more than just communication devices, they like to store the information for what we browse, like, do, watch, listen, search, where we go, Personally Identifiable Information, Mobile banking, e-commerce, social networking passwords, They are, in a way, a reflection of our personal identity.

For corporations it's about branding and law, Security flaws in banking and payment apps, Law suits on Apple, Pandora, Weather channel for privacy invasion, Congress has introduced a bill on how Geo Location services can be used in Mobile devices, For Marketers and Advertisers mobile devices and their apps have information that is worth a gold mine, A lot of attention from Media.

To make the device more robust in security mechanism, Android works with device developers and security implementers. Android is an open source platform in which developers uses advanced software and hardware to bring the advance security level. The Android platform provides an application environment to protect the data, device, network and also the confidentiality, integrity, and availability [2]. Securing this open source platform requires a strong level of security architecture. To build new secure applications in a stable platform, Android provides additional support to the developers. This additional support includes the Android security team which looks for the vulnerabilities in applications to detect loopholes and patch. For every other Android device which has an inbuilt Google play, play services delivers security OTA(Over The Air) updates or patches for critical software libraries, such as for OpenSSL, which is responsible for secure application communication. There is a tool for testing SSL that helps developers to find security issues on whichever platform they are developing [3].

To be the best platform on any smart device, Google provide a set of security services:

Android updates: Most of the Android devices are still running on older versions of Android. Half of its users are open to attacks due to running old versions of the Operating System(OS) which is more vulnerable to assault, so installing new updates on a daily basis reduces the possibility of getting intercepted. The Android update service delivers new security updates and patches, which can be through the web or an over the air(OTA) update [4].

Verify Apps: The newer versions of Android has the capability of detecting the harmful applications automatically which then warn to the user and automatically stops the installation process, and constantly scan applications on the device, and show warning threats about installing or removing harmful applications[4].

SafetyNet: Rooting the Android device gives the full access of the system to the user, one can even modify the kernel, but there are some applications like Google's Android Pay and Google Wallet which would not able to assist the user on any rooted device. To check the root access of the device Google uses SafetyNet to detect whether the device is rooted or not, if it turns to rooted it just block the access to those applications which can intercept user details. SafetyNet provides an extra security layer on running applications, it is an open source library for the Google Safety NetAPI[4].

SafetyNet Attestation: SafetyNet's attestation is a verification system that scans devices requesting for the app to run. It is designed to test the device for system compatibility and it can block any device which is in a tampered state. However, this system test is only designed to check for any signs of tampering within the device. The test does not cover whether the device is not up to date or its system vulnerable to tampering. SafetyNet attestation is a Google telling the app their opinion regarding the CTS compatibility status of a device. CTS normally stands for Compatibility Test Suite, which is a suite of tests a device must pass, prior to release, to be allowed to include Google Play Services[5].

Android Device Manager: Android has a great tool which can help locate the stolen Android device and can provide the feature in which user can remotely wipe out the device's data. This web based or Android based tool can be easily downloaded from the online market[6].

Encryption: Encryption is a method of protecting the data from people you don't want to see it. It is the way toward encoding all client information on an Android gadget utilizing symmetric encryption keys. Once a gadget is scrambled, all client made information is naturally encoded. Encryption guarantees that regardless of the possibility that an unapproved party tries to get to the information, they won't have the capacity to peruse it. Android has two techniques for gadget encryption: Full-plate encryption and Record based encryption.

Full-Disk Encryption : Android at least 5.0 sponsorships full-disk encryption. Full-disk encryption uses a lone key secured with the customer's contraption watchword to guarantee the whole of a device's userdata section. On the start of boot, the customer must give their accreditations before getting to any part of the plate. While this is extraordinary for security, it suggests that a huge bit of the middle handiness of the phone in not in a flash open when customers reboot their device. Since access to data is secured behind the single customer capability, highlights like alerts couldn't work, openness organizations were difficult to reach, and phones couldn't get calls [7].

File-Based Encryption: Android 7.0 or more backings file based encryption. File based encryption permits distinctive documents to be scrambled with various keys that can be opened freely. Gadgets that bolster file based encryption can likewise bolster another element called Guide Boot that permits encoded gadgets to boot straight to the bolt screen, in this manner empowering snappy access to imperative gadget highlights like openness administrations and cautions. With the presentation of file based encryption and new APIs to make applications mindful of encryption, it is workable for these applications to work inside a restricted setting. This can occur before clients gives their certifications while as yet securing private client data [7].

