3rd National Conference on Green Technology and Science for Sustainable Development
© 2020 IJSRST | Volume 5 | Issue 6 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
International Journal of Scientific Research in Science and Technology

Performance and Security Related to Mobile Application

Dr. A.S. Kapse[1], Shivani A. Mate[2], Sukanya v. Shelke[3],

[1]Professor (HOD), Department of CSE, Anuradha Engineering College, Chikhli, Sant Gadge Baba Amravati University, Maharashtra, India

[2,3] B.E, Department of CSE, Anuradha Engineering College, Chikhli, Sant Gadge Baba Amravati University, Maharashtra, India

ABSTRACT

In this advancing world of technology, mobile application are a quickly growing segment of the global mobile market, such as banking , social networking, Financial apps, entertainment and so on. Android is a cell phone working framework propelled by Google under the permit of apache. Android is for the most part utilized in the market. Individuals was utilizing android in their everyday life. While utilizing android telephone there are numerous security issues, to conquer that security issue that we find in this paper. The utilization of android will be simpler to utilize. Step by step includes gave by android has expanding security challenges. In this paper means to presented security of the application and noxious applications that numerous impacts or release touchy dada, for example, universal versatile gear personality number (IMEI)of gadget, credit or charge card data, etc. As per GSMA well known working framework utilized in the cell phones are Android and iOS. The most recent working framework. Android gives great security and security issue show up on account of security imperfections and ill-advised advancement of the applications. Android showcase is developing security chance has expanded and, in this way, centre ought to be given to the security.

Keywords : Android, mobile attack, application framework, android runtime layered approach, AA Sandbox.

I. INTRODUCTION

Mobile devices are having application for every activity of human life .mobile are used to perform bank transactions, E-mail, messages, some sensitive data etc . According to GSMA Intelligence, in 2017 there are 5 billion unique mobile subscribers around the world, and 3.3 billion mobile internet users. Whenever we are using mobile smart phones because of the moment of the phone. we can enter from the one network to another network. By increasing demand of smart phones increasing security problems. most popular operating systems used in mobile device are Android and ios. There are different version of Android operating system like nougat, lollipop, Marshmollow, etc, similarly different virsion of ios are ios 10 ,ios 9,ios 8etc. Day by day features provided by Android has increasing security challenges have also increased. Open web application security project (OWASP) [4] Analyses mobile risk, Data storage and insecure communication risks are most accurate problems in mobile security. Therefore, security requirements and issues within various mobile platforms become a targeted area of many studies and research. Generally, confidentiality, integrity availability are three fundamental categories of the security goals and objectives of information in an organization [3] [12].

In this peper focus on security in mobile application platforms and techniques has been analyzed in different outlook in which identify how both ios and Android platforms has implemented security models against threats. The platform of Android was officially announced and the SDK tools were available in october2008. According to the official Android website (Android2008) the platform is based into the four core features as shown in fig 1

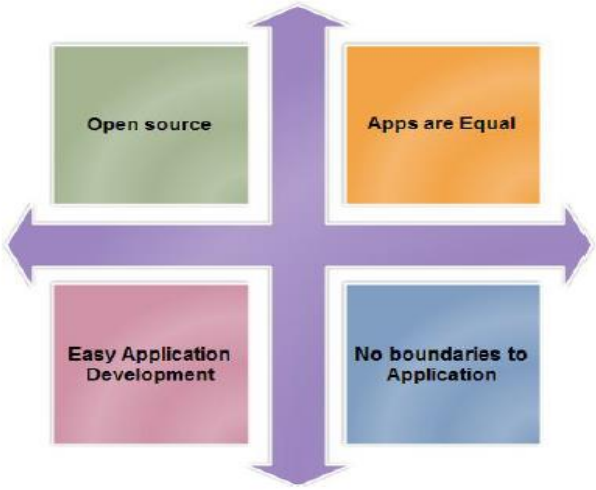

Figure 1. Four core features of the android platform

II. LITERATURE REVIEW

Studied the different security-related challenges for mobile users, mobile threats. Different types of mobile risk involved in their study are physical based threats, application based threats, network based threats and web-Based threats. According to one of important security defense mechanism for data privacy and mobile security is Biomatric authentication. Security mechanisms need to be involved in every stage of mobile application development.[2]Improvement in new technologies and developments in security measures needed to be parallel .The main issues with the mobile security are implementing proper security policies, integrating current security and protecting data in mobile devices .To secure business documents and data, corporate need to implement a secure environment for mobile devices, Threat management and security policies need to be independent of devices and operating system used in them. Analyzed the vulnerabilities found in mobile application related to health care. They categorized mobile health apps into six groups based on apps functionalities and downloaded ten android apps related to each group from Google play store to analyzed vulnerabilities. The greatest number of attack are targeted vulnerabilities and also vulnerabilities in these apps contain high-risk levels. The resultbof vulnerabilities are 64% in Health app related to untrusted input. According to threats predictions report [14] 2015 will the turning point for threat to mobile devices in which the total number of mobile malware sample exceeded 5 million in Q3 2014.Therefore, security requirements and issues within various mobile platforms become a targeted area of studies and researches.

