Preeti *et al*, International Journal of Computer Science and Mobile Applications,
Vol.3 Issue. 7, July- 2015, pg. 55-62 **ISSN: 2321-8363**

AN EMPIRICAL STUDY ON SMART ANDROID BASED SECURITY SURVILLANCE FOR DETECTIVE APPLICATIONS

Preeti (M.Tech Network Security)
CSE and IT Department
Bhagat Phool Singh Women University
Khanpur kalan Sonepat Haryana, India
preetytushir@gmail.com

Sunita Rani (Assistant Professor)
Department of CSE & IT
Bhagat Phool Singh Women University
Khanpur kalan Sonepat Haryana, India
sunita.bpsmv@gmail.com

ABSTRACT: **Private internet access gives multi-layered security with protection assurance utilizing VPN servers. The administrations work at the TCP/IP interface level, which implies the majority of the customers applications will be secured, not simply his web program.**

A few, simple to utilize and promptly accessible programming packages that permit spammers and crooks to capture your information exist, with additionally developing every day. The client's information, documents and security may be at danger. The papers describe the functions of android system and VPN. VPN or Virtual Private Network is mostly used in network industry Through the VPN the communication or data transaction is more secure so mostly industry used VPN. Android based systems are widely used as compared to another system.

Introduction

Private internet access gives multi-layered security with protection assurance utilizing VPN servers. The administrations work at the TCP/IP interface level, which implies the majority of the customers applications will be secured, not simply his web program. It is turning out to be progressively more straightforward to seize and take information and data from insecure connections. On the off chance that a client get to the web through public wifi hotspots, shared internet routers, or even through the client's very own provider, client's data, files and privacy may be at risk. The clients information, documents and security may be at danger. Android Sensors supports several sensors. The Sensor class defines several constants for accessing the different sensors.

- Sensor. TYPE_GYROSCOPE
- Sensor.TYPE_MAGNETIC_FIELD
- Sensor.TYPE_ORIENTATION
- Sensor.TYPE_ACCELEROMETER

Most Android devices allow to determine the current geolocation. This can be done via a GPS (Global Positioning System) module, via cell tower triangulation or via wifi networks. In the proposed work , VPN with UDP is used to track the android devices .Till know the researchers were working on the Location tracking using the webservices which is not secure .

VPNs replace a client's IP address with one from the VPN server. IP locations are what sites and third party utilization to distinguish clients and their areas. Since a client's IP location is supplanted by one from the VPN server, sites and third parties can't assemble a profile about the client or tell where they are found. A Virtual Private Network goes about as an encryption passage in the middle of the user and the Internet, verifying that Internet access is mysterious and that your web searching is secure. Many computers connected with a VPN, and the information of these computers is encoded before they interface with the Internet.

Network access Providers consistently utilize Deep Packet Inspection to see what client's do on the web. They utilize this data to utmost association speeds. At the point when a client join with the Internet utilizing an Android VPN, the ISP can just see encoded information and the VPN server but it cannot reach to the data.

1. 2 VIRTUAL PRIVATE NETWORK

A virtual private system (VPN) augments a private system over an open system, for example, the Internet. It engages a PC or network enabled devices to send and get data across over shared or open frameworks as if it were clearly connected with the private framework, while benefitting from the security, convenience and organization plans of the private system. A VPN is made by setting up a virtual point-to-point association through the utilization of committed associations, virtual burrowing conventions, or activity encryptions. Virtual Private Network as a term determines: Virtual – implies that the affiliation is dynamic. It can change and attempt to adjust to unmistakable circumstances utilizing the web's need tolerant limits. Right when an affiliation is obliged it is situated up and kept up paying minimal notice to the framework establishment between endpoints. When it is no more obliged the association is ended, diminishing expenses and the measure of excess base. Private –means that the transmitted data is continually kept mystery and must be gotten to by endorsed customers. This is key in light of the way that the web's remarkable traditions –TCP/IP (transmission control tradition/web tradition) – were not planned to give such levels of protection. In this way, protection must be given by different

means, for example, extra VPN equipment or programming. System –is the whole framework between the endpoints of clients, destinations or hubs that conveys the information. It is made utilizing the private, open, wired, remote, web or whatever other proper system asset accessible.

