Gap analysis of Smartphone Application Security

Pradnya khalane

ABSTRACT

According to the '5th Annual State of Application Security Report, January 2016', of Arxan Technologies, 'The majority of mobile health and finance apps contain critical security vulnerabilities. Mobile health apps approved by regulatory/governing bodies are just as vulnerable as other mobile apps.'[1]

But in 'Android's security report- 2015' it is emphasized that, Google is committed to ensuring that Android is a safe ecosystem for users and developers. Google provides multiple layers of protection, security applications and services, constantly strengthen the core Android platform, and foster an ecosystem rich with security innovation, also regularly measure the effectiveness of these efforts by collecting, analyzing, and sharing data about the security of the Android ecosystem.[2]This shows that there is a gap between provided security and user experienced security. The purpose of this study is to analyze this gap and determine the remedies to minimize this gap to provide user safe and protected mobile ecosystem. The study focuses on exploring the potentially harmful mobile apps, security precautions to be followed by user, security problems faced by users, problems in using different security functions of apps by gathering primary data from the Smartphone users. Considering the majority of user's Smartphone OS, this study is restricted to Android Smartphone users only.

Keywords: *application security, PHA, threat vector, malware, SafetyNet, VerifyApps.*

I. INTRODUCTION

There are almost 87% of Android Smartphone users all over the world. These users download and use different apps as per their needs to complete various activities, so that they could complete their task easily. Apps are manufactured in very user- friendly way to satisfy the user needs. But these apps may provide a potential harm to the Smartphones and in turn to users in different ways. Even the mobile apps approved by regulatory bodies like FDA may also harmful to users.Most of the mobile health apps were susceptible to application code tampering and reverse-engineering. Such vulnerabilities could result in privacy violations, data theft, a health app being reprogrammed to deliver a lethal dose of medication, or a finance app to redirect the transfer of money. So before installing and using an app a user should be aware of all these security problems and take proper care regarding this issue. In this paper, researcher is trying to analyze the gap between android provided security and user experienced security, due to user's ignorance of security alerts provided by Smartphone OS and other problems.

Assistant Professor,
Modern College,Shivajinagar, Pune
E-mail:khalanepradnya@gmail.com,Ph:9075102499

II. LITERATURE REVIEW

Smartphones are being exposed to a variety of information security risks and threats. These threats can be grouped into three categories:

Table 1

Device based threat vectors	Network based threat vectors	User based threat vectors
Data can be compromised in a variety of ways due to: •Always-on connectivity which could allow unauthorized parties to access data. •Software vulnerabilities that allow "jailbreak" or "rooting" of devices. •Portable form-	Users might often rely on un-trusted public networks enabling malicious parties to access and intercept transmitted data using •Rogue access points •Wi-Fi sniffing tools •Sophisticated Man-in-the-Middle attacks	Users often indulge in risky behaviors that could compromise data. For eg. •Using un-approved cloud-based apps to share and sync data •Using un-approved productivity apps that maintain copies of corporate data

factor making the devices susceptible to theft and misplacement.		•Jail breaking/ rooting devices to bypass security controls •Using malicious apps from un-approved app-stores •Exposing business data with malicious intent

In 2015, Android devices experienced, the largest threat was installation of Potentially Harmful applications (PHAs), or applications that may harm a device, harm the device's user, or do something unintended with user data. These PHA includes intentionally malicious apps like phishing apps or ransom ware, but it also includes non-malicious apps. For example, a game that transmits a list of a device's installed apps without user consent is classified as a PHA.

For eg. Android: Droid Dream Malware

- Infected 58 apps on Android Market, March 2011
- 260,000 downloads in 4 days

2.1 Potentially Harmful Application (PHA) Classifications [2]

1. Backdoor- hackers control your device, unauthorized access to data
2. Call fraud- making costly calls without user information
3. DDOS- denial of service attacks against other systems and resources
4. Generic PHA- can damage device, add hidden charges to mobile bill, or steal personal information
5. Harmful site- this app comes from a website that distributes Potentially Harmful Apps
6. Non-Android- can harm non-Android devices
7. Phishing- this app is fake, can steal personal data, such as passwords
8. Privilege escalation- can permanently damage device or cost user money
9. Ransom ware- can restrict access to device until a sum of money is paid
10. Rooting malware- contains code that attempts to bypass Android's security protections
11. Rooting (non-malware)- contains code that attempts to bypass Android's security protections
12. SMS Fraud- can add charges to mobile bill by sending costly SMS messages without informing user
13. Spam- can be used to flood targeted tablets, PCs, and mobile phones with messages
14. Spyware- can spy on you by sending your personal data to unauthorized parties
15. Trojan- this app is fake, it can damage device and steal data
16. Windows- can harm a device running Windows
17. WAP Fraud- can add charges to mobile bill without asking user.

