Recent Development and Techniques in Android Application Security

Rushali Pawade, Deepa Hosur, Menaka, Soumya Biradar, Ashalatha Ramegowda, Shivanand S Rumma

Department of P.G. Studies and Research in Computer Science, Gulbarga University, Kalaburagi

rushalipawade31897@gmail.com, hosurdeepa044@gmail.com, menakaanand043@gmail.com, biradars777@gmail.com, ashalatha.dsce@gmail.com, shivanand_sr@yahoo.co.in

ABSTRACT

An android operating system is an open-source and Linux-based operating system for smartphones and tablet PCs. The android operating system is built basically for mobile phones, and the software is based on the Linux Kernel and other open-source software. Android is very popular nowadays among students for choosing Android for the sake of their projects. Therefore, a beginner must build baby Android apps to learn Android software. Android is a sort of mobile operating system used in electronic gadgets such as smartphones, tablets, and television. It also provides an adaptive framework that allows the developer to create apps more simply. Furthermore, Android is an open-source tool where developers can develop and expand new features to make their applications better. This paper aims to concentrate on the security scanning process and the features of android application development for mobile phones.

Keywords: Android, Application, Smartphone, Security

1. INTRODUCTION

Android Inc started android app development, later bought by Google in the year 2005. its first commercial version was released in September 2008. since then, a different number of versions have been released with excellent features. Android has a user-friendly and straightforward interface program. It has simplicity with a touch of sophistication which the user interface of an Android app should be. Also, creating a shortcut for essential functions will be an added advantage. Thus, in turn ultimately leads to user experience enhancement [1].

Android is software primarily used in handheld devices that act as an intermediate between the user and the device hardware. It is a mobile operating system currently developed by Google used for touchscreen mobiles like smartphones and tablets. Android requires a readymade, low-cost, and customizable operating system for high-tech devices. Android supports various connectivity technologies like GSM, EDGE, Wi-Fi, Bluetooth, WiMAX, CDMA, EV- DO, NFC and IDEN, etc. Android supports various security measures for protecting the user data for security isolation of applications. Moreover, it checks enormous system resources like hardware and software, etc [2].

2. LITERATURE SURVEY

Many researchers have gained various recent solutions for android application security. Nawaz et al. have used hybrid analysis features for android applications. The performance has been gained through the feature selection procedure having an info gain method [3].

Omer et al. have analysed various malware detection characteristics. In addition, they have addressed different malware detection strategies [4]. Long et al. have proposed the CNN method for android applications. This method is used to detect malware and classify various malicious applications [5].

Sharma et al. have proposed a machine learning framework for detecting android ransomware. This method has used a learning model to achieve efficiency in android applications [6]. Li et al. have proposed a feature-based selection procedure for malware detection over android phones. A multiple feature set sample algorithm is designed and implemented [7].

Hadidjaja et al. have proposed a Bluetooth-based implementation model for android applications [8]. Krishna et al. have found an intelligent security system for women using a GPS module [9].

3. ANDROID APPLICATION DEVELOPMENT

Security is defined as the risk has the vulnerability along with threats and consequences. Unfortunately, various researchers recently have found new android application security features. Some of the android security features include finding the mobile device, locking the screen preferences, getting app permissions, safe browsing, multi-factor authentication, etc [10].

i.App development steps

The app developers and the researchers have to know the various security steps while developing an android mobile app. The actions and solutions are given in Table 1.

Table 1. Security solutions

Step no.	***Required step to do***
1.	Write a secure source code
2.	Encrypt the given data
3.	Be careful while using libraries
4.	Use authorized API
5.	Use high level authentication code
6.	Use tamper detection techniques
7.	Provide least privileges for app
8.	Have proper session management
9.	Use legible cryptography tools and techniques

10.	Test repeatedly

4. RECENT CHALLENGES IN ANDROID SECURITY

Figure 1 represents the security features for android security applications. They include Avast mobile security, VIPRE, NOX, Bouncer, Safe security, Malware bytes, lookout, Firefox focus etc [11].

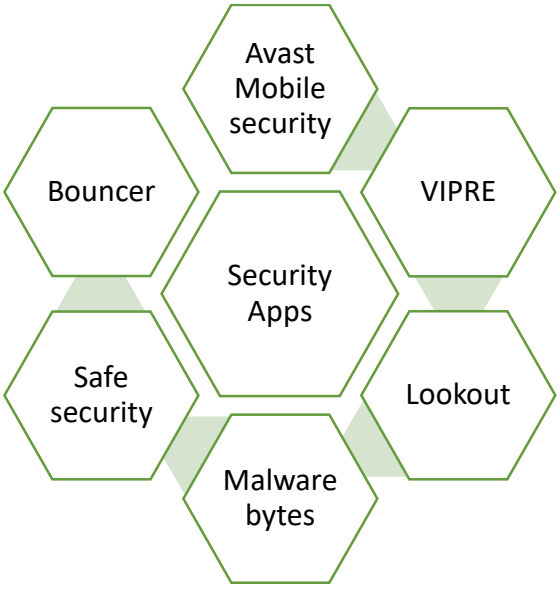

Fig 1. Android security apps

i.Recent research challenges

Some of the research challenges in android application security are given as follows.