1.2.1 Types of VPN

There are 2 ordinary sorts of virtual private system, which are remote access VPN and site-to-site VPN.

1.2.1.1 Remote Access: VPN Remote access VPN is incredibly ordinary VPN organization that you can set up in your office or home framework. It can be realized by setting up a VPN entry or server and you can interface with it by using VPN client from distinctive regions.

1.2.1.2. Site-to-Site VPN: Page to-site VPN is the VPN affiliation situated up between two VPN passages that live in two special frameworks over the Internet, so that both frameworks' PCs can exchange data securely. There is no VPN client needed on customer PCs. The VPN affiliation will be set up between both VPN sections. Both VPN entries will scramble and unscramble the correspondence data to ensure the security and respectability of data . The site-to-site VPN can be supported by IPsec tunnel mode, PPTP, L2TP over IPsec tunneling traditions.

1.2.1.2.Android Operation System and Components : Android is a working structure bringing into record Linux with a Java programming interface. The Android Software Development Kit (Android SDK) gives each and every essential device to make Android applications. This joins a compiler, debugger and a contraption emulator, furthermore its own specific virtual machine to run Android programs. Android is at present fundamental became by Google. Android licenses establishment get ready, gives a rich customer interface library, reinforces 2-D and 3-D outlines using the OpenGL libraries, access to the record structure and gives an introduced SQLite database.

1.3 Features of Android

Android is widely used and it is open source and wholeheartedly available to producers for customization, there are no settled gear and programming setups. Regardless, Android itself supports the going hand in hand with parts: Storage — Uses SQLite, a lightweight social database, for data stockpiling.

Connectivity: Supports GSM/EDGE, IDEN, CDMA, EV-DO, UMTS, Bluetooth (fuses A2DP and AVRCP), WiFi, LTE, and WiMAX.

Messaging: Supports both SMS and MMS.

Web program: Based on the open-source Web Kit, together with Chrome's V8 JavaScript engine

Media support: Includes support for the going with media MPEG-4 SP, AMR, AMR-WB (in 3GP holder), AAC,HE-AAC , MP3, MIDI, Ogg Vorbis, WAV, JPEG, PNG, GIF, and BMP **Hardware support:** Accelerometer Sensor, Camera, Digital Compass, Proximity Sensor, and GPS

Multi-touch: Supports multi-touch screens **Multi-tasking**: Supports multi-tasking applications

Components of Android

1.5.1. Activity: It provides to the presentation layer of an Android application. An Activity is a screen. This is somewhat wrong as Activities can be shown as dialogs or straightforward.

1.5.2. Views and viewgroups Views are client interface widgets, e.g. Textview or Button. The base class for all Views is android. The Views frequently have properties which can be utilized to change their appearance and conduct.

1.5.3. Intents: Intents are messages which permit the application to demand usefulness from different segments of the Android system, e.g. from Services or Activities

1.5.4. Services

Services perform foundation undertakings without giving a UI. They can advise the client by means of the warning structure in Android.

1.5.5. Content Provider

Content Provider gives an organized interface to information. By means of a Content Provider your application can impart information to different applications.

1.5.6. BroadcastReceiver

Broadcast Receiver can be enrolled to gets framework messages and Intents. Broadcast Receiver will get advised by the Android framework if the predetermined circumstance happens.

