Detection and Suppression of Malware Based on Consortium Blockchain

IOP Conf. Series: Materials Science and Engineering **490** (2019) 042031 doi:10.1088/1757-899X/490/4/042031

Detection and Suppression of Malware Based on Consortium Blockchain

Yitong Du[1,*], Chuanchang Liu[1] and Zhiyuan Su[2]

[1] State Key laboratory of Networking and Switching Technology, Beijing University of Posts & Telecommunications, Beijing, China
[2] School of Automation, Beijing University of Posts & Telecommunications, Beijing, China

*Corresponding author e-mail: 17611628283@163.com

Abstract. The propose of the paper is to explore a possible way which is based on consortium blockchain to detect and control the propagation and generation of the malware innovatively. Taking many factors into consideration, such as the deficiency of storage space and limited computer power on the mobile platform, we do not directly join the mobile platform to the blockchain. Instead, we use a detection and reporting framework based on log analysis to search for malicious behaviour on the mobile phone. Then through the daemon process resident in memory we record system log information, use the Aho-Corasick automata algorithm to match log information that may have malicious behaviour, identify and report malicious behaviour of the application. According to the experimental result, the method can effectively detect and identify malicious applications, and it can even control malicious application on the Android platform.

1. Introduction

Android is a mobile operating system developed by Google, based on a modified version of the Linux kernel and other open source software and designed primarily for touchscreen mobile devices such as smartphones and tablets [1]. According to Kantar's second edition of 2018 The Quarterly Smartphone Industry Market Research Report [2], it shows that as of July 2018, Android operating system in the smartphone market is still above 78.4%, which is in an absolute advantage. At the same time, due to the open source nature of Android, the harm of malicious applications on the mobile side is particularly evident on the Android platform. In contrast, IOS security is often well protected due to the extremely strict rights management of the system and the review of published applications by the Apple Store. In the domestic due to the lack of Google Store, Android users have to install applications from various application market, however, because of the review mechanism of each application market is not exactly the same, and it is not perfect enough, thus bringing Android users a greater hidden danger. So how to detect and suppression malicious applications effectively has become an urgent problem to be solved.

Related Work: At present, domestic and foreign research shows that Android-based malicious applications detection mainly have the following major categories: static analysis [3], dynamic detection [4], and machine learning-based malicious application detection [5]. Static analysis mainly analyzes the program installation package or decompile, pattern recognition, decryption, etc. and extracts the static features of the analysis program to determine whether it is a malicious application.

This method has a high coverage, but since there is no actual running program, the error rate is high. The dynamic detection method refers to detecting the behavior of the application and matching the features while the application is running. The identified ones are generally real malicious applications, but the overhead is high due to the complicated execution process. The detection method of malicious application based on machine learning and data mining needs to construct the feature classifier through learning permission and function calling feature to judge the maliciousness of Android application, but it actually need to collect a large number of applications for model training, which takes a long time. And since there is no actual running application, the error rate is also high.

In recent years, as a new technology, blockchain has attracted great attention from academia and industry. Many scholars believe that blockchain technology is the revolution of Internet technology in the future and is a huge innovation of information infrastructure technology [6]. It is used in a wide range of applications, including financial transactions, auditing, notary, insurance, etc. The blockchain can be divided into two categories according to the permission mechanism: permissioned blockchain and permission-less blockchain. The permissioned blockchain means that each node participating in the system is licensed, permission-less no need to be licensed, and anyone can join. The permission-less blockchain refer to the public blockchain, and the permissioned blockchain includes consortium blockchain and private blockchain. Public blockchain is open to anyone, so everyone can participate; and the consortium blockchain is a blockchain that requires registration to join. The private blockchain is privileged, individuals cannot join in the blockchain network unless invited by the network administrator, members and nodes on the blockchain are restricted. The consortium blockchain is limited to the participation of alliance members. The size of the alliance can be as large as between countries, or between different institutions. The read and write permissions on the blockchain and the participation in accounting permissions are determined according to the rules of the alliance. The entire network is jointly maintained by member institutions. Network access is generally accessible through the gateway nodes of the member institutions, and the consensus process is controlled by pre-selected nodes. The consortium blockchain is equivalent to between the private blockchain and the public blockchain. Several organizations work together to maintain a blockchain. The use of the blockchain must be restrictedly accessible with permissions, and related information will be protected, such as the supply blockchain: institutional or banking union.

