International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-7 Issue-4s, November 2018

Threats to Mobile Security and Privacy

Thiruvaazhi.U, Arthi.R

Abstract: ***Market research reports from Forrester estimates the global mobile penetration to be around 50% in 2017 and is forecast to reach 66% by 2022. In India, Mobile Internet Penetration using Smart Phone has reached 36% as of 2016 from 0.1% in 1998. With the grand new push towards Digital India and low cash transactions, mobile transactions including mobile payments have seen significant thrust in the recent times. Many startups as well as major enterprises and government has been continually providing and promoting many mobile apps for variety of transactions from multimedia messaging to digital payments. In this paper, we present a survey of the threats and a clear demonstration of the risks of usage of mobile on security and privacy of the person using it and his/her communications.***

Keywords: ***Smart Phone has reached 36% as of 2016 from 0.1% in 1998.***

I. INTRODUCTION

As we all know, there are several uses of mobile phones and communications and services that can be carried out through that medium, which can fuel development of individuals and nation. At the same time sustainability of such development can be ensured only by properly addressing the challenges to security and privacy of mobile usage. This paper is to illustrate the threats of mobile usage, so that we are aware of the risks of uncontrolled usage. In the rest of this section, we give the statistics of mobile penetration and trends and provide the summary of mobilevulnerabilities and threat vectors based on survey of available literature. In section 2, we demonstrate real attacks that validates the reality of the risks involved. In section 3 we show that if a mobile user is aware of the risks involved and implement few simple preventive steps, the user could effectively control the risks involved and still continue to derive the utility value of using such a mobile. In section 4 we summarise and conclude this work.

A. Growth of Mobile Usage

Forrester report [Forrester, 2017] estimates that the global smartphone penetration will increase from 21% in 2013 to be 66% in 2022. The number smartphone subscribers are estimated to be 3.8 billion in 2022. eMarketer statistics [Statista 2015] of Indian smartphone penetration estimates that from 21.2% in 2014, the penetration will increase to 39% in 2019 as shown in figure below.

Manuscript published on 30 November 2018.
*Correspondence Author(s)
Thiruvaazhi, Kumaraguru College of Technology, Coimbatore (Tamil Nadu), India.
Arthi.R , Kumaraguru College of Technology, Coimbatore (Tamil Nadu), India.

B. Mobile Threat, Risk and Impact Reports from Literature

Symantec Mobile Threat Intelligence report [Symantec MTIR 2018] says that there is an 80% growth in the reported number of Mobile Common Vulnerabilities and Exposures (CVEs) from 2016 t0 2017.