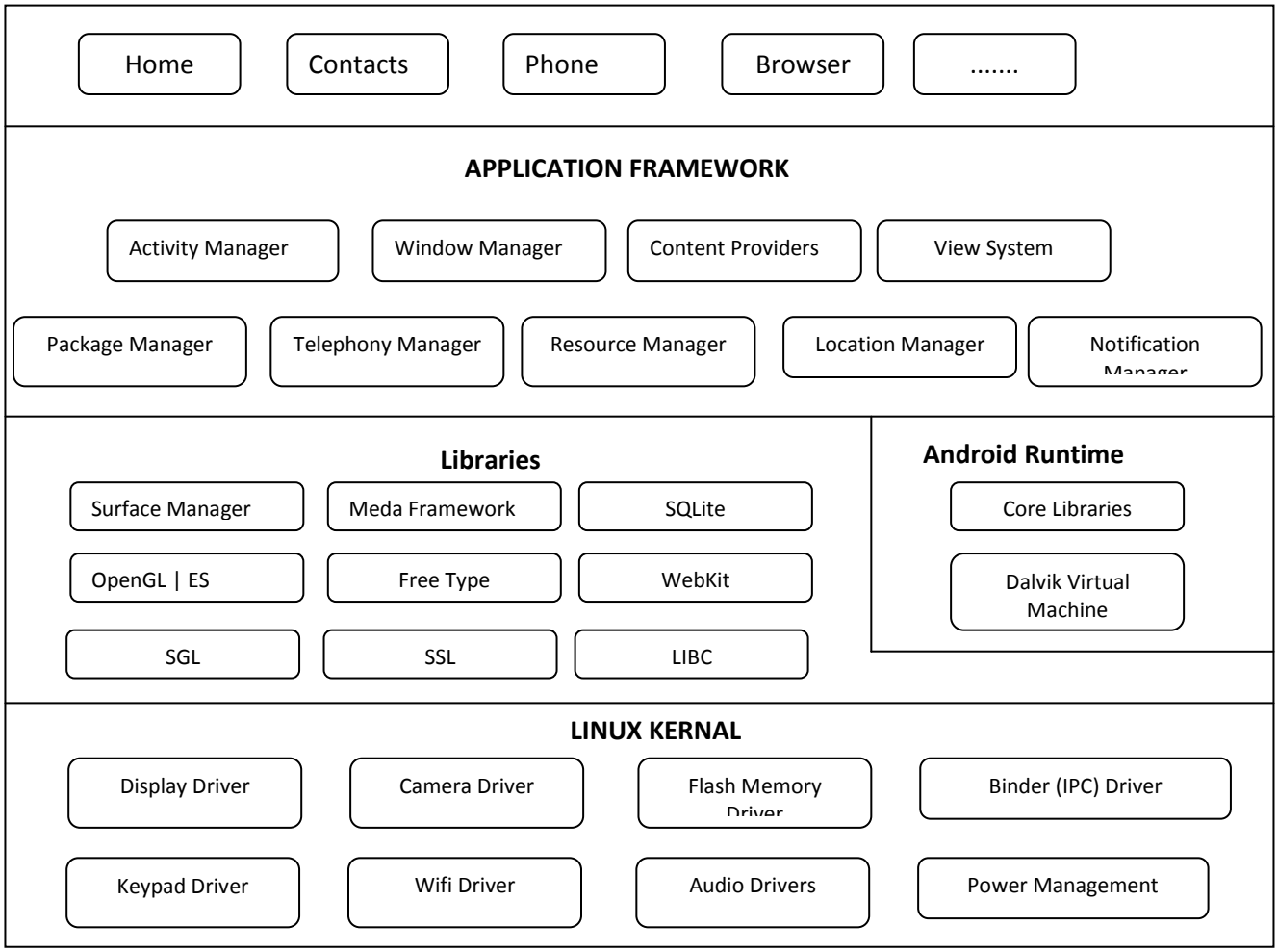
1.5.7.(Home Screen) Widgets: Gadgets are intelligent segments which are essential utilized on the Android home screen. They commonly show information and permit the client to perform activities through them.

1.6 Android Development Tools

Google gives the Android Development Tools (ADT) to create Android applications with Eclipse. ADT is a situated of module which augmented the Eclipse IDE with Android improvement abilities. bytecode which is not quite the same as Java bytecode. Accordingly you can't run standard Java bytecode on Android. The Android framework utilizes an extraordinary virtual machine.

Architecture of Android

Figure 1-1, which shows the various layers that make up the Android operating system (OS).