3. ARCHITECTURE OF ANDROID OPERATING SYSTEM

Android system is made up of different layers of software, basically there are five layers [8], and each layer provides different services to the layers of architecture. Android has its own particular libraries which are composed in C/C++ which helps in developing and designing of any Android based applications. All the different layers will combine together to make the complete OS and applications and shown as below in the Figure 1:

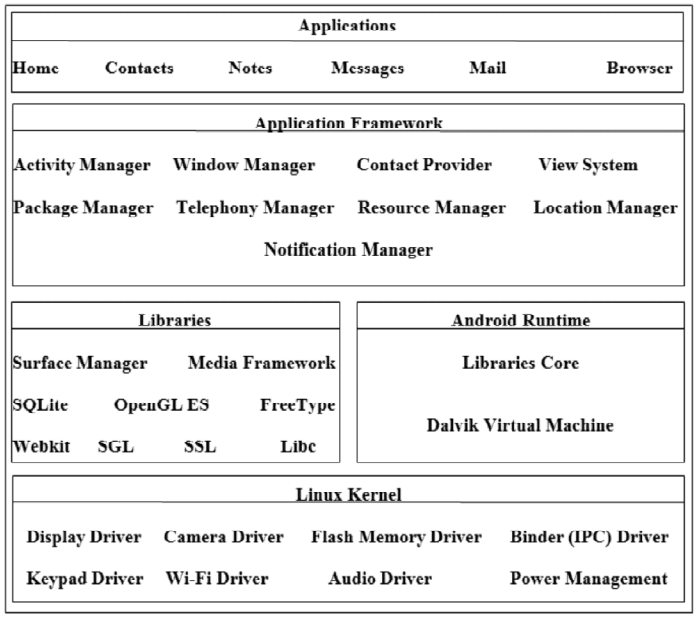

Figure 1: Android Architecture

3.1. Linux Kernel

Android operating system is built on the top of the Linux 2.6 Kernel [9]. Linux Kernel 2.6 is placed at the bottom of the software layer. The Android working framework is completely based on this base layer with a few changes made by the maker: Google. This bottom layer provides various services like memory management, device management, process management and security etc. which deals with the hardware mechanism, with this layer Android operating system interacts with the hardware part of the device. This layer makes the scaffold amongst equipment and programming application for instance portion equipment must have a bluetooth driver introduced on it, to speak with the Bluetooth application. Linux bit layer is additionally in charge of overseeing virtual memory, systems administration, drivers, and power administration[10].

3.2. Libraries

The following layer is the Android's local libraries. Every one of these libraries are composed in C or C++. This layer is in charge of empowering the gadget to deal with various sorts of information inside a casing. These libraries can't be gotten to specifically from outside, to get to these libraries we require the need of utilization system, with the assistance of use structure, we can get to these libraries. There are numerous libraries like web libraries to get to web programs, libraries for Android and video groups and so forth. Android's local libraries are at the second from Linux part layer. There are some critical local libraries, for example, Surface Chief, SQLite, Webkit, Media Structure, OpenGL and Libc. Surface Chief manages the surface parts that are and deals with the show of the gadget. SQLite is the database motor utilized as a part of Android for information stockpiling purposes which is accessible to all application on the gadget. WebKit gives different instruments to perusing the web. Media Structure is in charge of recording of various sounds comprise of various bundles of codec's. OpenGL used to render 2D or 3D design substance to the screen and Libc contains the framework related C libraries[11].

3.3. Android Runtime

It gives the usefulness of the JAVA Programming Dialect. In this little area, all the Android applications are executed. Android utilizes its own particular Virtual Machine (Dalvik VM) to execute the Android application, client can likewise run and executes numerous applications in the meantime with the utilization of DVK. It is situated on an indistinguishable level from the library layer [11]. Dalvik Virtual Machine is a kind of Java Virtual Machine utilized for running applications on Android gadget. DVM is created by Dan Bornstein from Google [12] . DVM requires more opportunity to execute an application. So with the new arrival of Android Google has presented another virtual machine called as ART(Android Runtime). Candy was the first to have supplanted DVM machine by Workmanship. Craftsmanship has many preferences over DVM, for example, AOT (Early) and enhanced trash gathering which help the execution of applications altogether.

3.4. Application Framework

In this layer, there are the supervisors which empower the consent of getting to the information for those applications which are in creating mode. In spite of the fact that it is a structure anybody or any application can specifically connect with it. This layer deals with the fundamental elements of telephone like asset administration, voice call administration and so forth. The Application Structure layer gives numerous larger amount administrations. Application designers are permitted to make utilization of these administrations in their applications [13,14]. There are some imperative pieces of Use Structure, for example, Action Director, Content Suppliers, Communication Supervisor, Area Chief, Asset Administrator. As the name proposes movement director, deals with all the action of an application and it additionally deals with the life cycle of uses and Substance Suppliers deals with the information sharing amongst applications and furthermore oversees how to get to information from different applications by means of making a vacant system in like manner Communication

Chief deals with all voice call related functionalities and Area Supervisor is utilized for Area administration, utilizing GPS or cell tower, Asset Administrator deals with the different sorts of assets utilized as a part of use [13,14].