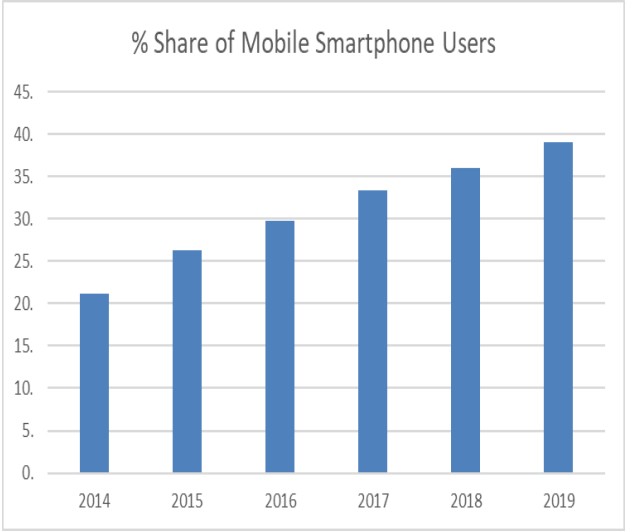


Fig.1. Share of Mobile Smartphone Users, Source: Statista.com

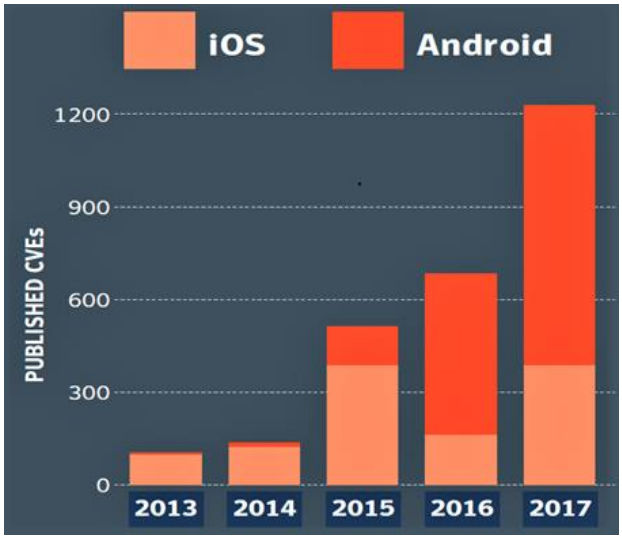


Fig.2. Mobile CVEs from 2013-2017, Source: Symantec

Further Symantec's Internet Security Threat Report [Symantec ISTR 2018] states that the number of new mobile malware variants increased from 17000 in 2016 to 27000 in 2017 demonstrating 54% increase in the mobile malware variants in just last one year. It also states that on an average 24000 malicious mobile apps were blocked every day.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

According to Symantec endpoint mobile risk scores 34% of mobiles are rated as medium to high risk. The hopes of updates controlling some of these risks are also diluted by the fact that only 20% of android mobiles are running the new major version and only 2.3% are running the latest minor version. iOS devices are not altogether updated though better than android. Zimperium Global Threat Report [Zimperium 2017] shows that 23% of iOS devices are not with the latest updates, despite updates available for more than 45 days. The impact of such risks to enterprises is captured by the Verizon Mobile Security Index of 2018. [Verizon MSI 2018] states that 32% of the companies sacrificed mobile security for expediency and that they are 2.4x times more likely to suffer downtime or data loss as compared to those who chose to secure their employees mobiles. It also states that 27% of the organizations experiences a security incident directly attributable to a mobile device last year.

McAfee Mobile Threat Report [McAfee MTR Q1 2018] gives the breakdown of the dynamics in the threat vectors last year targeting Google Play store as shown in the chart below.

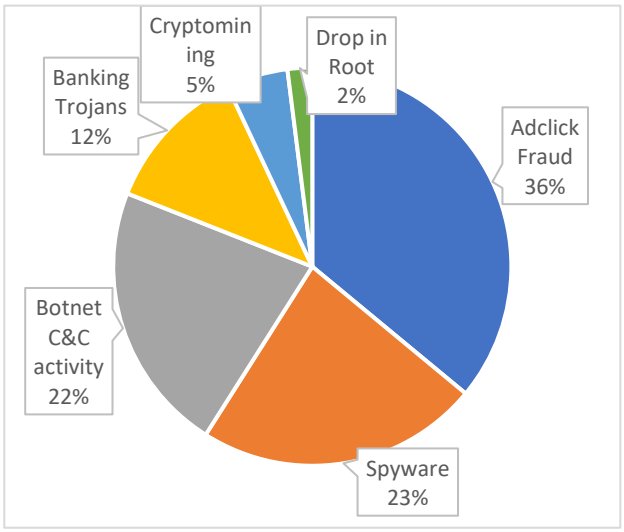


Fig.3. Chart of the growth of Android Threat Vectors

McAfee further reports that in the third quarter of 2017 alone, it saw 16 million mobile malware infestations. All these give enough indications of the impact that it could have on the lay mobile users and the security and privacy of their mobile communications.

