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 6, June 2016

Camera Based Attack Detection and Prevention Techniques on Android Mobile Phones

Ashish Kale, Ramesh G Patole

M.E Student, Dept. of Computer Engineering G.H.Raisoni College of Engineering, Ahmednagar, Savitribai Phule Pune University, India

Assistant Professor. Dept. of Computer Engineering, G.H.Raisoni College of Engineering, Pune, Savitribai Phule Pune University, India

ABSTRACT: Security is measure concern related to smart phone. The main security issue is related to camera.Mobiles users are misusing the mobile camera.There are lots of application when user download it from play store uses the front camera without knowing the user.These are nothing but the attacks generated by the application. So to prevent this kind of attacks some camera based attack prevention techniques should be used. To prevent these attack first they must be detected.If user phone is get stolen then to find the smart phone user have to activate the service once it has been activated then user can get the thief snaps,videos and locations.For this GPS API required to locate the mobile location.Attack detection prevention will be done with the help of background process which continuously check the user phone flag status.

KEYWORDS: Passcode inference; limbus; eye tracking; remote controlled.

I. INTRODUCTION

Android is the most popular OS in all over the world.The android OS has captured the 79.3 percent market share.But there are lots of security issues related to smart phones and their users.If user is installing a new app from play store then it will gives the permission list means this particular app requires the all these permissions but only few user are having the knowledge of that.Now a days apps also get increased to protect the smart phones.Most of the anti virus companies have published the Android version software to protect the smart phones to block the malicious applications and viruses. 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.Attacker can use the front camera as spy camera such as launching the front camera automatically without device owner notice and users.Camera usage has been increase by the various applications.This paper introduce the camera based attack revention and detectiontechniques so that it will be easy and safe for the smart phone users.To communicate the android application and database KSOAP is used.Thewebservices are used to communicate the android application and that will be written in KSOAP.KSOAP are lightweight and easy to handle the communication.One background process is developed which will continuously check the flag status once the flag becomes true then it will get activated and then it will capture the photos and videos. A huge concern for Mobile security in today's world is to recover the important credentials inside the mobile phone. There are various kinds of android application are availableinto a market for anti-theft solutions of smart-phone. This application helps to providea security for entire mobile environment,which has ability to detect or trace a smart-phoneanywhere across the globe. To recover a mobile phone data due to lost,stolen and misplaced,mainly you can protect your smartphone by remote-control through email,via SMS,Automatic Alerts. User can configure the can take photos and videos of the smart phone

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 6, June 2016

II. RELATED WORK

In [2] authors used average residual battery level of the entire network and it was calculated by adding two fields to the RREQ packet header of a on-demand routing algorithm i) average residual battery energy of the nodes on the path ii) number of hops that the RREQ packet has passed through.According to their equation retransmission time is application, to enable some options to make impossible for thief to disable smart-phone security features like tracking option,locationsearch,camera on click for unknown person and password security options .Power menu option can also block to prevent the thief from shutting down the device. Remote control and Automatic alerts are used to track and locate the device,clear out all important personal credentials from user smart-phone internal memory card and SD card. Get the information of WiFi network and smart-phone network. If SIM card is changed in user smart-phone ,it will alert a user by sending email and SMS. In Section II consider the literature survey of based paper or few reference paper and discover all dis-advantage of all these paper in Section III to be consider for proposed system to avoid all dis-advantage to arise in literature survey also involved proposed system architecture, algorithms
and mathematical module .in Section IV consider Result of these system and discuss
these result and finally acknowledgment for all supported persons. To communicate the android application and database KSOAP is used.Thewebservices are used to communicate the android applicationand that will be written in KSOAP.KSOAP are
lightweight and easy to handle the communication.One background process is developed which will continuously check the flag statusonce the flag becomes true then it will get activated and then it will capture the photosand videos.