3.5. Application Layer

This Application layer is the topmost layer in the Android architecture and this is where our applications are going to be placed for different operations. It is the most upper and last layer in Android architecture. All the applications such as camera, Google maps, browser, SMS, calendars, contacts are native applications and used to run in this layer. These applications work with end user with the help of application framework to operate. Some applications are preinstalled with every device such as SMS app, Dialer view, Web browser, Contact manager ad gallery etc. A developer can write his own applications using different platforms which can be replaced with the existing applications [13,14].

4. RELATED WORK

Android creators have certain ways to protect the privacy of a user but at the same time there are many loopholes in this protection system which hackers exploit for personal gains. There are various researchers who highlighted the vulnerability issues in profound details. Android platform provides functions that are easily accessed by allowing various forms of attacks based on its openness and portable feature[15]. We can classify malicious apps into Repacking, Update-Attack, and Drive-by-Download and stand alone [16] [17].

In repacking hackers download an already registered application and modifies its source code with the malicious content [18]. These types of apps are capable of leaking all sorts of private info from personal to financial information.

In an update attack hackers create a new version of the app that is already there in users Smartphone [18]. As soon as the user downloads the new version of the app his phone is infected with the virus.

In Drive-by-download malicious software is downloaded without the user's knowledge. The app itself in this case is not infected but rather downloads the infected app from private servers [19]. These infected apps generally contain Trojans and spyware to keep tabs on user's sign-in and sign-outs from accounts.

There is an existing security system which is implemented by the Google is known as Crowdroid. Existing Crowdroid system uses Strace tool, which can be run on Android based kernel in a bid to collect system call events from mobile devices. In this system both normal and malicious apps are executed [20]. After the execution the app calls some system events that are necessary in order to execute the app. There is difference between system events executed in the normal app and the malicious app and we can determine the difference between the executions and hence would be able to differentiate between a harmless and a rouge app. For example if there are 17 different events being executed in the rouge application than that app would be automatically characterized as a malicious app [21]. However this system has flaws that can be discriminated by the hackers in order to exploit Android users. This system also does not support real time app evaluation meaning that data is sent after the app is executed therefore spreading the virus.

Ham & Lee (2014) presented various techniques to effectively detect the malicious apps which are easy to install and use on its Android based commercial mobile device environment. They have introduced a model to perform real time call evaluation. They also suggested a malicious app distinction method by assign weighted value k to activated event in the malicious event group to distinguish the malicious app through the analyzed similarity.

This method helps to find the characteristics of system call events occurring upon executing malicious apps and it can be applied in order to discriminate malicious apps from normal apps. This is not the only method

to detect malicious behavior. System can detect mobile malware by identifying suspicious network activities through real-time traffic analysis, which only requires connection establishment packets.

[22] Endeavored to identify another kind of versatile malware with self-redesigning abilities that were as of late found on the official Google Android commercial center. [P. B &Chandre(2015)] utilized Semi-Administered machine realizing, which is only a piece of counterfeit consciousness intends to give application the capacity to take in the framework without being modified, techniques are utilized for taking in the ordinary conduct of any application and use to identify the startling conduct of the application. These strategies were actualized and assessed on Android gadgets by P.B and Chandre in 2015. The assessment tests exhibit that different applications have particular system movement designs and certain application classifications can be recognized by their system designs; Diverse levels of deviation from typical conduct can be identified precisely, On account of self-overhauling malware, unique and contaminated renditions of an application have distinctive and discernable system activity designs that as a rule, can be distinguished inside a couple of minutes after the malware is executed while introducing low false alerts rate; and neighborhood learning is practical and has a low execution overhead on cell phones. Distinctive applications have diverse system activity designs over the system which can be utilized to distinguish the malevolent substance in a way like, if there exists two same utilization of various sorts, for instance, on the off chance that one is a unique application and another is fixed then the system movement design dependably be not quite the same as each other for those two applications [23].

The bundles sent over the system and got by the system dependably have an alternate example of way which recognized the two applications. This review created independent applications in two forms one was in J2SE (Java stage, Standard Version for desktop environment) and another was in J2ME (Java stage, Small scale Release). The applications were situated in an online customer to distinguish the movement designs over the system. Along these lines, the review introduced framework for recognizing the applications over the system movement design [24].

For giving a layer of security, Android applications keep running in an application sandbox. It is the dividers of a sandbox which keeps the sand from getting out. A sandbox is a security instrument for isolating running projects. It is regularly used to execute untested code or projects from un-confided in clients and sites. By utilizing sandboxing method constrained access to gadget's assets is given. Along these lines security of the framework is expanded. Sandboxing innovation is habitually used to test unsubstantiated projects which may contain an infection or other malware code, without permitting the product or code to hurt the host gadget. With the assistance of sandbox un-trusted program get to just those assets of the gadget for which authorization are allowed. Authorization is denied on the off chance that it tries to get to different assets of the gadget.