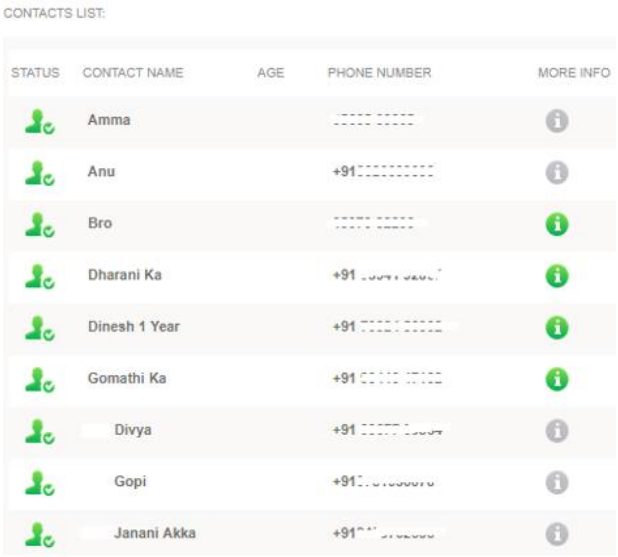
II. ATTACKS ON MOBILE SECURITY AND PRIVACY

In the earlier section we have seen the summary trends of the vulnerabilities, threats and the impacts to individuals and organizations from top primary reports of organizations having customer data on such activities. While much of these have been in literature for last few years, most users tend to ignore the direct relevance and impact that it could have on their own mobile use. Hence the objective of this work is to demonstrate the reality of the threats by installing one such malware on our own mobile and demonstrating some of what it can do, so that this work improves the awareness towards these threats.

In the subsequent sub-sections, we give you snapshots of a spyware at work on the mobile. Each subsection carries a snapshot of the information in / about / communicated from mobile accessed from an internet server to which the spyware forwards a copy of the mobile data. We should let the readers know that it takes only a few minutes to install one such spyware on the target mobile typically running an older version of the android / iOS device and thereafter no further access to the mobile is necessary. We will show you that the attacker can view much of the communications and private files on the victim's target device from internet. While some features will work on an unrooted android running slightly older versions, or non-jail-broken iOS device, some of the advanced features like accessing encrypted communications or speakers etc... will require that the spyware's privileges to be escalated by rooting / jail-breaking.

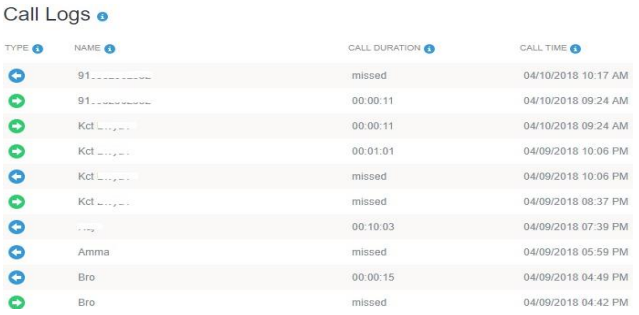
C. Contacts

Snapshot below shows the entire contact list of victim mobile user.



B. Call logs

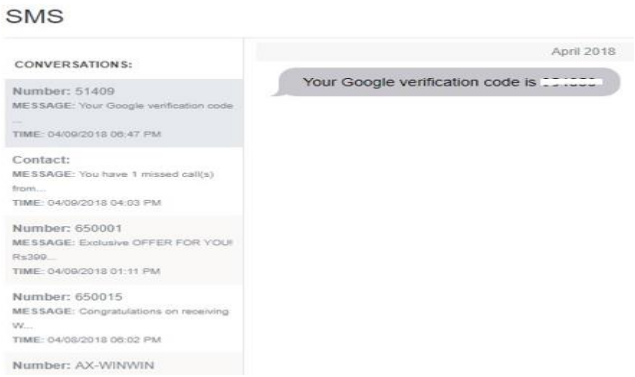
Snapshot below shows all the call logs of the target victim using the mobile.



D. Text Messages

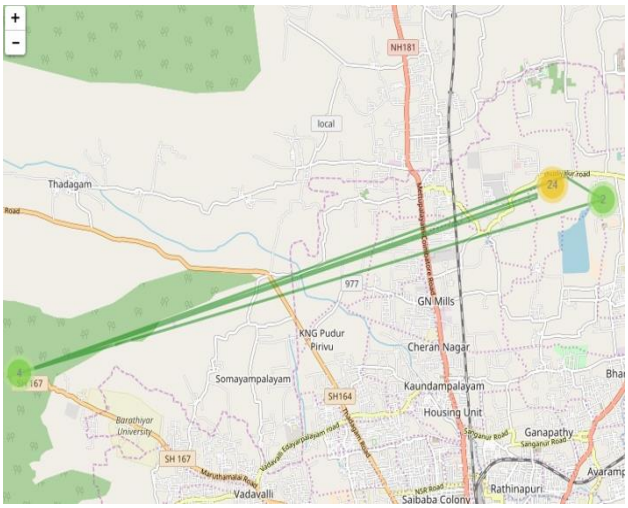
The snapshot below shows the clear plaintext of all the SMS messages sent and received.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)