a. Device Fragmentation

Mobile application testing requires the association of security vulnerabilities particular to devices makes performance testing a problematic task. The testing team cannot test releases quickly as the development team, so they become a bottleneck in the releasing issue [12].

b. Tools required for Mobile Automation Testing

The fragmentation method requires an automation testing process. The traditional testing tools, such as the Selenium software tool, Quick Test Professional (QTP), are not designed with cross-platform in mind. Therefore, there is a shortage of security testing tools.

c. Weak Encryptions

The mobile application accepts the data from different sources, and hence attackers could modify inputs such as cookies and environment variables.

d. Weak Hosting controls

Businesses expose to server-side systems that are inaccessible to outside networks. The servers of various third-party systems may access the app, and the back-end systems need to be secured against malicious software attacks.

e. Insecure Data Storage

In most apps, consumers enter their passwords when activating the payment portion of the app and use it repeatedly [13].

ii.Security solutions

Various android security solutions are listed as follows.

1) Robust Code Protection

Robust code protection means allowing the code files for security such as DEX, DLL, and SO type files.

2) Rooting & Emulator Detection

Rooting and emulator detection involves an android real-time emulator used to secure the app working in compromised environments [14].

3) Cheat Tool Detection

Cheat tool detection is used to neutralizes the cheat tool.

4) Network Packet Sniffing and spoofing detection.

The network packet sniffing is used for securing the data packets and spoofing detection [15].

5. CONCLUSION

Android phones are the most extensively used mobiles in recent days. Improvising the security of an Android operating system is very important to safeguard the user's privacy and confidential information. In this work, we have tried to show various techniques for avoiding misusing app permissions using Android.

REFERENCES

1. Negi, C., Mishra, P., Chaudhary, P., & Vardhan, H. (2021). A Review and Case Study on Android Malware: Threat Model, Attacks, Techniques and Tools. *Journal of Cyber Security and Mobility*, 231-260.
2. Yasin, H. M., Zeebaree, S. R., Sadeeq, M. A., Ameen, S. Y., Ibrahim, I. M., Zebari, R. R., ... & Sallow, A. B. (2021). IoT and ICT based Smart Water Management, Monitoring and Controlling System: A Review. *Asian Journal of Research in Computer Science*, 42-56.
3. Nawaz, A. (2021). Feature Engineering based on Hybrid Features for Malware Detection over Android Framework. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(10), 2856-2864.
4. Omer, M. A., Zeebaree, S. R., Sadeeq, M. A., Salim, B. W., x Mohsin, S., Rashid, Z. N., & Haji, L. M. (2021). Efficiency of malware detection in android system: A survey. *Asian Journal of Research in Computer Science*, 59-69.
5. Vu, L. N., & Jung, S. (2021). AdMat: A CNN-on-Matrix Approach to Android Malware Detection and Classification. *IEEE Access*, *9*, 39680-39694.
6. Sharma, S., Challa, R. K., & Kumar, R. An Ensemble-based Supervised Machine Learning Framework for Android Ransomware Detection.
7. Li, X., Kong, K., Xu, S., Qin, P., & He, D. (2021). Feature selection-based android malware adversarial sample generation and detection method. *IET Information Security*.
8. Hadidjaja, D., Wisaksono, A., Ahfas, A., Syahrorini, S., & Untariningsih, D. H. (2021, March). Bluetooth implementation on automation of Android-based gate doors. In *IOP*

Conference Series: Materials Science and Engineering (Vol. 1098, No. 4, p. 042061). IOP Publishing.

9. Krishna, S. S., Murugan, G. S., & Janani, S. R. (2021). Smart Women Security System: An Android Application Using GPS. *International Journal of Research in Engineering, Science and Management*, *4*(3), 188-189.

10. Pahuriray, A. V. SCHOOL ANDROID BASED E-SERVICES.

11. Ansari, M. T. S. R. N., Khemariya, A., & Tiwari, A. (2021). Android Phone Data Security using Special Features.

12. Grispos, G., Flynn, T., Glisson, W., & Choo, K. K. R. (2021). Investigating Protected Health Information Leakage from Android Medical Applications. *arXiv preprint arXiv:2105.07360*.

13. Khan, M. R., & Jain, M. K. (2021). Protection android app with multiDEX and SO files from reverse engineering. *Materials Today: Proceedings*.

14. Saravanan, D., Feroskhan, J., Parthiban, R., & Usharani, S. (2021, January). Secure Violent Detection in Android Application with Trust Analysis in Google Play. In *Journal of Physics: Conference Series* (Vol. 1717, No. 1, p. 012055). IOP Publishing.

15. Olaleye, S. B. (2021). Security of Sensitive Data on Android Smartphones Using Cloud Storage with Reference to Gravitational Search Algorithm.