For inter-process correspondence a few applications still utilize conventional Linux procedures, for example, arrange attachments, record framework and shared documents. Be that as it may, Android working framework additionally gives new component to bury prepare correspondence, for example, Folio (an element which permits exercises and administrations acquire a reference to another administrations. It permits not just send messages to administrations but rather specifically conjure strategies on them), Administrations, Aims (are messages which parts can send and get. It is an all inclusive component of passing information between procedures. With help of the expectations one can begin administrations or exercises, summon communicate collectors etc) and Content Suppliers. All these instrument permits engineers to check the personality of use and furthermore used to set the security strategies.

Different authors have proposed different Intrusion detection systems to tackle these malware attacks-

4.1. Security as a Service Based Anomaly IDS

In [25] the creator had proposed a cloud based IDS and recuperation framework for Android. The proposed engineering utilizes the cloud administrations i.e., stage as an administration and security as an administration

for performing interruption location. A lightweight portable host is introduced on the cell phone which investigates the document movement on the framework. Firstly, the objective gadget is enlisted on the cloud server application. The cloud server application sends security techniques, for example, emulator, memory scanners, framework call peculiarity identification and antivirus programming. The portable host produces a special identifier of the record, which is looked at against a store of past dissected records and is sent to the in-cloud arrange examination if the document is not present. After the investigation of record, the outcomes are put away in both neighborhood store on the portable host operator and a mutual remote reserve in the cloud figuring administrations. The intermediary server goes about as a middle person which reflects the continuous activity between the versatile gadget and web and sends it to cloud administrations for further investigation. It controls the entrance of gadgets to different applications and administrations.

4.2. Signature-Based HIDS

In [26] author proposed a framework in which the client needs to confirm to the framework by making a record. The log records from the gadget are nourished to the framework. The Log Document Decoder Module sorts the record into a characterized and organized fashion for framework investigation and the outcome is sent to the Location engine which contrasts the records and the govern sets. If there should be an occurrence of no coordinating thing, common activity is done and the framework goes to this next record to handle. With the motivation behind adjusting the changing Web and new interruption conduct, the proposed framework has Upgrade Run set interface to redesign lead set which is empower to identify.

4.3. AMOXID IDS

In [27] the creator proposes a host based IDS named AmoxID for cell phones. The model proposes classification of dangers into three primary classifications: 1-Dangers to client's involvement; 2-Cost producing dangers; 3-Protection in-bordering dangers. Every class is dissected independently and manages three diverse subsystems in IDS for cell phones. The model proposes arrangement of strategies relying upon the client's present system, distinctive approach levels is connected. To make the confirmation of idea the model is utilized as a part of an organization where workers are given a cell phone which obliges them to take after certain strategy. In the event that organization sends private messages and gives secret information to workers that are gotten to through cell phone, then it is vital to secure this data. Uncommon outlining approaches are incorporated into pre-constructed IDS authorizing different arrangements relying upon the client's current system. The elements, for example, quantities of active call, active SMS, association with GPRS are followed utilizing SVM order.

4.4. Andromaly Framework

The paper [28] proposes an anomaly behavioral-construct recognition system which acknowledges in light of HIDS observing different elements and occasions from the gadget. Machine learning techniques are connected to group the gathered information as ordinary or stomach muscle typical. The structure assesses diversions and apparatus applications adequately identifying application having comparable conduct. The component extractor gathers different elements from the gadget and pre-handles the crude elements. The processor performs examination and produce yield dangers appraisal which are given to the danger weighting unit. The risk weighting unit applies group calculations, (for example, Dominant part Voting, Conveyance Summation and so forth.) to infer a last intelligible choice with respect to the contamination level in gadget. The administration specialist is a vital part which synchronizes highlight accumulation, ready process and malware discovery. The graphical UI arranges the operator's parameters, initiate or deactivate, visual investigation and visual cautioning of gathered information.

Anomaly Based IDS The paper [29] proposed a proactive protection instrument in which the cell phone client is given the alarm before downloading the document. The creator made a web server where substances are

entered. The properties of all the documents go into a cloud server and furthermore a string coordinating calculation is gone into the cloud for correlation. The client first registers itself indicating the gadget OS and application records, so an imitated picture is made in cloud. The correspondence between the cell phone and the Web is copied and sent to the emulator in cloud where the location, crime scene investigation examinations are performed. The observing and recognizing process is produced in cloud for recognizing any interruption in the web server. At the point when the demand is send by the customer it is sent to the cloud where cloud server distinguishes any adjustment in the substance of the document in light of the string coordinating calculation. On the off chance that any unsecured record or rowdiness is recognized, framework takes the comparing reaction activities to deal with the danger. This framework produces exact interruption identification and is versatile to any number of clients.

5. TYPES OF ATTACKS

Malevolent programming ("malware") that is planned particularly to focus on a cell phone framework, for example, a tablet or cell phone to harm or disturb the gadget. Most versatile malware is intended to cripple a cell phone, permit a noxious client to remotely control the gadget or to take individual data put away on the gadget.