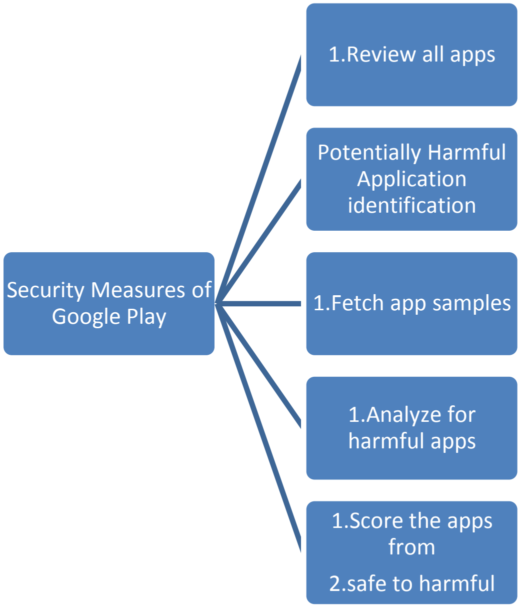
Security Measures of Google Play
1.Review all apps
Potentially Harmful Application identification
1.Fetch app samples
1.Analyze for harmful apps
1.Score the apps from
2.safe to harmful

Fig 1: Security measures provided by Google

Android includes a feature called VerifyApps. VerifyApps continually scans for potentially harmful apps. If an app is discovered later to be potentially harmful, VerifyApps will disable the app and request for you to remove it. VerifyApps also checks apps you install from outside of Google Play.If any app looks malicious, it warn user before the installation proceeds. VerifyApps is available on every Android device (2.3+) that has Google Play installed.

With Safety Net, security sensitive events and settings changes are used as signals to identify suspicious app behavior across the Android ecosystem. For example, attempts to send SMS to premium services without user consent are logged and analyzed to identify potentially harmful apps. Safety Net also observes attempts by apps to exploit known vulnerabilities, allowing systems to classify such apps as dangerous and subsequently block their installation with Verify Apps. [3]

2.2 Countermeasures provided by security providers for data loss prevention

Implementing data loss prevention on Smartphones requires a layered security approach. This layered security approach can be implemented using the controls listed below:

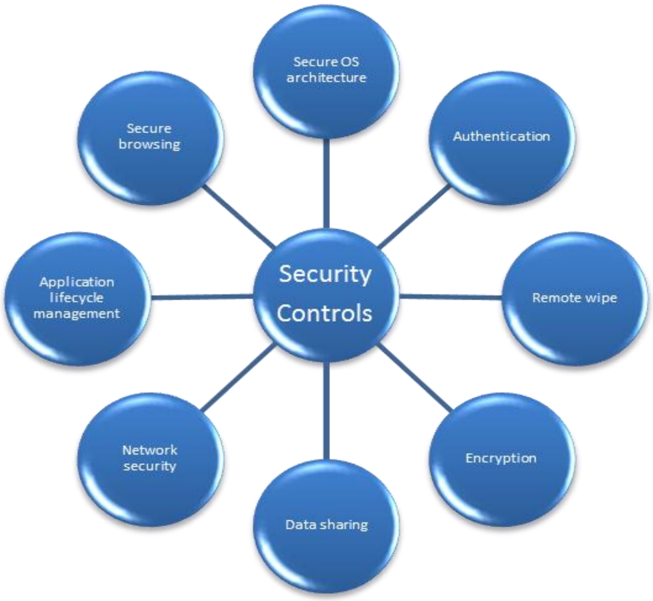

Fig 2: Controls

III. RESEARCH METHODOLOGY

An explorative study has been conducted by the author to analyze the gap between OS provided security and user experienced security. Respondents having Android Smart phones are considered for this study. Survey method with random sampling is used to collect primary data. Primary data has been gathered

by 32 valid respondents out of total 35 respondents. Questionnaire Technique has been used to collect the data. The questionnaire is being designed into two sections-

1. General awareness about the PHA's
2. Problems or issues faced by user in using the security measures provided by Google Play.

Secondary data has been gathered from articles and research papers published in books and journals.

Objectives of study

The main objective of this study is:

•To understand the gap between Smartphone OS provided security and user experienced security.

The sub objectives are:

•To explore different types of potentially harmful applications.

•To explore the security measures and countermeasures provided by Security provider companies.