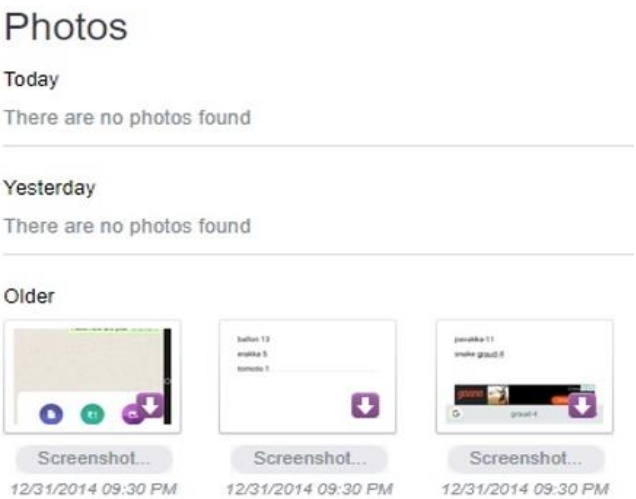
D. Locations

The snapshot below shows the location of the victim mobile user



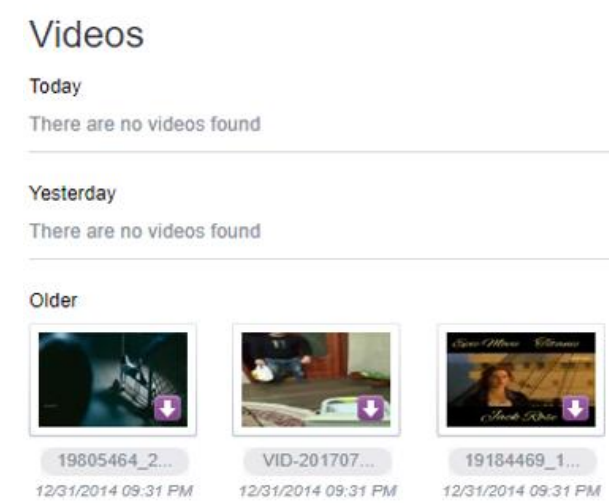
E. Photos

The snapshot below shows all the photos captured/stored in the victim mobile. They can all be downloaded as per the wish of the attacker.



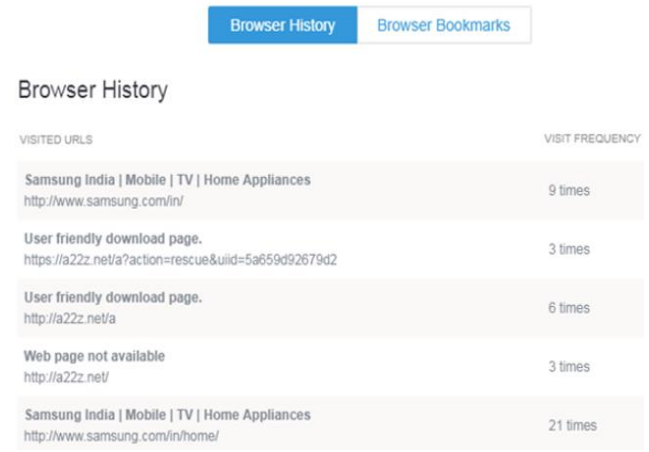
E. F. Video files

The snapshot below shows the list of the video files available in the victim's mobile. As earlier, the attacker can select and download any of the video files.