III. ARCITECTURE

Android is a software stack for mobile devices that includes an operating system and key application. Android based on linux version 2.6. The system services such as security, memory management, process management are controlled by linux shows android architecture.

Figure 2. Architecture of Android

Android is a mobile operating system and platforms for mobile application development. The architecture of android system is basically following four layers

Application layer- It includes all the applications.

1)Application framework layer- This layer provides high level services for application development in the form of Java classes. Application developers are allowed to make use of these classes in their applications. These services include Activity Manager, Location Manager, Content Provider, Notification Manager, Package Manager, View System and so on.

2) Libraries-The Android system provides some C/C++ libraries. Different components of the Android system can utilize these libraries. All these libraries are accessible with the help of the application framework.

3)Android Runtime- It deals with compilation of android app under the Dalvik Virtual Machine (DVM) which produces the optimized code for mobile phones.

4) Linux Kernel- It is the last layer in the android architecture which has direct communication with hardware and which provides basic service like Inter Process Communication (IPC), security and so on. Linux kernel provides uid for each process, pre-emptive multitasking, etc. Each application has its own uid and it runs in its own virtual machine. In addition to this android also provide permission mechanism and Application and signing mechanism for security purposes.

IV. APPLICATIONS

- ✓ Unsafe file creation
- ✓ Improper database storage
- ✓ Unsafe use of shared preferences
- ✓ Storage of sensitive data on mass storage device
- ✓ Content provider SQL injection
- ✓ APN or proxy modification

V. ADVANTAGES AND LIMITATIONS

Advantages

- ✓ Direct Communication and Geo-targeting Marketing
- ✓ Increased Recognition Builds Customer Loyalty
- ✓ Website Creates Awareness And The App Makes The Sale
- ✓ A Great Tool For Customer Engagement
- ✓ Improved visibility

Limitations

- ✓ Accelerate Information Overload
- ✓ Privacy and Security
- ✓ Costs of developing and marketing

VI. CONCLUSION

From the above it is included that even through android provides good security but sill, vulnerabilities and security problem arrive because of security flaws and improper development of the applications. for this reason a proper security mechanism is needed to avoid the security risks and identify the malicious apps for the security of the sensitive data

VII. REFERENCES

[1] Manvindar Singh Chauhan, Kulvinder Singh, “Security Risk Associated with Android Applications”, Department of CSE, DIET Rishikesh, Uttarakhand, India

[2] Taranjeet Kaur Chawla, Aditi Kajala, 4, April 2014, 1204-1268, “Transfiguring of an Android App Using Reverse Engineering”, International Journal of Computer Science and Mobile Computing Vol. 3 Jssue.

[3] Enck, William et al., 2011, "A Study of Android Application Securit y", USENIX security symposium.

[4] QBRST, July 2014, “Mobile Application Security”, Best Practices to Optimize Security.
[5] Jae-Kyung Park* and Sang-Yong Choi, “Studying Security Weaknesses of Android System”, International Journal of Security and Its Applications, 9(3).
[6] Sascha Fahl, 2015, 7-12, Marian Harbach et al “Why Eye and Mellory Love Android : “An Analysis Of Android SSl (In) Security”.
[7] Whatisandroid?http://developer.android.com/guide/basics/what-is-android.html
[8] 3G Mobile Terminal Development Trend of the operating system[M/OL]. http://pda.c114.net/32/c4948.html, 2007
[9] Dr.A.S.Kapse, Shivani A. Mate, Harshada D. Raut, Sukanya V. ,“Cross Platform User Campatible system”, IRJET Volume 6,Issue 10, October 2019 , e-ISSN: 2395-0056, P-ISSN: 2395-0072. https://www.irjet.net/archives/V6/i10/IRJET-V6I10123.pdf
[10] Static detection of malicious code in executable programs by J.Bergeron, M. Debbabi, J. Desharnais, M. M. Erhioui, Y. Lavoie, and N.Tawbi.
[11] An Android Application Sandbox System for Suspicious Software Detection, by Thomas Bl¨ asing, Leonid Bat yuk, Aubrey-Derrick Schmidt, Seyit Ahmet Camtepe, and Sahin Albayrak
[12] Cifuentes, Y., Beltrán, L., & Ramírez, L. (2015, August). Analysis of Security Vulnerabilities for Mobile Health Applications. In 2015 Seventh International Conference on Mobile Computing and Networking (ICMCN 2015).
[13] Choo, K. K. R. (2014). Mobile cloud storage users. IEEE Cloud Computing, 1(3), 20-23.
[14] Agasi, O. (2015). Encapsulating mobile security. Computer Fraud & Security, 2015(6), 10-12.

AUTHORS PROFILES

Dr. Avinash S. Kapse received his BE degree in Computer Science & Engineering from Sant Gadge Baba Amravati University, Amravati in 2005 and ME from Government College of Engineering, Aurangabad University in 2010. He has received Ph.D. degree in Computer Science and Engineering from Singhania University
in Sept2017.

Ms. Shivani A. Mate pursuing Bachelor of Engineering in Computer Science & Engineering Department from Anuradha Engineering College of SGBAU Amravati University Maharashtra.

Ms. Sukanya V. shelkepursuing Bachelor of Engineering in Computer Science & Engineering Department from Anuradha Engineering College of SGBAU Amravati University Maharashtra.