RESEARCH ARTICLE OPEN ACCESS

Security Ads in Mobile Apps

Manasvi Kalra, Indrajeet

Abstract
The apps consist of advertisements to promote their products. Not all of them are appropriate to resume. Therefore various algorithms have been used in order to block those apps from existence but none of them is completely successful. In our app we are using an antivirus which can by default block those spy apps and remove them from the web page. The algorithm which has been used makes use of various ant viruses in the background which detect irrelevant and intimate apps and then our algorithm will demolish them.

Certain apps are non-trustworthy where one click can spy all the mobile data. They block those apps and works on security. We are working on secure ads for mobile apps. It can also work as a basic antivirus where it detects the viruses like malwares in any of your installed apps or downloads. It will create a popup of discarding or keeping it. Mobile applications can be downloaded from anywhere like amazon, googleplay, apps store etc. There is no rigorous verification of an application when it is uploaded to the market. One can easily develop a malicious application and upload it to the app market. The user itself is responsible for accepting the risk of an app available from secondary markets.

Therefore, we have decided to develop this app to make the market more secure and bounded. In future, It will take the mobile market while consuming minimal additional resources and preserving user privacy.

Keywords: security, ads, antivirus, hacking.

I. INTRODUCTION

Nowadays, mobile devices are an important part of our everyday lives since they enable us to access a large variety of ubiquitous services. The importance of ad revenue in technological innovation cannot be understated.

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. Maintaining privacy in our personal communication is something everyone desires.

To help understanding the current security problems affecting smart phones, we review threats, vulnerabilities and attacks specific to smart phones and examine several security solutions to protect them.[2]

In this paper, we basically provide an idea to develop an app which works on the security of other apps.

- We block the spy and unwanted ads which can cause harm to mobile and user information present in the mobiles.
- We also indulge an antivirus installation procedure which provides the basic antivirus facilities and remove the blocked apps.

Our popularity-focused security analysis provides insight into the most frequently used applications.

II. NEED OF SECURITY

- Mobile devices are stolen frequently which results in loss of user data.
- Mobile Devices can connect through network using internet.
- Mobile apps can contain sensitive intellectual property. With web apps, your intellectual property is often protected as your business logic is implemented on the server side.
- Mobile apps collect rich data. Hackers find mobile apps attractive targets because they manage customers' behavioral and other confidential data.
- Broken cryptography since the keys are common across all app installs, the security is negated because anyone who gains access to someone's encrypted data can decrypt it.

III. MOBILE ADVERTISEMENTS

Mobile advertising is a form of advertising via mobile (wireless) phones or other mobile devices. It is a subset of mobile marketing.

In addition to standard mobile display banners, a growing trend is to include rich media execution within the banner ads. This includes banners that would expand to a larger size, offering advertisers a larger display to communicate their message. Games within the banner to make the experience more interactive or a video within the banner space.

There are limitations to rich media on mobile because all of the coding must be done in HTML5, since the iOS does not support flash. However, mobile devices are encountering technological bottlenecks in terms of battery life, formats, and safety issues. [1]

In a broad sense, mobile devices are categorically broken down into portable and stationary equipment.

IV. ANTIVIRUS AND VIRUS

Malware is any kind of hostile, intrusive, or annoying software or program code (e.g. Trojan, root kit, backdoor) designed to use a device without the owner's consent. Malware is often distributed as a spam within a malicious attachment or a link in an infected websites. Malware can be grouped in the following main categories, according to its features (e.g. the vector that is used to carry the payload) [5]:

- Virus;
- Worm;
- Trojan;
- root kits;
- Botnet.

A virus is a piece of code that can replicate itself. Different replica of a virus can infect other programs, boot sector, or files by inserting or attaching itself to them.

A worm is a program that makes copies of itself, typically from one device to another one, using different transport mechanisms through an existing network without any user intervention. Usually, a worm does not attach to existing programs of the infected host but it may damage and compromise the security of the device or consume network bandwidth. Malware can also come packaged as a Trojan, software that appears to provide some functionality but, instead, contains a malicious program.

