Research on Security Detection and Risk Evaluation Technology of Android Mobile Application

Dongyang Cai(✉), Yongmin Cao, Kaili Zhao, Xuening Zhang, and Rui Bo

State Grid Tangshan Power Supply Company, Tangshan, Hebei, China
839911455@qq.com, {cao.yongmin,zhao.kaili,zhang.xuening,
bo.rui}@jibei.sgcc.com.cn

Abstract. In recent years, with the rapid development of the mobile Internet and the continuous growth of smart terminal users, the development of mobile applications has become increasingly mature and diversified, bringing users a fast application experience, while completely changing people's lifestyles and even social patterns. Terminal manufacturers, network operators, and major industry platforms use App-based information technology carriers to collect user data on a large scale through technologies such as data collection, big data analysis, and character portraits. Related data security issues have also arisen, especially how to protect sensitive personal privacy data. In order to improve the security operation level of mobile applications and maximize the protection of users' personal sensitive data, it is necessary to strengthen the security development, security test, and security reinforcement of mobile applications. To this end, this paper proposes a mobile application security assessment method based on the entropy weight method to provide support for the security construction of the mobile application.

Keywords: Android · Mobile Application · Evaluation · Risk

1 Introduction

For the sake of adapting to the ever-increasing user demands, more and more mobile applications are developed and launched. The mobile application has greatly changed people's way of life while bringing users a convenient and flexible application experience with the growing maturity and diversification of its development. At the same time, issues such as security risks surrounding mobile applications and illegal collection of personal information have become increasingly prominent, triggering national supervision to attach great importance to application security.

In the process of building a network information security system, mobile security is prone to being overlooked by everyone. A large number of security operators and maintainers have misjudged the mobile security risk situation, and often unilaterally believed that efforts to maintain good application-level security reinforcement are also intended to do a good job of comprehensive protection. However, mobile security is still confronted with a large number of business security risks. In recent years, the functions of mobile applications have become more and more powerful, and more and more

K. Subramanian et al. (Eds.): CTMCD 2022, ACSR 99, pp. 186–195, 2023.
https://doi.org/10.2991/978-94-6463-046-6_23

multi-dimensional information of users is collected and stored on the mobile terminal [10]. Facing the temptation of interest, the probability of malicious attacks on mobile terminals is increasing. Therefore, while the mobile business system is being built, it is urgent to conduct comprehensive detection and supervision of the security risks of various mobile applications to reduce the risk of business continuity operations. This paper proposes a mobile application security assessment method based on the entropy weight method, which provides strong support for the construction of mobile business application scenarios.

2 Manuscript Preparation

Typical mobile Internet business application scenarios is shown in Fig. 1, which includes servers, mobile clients, security protection equipment, network equipment, communication transmission links, etc. [8]. The server is responsible for providing business function management, user information maintenance, system configuration maintenance services, data publishing services, and other functions. The mobile client is in charge of data browsing, information entry, user interaction, etc. The mobile terminal mainly uses mobile communication for data access, while the server is interconnected by wired communication.

2.1 Analysis of Mobile Security Risks

The security of mobile applications mainly includes the local security of mobile applications, communication security and server security [5]. Currently, mobile applications generally use Web API to interact with server data, which binds mobile application security and Web service security together. Current mobile application reverse analysis, secondary packaging, code tampering, application phishing, memory injection, dynamic debugging, data theft, transaction hijacking and other malicious attacks, more and more attention. However, due to the professionalism of mobile application security, developers and users cannot fully understand the security risks and vulnerabilities of applications,

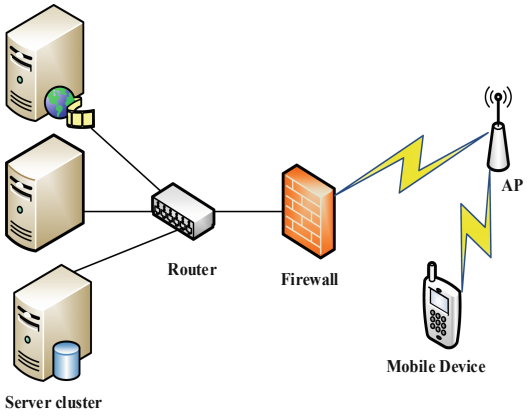

Fig. 1. Typical mobile application interconnection scenario.

and it is difficult to make in-depth assessment and analysis of application security [7]. Moreover, they lack professional knowledge to solve the security problems one by one. Common security risks and hidden dangers of mobile applications mainly include the following types:

2.1.1 Local Security of Mobile Applications

The APK package is vulnerable to being decompiled into a readable file and repackaged into a new APK with minor modifications [3]. There are risks such as software cracking, logic modification, and insertion of malicious code; risks of data storage and transmission, as well as leakage and tampering of sensitive information, are present occasionally; permissions invocation and component exposure problems are prevalent; there are dangerous vulnerabilities such as Webview, AllowBackup, etc.