Contribution:(1) Constructing a malware control scheme using consortium blockchain;

(2) Realize the system log analysis based on Aho-Corasick automata algorithm for Android platform malicious behavior detection and reporting framework.

2. Design and Implement

As mentioned above, because the consortium blockchain is more efficient and flexible, we design a malicious application detection and suppression model based on the consortium blockchain on Android platform, which is composed of major Android application markets. Compared with the strong openness of public blockchain, the consortium blockchain is jointly maintained by participating member institutions, and provides a full set of security management functions such as management, certification, authorization, monitoring, and auditing of participating members. The use of the consortium blockchain only allows the authorized application market to join the consortium blockchain, which improves the security and reliability of the consortium blockchain.

Three basic consensus mechanisms need to be reached between the application markets that join the consortium blockchain: reliable reliability, incentives, and credit quantification. First, we use the consortium blockchain to implement our blockchain, ensuring that the nodes (application markets) that are added to the consortium blockchain are honest and reliable; the incentive mechanism depends on the release of an application market or developer. The amount of malicious applications will directly or indirectly affect the amount of revenue. As is often the case: the more malicious applications are released, the lower the credibility is, the lower the number of users, the lower the turnover is, and vice versa. The quantification of credit mechanism refers to measuring the degree of credibility of each node in the consortium blockchain, and we introduce a variable to describe this value.

The schematic diagram of our main implementation is shown in Fig. 1. By registering the application market as a node of the blockchain, every application released by the market will be

recorded by the consortium blockchain, and its behavior will be directly fed back to the credit value of the application market. So the application market that often publishes malicious applications will have a low credit value, and it will be difficult for him to attract users again. Over time, it will decline. A developer who frequently publishes malicious applications will also be reflected on his credit value, thus losing the application market cooperate with him and facing unemployment. Only in this way can we control the release and propagation of malicious applications from the source, and curb malicious applications and code flooding effectively.

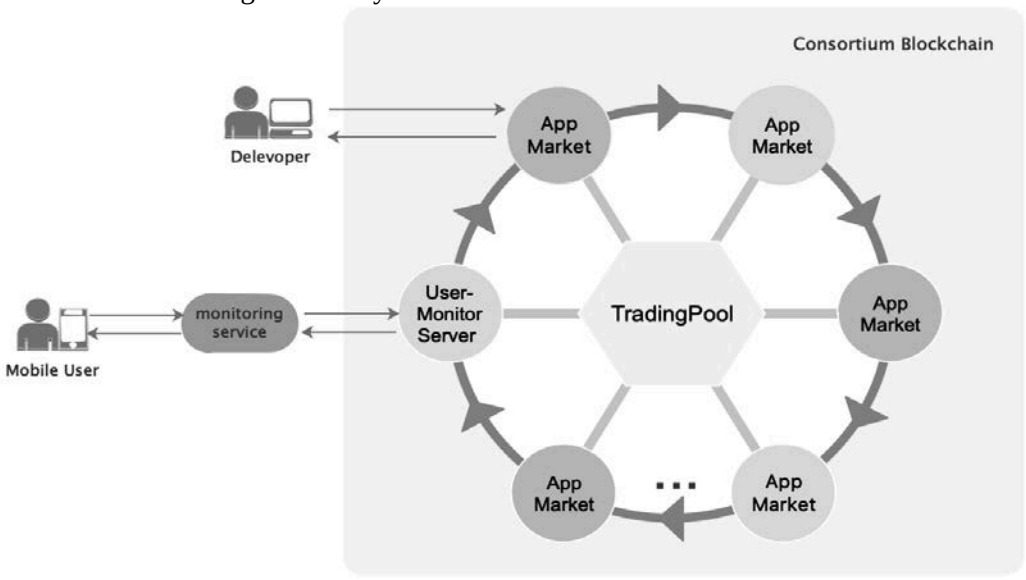

Figure 1. Consortium blockchain malware detection model.