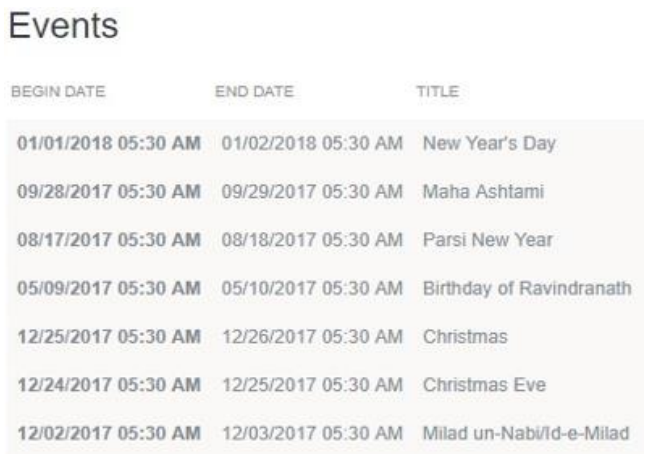
F. G. Browser history

The snapshot below shows the victim's mobile browser history



G. Events

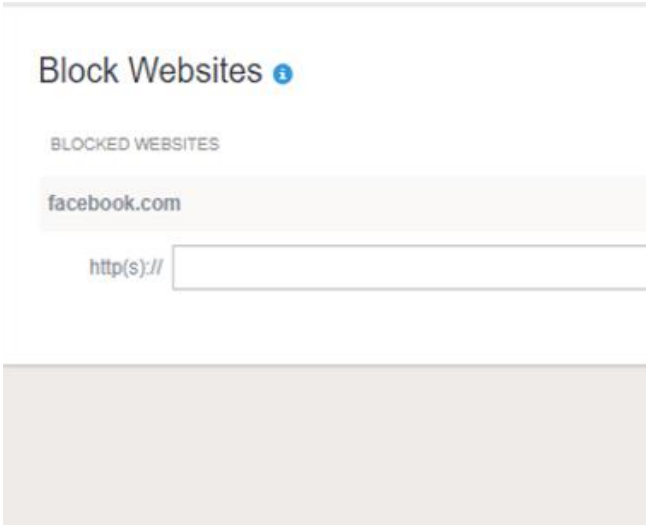
The snapshot below shows the personal calendar events of the victim mobile user.



Block websites

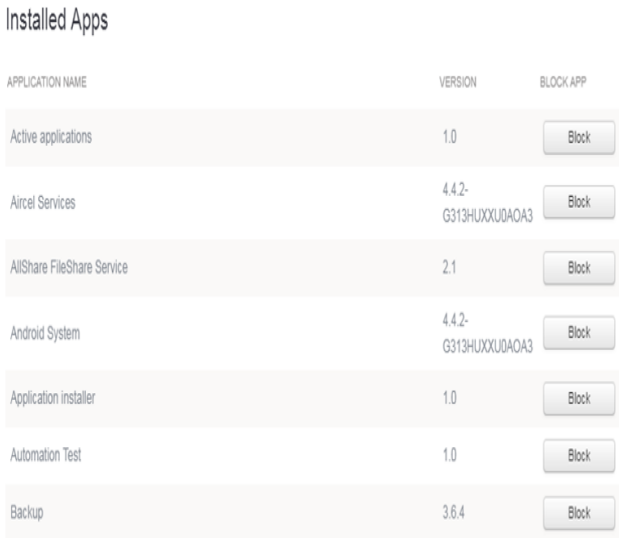
The attacker can see the blocked website and could also add certain websites in the blocked websites list so that the victim cannot access such websites from the victim's mobile.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)



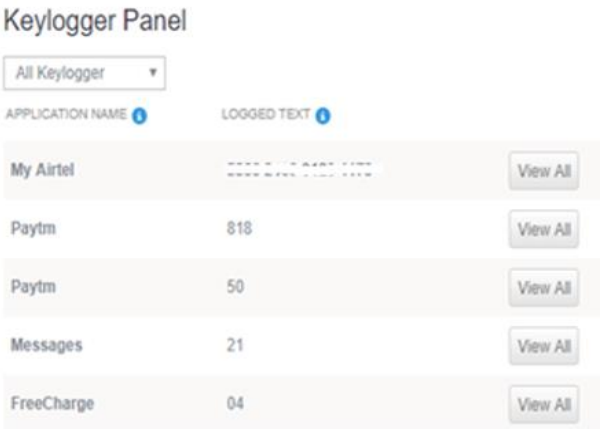
H. J. Installed Apps

The attacker could see all the mobile applications installed on the victim mobile as well as block some of the installed mobile apps.