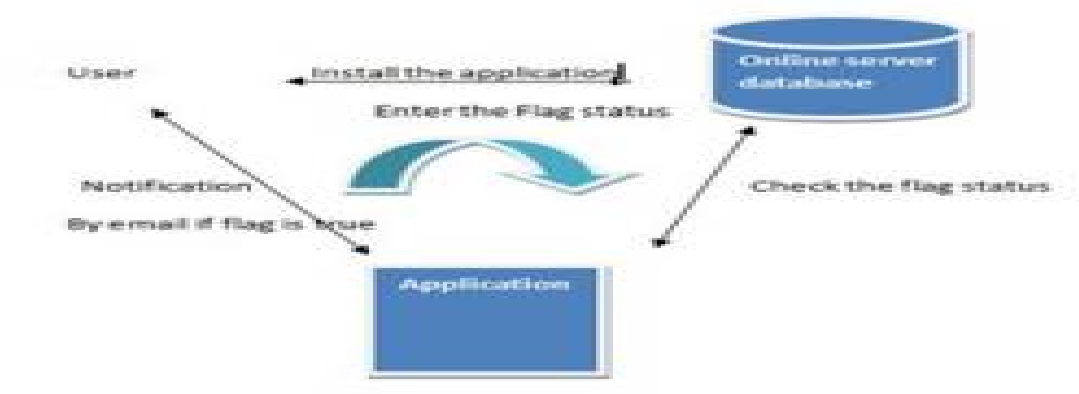

Fig1. System Architecture

III. LITERATURE SURVEY

A number of recent works have studied the issue of obtaining private information on smartphones using multimedia devices such as microphones and cameras. For example, Soundcomber [2] is a stealthy Trojan that can sense the context of its audible surroundings to target and extract highvalue data such as credit card and PIN numbers. Stealthy audio recording is easier to realize since it does not need to hide the camera preview. Xu et al. [3] present a data collection technique using a video camera embedded in Windows phones. Their malware (installed as a Trojan) secretly records video and transmits data using either email or MMS.Windows phones offer a function, ShowWindow(hWnd, SW HIDE), which can hide an app window on the phone screen. However,it is much more complicated (no off-the-shelf function) to hide a camera preview window
in an Android system. In this work, we are able to hide the whole camera app in Android.
Moreover, we implement advanced forms of attacks such as remote-controlled and real-time monitoring attacks. We also utilize computer vision techniques to analyze recorded videos and infer passcodes from users eye movements. Several video-based attacks targeted at keystrokes have been proposed. The attacks can obtain user input on touch
screen smartphones. Maggi et al. [4] implement an automatic shoulder surfing attack against modern touch-enabled smartphones. The attacker deploys a video camera that can record the target screen while the victim is entering text.

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 6, June 2016

Then user input can be reconstructed solely based on the keystroke feedback displayed on the screen. However, this attack requires an additional camera device, and issues like how to place the camera near the victim without catching an alert must be considered carefully. Moreover, it works only when visual feedback such as magnified keys are available. iSpy [5], proposed by Raguram, shows how screen reflections may be used for reconstruction of text typed on a smartphones virtual keyboard. Similarly, this attack also needs an extra device to capture the reflections, and thevisual key press confirmation mechanism must be enabled on the target phone. In contrast,our camera-based attacks work without any support from other devices.

IV. PROPOSED WORK

Pros and cons of the spy camera

Leakage of the information:

Front camera functions like a thief if it leaks some information. It has a process which will run and the take the pictures and videos secretely. These photos and videos are sent to wherever the attacker wants to send.

Watching others mobile:

Front camera can easily take the pictures of the user without knowing the user of the phone.

Prevention;

When mobile phone owner losses his/her phone the they can switch on the mobile phone front camera to captures the thief photos and videos through certain web services.It will also captures the thief current latitude and longitude.The latitude and longitude will be captured through GPS.For this google map API should be imported.