Mobile malware can spread through several and distinct vectors, such as an SMS containing a link to a site where a user can download the malicious code, an MMS with infected attachments or infected programs received via Bluetooth. The main goals of malware targeted at smart phones include theft of personal data stored in the phone or the user's credit.

Recently, a growing number of viruses, worms, and Trojans that target smart phones have been discovered. As we have already pointed out, the reason of the growing number of mobile malware is due to the widespread use of smart phones.

Furthermore, we have to consider that most of the smart phones lack any kind of security mechanisms and are not well prepared against new threats.

Antivirus are the set of programs that are designed to prevent, remove and detect software viruses and other malicious software like worms, Trojans, adware, and more.

Basic working of Antivirus:-

- Scan specific files or directories for any malware or known malicious patterns
- Allow you to schedule scans to automatically run for you
- Allow you to initiate a scan of a specific file or of your computer, or of a CD or flash drive at any time.
- Remove any malicious code detected – sometimes you will be notified of an infection and asked if you want to clean the file, other programs will automatically do this behind the scenes.
- Show you the 'health' of your computer

In order to create your own antivirus is a difficult and time taking process. There is the requirement of lots of malware databases to create it.

A. Insecurity in apps

- Security Isn't a Priority- This is partly due to the fact that shipping a product late or with fewer features has more tangible consequences than software security. But it's also a problem of perception - developers (and executives) often take the attitude that insecure software doesn't pose that much of a risk to begin with, assuming that flaws can simply be patched later, as they're discovered.
- Code Reuse - Developers continue to write code in C/C++ because it's easy to reuse and extend, plus apps written in these languages have much better performance than most other languages. But these unmanaged programming languages have a number of security issues.
- Lack of Experience - Developers often make the mistake of thinking they know security because they're good at coding - and that security mistakes are only made by bad developers.

Due to these very and else other reasons the apps face a vast amount of insecurity. Insecurity in apps make attackers to conquer the mobiles easily where they can effortlessly create anything useful for users which can make them more prone to attackers. This could be in the form of advertisements which come on their way while using any app.

V. UNWANTED ADS

Mobile security and its craving is increasing day by day. It is of particular concern as it relates to the security of personal and business information now stored on smart phones [3].

Fig I A hacker performing hacking on a password block

Mobile app hacking is becoming easier and faster now:-

- It's Fast
- It's Relatively Easy
- Unprotected binary code in mobile apps can be directly accessed, examined, modified and exploited by attackers[8]

There are few android apps that can turn your mobile device into a hacking device. Although, these apps have so many limitations and can only be used for few specific tasks.

As we already said that mobile is ruling smart phone and tablet, developers are also creating more apps for Android devices. This is the reason why the app market has millions of apps. Like websites, apps also need penetration testing to check for various vulnerabilities. Security testing for mobile apps will need to have a penetration testing environment on your mobile device.

The need of mobile ads in apps is of keen importance [6]:-

- Improve your performance. Get more new customers, leads or conversions and reach more mobile users.
- Build your brand. Make an impact with engaging, interactive, rich-media display ads on smart phones and tablets.

Mobile ads are of different types which supports the browser platform and apps base:-

- On mobile device with full browser support
  - ϖ Text ads
  - ϖ Image ads
  - ϖ App promotion ads
- Within Apps

ϖ Text ads
ϖ Image ads
ϖ App promotion ads
ϖ Image app promotion ads
ϖ Video app promotion ads

- Only on device that can make calls

ϖ Call-only ads

I. Mobile Text Ads

Mobile text ads look like standard text ads that you'd see on a desktop computer. The main difference is that we can show more ads per page when someone's searching on a desktop computer, and fewer ads per page when someone's searching on a mobile device.