2.1.2 Security of Communication

There are risks in network communication security [11]. Through network packet capture, data packet analysis, etc., it is possible to obtain application transmission information; there are situations in which key data is transmitted in plain text and weakly encrypted in communication transmission; server-side user login verification is not strict, and there are bugs such as unauthorized access, traversal, replay, etc.

2.1.3 Security of Server

There are common web vulnerability risks on the mobile application server-side [6], such as SQL injection, cross-site scripting, file upload, directory traversal, etc. The server-side security is tested after obtaining the server address through the mobile application.

2.2 Attack and Defense Technology of Mobile Application

2.2.1 The Risk of Static Attack

The Java development language used in the Android mobile APP makes the APP easy to be decompiled and reversely analyze the source code, resulting in risks such as cracking, tampering, advertisement placement, secondary packaging, counterfeiting/phishing applications, etc. [2].

2.2.2 Dynamic Attacks in the Running Process

Due to the uncontrollable running environment of the APP and operation behaviors of users, the APP faces various dynamic attacks during the running process, such as simulators, multi-openers, accelerators, injection attacks, dynamic debugging, device tampering, and location fraud [1].

2.2.3 Business Cheating Attacks

A large number of businesses have been transferred from offline and web terminals to mobile APPs [4]. At present, underground black products are usually batched and

machined in APP registration, login, and marketing activities, threatening platform interests and user account security.

3 Security Test Method of Mobile Application

For the Android mobile application technology architecture, the attacker's entry point may come from any of the nodes. Therefore, the security testing research needs to be carried out on each node of the architecture. This section mainly conducts security tests from the aspects of mobile application client, communication transmission security, and server application security [9].

3.1 Security Test of Mobile Application Client

- Protection test of mobile application code. It checks whether the application has taken anti-reverse measures and whether it can decompile the mobile application and obtain the source code and resource configuration file. Malicious code detection is to detect whether there is malicious code, implanted plug-ins, etc.
- Login test. It tests whether the login interface can be hijacked by phishing, whether it can bypass the login authentication and directly enter the application system, whether it has a login failure lock function, etc.
- Sensitive data leakage test. It detects whether the SD card storage file, database file, configuration file, etc. can be exported, and check whether there is a leakage of sensitive information, whether there is an AllowBackup vulnerability, etc.
- Application permission test. It checks the configuration file to see if there are dangerous permissions in the open permissions, and it is needed to pay attention to the permissions to obtain mobile phone and text verification information.
- Component call test. It detects whether Activity, Service, Broadcast Receiver, and Content Provider have component exposure and call verification vulnerabilities.

3.2 Security Test of Communication

- Network packet capture test. It configures the HTTP proxy tool, the BurpSuite tool, and the wireless settings of the simulator, captures the communication between the mobile application and the server through the BurpSuite proxy, and analyzes it; the tcpdump is used to export the communication packets caused by the application operation in the device, and the Wireshark is used to view.
- Clear text transmission of key data. It detects whether there is a clear text transmission or encryption method exposure of key data such as passwords and cookies.
- Session security. It detects whether there is a vulnerability in the session management process.

3.3 Security Test of Server-Side

- Port and vulnerability scanning. It scans the server's open ports and the presence of medium or high-risk vulnerabilities.

- Data leakage test. From the mobile method description, the test detects whether there are vulnerabilities such as SQL injection, directory traversal, file upload, remote command execution, cross-site scripting, etc., and whether there is a sensitive information leakage problem.
- Permission verification test. It checks whether there are problems such as lax user login authentication, replay attacks, and unauthorized access.

4 Security Assessment Method of Mobile Application

With the popularity, openness and interconnection of mobile Internet, Android mobile applications are not only facing traditional security vulnerabilities, but also facing many new problems. Therefore, it is necessary to strengthen the security evaluation of Android mobile applications and improve the security protection level of mobile applications. The security evaluation process of Android mobile application is shown in Fig. 2.