The **Android Walkinwat malware** covers itself in tainted renditions of "Walk and Content," in a sort of assault known as "Shameware," which communicates something specific or endeavours to urge activity by openly humiliating the client. Amid the Walk and Content assault, the malware peruses through the contacts on the client's Android cell phone so as to impact out a mortifying SMS message calling attention to that the application the client has downloaded is in certainty a modest, pilfered duplicate. Combined with the instant message impact, the assault will likewise show a discourse to the client, offending him or her for downloading a pilfered application. The expectation of the assault is an angled endeavor to disgrace the client into acquiring the true blue application.

Dog Wars-Beta Like the Walk and Text risk, this assault is outlined exclusively to send a political message and disgrace the client. Amid this Android Trojan assault, clients are made a request to allow authorization to introduce an application on their telephone that indicates to be the Android diversion Dog Wars. Once introduced, the show symbol of the false Dog Wars application packaged with the Trojan shows up practically indistinguishable to that of the true blue application. In any case, one little contrast is that the symbol of the malignant application peruses PETA rather than BETA. The Trojan code is then infused as a bundle called Dogbite. Once the contaminated gadget begins up, an administration called, "Rabies" dispatches out of sight. As the Rabies administration is executed, it conveys an instant message to everybody on the contact rundown of the client's telephone.

At its center, **Zitmo** works as a man-in-the-center assault by blocking two-step confirmation that banks use to approve the character of the record holder when entering login certifications, commonly with a one-time secret key that is sent to a cell phone by means of SMS. Amid the assault, the malware basically lifts SMS writings containing financial balance, passwords and other touchy data sent to the client, which are then quickly piped to a remote server. Regardless of the possibility that a specific bank doesn't require two-calculate verification, Zitmo can forward and keep an eye on all SMS messages, making it a substantial risk.

Droid Kung Fu, bit of Android assault, targets cell phones running Android 2.0 or more prominent, associates contaminated Smartphone to a remote server. Once traded off, the clients' Android gadget will be able to take after charges forced by the order and control server, including uninstalling a given bundle, downloading a pernicious bundle and introducing it, opening a malevolent URL in the telephone's program and running a tainted application. The tainted telephone likewise reports some individual and framework information back to a similar server, including whether the telephone is established or not, te OS sort, SDK variant, and accessible memory on the SD card, in addition to other things. This malware has been accounted for on informal Android markets.

Android.Lightdd and Android.Jsmshider are two Android malware dangers that open secondary passages on tainted gadgets. The assaults are one of a kind in that they obtain an organized downloader methodology from conventional PC malware trying to muddle disease to the point where a client can't uninstall the vindictive applications.

Android PJ Applications, like most other Android Trojans, spreads by means of changed adaptations of true blue applications facilitated on unregulated third-get-together Android commercial centers. With an end goal to lure potential casualties, the malware takes on the appearance of the well known "Hot Window" application. In any case, while the noxious application includes a portion of indistinguishable capacities from the first, it comes outfitted with extra usefulness that permits an assailant to construct a botnet. In addition to other things, the malware can introduce applications, explore to sites, add bookmarks to the client's program, send instant messages and piece instant message reactions. It likewise sends delicate client data put away on the Android gadget back to the aggressor. In light of its risk abilities, analysts trust it was planned and might be utilized to sell promotion crusades and to acquire profits by the utilization of outsider premium rate administrations to clients' detriment.

Autosub SMS, Android assault known as Android os Autosubsms.A, is a Trojanized variant of an application found on outsider application stores in China. In particular, the Android malware screens instant messages and manhandle premium administrations, and also particular watchwords in instant messages to subscribe influenced clients to a superior administration without their assent, subjecting them to unforeseen charges.

Nicki Spy known as Nicki See, draws casualties by acting like a welcome to Google's new informal organization Google+. Nonetheless, once introduced, the Nicki Spy Trojan plays out a variety of malignant capacities that can likewise be utilized to direct secret activities exercises, for example, gathering instant messages, call logs and GPS area from contaminated gadgets. Every single lifted correspondence are then transferred to a specific URL through port 2018. The Android malware additionally can get charge through instant messages; record telephone calls produced using tainted gadgets and answer approaching calls consequently.

Lovetrap camouflages itself as an affection test application, a digital book peruser or an area tracker. It then continues with its vindictive exercises by recovering the influenced clients' Global Versatile Supporter Personality (IMSI) and sending it to a specific URL. The malware additionally conveys instant messages to subscribe to certain spontaneous administrations, which thus, gather undesirable charges for the influenced client.

Malignant programming ("malware") that is planned particularly to focus on a cell phone framework, for example, a tablet or cell phone to harm or upset the gadget. Most portable malware is intended to incapacitate a cell phone, permit a pernicious client to remotely control the gadget or to take individual data put away on the gadget.