II. Mobile Image Ads

Image ads on mobile devices are similar to normal image ads that you'd see on a desktop computer, but they can link to your mobile website or to your app. To have your image ads run on mobile devices, just make sure that your campaign is opted in to the Display Network.

However, to run ads on mobile apps and websites that are designed for mobile devices, your image ad size should be 320 x 50. Image ads can show as banner ads or interstitials in mobile apps

III. App Promotion Ads

Google's app promotion ads are designed to get apps in front of the right audience when the information a person is searching for lives inside an app. You can run these ads across search and display using the App/digital content ad format.

IV. Call Only ads

Call-only ads only appear on devices that can make phone calls, and the ads are designed to encourage people to call. All clicks on these ads send potential customers to call you from their smart phones.

In order to block the unwanted ads there are certain instances that need to be taken into consideration Ad-blocking extensions like Ad block Plus are profoundly used to block the ads.

Their weakness: These extensions only work with the browser you've installed them on. If you're interested in blocking advertising from specific domains globally, you can edit your computers (or, better yet, your routers) hosts file to stop your browser, your phone's browser, or any other application from visiting that advertising server completely.

Ads are however destructive and in just one click complete data goes into the hands of the hacker. All data becomes sharable or may be completely blocked for the user who only has right to access it.

Ads that are unwanted can be removed temporarily but the permanent solution is still under consideration.

- Mute ads that you don't want to see - You can mute ads on the Display Network that you don't want to see. When possible, after an ad is muted, the ad fades away and the space previously occupied by the ad collapses smoothly, allowing the content surrounding the ad to fill the space.

- Manage your ads settings- Add or remove the interests and demographic details that are used to show you ads.

For eg: You purchased a dinner set as a wedding gift but don't want to see ads for tableware when you're reading the news and everywhere else that you go on the web. You can remove interests related to dishware, like "Shopping". You may still see ads for tableware – if you're on a blog where all visitors see ads for tableware, for example – but editing your interests can help minimize unwanted ads.

VI. CONCLUSION

For a permanent solution to all the spy and hackers or any kind of unwanted apps this idea of hidden app has been formulated which blocks those apps on attaining the running mode. It basically consist of an antivirus which not only performs the basic antivirus features of finding viruses in any of the apps or recognize it again and block it automatically without asking but also demolishes the ads of no use to the user besides the apps which could be send by the attackers.

VII. Acknowledgment

An indebted gratitude is expressed to Genesis Futuristic Technologies Ltd., Noida who has encouraged to visualize the plan through paper. We would wish to acknowledge the same which has helped us to great extent for the design and development of this utility.

References

[1] Hengshu Zhu, Hui Xiong, Yong Ge and Enhong Chen, "Mobile App Recommendations with Security and Privacy Awareness," *KDD'14,* August 24–27, 2014, New York, NY, USA.

[2] G. Delac, M. Silic and J. Krolo, "Emerging Security Threats for Mobile Platforms "Faculty of Electrical Engineering and Computing, University of Zagreb, Croatia Google Inc., New York, USA

[3] Suman Nath, Felix Xiaozhu Lin and Lenin Ravindranath, "Smart Ads: Bringing Contextual Ads to Mobile Apps," MobiSys' 13, June 25–28, 2013, Taipei, Taiwan.

[4] Prashant Kumar Gajar, Arnab Ghosh and Shashikant Rai, "Bring your own device (BYOD): Security risks and mitigating strategies," Volume 4, No.4, April 2013 Journal of Global Research in Computer Science.

[5] Priyanka Goyal, Sahil Batra, Ajit Singh, "A Literature Review of Security Attack in Mobile Ad-hoc Networks," International Journal of Computer Applications (0975 – 8887) Volume 9– No.12, November 2010.

[6] https://support.google.com/adwords/answer/2472719?hl=en

[7] http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3636327/

[8] http://www.huffingtonpost.com/rohit-sethi/why-developers-build-inse_b_5549482.Html?ir=India&adsSiteOverride=in