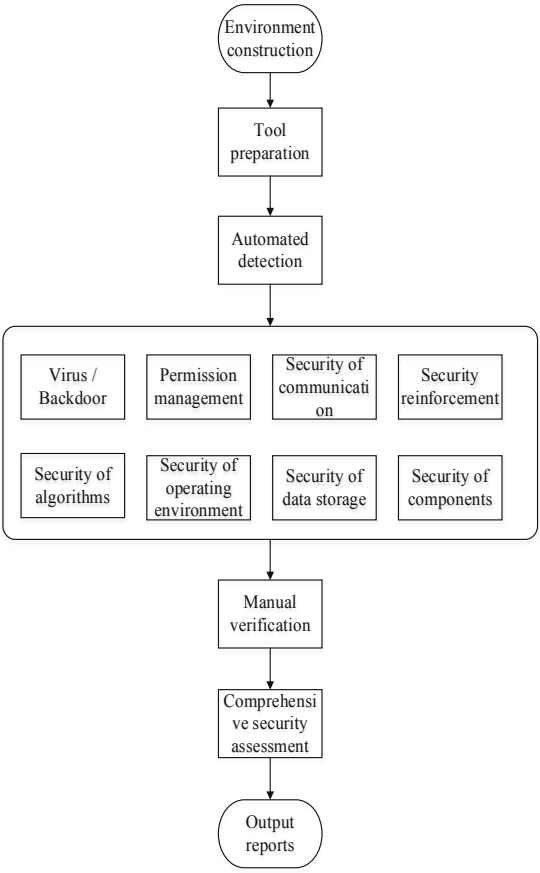

Fig. 2. Security assessment process of Android mobile applications.

Table 1. Risk degree assignment of Android mobile application security function defect.

Level	Notation	Definition
1	Very low	If the defect is exploited, it will cause ignored damage to the mobile application
2	Low	If the defect is exploited, it will cause minor damage to the mobile application
3	Medium	If the defect is exploited, it will cause general damage to the mobile application
4	High	If the defect is exploited, it will cause general damage to the mobile application
5	Very high	If the defect is exploited, it will cause complete damage to the mobile application

4.1 Establishment of Safety Evaluation Indicators

According to the exposure degree of Android mobile application security function defects to assets, the difficulty of technical realization, popularity, etc., the risk degree of the identified Android mobile application security function defect indicators is assigned in a hierarchical manner. The higher the rating value is, the higher the risk level of the Android mobile application security function defect indicator will be. This paper divides the risk degree of Android mobile application security function defect indicators into five levels. Table 1 provides the risk degree assignment method of Android mobile application security function defect indicators. The Android mobile application security function defect indicator system is shown in Table 2. The Definition of Android mobile application security function defect indicator is shown in Table 3.

4.2 Calculation of Indicator Weights

In order to achieve a comprehensive assessment of the risk of Android mobile application security function defects, the entropy method is used to determine the weights of the 19 secondary evaluation indicators in Table 2. The entropy method is an objective weighting method that uses the information entropy to evaluate the degree of variation of the obtained information, thereby determining the weight of the indicator. This method can reduce the interference of human factors in the evaluation process. Therefore, for the above evaluation indicators, the entropy method can be used to determine their weights, the comprehensive evaluation value of the Android mobile application security function defect risk can be calculated. In the problem of given n Android mobile applications to be evaluated and $m(m = 19)$ secondary evaluation indicators, the entropy value of the j-th indicator is defined as:

$$E_j = -\frac{1}{\ln n}\sum_{i=1}^{n} f_{ij} \ln f_{ij} \tag{1}$$

Table 2. Android mobile application security function defect indicator system.

First-level indicators	Secondary indicators
Virus/Backdoor	Virus sample
	Backdoor file
Authority management	Normal permissions
	Sensitive permissions
Security of communication transmission	Transmission confidentiality
	Transmission integrity
	Webview bypass certificate verification
Security reinforcement	Security reinforcing
Security of algorithms	National secret algorithm
	Key hardcoded
Security of operating environment	Superuser privileges
	Emulator running
Security of data storage	Plaintext digital certificate
	Password storage of Webview in plaintext
	Arbitrary backup of application data
Security of components	Arbitrary call
	Illegal hijacking
	Denial of service
	Remote code execution

$$f_{ij} = \frac{x_{ij}}{\sum_{i=1}^{n} x_{ij}} \tag{2}$$

Where E_j is called the entropy value of the j-th indicator, $j = 1, 2, \ldots, m$; x_{ij} represents the standard value of the j-th indicator of the i-th Android mobile application, and it is assumed that when $f_{ij} = 0$, $E_j = 0$. Then the weight of the j-th indicator is defined as:

$$w_j = \frac{1 - E_j}{m - \sum_{j=1}^{m} E_j} \tag{3}$$

Where w_j is the entropy weight of the j-th indicator.

4.3 Comprehensive Risk Assessment

The comprehensive security risk assessment is based on the risk level of each secondary indicator and the weight corresponding to each secondary indicator calculated by the

Table 3. The Definition of Android mobile application security function defect indicator.