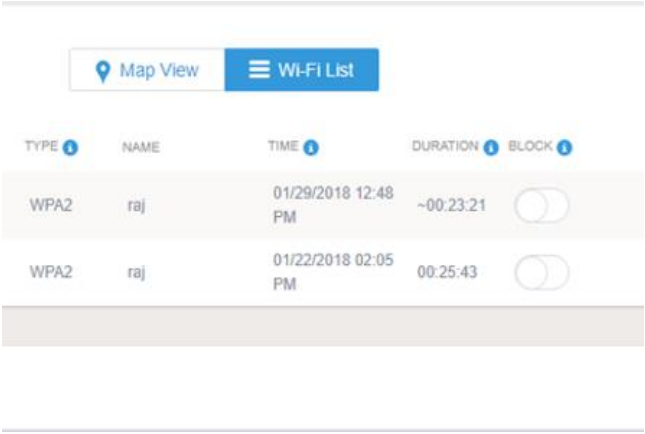
I. Keylogger

This one can be highly dangerous. Through keylogger the attacker could see all the keystrokes of the victim mobile user. The keylogger could show any typing done on mobile including private messages sent on any end to end encrypted app or even passwords and financial information typed on the victim mobile.



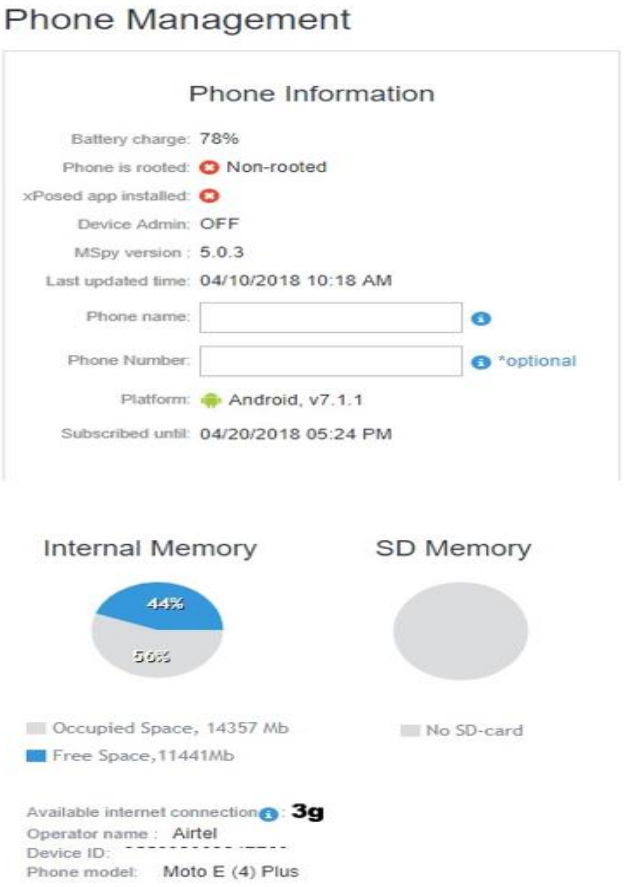
M.Wi-fi networks

The snapshot below shows the Wi-Fi networks of the victim mobile



J. Device Management

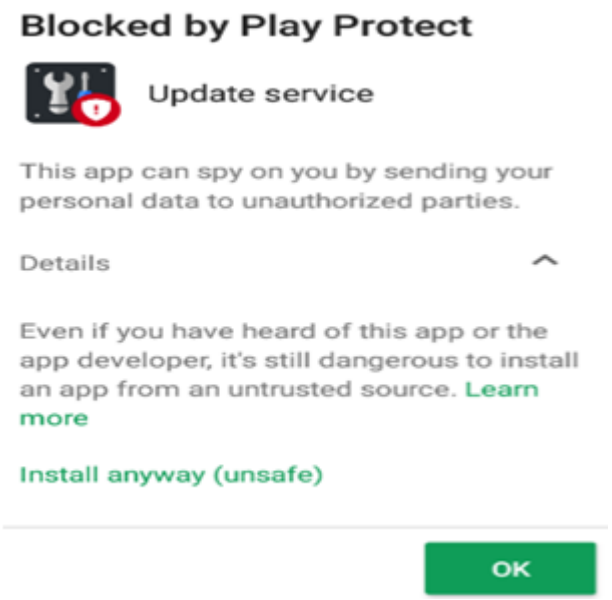
The snapshot below shows all the essential mobile device information.



K. Other Possibilities

Like the above we could go on and show for a rooted mobile almost any aspect of the mobile phone like WhatsApp chat, Facebook message, automatic recording of a live call, or even recording of the ambient sound where the victim mobile is located can all be recorded and uploaded on to the internet from where the attacker can access such private information.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)



III. PREVENTIONS METHODS FOR SPECIFIED ATTACKS

The earlier sections demonstrated clearly the reality of the threats and whether one is attacked or not is a question of choice of the attacker and the vulnerability of the victim. We know that the fundamental security principle is that our security should not be dependent on the goodwill of a possible enemy but should be based on invincibility of our state. In this section we will show you some of the basic protections that the mobile user should do with his mobile phone to reduce significantly the vulnerability of his mobile against such threats.

A. Timely Update of Operating System

[Symantec ISTR 2018] and [Zimperium 2017] reports show that 80% of android mobile and 23% of iOS devices are not running the latest operating system, thus making it vulnerable to a large share of the malicious apps that typically run on older operating system versions get to the mobile device. Entry for such apps could have been easily restricted if the mobile is running the latest major and minor version of the operating system. It would be appropriate to let you know that the spyware used for demonstration of the attacks will not work on the latest operating system.

B. Avoid Rooting / Jail-Breaking OS

Though certain advanced users and developers for their own personal liberty and choices would want to do away with the operating system controls, all normal users of the mobile need to be cautious in doing away with the inbuilt operating system protection. Hence the user should know that the responsibility for security and privacy of the mobile at hand completely shifts to that of the user when he/she chooses to root / jail-break the mobile. It would be useful to know that advanced features of spyware like call recording, capturing of ambient sounds, capturing plaintext of end to end encrypted messages will work on mobiles which are rooted and usually not on mobiles with operating system protection intact.