6. INTRUSION DETECTION SYSTEM

An intrusion detection system (IDS) is a gadget or programming application that screens a system or frameworks for malevolent movement or approach infringement. Any recognized movement or infringement is ordinarily announced either to an overseer or gathered halfway utilizing a security data and occasion administration (SIEM) framework. A SIEM framework joins yields from numerous sources, and uses alert separating systems to recognize noxious movement from false cautions. There is a wide range of IDS, changing from antivirus programming to progressive frameworks that screen the movement of a whole spine network. The most well-known characterizations are Network intrusion detection system (NIDS) and host-based intrusion detection system (HIDS). A framework that screens imperative working framework records is a case of a HIDS, while a framework that breaks down approaching system movement is a case of a NIDS. It is additionally conceivable to arrange IDS by identification approach: the most surely understood variations are mark based discovery (perceiving terrible examples, for example, malware) and abnormality based recognition (distinguishing deviations from a

model of "good" activity, which frequently depends on machine learning). A few IDS can react to distinguished interruptions. Frameworks with reaction capacities are regularly alluded to as interruption avoidance framework.ntrusion Detections systems

IDS can be characterized by where recognition happens (system or have) and the identification technique that is utilized.

6.1. Network intrusion detection systems

NIDS are put at a key point or indicates inside the system screen movement to and from all gadgets on the system. It plays out an examination of passing movement on the whole subnet, and matches the activity that is passed on the subnets to the library of known assaults. Once an assault is distinguished, or anomalous conduct is detected, the caution can be sent to the manager. A case of a NIDS would introduce it on the subnet where firewalls are situated keeping in mind the end goal to check whether somebody is attempting to break into the firewall. Preferably one would check all inbound and outbound movement, however doing as such may make a bottleneck that would weaken the general speed of the system. OPNET and NetSim are regularly utilized instruments for reproduction arranges interruption discovery frameworks. NID Frameworks are likewise equipped for contrasting marks for comparative parcels with connection and drop destructive identified bundles which have a mark coordinating the records in the NIDS. When we order the outlining of the NIDS as indicated by the framework intuitiveness property, there are two sorts: on-line and disconnected NIDS. On-line NIDS manages the system progressively. It examinations the Ethernet bundles and applies a few guidelines, to choose on the off chance that it is an assault or not. Disconnected NIDS manages put away information and goes it through a few procedures to choose on the off chance that it is an assault or not [30].

6.2. Host intrusion detection systems

HIDS keep running on individual hosts or gadgets on the system. A HIDS screens the inbound and outbound parcels from the gadget just and will alarm the client or director if suspicious movement is recognized. It takes a depiction of existing framework documents and matches it to the past preview. On the off chance that the basic framework documents were changed or erased, a caution is sent to the director to examine. A case of HIDS utilization can be seen on mission basic machines, which are not anticipated that would change their arrangements [31].

6.3. Discovery methods

6.3.1. Signature-based

Signature-based IDS alludes to the recognition of assaults by searching for particular examples, for example, byte successions in system activity, or known malevolent direction arrangements utilized by malware. This wording starts from against infection programming, which alludes to these recognized examples as marks. In spite of the fact that mark based IDS can without much of a stretch recognize known assaults, it is difficult to identify new assaults, for which no example is accessible.

6.3.2. Anomaly based

Anomaly based interruption identification frameworks were basically acquainted with distinguish obscure assaults, partially because of the fast improvement of malware. The essential approach is to utilize machine figuring out how to make a model of reliable action, and afterward look at new conduct against this model. In spite of the fact that this approach empowers the recognition of beforehand obscure assaults, it might experience the ill effects of false positives: already obscure authentic movement may likewise be delegated malignant.

6.4. Intrusion prevention

A few frameworks may endeavor to stop an interruption attempt yet this is neither required nor expected of a checking framework. Intrusion detection and prevention systems (IDPS) are essentially centered on recognizing conceivable episodes, logging data about them, and revealing endeavors. Moreover, associations utilize IDPSes for different purposes, for example, distinguishing issues with security approaches, recording existing dangers and stopping people from damaging security strategies. IDPSes have turned into a fundamental expansion to the security framework of almost every organization [32].

Intrusion prevention systems (IPS), generally called intrusion detection and prevention systems (IDPS) are framework security contraptions that screen framework or system practices for malignant activity. The essential components of intrusion prevention structures are to perceive malignant development, log information about this activity, report it and attempt to piece or stop it.Intrusion prevention systems are considered augmentations of intrusion detection systems since they both monitor networks movement and additionally framework exercises for vindictive action. The principle contrasts are, not at all like intrusion detection systems, intrusion prevention frameworks are put in-line and can effectively anticipate or square interruptions that are detected. IPS can take such activities as sending a caution, dropping distinguished malevolent parcels, resetting an association or blocking movement from the culpable IP address. [33] An IPS likewise can remedy cyclic repetition check (CRC) blunders, defragment bundle streams, alleviate TCP sequencing issues, and tidy up undesirable transport and system layer choices.