IV. DATA ANALYSIS

Data is gathered through questionnaire by interacting with various Smartphone users. Primary data is analyzed to know the intensity of the gap between provided and experienced security of Smartphone apps. Thirty two valid responses were received from all age groups of people. Data gathered is analyzed and the results are summarized as follows:

Following table shows the percentage of users which think the respective harm caused by a PHA is most serious. So they do not want to experience these harms throughout their life span.71% users think unauthorized access to their device is most harmful, 100% i.e. all users think Premium SMS or calls from device is most harmful and so on. Here, all the threats are serious, but it's impact on different users is different according to their use of Smartphone.

Table 2

Possible harms due to PHA	Unauthorized access	Call / SMS fraud	Denial of service	Damage device	Steal personal information	Steal password
No. of Users	71%	100 %	41%	97 %	91%	53%

Smartphone users are facing some problems like un-awareness about the possible harms caused by the Malicious apps or potentially harmful apps, the securities provided by the Google, the antivirus and security applications in the android market, don't understand the need of using these security apps, old security models are no longer relevant etc. Following graph shows the percentages of these users who are aware, partially aware and not aware of all the above issues.

- 11% of users are aware
- 57% are partially aware
- 32% are not aware

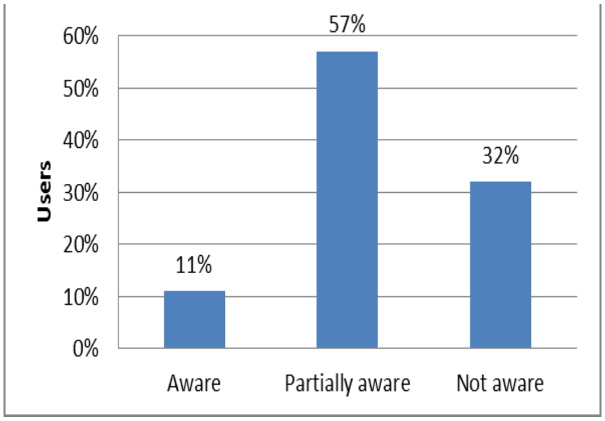

Fig:3 User Awareness

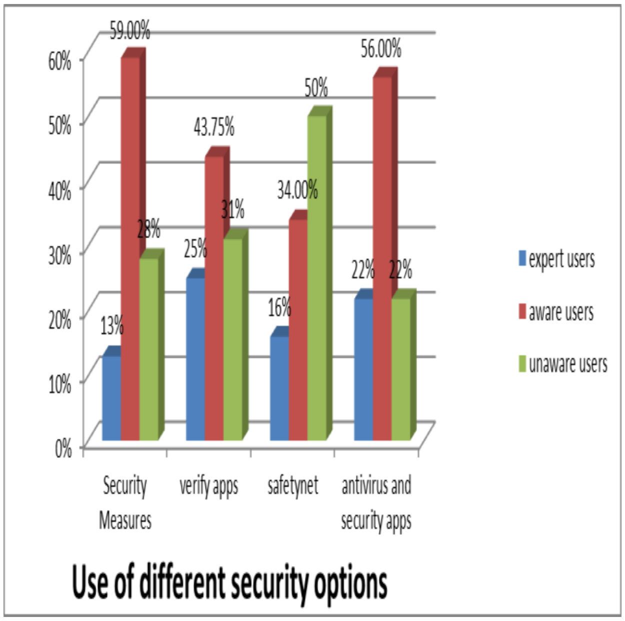

Fig:4 Use of different security options

Next, if the android provided security measures, verify apps, Safetynet, antivirus and security apps and their association with the user's awareness is considered. It is clear from the graph that large number of users do not aware of these facilities. Some users are aware but they do not use it. Some users are aware, use this securities but faces problems in their functioning. i.e. There is a big gap between provided security and user experienced security. Thus, there are greater chances of vulnerability. Therefore, there is a need to aware them and minimize this gap and in turn minimize their harm caused by the Smartphone apps threats. This awareness can be provided by Google play store or by some Social organizations. So the users can protect themselves and use their Smartphone securely.

V CONCLUSION

Android works to keep the devices safe from all angles. Google Play reviews developers and applications before they come to devices, and continually updates its security-detection system to learn more ways to keep harmful applications away. Android has multiple layers of built-in security, like VerifyApps, SafetyNet, sandboxing, and runtime permissions i.e. working hard to make sure the device never meets a harmful application. It also constantly collaborating with developers, academic and industry researchers, and users to make Google Play and Android safe.But on user's side also there should be constant updation of Smartphone OS and keep attention on the messages provided by Android while downloading or installation of any app to keep the device safe. So there is a need to increase user awareness and encourage users to use required security measures.

REFERENCES

1.www.arxan.com/2016/01/12/arxans-5th-annual-state-of-application-security-report-reveals-disparity-between-mobile-app-security
2.Google_Android_Security_2015_Report_Final_pdf, white paper by Google, april 2016.
3.Android Security / February 2016