Secondary indicators	Definition
Virus sample	The Android-based mobile application contains virus files
Backdoor file	The Android-based mobile application contains backdoor files
Normal permissions	A process or module is invoked with normal permissions
Sensitive permissions	A process or module is invoked with sensitive permissions
Transmission confidentiality	No encryption protection is used for data transmission between clients and servers
Transmission integrity	No integrity check is used for data transmission between clients and servers
Webview bypass certificate verification	When the client's Webview component accesses the URL encrypted with the HTTPS protocol, if the server certificate verification is incorrect, the client does not refuse to continue loading the page
Security reinforcing	Android-based mobile applications are unpacked and cannot effectively prevent the cracking of decompilers
National secret algorithm	Encryption and decryption algorithms approved by the state management department are not used
Key hardcoded	The encryption algorithm's key is set to a fixed value directly in the mobile application code
Superuser privileges	Mobile applications can be used with superuser privileges
Emulator running	Mobile applications can run under the emulator
Plaintext digital certificate	If the plaintext certificate is stolen, the transmitted data may be intercepted and decrypted, and user information may be leaked.
Password storage of webview in plaintext	Username and password will be stored in plaintext in the application directory databases/webview.db
Arbitrary backup of application data	Attackers can back up and restore the App's application data through adb backup and adb restore, thereby potentially obtaining sensitive user information stored in plaintext
Arbitrary call	The transmitted data is arbitrarily called by unknown third-party applications

(*continued*)

Table 3. (*continued*)

Secondary indicators	Definition
Illegal hijacking	The transferred data is hijacked by unknown third-party applications
Denial of service	The component has a denial of vulnerability for service attack
Remote code execution	Remote code execution vulnerability exists in Webview Component

entropy weight method, and a weighted calculation is performed to obtain a comprehensive security risk index of each Android mobile application security function defect. The calculation method of the Android mobile application security function defect risk composite index is as follows:

$$P = \sum_{i=1}^{m} w_i p_i \tag{4}$$

Where P is the Android mobile application security function defect risk comprehensive index, p_i means the risk level of the i-th secondary indicator, w_i denotes the entropy weight of the i-th secondary indicator, and $m(m = 19)$ represents the number of secondary indicators.

5 Conclusions

With the development of mobile Internet technology, mobile applications based on Android are widely used in all walks of life. The more powerful the function of mobile application is, the user's multi-dimensional information is entered and stored in the mobile client, and the security of personal data depends more on mobile security. This paper deeply studies the Android mobile application security detection technology, and proposes a mobile application security evaluation method based on entropy weight method, which can guide enterprises to carry out mobile security detection and evaluation. The next step will be to develop an automatic security function defect detection platform in combination with the Android mobile application security function defect index system to effectively support the safe operation of enterprise mobile application interconnection system.

References

1. Cai Yingshui, Shi Yirong & Qiu Chenxu, 2018. Mobile application security depth detection capability open platform and deployment key technologies. *Telecommunications Science* (03), 41-49
2. Ding Hao, 2018. Research on application software security detection system on Android platform. *Digital communication world* (04), 38

3. Hu Tongpu, 2018. Key technologies of mobile application security system in power industry. *Electronic technology and software engineering* (20), 202
4. Lai Haichao, Zhang Jun & Zhu Chenming, 2018. Mobile app security and detection system analysis. *Computer Era* (01), 27-29
5. Li Nanfang, Li Zongrong & Zhao Lei, 2019. Research on Key Technologies of mobile application security system in power industry. *Information communication* (01), 168-169
6. Song Jie, Li Wenhu & Wu Siyuan, 2018. Analysis of mobile application security situation and development trend. *China transportation informatization* (05), 141-143
7. Wang Zhe, 2019. Research on data security detection method of Android mobile terminal. *Network security technology and application* (01), 63-64
8. Wu yingzi & Xiao Rong, 2020. Research and application of key technologies of mobile application security. *Electronic technology and software engineering* (05), 256-25
9. Xu Junfeng, Wu Shizhong & Zhang Li, 2017. Android Software Security attack and defense countermeasure technology and development. *Transactions of Beijing Institute of Technology* (02), 163-167
10. Zhao Yifan, Lin Yifeng, Zhang Hongfei & Ge Yizhong, 2021. Design of mobile application security detection system based on Android system. *Information construction* (04), 57-58
11. Zhu Hongyu, Tian Jianwei, Tian Zheng & Qiao Hong, 2018. Research and application of power mobile security diagnosis technology. *Hunan Electric Power* (04), 15-17