6.5. Limitations

Commotion can extremely confine an interruption discovery framework's adequacy. Terrible parcels produced from programming bugs, degenerate DNS information, and nearby bundles that got away can make a fundamentally high false-caution rate. It is normal for the quantity of genuine assaults to be far underneath the quantity of false-cautions. Number of genuine assaults is frequently so far underneath the quantity of false-cautions that the genuine assaults are regularly missed and ignored. Many assaults are intended for particular adaptations of programming that are normally obsolete. A continually changing library of marks is expected to moderate dangers. Obsolete mark databases can leave the IDS powerless against more up to date strategies. For mark based IDSes there will be slack between another risk revelation and its mark being connected to the IDS. Amid this slack time the IDS will be notable recognize the threat. It can't make up for a powerless ID and validation systems or for shortcomings in system conventions. At the point when an aggressor obtains entrance because of feeble confirmation system then IDS can't keep the enemy from any misbehavior. Scrambled bundles are not prepared by the interruption location programming. Accordingly, the encoded bundle can permit an interruption to the system that is unfamiliar until more critical system interruptions have happened. Interruption recognition programming gives data in light of the system address that is related with the IP parcel that is sent into the system. This is helpful if the system address contained in the IP bundle is exact. Be that as it may, the address that is contained in the IP parcel could be faked or mixed. Because of the way of NIDS frameworks, and the requirement for them to break down conventions as they are caught, NIDS frameworks can be powerless to same convention based assaults that system hosts might be helpless. Invalid information and TCP/IP stack assaults may bring about a NIDS to crash

7. PROPOSED SOLUTION TO MINIMIZE THE SECURITY RISK

The common problem with the available intrusions detection systems are the accuracy and false alarming of apps. Some time normal apps become categorized into malicious app. This could occur because of the following reasons-

- A miss-match of system calls events done by the intrusion detection system.

- The credibility of app and its creator.
- False alarm by the present intrusion detection system.

Rather than having to invest ones resources on intrusion detection systems we suggest a more Android environment friendly approach. We suggest use of an integrated development environment authorized by Google itself. This environment would contain pre-written directories that would ensure the integrity and authenticity of the app.

As seen earlier most of the attacks that have taken place in past few years were because of unauthorized apps. Most of these apps were repacked with Trojan viruses. They were available freely on the internet but were unauthorized by the Google play store. So to counter these problems this integrated developing environment would ensure that every app that is being downloaded by user on their Smartphone is indeed classified as secure by Google play itself. This integrated environment would maintain the developing environment for creators as it would allow them to develop and execute their application with properly imposed legal guidelines and standards. This integrated environment will act like a framework for properly executing applications which would not only analyze system call but would also give them permission to execute them. This way the applications won't be able to execute application's system call events which are unnecessary and uncalled for. Since this app would be approved by Google therefore any un-authorized application won't be able to access resources of Android operating system. It would also provide special environment for developers so that they are able to properly develop their applications without worrying about the denial of permission to access system resources.

8. CONCLUSION AND FUTURE SCOPE

In this paper we reviewed and analysed the available measures used for countering Android intrusion threats in Android operating system and at the same time suggesting improvement in the existing system. The paper highlighted the various intrusions detection systems that are currently available and evaluated works of various authors in this field. In this paper we also suggest our idea of tackling these threats while simultaneously overcoming the disadvantages of currently available intrusion detection system.

REFERENCES

[1] "Android, the world's most popular mobile platform" Tamzin Taylor, Partner Development at Google Play

[2] "Android Security" Adam Donenfeld et al. of Check Point Software Technologies Ltd.

[3] Android Security" Dominik Schürmann of Institute for Operating Systems and Computer Networks, TU Braunschweig

[4] Android Open Source Project. Android Security Overview, 2012.

[5] "Tampered devices via safetynet" 1, September 24, 2015 -Matthias Tan.

[6] "Android Device Manager"Saturday, Jun 28, 2014 -Jerry Hildenbrand.

[7] "Encryption" Dmitry Vyukov of Google Dynamic Tools team.

[8] Wilner Nina (2009) " Android On Power Architecture", ELC, Grenobles

[9] "An Introduction to Android " 16 October 2012 -Michalis Katsarakis

[10] "Android History and Android OS Architecture" 09/16/2013 –compiletimeerror

[11] Wilner Nina (2009) " Android On Power Architecture", ELC, Grenobles.