C. Mobile App Management:

Installation of the mobile apps should be done through the authentic store: Google Play Store / iTunes Store / App Store. When apps are updated, they are also fixed for the earlier detected vulnerabilities. Hence it should be a good practice to turn on automatic updates of the installed apps on the mobile phone. Additionally, we should note that the mobile apps are automatically scanned to find if they are malicious. Though there are options provided say in Android intended for developers to bypass that protection of installation from unknown sources, we should avoid activating that and we should keep controls like Google Play Protect turned on always. We should let you know that when we installed the malicious app on the mobile we had to turn on installation from unknown sources, turn off google protect and only then we were able to install it on the target mobile. Additionally, the user would be glad to know that as soon as google play protect is turned on, the malicious app was automatically uninstalled from the target mobile. Figures below show the Google Play Protect in action.

D. Mobile Antivirus

Mobile antivirus is generally considered redundant for Android as Google Play already scans the mobile for malwares. iOS does not give the antivirus the necessary permissions that it might need to see if another app is a malware or not. Hence antivirus in iOS is incompetent to detect a malware in iOS. In android though antivirus can also in addition to Google Play Services, additionally scan other apps and can also come up with other convenient controls, though at the cost of using considerable resources. The user can decide on case to case basis based on his/her context to decide if a particular packaging of antivirus services would be useful to him/her towards protecting security and privacy of the mobile. Snapshot below shows that one such antivirus identifies the spyware. It would be useful to know that some antivirus software alert the user on the potential malware but also give the privilege to the user to ignore the alert. If such is the case with the antivirus software, then the attacker can install the malware on the mobile, run the scan and when alerted he could specify the antivirus to ignore the alert and hence thereafter when the victim runs the antivirus he/she does not get the alert and hence can wrongly conclude that his/her mobile is safe without malware.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Hence user awareness to these issues are key to the safe use of the antiviruses in the context of android.