Web service to activate the front camera:

Initially when user install the application then the IMEI number of the mobile is get stored of that mobile.Application will set the flag of the mobile to false initially.When flag is false then application will check whether any other application which is installed in the phone is using the front camera or not.If any other application tries to open the front camera then application will give the pop-up message that anther applications are using front camera.If flag is become true that means users mobile get stolen then one background process is get activated which will capture the thief photos and videos from front camera also capture the smart phone current latitude and longitude so as to understand the current location of themobile.The capture photos and videos will directly come to users mail id which will help to spot the thief or the smart

The Video Based Pass code Inference Attack:

In this paper, there is a technique of eye tracking that can be utilized to capture the face of the user.

The Application-level Attack:

In this type of attack the attacker aims at getting credentials of the user.Most of the social networking application require certain pin or the virtual keyboard to authenticate the user.User can lock the certain application using application locker.

The Screen Unlocking Attack:

Attacker can unlock the user lophone lock pattern.This can be done when user is entering the pattern to unlock the phone.

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 6, June 2016

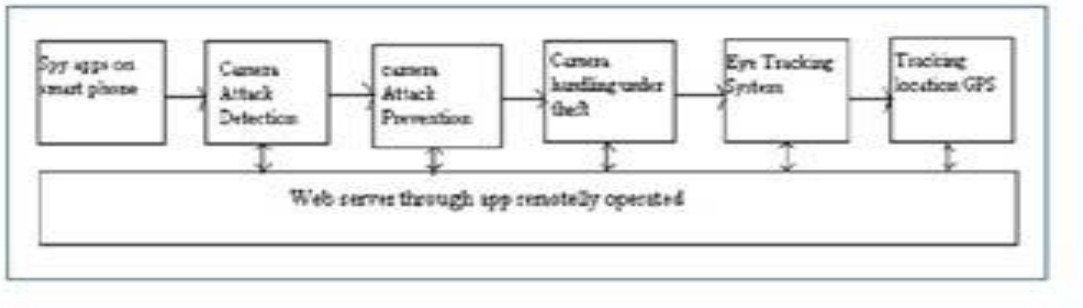

Fig 2. Flow of the system

Algorithm 1:
1.Initially all user flag is false and capture IMEI number of the smartphone
2.If flag==False then
3. Check whether any other application is using front camera
4.If yes then block or close the application and give notification to the user.
5.If flag==True
6.Activate the front camera of the respective IMEI number also activate the GPS and capture images of the user and lattitude and longitude of the phone.
7.Use SMTP to transfer the images and location from the email to the smartphone user mail
Algotithm 2:-
1.Localization of the face region.
2.Detect the face texture features and iris candidates.
3.Selection of pair of irises.
4.Give the input to SMTP.

Web Services:
Web services are used to communicate the android application and database server. KSOAP is used as a web service. It is a lightweight and efficient library.It is also used in literal encoding.
It uses pull parsing technique to parse the data.It is open source library which can be easily use to parse the values.It takes the input as per the user specified and perform accordingly.

V. MATHIMATICAL MODULE

Let S be the proposed system which can be represented as
S=I1,I2,O
Where
I1=Flag value.
I2=IMEI number of the device.
P is testing algorithm
Input=(Flag which is false)
Output=Notification of other apllication for using front camera
P=(Fx— Iput Output)
Fx is the function which take the input flag and give output as id of the application.
Q is testing algorithm
Input=(Flag is True and IMEI number)
Output=(Thief photos and videos and latitude and longitude)
Q=(Fc— Input Output)

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 6, June 2016

Fc is the function which is called when flag becomes true and will capture the photos , videos, and lattitue and longitude of the user.

Flag	Action
Flase	Application ID
True	Activate process and capture the photos,video,lattitude,longitude

Table 1:Flag Action

Sr.no	Flag sta-tus	Internet Speed	Accuracy	False Rate
1	False	2G	88%	12%
2	False	3G	94%	6%
3	True	2G	76%	24%
4	True	3G	89%	11%

The above result analysis shows accuracy of the application tested by varying the internet speed.To increase the accuracy internet speed should be 3G.Below mentioned graph shows that precision and recall values based on the mail received by the user once the flag becomes true.Precision is number of emails receives to respective user out total number of user and recall is number emails not receives to user out of total users.