1.8. The Current State of Android

At first fuelled by the presentation of the iPhone, the cell phone business is becoming exponentially, however there is one OS specifically that has been appreciating especially quick improvement as of late. That framework is Google's Android, which as per Gartner has developed from a 23% piece of the pie a year ago, to turn into the prevailing business power at 38% in 2011[1]. As the client base has developed so too has the dangers connected with the OS. The explanation behind the ascent of Android is decision – buyers have the capacity to browse an expansive scope of makers and value levels restricted to Apple's mono-gadget approach (in spite of the fact that an iPhone "light" has long been reputed). With such a variety of joined gadgets entering pockets and purses, what is the danger for bosses? What measures can purchasers and ventures take to secure the data put away and got to by these gadgets? In spite of some difficult the effect of portable malware as overhyped, new figures would propose something else. Versatile malware was constantly overflowing on Symbian however fast selection of portable stages by both individual and business clients has seen to end up more alluring to cybercriminals. In the most recent year, 20% of all cybercrime in UAE happened on portable devices[2] and Goode Intelligence found that up to 18% of associations in the UK had encountered a versatile malware incident[3]. Such figures exhibit that it is not simply shoppers who are at danger to such dangers however endeavors too that are neglecting to execute viable portable efforts to establish safety. Patterns in portable dangers have coordinated what we see at a more extensive industry level, with Android turning into the most-focused of the versatile stages, as per McAfee, much as Windows has on the PC. The quantity of Android gadgets under botnet control has crested at 40,000 Android gadgets worldwide on a few occasions4, and the issue is deteriorating with Lookout asserting 0.5-1 million clients were tainted in the first 50% of 2011[5]. In Q2 this year there were no new malware marks identified for iOS , while there were 44 for Android in that same time period6. The danger is quite undeniable, and quickly creating. In developing as the top portable stage, Google's minimal green Android has painted a major red focus on itself. The dangers we see showing up on versatile, are not going to be another idea to the security proficient – rootkits, Trojans, and even botnets are showing up. Surely the SpyEye botnet has effectively transitioned from the PC to Android, highlighting the commercialisation of versatile malware.

REFERENCES

1.http://www.webopedia.com/TERM/V/VPN.html

2. MohdNazri Ismail and MohdTaha Ismail; "Analyzing of Virtual Private Network over Open Source Application and Hardware Device Performance"; European Journal of Scientific Research (EJSR), Vol. 28 No.2, pp. 215-226, Euro Journals Publishing, ;Inc. 2009.

3. CISCO VPN and VPN technologies.

4. Author Name: S.Kumudu and A.Seyed Shahrestani, Books: "Wireless VPNs: An Evaluation of QoS Metrics and Measures, Year: 2005 IEEE

5. Author Name: Aruna Malik, Harsh K Verma, Raju Pal Books: "Impact of Firewall and VPN for securing WLAN",International Journal of Advanced Research in Computer Science and Software Engineering, Year: May 2012.

6. Yan Michalevsky, Dan Boneh and Aaron Schulman," PowerSpy: Location Tracking using Mobile Device Power Analysis",arXiv:1502:03,Feb 2015.

7. Aman Kansal, Michel Goraczko, and Feng Zhao,"Building a Sensor Network of Mobile Phones", IPSN'07, April 25-27, 2007, Cambridge, Massachusetts, USA. ACM 978-1-59593-638-7/07/0004**.**

8. A New Sensors-Based Covert Channel on Android, Ahmed Al-Haiqi, Mahamod Ismail, and Rosdiadee Nordin, Sep 2014.

9. Towards Vehicular Sensor Networks with Android Smartphones for Road Surface Monitoring, Girts Strazdins, Artis Mednis, Georgijs Kanonirs, Reinholds Zviedris, Leo Selav, 2011.

10. Wireless Sensor Network Software Design Rules,G Strazdins, L Selavo - 2014

11. Implementation of Participatory Sensing Approach in Mobile Vehicle Based Sensor Networks, A Mednis,Baltic Journal of Modern Computing 1 (1-2), 1-8.

12. Real-time object tracking in 3D space using mobile platform with passive stereo vision system,H Grinbergs, A Mednis, M Greitans.

