ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

Anti-Theft Camera Based Attacks On Mobile Phones

Bhalekar Rohini[1], Devkhile Bhagyashri[2], Gawade Ashwini[3], Prof. Aher S.M.[4]

B.E Student, Dept. of Computer Engineering, SCSMCOE, Nepti, Ahmednagar, Maharashtra, India[1 2 3]

Asst. Professor, Dept. of Computer Engineering, SCSMCOE, Nepti, Ahmednagar, Maharashtra, India[4]

ABSTRACT: Mobile Anti-Theft system is an application based on Android used for tracing back stolen or lost mobile. Once our system is installed onto a mobile phone and an alternate number is fed into the software (ATS). The owners SIM card gets registered in the database. Whenever phone is rebooted ATS is invoked in stealth mode and verifies whether if the SIM card present in mobile phone is of owner. If the SIM belongs to owner (registered in database), the software doesnt do any activity. If SIM is been changed and that SIM is not registered in the database then, ATS sends a message to the alternative mobile number (friends / relatives number which is been saved while installing the application) in stealth mode and starts listening for incoming SMS messages. Now if owner send a SMS request to ATS asking for GPS co-ordinates, ATS would do so. Since our system is based on GOOGLE Android operating system our system would send the complete address (postal address) as to where the mobile is.

KEYWORDS: Android, MMS, Multimedia Message, Snapshots, Emails.

I. INTRODUCTION

An Android operating system (OS) has enjoyed an incredible rate of popularity. As of 2013, the Android OS holds 79.3 percent of global smartphone market shares. Mean-while, a number of Android security and privacy vulnerabilities have been exposed in the past several years. Al-though the Android permission system gives users an opportunity to check the permission request of an application (app) before installation, few users have knowledge of what all these permission requests stand for; as a result, they fails to warn users of security risks. Meanwhile, an increasing number of apps specified to enhance security and protect user privacy have appeared in Android app markets.

Most large antivirus software companies have published their Android-version security apps, and tried to provide a shield for smart phones by detecting and blocking malicious apps. In addition, there are data protection apps that provide users the capability to encrypt, decrypt, sign, and verify signatures for private texts, emails, and files. However, mobile mal-ware and privacy leakage remain a big threat to mobile phone security and privacy.

II. LITERATURE SURVEY

Literature Review As, all the smart phone uses the application from the market, smart phones are possible to get attacked through such malicious application. Next section gives the detail about such security threats. A. Mobile Device Threats Numerous attack exist which compromises security of mobile devices. Three main categories of attacks could be carried over mobile devices which includes- malware attacks, grayware attacks and spyware attacks described as:- 1. Malware These kinds of attacks steal personal data from mobile devices and damage devices. With device vulnerabilities and luring user to install additional apps, attacker can gain unauthorized root access to devices.

Some of the malware attacks are listed as:- (i). Bluetooth Attacks With Bluetooth attacks; attacker could insert contacts or SMS messages, steals victim’s data from their devices and can track user’s mobile location. Blue-bugging is kind of blue-tooth attack through which attacker could listen conversations by activating software including malicious activities . (ii). SMS Attacks Through SMS attacks; attacker can advertise and spread phishing links. SMS messages can also be used by attackers to exploit vulnerabilities . (iii). GPS/Location Attacks User’s current location and movement can be accessed with global positioning system (GPS) hardware and then information can be sold to other companies involved in advertising .

DOI: 10.15680/IJIRCCE.2016. 0409070

III. EXISTING SYSTEM

In existing system the detection of spy camera is done but it does not provide sufficient detail about the spy camera activities .After detection it is not uninstall from the device .Hence there is no privacy for the mobile user. It continues to running in the background without user knowledge and it makes the mobile to run abnormally. These disadvantages can be overcome by implementing the lightweight defense application.

A. *PROBLEM DEFINITION*

Mobile devices often do not have passwords enabled. Mobile devices often lack passwords to authenticate users and control access to data stored on the devices. Many devices have the technical capability to support passwords, personal identification numbers (PIN), or pattern screen locks for authentication. Some mobile devices also include a biometric reader to scan a fingerprint for authentication. However, anecdotal information indicates that consumers seldom employ these mechanisms. Additionally, if users do use a password or PIN they often choose passwords or PINs that can be easily determined or bypassed, such as 1234 or 0000. Without passwords or PINs to lock the device, there is increased risk that stolen or lost phones' information could be accessed by unauthorized users who could view sensitive information and misuse mobile devices.

IV. PROPOSED SYSTEM

Light weight Defense application is installed in the device after getting user's permission and it silently runs in the background without interrupting the user's activities. It detects the Spy cam app which is hidden in any of the running application that calls the camera service. The defense app gives notifications to the user about the malicious app installed unknowingly. After giving the notifications it uninstalls the malicious app from the user's device. The notifications are Beep sound, Voice message, Alert message.

A. *IMPLEMENTATION AND EVALUATION*

- integration with a GSM network is required (except for the database of cell ids – but this can be created by the online users)
- Client/server architecture – only one machine required for user administration, advertising management, profiling, locations database.

B. *ALGORITHM:*

To implement the attacks on real phones, and demonstrate the feasibility and effectiveness of the attacks. To develop an Android application such that when a user loses his/her phone, the spy camera could be launched via remote control and capture what the thief looks like as well as the surrounding environment. Then the pictures or videos along with location information (GPS coordinates) can be sent back to the device owner so that the owner can pinpoint the thief and get the phone back. In this paper we are using Viola-Jones foreface Detection. The Viola-Jones Object Detection Framework is a generic framework for object detection, which is particularly successful for face detection.

V. CONCLUSION

In this project, the proposal is the advanced detection of spy camera application with enhanced features. Lightweight defense application is one of the android applications which enable the user to protect their mobile from hackers. This application automatically detects the spy camera application. This application is user friendly and it can be installed without any technical knowledge for the user. It is also cost effective and it utilizes the minimal resources from the mobile. The installation of this application is a simple process and takes only a few minutes. Hence the user can protect their personal data and privacy from the hacker. It does not involve any difficult task to identify the spy camera application.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

REFERENCES

1. Azeem Ush Shan Khan, Mohammad Naved Quereshi,Mohammad Abdul Qadeer,"Anti-Theft Application For Android Based Devices" In 978-1-4799-2572-8/14/$31.00 © 2014 IEEE
2. Longfei Wu and Xiaojiang Du, Temple University Xinwen Fu, University of Massachusetts Lowell," Security Threats to MobileMultimedia Applications" 0163-6804/14/$25.00 2014 IEEE
3. Mobile Tracking Application For Locating Friends Using LBS -By Abhijeet Tekawade,Ravindra Shinde on 2, April 2013
4. A Model For Remote Access And Protection Of Smart phones Using SMS -By K.S. Kuppusamy on 1, February 2012
5. http://www.ijitet.com/ICITET15/IC15026.pdf
6. http://www.ijircce.com/upload/2015/december/125_27_CAMERA.pdf