[12] Enck William, Octeau Damien, McDaniel Patrick and Chaudhuri Swarat "A Study of Android Application Security", Department of Computer Science and Engineering, the Pennsylvainia State University

[13] Zhou Yajin, Zhang Xinwen, Jiang Xuxian, W.French Vincent "Tamming Information Stealing Smartphone Application", Department of Computer Science, NC University

[14] Google Android for Work Security white paper, 2015.https://static.googleusercontent.com/media/www.google.co.il/iw/IL/work/Android/files/Android-for-work-security-white-paper.pdf

[15] Rohit S. Thune, J. Thangakumar,"A Cloud-Based Intrusion Detection System for Android Smartphones,".

[16] Muhamed Halilovic, Abdulhamit Subasi, "Intrusion Detection on Smartphone".

[17] Dr. Marwan Omar, Dr. Maurice Dawson,"Reseach in Progress-Defending Android Smartphones from Malware Attacks," Advanced Computing and Communication Technologies (ACCT), 2013 Third International Conference on, vol., no., pp.288-292, 6-7 April 2013.

[18] Masoud Ghorbanian, Bharanidharan Shanmugam, Ganthan Narayansamy, Norbik Bashah Idris,"Signature-Based Hybrid Intrusion Detection System(HIDS) for Android Devices," Business Engineering and Industrial Applications Colloquium (BEIAC), 2013 IEEE, vol., no., pp.827-831, 7-9 April 2013.

[19] Asaf Shabtai, Yuval Elovici,"Applying Behavioral Detection on Android-Based Devices," Mobile Wireless Middleware, Operating Sys-tems, and Applications, Springer, vol.48, no., pp.235-249, 2010.

[20] Y. J. Zhou and X. X. Jiang, "Dissecting Android malware: characterization and evolution," in Proc. the 33rd IEEE Symposium on Security and Privacy, 2012, pp. 95-109.

[21] Y. J. Zhou and X. X. Jiang, "Dissecting Android malware: characterization and evolution," in Proc. the 33rd IEEE Symposium on Security and Privacy, 2012, pp. 95-109.

[22] X. X. Jiang and Y. J. Zhou, Android Malware, NY, USA: Springer,2013.

[23] M. Nauman, S. Khan, and X. Zhang, "Apex: extending Android permission model and enforcement with user- defined runtime constraints," in Proc. the 5th ACM Symposium on Information, Computer and Communications Security, 2010, pp. 328-332.

[24] Y. J. Ham, W. B. Choi, H. W. Lee, J. D. Lim, and J. N. Kim, "Vulnerability monitoring mechanism in Android based smartphone with correlation analysis on event-driven activities," in Proc. 2012 2nd International Conference on Computer Science and Network Technology, 2012, pp. 371-375

[25] D. James, Android Game Programming For Dummies, Hoboken, New Jersey: John Wiley & Sons, Inc., 2013.

[26] I. Burquera, U. Zurutuza, and S. Nadjm-Tehrani, "Crowdroid: behavior-based malware detection system for Android," in Proc. The 1st ACM workshop on Security and privacy in smartphones and mobile devices, 2011, pp.15-26.

[27] A.P. Felt, et al., "A Survey of Mobile Malware In The Wild," 1st Workshop on Sec. & Privacy in Smart phones and Mobile Devices, 2011.

[28] Rohit S. Thune, J. Thangakumar,"A Cloud-Based Intrusion Detection System for Android Smartphones,".

[29] Muhamed Halilovic, Abdulhamit Subasi, "Intrusion Detection on Smartphone".

[30] Dr.Marwan Omar, Dr. Maurice Dawson,"Reseach in Progress-Defending Android Smartphones from Malware Attacks," Advanced Computing and Communication Technologies (ACCT), 2013 Third International Conference on, vol., no., pp.288-292, 6-7 April 2013.

[31] Masoud Ghorbanian, Bharanidharan Shanmugam, Ganthan Narayansamy, Norbik Bashah Idris,"Signature-Based Hybrid Intrusion Detection System(HIDS) for Android Devices," Business Engineering and Industrial Applications Colloquium (BEIAC), 2013 IEEE, vol., no., pp.827-831, 7-9 April 2013.

[32] Asaf Shabtai, Yuval Elovici,"Applying Behavioral Detection on Android-Based Devices," Mobile Wireless Middleware, Operating Sys-tems, and Applications, Springer, vol.48, no., pp.235-249, 2010.

[33] Abdullah A. Mohamed, "Design Intrusion Detection System Based On Image Block Matching", International Journal of Computer and Communication Engineering, IACSIT Press, Vol. 2, No. 5, September 2013.

[34] "Gartner: Defining Intrusion Detection and Prevention Systems". Retrieved September 20, 2016.

[35] Scarfone, Karen; Mell, Peter (February 2007). "Guide to Intrusion Detection and Prevention Systems (IDPS)" (PDF). Computer Security Resource Center. National Institute of Standards and Technology (800–94). Retrieved 1 January 2010.

[36] Tim Boyles (2010). CCNA Security Study Guide: Exam 640-553. John Wiley and Sons. p. 249. ISBN 978-0-470-52767-2. Retrieved 29 June 2010.