Table 2:Application Performace

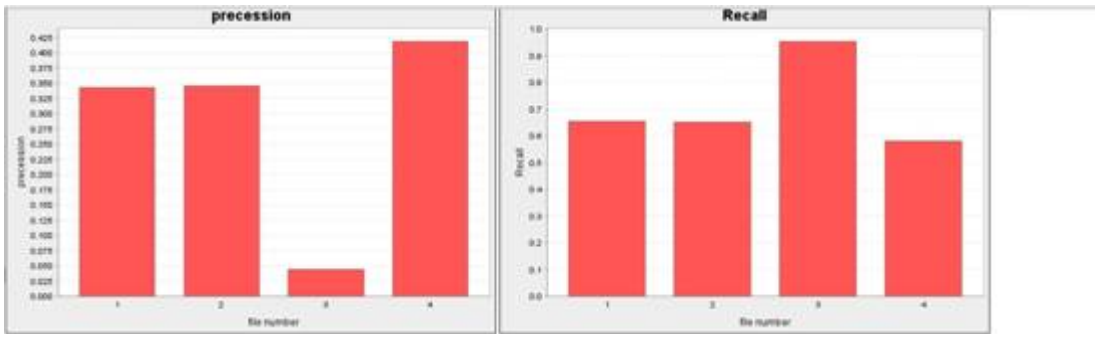

Fig3:System Accuracy

VI. CONCLUSION

In this paper,we study camera related attackes on the mobile phones . Also studied the roles of the spy camera one is as attacker and another is a preventor as per the flag status.This application will help the smart phone user to protect their phone from various attack as well as getting stolen.But the major thing is internet should be on in both the cases then only this application will work properly.

ACKNOWLEDGEMENT

We would like to take this opportunity to express my sincere gratitude to my Project Guide Prof Ramesh G Patole (Assistant Professor,Computer Engineering Department) for his encouragement, guidance, and insight throughout the

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 6, June 2016

research and in the preparation of this dissertation. He truly exemplifies the merit of technical excellence and academic wisdom.

REFERENCES

[1]. Y. Zhou and X. Jiang, "Dissecting Android Malware: Characterization and Evolution", IEEE Symp. Security and Privacy 2012.
[2] . R. Schlegel et al., "Soundcomber: A Stealthy and Con- text-Aware Sound Trojan for Smartphones, NDSS, 2011.
[3] . N. Xu et al., "Stealthy Video Capturer: A New Video-Based Spyware in 3g Smartphones", Proc. 2nd ACM Conf.Wireless Network Security, 2009.
[4] . F. Maggi, et al.,"A Fast Eavesdropping Attack against ouchscreens, 7th Intl. Conf.Info. Assurance and Security",2011.
[5] . R. Raguram et al., ispy: "Automatic Reconstruction of Typed Input from Compromising Reflections", Proc. 18th ACM Conf. Computer and Commun. Security, 2011.
[6] . Android-eye, https://github.com/Teaonly/ android-eye,2012.
[7] .Nanohttpd, https://github.com/NanoHttpd/ nanohttpd.
[8] . A. P. Felt and D. Wagner, Phishing on Mobile Devices,Proc. WEB 2.0 Security and Privacy, 2011.
[9] . D. Li, D. Winfield, and D. Parkhurst, "Starburst: A Hybrid Algorithm for Video-Based Eye Tracking Com- binningFeature-Based and Model-Based Approaches", IEEE Computer Soc. Conf. Computer Vision and Pattern RecognitionWorkshops, 2005.
[10] . P. Adrian, "Fast Eye tracking, http://www.mathworks.com/matlabcentral /file exchange/25056-fast-eyetracking",2009.