IV. CONCLUSION

Supported by global enterprises and governments, the drive towards digital connectivity is rapidly increasing the mobile penetration across the globe. Decreasing costs and explosion of services is making the smartphone affordable to most of the mobile users. While all these trends enhance the connectivity and utility of the mobile communications and services over it, these lay mobile users also become an easy target of attackers worldwide. This work summarized the threats, its growing trends, the vulnerabilities that make this possible and a glimpse of the impact that it could have for individuals and organizations. While such literature has been there for some time in the security community, what is necessary to control the risks arising out of this is the user awareness of the risks and its controls. In this work we have demonstrated the reality of the threats by demonstrating attacks to security and privacy of the personal data on the victim's mobile. We have also shown simple steps through which the entry points for such attacks could be easily closed. We show how the lack of user awareness in these existing security controls creates the vulnerability, which is exploited by the threat vector resulting in the attack on security of the mobile phone compromising severely on the privacy of the user and his/her data and communications. By this we hope that the user is equipped to manage his/her risk in mobile usage without undue fear on the threats to security and privacy.

REFERENCES

1. [Forrester, 2017] Forrester Report of SatishMeena and Sanjay Kumar, "Forrester Data: Mobile, Smartphone, And Tablet Forecast, 2017 To 2022 (Global)" accessed from
2. https://www.forrester.com/report/Forrester+Data+Mobile+Smartphone+And+Tablet+Forecast+2017+To+2022+Global/-/E-RES138971 , July 2017, Forrester
3. [Statista 2015] Statista Data on "Share of mobile phone users that use a smartphone in India from 2014 to2019 "accessed from
4. https://www.statista.com/statistics/257048/smartphone-user-penetration-in-india/ , 2015, Statista.com
5. [Symantec MTIR 2018]Symantec "Mobile Threat Intelligence Report 2017" accessed from https://www.symantec.com/content/dam/symantec/docs/reports/mobile-threat-intelligence-report-2017-en.pdf, April 2018
6. [Symantec Q1 MTIR 2018] Symantec "Ten Years of (Hacking) iOS", Q1 2017 Mobile Threat Intelligence Report from
7. https://www.symantec.com/content/dam/symantec/docs/reports/skycure-mobile-threat-intelligence-report-q1-2017-en.pdf , 2017
8. 5. [Symantec ISTR 2018] Symantec "Internet Security Threat Report 2018", from
9. http://resource.symantec.com/LP=5538?cid=70138000000rm1eAAA , March 2018
10. 6. [Verizon MSI 2018] Verizon "Mobile Security Index 2018", from
11. http://www.verizonenterprise.com/verizon-insights-lab/mobile-security-index/2018/ , 2018
12. 7. [Zimperium 2017], Zimperium Global Threat Report 2017 from
13. "https://go.zimperium.com/threat_report_q2_2017",
14. 2017
15. 8. [McAfee MTR Q1 2018], "McAfee Mobile Threat Report Q1, 2018", from
16. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-mobile-threat-report-2018.pdf , 2018
17. 9. G. Delac, M. Silic and J. Krolo, "Emerging security threats for mobile platforms," 2011 Proceedings of the 34th International Convention MIPRO, Opatija, 2011, pp. 1468-1473.
18. 10. L.Latha, S.Thangasamy, "A robust person authentication system based on score level fusion of left and right irises and retinal features", Procedia Computer Science, Volume 2, 2010, Pages 111-120, ISSN 1877-0509, from
19. http://www.sciencedirect.com/science/article/pii/S1877050910003443.
20. 11. L Latha and S Thangasamy. "Providing multimodal biometric authentication using five competent traits", The Imaging Science Journal, Volume 61, Pages 212 – 218, Taylor & Francis, from
21. https://doi.org/10.1179/1743131X11Y.0000000033

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)