IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 8, August 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.569

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008172|

Advanced Mobile Application Security

Hiten Ovalekar[1], Vidula Suryawanshi[2]

U.G. Student, Department of Information Technology, B.K Birla College, Kalyan, Maharashtra, India[1]

U.G. Student, Department of Information Technology, B.K Birla College, Kalyan, Maharashtra, India[2]

ABSTRACT:With the Explosive global adoption of mobile applications has been fraught with security and privacy issues. App users typically have a poor understanding of information security; worse, they routinely ignore security notifications designed to increase security on apps.In the past we have rapid prevalence of smart mobile devices, the number of mobile Apps available has exploded over these few years. To facilitate this choice of mobile apps, existing mobile app recommender systems typically recommend popular mobile Apps to mobile users. However, mobile Apps are highly varied and often poorly understandable , particularly for their activities and functions related to privacy and security. Therefore, more and more mobile users are reluctant to adopt mobile Apps due to the risk of privacy invasion and other security concerns. In this paper, we propose to develop a mobile app system with privacy and security awarenessand these is what we can do in these research paper

KEYWORDS:. Android IOS, PC's , API's

I. INTRODUCTION

The Mobile application security focuses on the software security posture of mobile apps on various types of platforms like Android, iOS, and Windows Phone and It involves assessing applications for security issues in the contexts

of the platforms that they are designed to run on, the frameworks that they are developed with, and the very anticipated set of users. All of these popular mobile platforms provide security controls designed to help software developers build secure applications and a lack of vetting can lead to security feature implementation that can be easily circumvented by attackers. These Mobile devices including smartphones and tablets, enable users to access there corporate data from anywhere.These paper focuses on the increasing need for mobile business and its related mobile device security concerns andWe propose that future ofIT professionals should be aware of these issues and learn how to secure the mobile devices through the integration of the topic into this It model curriculum.

II. RELATED WORK

The number of studies have examined individual vulnerabilities related to their vulnerability classes we study and none one look at datasets of the same scale or are able to discuss trends in vulnerable apps. In each case, as we explained below, our work expands beyond the prior understanding of thesetypes of vulnerabilities. et al. , Chin et al. And Georgiev et al. Studied attacks on the mobile web apps from the untrusted content. Luo et al. Manually analyzed the small set of apps for vulnerability but incorrectly assumed that mobile web apps allow navigation to arbitrary web content and therefore failed to explore the effect of navigation control on the mobile web app security. Chin et al. Builted a static analyzer to find the apps that allows navigation to untrustable content and the authors understand the importance of the should Override UrlLoading method but handle it using a simple heuristic that fails to capture its behavior accurately. These authors also do not consider implementations of shouldInterceptRequest in there analysis. Georgiev et al. Studied the JavaScript Bridge in a mobile web apps developed using the PhoneGap and analyzed several thousand mobile web apps for vulnerabilities but their experiment is limited to apps built using the PhoneGap, and, like Luo et al. , they do not explore the effect of these navigation control. The scope ofthese attacks from untrusted web content, our work extends beyond these results by accurately capturing the effect of navigation control methods when identifying apps that navigate to untrusted web content and the

Fahl et al. And Tenduklar et al. Analyzed Android apps for errors in their SSL implementations and found that the many apps validated certificates incorrectly. Sounthiraraj et al. Builted a dynamic analysis tool to thise detect apps that incorrectly validate SSL certificates. However, this studies overlook onReceivedSslError as a method of incorrectly validating SSL certificates and do not measure how freqently developers implement it unsafely. The results of our are

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008172|

therefore orthogonal to these results and combine to demostrate that incorrect use of SSL is a widespread problem in Android apps.

Chen et al. Studied several popular OAuth providers for mobile apps and identified how the differences between the mobile and browser environments can lead to OAuth vulnerabilities. One vulnerability they have describe is how a leaky URL vulnerability can expose OAuth credentials to malicious apps. Their work focuses specifically on the OAuth and does not consider the more general vulnerability class of leaky URLs or the broader vulnerability classes we consider.

Many severalstudies have explored exposed app components as a mechanism to perform privilege escalation attacks in Android. Davi et al. Demonstrated that inter-app communication can leak privileged operations to other apps. Grace et al. And Lu et al. Builted a systems for identifying apps that leak privileges. Felt et al. Proposed a mechanism for the preventing privilege leaks using IPC inspection, and Bugiel et al. [14] provided another solution to prevent privilege leaks at the operating system level. The mechanism for these vulnerabilities is similar to the mechanisms behind the exposed of the POST request vulnerability but represent attacks on the mobile device and its APIs instead of an attack on the mobile web application.

III. METHODOLOGY

This section, we present a methodology to conduct secu-rity audit of mobile applications covering the analysis blocks presented in Section III, and thus, the OWASP Top Ten Mobile Risks. This methodology allows finding vulnerabilities, to detect malicious behaviours, and even to analyse application performance. The methodology also aims at covering a broad number of aspects when auditing a mobile application, suchas detecting coding flaws or insecure design.The methodology consists of three main phases subdivided into several tasks: Pre-runtime, which encompasses the anal-ysis of the application before executing it; Runtime, which describes the analysis performed to an application under execution; and Post-runtime, which encompasses the analysis tasks after an application execution. Fig. 1 depicts a flowchart of the proposed methodology

IV. EXPERIMENTAL RESULT

Our snapshot of the Google Play store contains 1,172,610 apps, 998,286 (85%) of which use a WebView in some fashion. These apps represent a complete snapshot of the free mobile web apps on the store as of June, 2014. Along with the apps, we collected data about each app including the number of times it has been downloaded and the most recent date that it was updated. We performed our analyses on 100 Amazon EC2 c3.4xlarge virtual machines for approximately 700 compute hours. Table 1 shows the percentage of mobile web apps that use features relevant to this study. In total, 28% of mobile web apps in our dataset contained at least one vulnerability. We are currently reporting these vulnerabilities to the developers of the most popular apps and libraries.

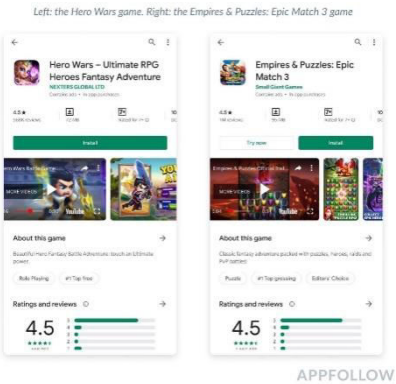

fig.1.Combine landscape and portrait layouts for screenshots and videos.

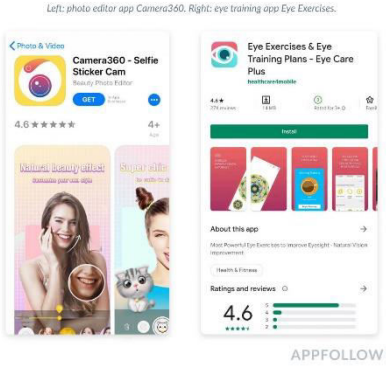

Fig.2.Portrait screenshot and video.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008172|

V. CONCLUSION

In conclusion, the introduction and analysis of various mobile devices and mobile application security issues by providing wider techniques of threats in mobile. The bigger risks as well as major threats that faced smart phones compared to the PCs have been highlighted. Some more, from the literature study and researcher prospective threats in data security and communication are going to become more difficult to manage because hackers are looking of different ways to breach smart device platform. This can be done through added levels of security and manufactures access points as well as application programming interfaces API's. Hence, mobile applications tackle eachof the aspect of our life and simplified the way that apps can be used for: business, social networking, shopping, travel, education, banking and network utility. In addition the security is one of the potential and challenging activities which need to be taking into consideration during the developing phases. More importantly, developers must be consider their application's levels of security within different popular platforms such as iOS and Android. This can be identified that the number of mobile end users who are downloading applications are increasing rapidly. Therefore, we are applying better security mechanisms should be in place during application signing. To conclude the further education for user about how to use mobile safely found to be crucial to degrade the number of data lose, attacks as well as threats.

.

REFERENCES

1. Wu, D., Moody, G., Zhang, J., & Lowry, P. (2020). Effects of the design of mobile security notifications and mobile app usability on users' security perceptions and continued use intention. Information & Management, 57(5), 103235. doi: 10.1016/j.im.2019.103235
2. Patil, K. (2017). AN INSECURE WILD WEB: A LARGE-SCALE STUDY OF EFFECTIVENESS OF WEB SECURITY MECHANISMS. ICTACT Journal On Communication Technology, 08(01), 1466-1471. doi: 10.21917/ijct.2017.0217
3. Grover, J. (2013). Android forensics: Automated data collection and reporting from a mobile device. Digital Investigation, 10, S12-S20. doi: 10.1016/j.diin.2013.06.002

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.569

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details