The specific interaction process of each node in the consortium blockchain (node members including developers, users, and application markets) is described as follows:

2.1. Consortium blockchain transaction process

There are three main types of transactions in the entire consortium blockchain: upload transactions, download transactions, and feedback transactions. Developers upload applications to the application market, which generate corresponding upload records and form upload transactions. The user submits a download request from the application market which forms a download transaction. Then the user feedbacks on the application market and the application market feedbacks the developers, a feedback transaction is formed.

2.1.1. The interaction between the developer and the application market. When the developer wants to upload an application, the blockchain system will generate a transaction message. First, the market will perform an operation on the application to determine whether to accept the application, because maybe it is a malware. If market agree to receive it, the developer will sign the transaction; if market refuse to receive it, it proves that the application is a malicious one, the application market will sign the transaction. If it is directly reported as a malicious program during the application upload process, it will become part of the feedback transaction. When more than 6 application markets refuse to accept the application at the same time, the upload transaction will be converted to the developer's negative feedback. The transaction is passed to the transaction pool through the network, waiting for new blocks to be generated and written into the blockchain. When the rejected upload transaction waits too long in the transaction pool, the upload transaction will be cleared by the transaction pool. When cleared, if the number of partial feedback transactions for the transaction is less than or equal to 3, it is converted to negative feedback to the application market. The reason is that the application market may misjudge or intentionally determine that the application is malicious.

2.1.2. Transaction process between users and the application market. The user submits a download request to the application market, which form a download transaction; when the user downloads an application, the consortium blockchain system generates a transaction information, and the application market signs the transaction information with its own private key; If the user meets malicious behaviour in the process, he can feedback to the application market at once. When the application is delivered to the user level, it is already on the mobile phone. At this time, the difficulties of mobile devices accessing the consortium blockchain cannot be neglected, it is mainly subjected to three points: storage space, computing power and network reliability. In the traditional blockchain, since the verification data requires complete full data and the latest unconfirmed transaction, the node needs to store the full amount of data and keep it in real time to ensure that the latest transaction can be obtained, but the mobile device cannot guarantee that it is always online. The network may be turned off anytime, anywhere. Most of the users lack security awareness, and the malicious behaviour of most malicious applications is relatively hidden. Maybe an application in the mobile phone already has malicious behaviour but the user does not know it, so we adopt the system log analysis in Android platform. The log information of the memory recording system is resident in the background through the process daemon mechanism, and the Aho-Corasick automata algorithm is used to match the malicious behaviour model constructed by us to analyse the malicious behaviour of the recognition software. When the malicious behaviour of the software is recognized, it is automatically packaged into a malicious application feedback message and sent to the server of our log analysis application. Here we connect the log analysis server to the consortium blockchain, and then the server can send this malicious behaviour through the network to the transaction pool through the network, waiting for the block constructed by the new transaction message.

2.2. Detection and reporting of malicious behaviour of Android system based on log analysis
In view of the above-mentioned mobile terminal participation feedback mechanism in the consortium blockchain, considering various problems that the mobile terminal is inconvenient to access to the blockchain, we designed and implemented a mechanism based on Android log analysis to detect malicious application behavior. First install the application on the client side. Second, use the daemon process mechanism to record log information of the system. Finally, the Aho-Corasick automata algorithm is used to match the log information to analyze the malicious behavior of the identification software. When the suspected malicious application is analysed, the analysed malicious application is automatically packaged it into a feedback message, which is transmitted to the server of the monitor app through the network, and the malicious message received on the server will be sent to the transaction pool for verification by other nodes in consortium blockchain. The detection and reporting model of malicious behavior is shown in the following Fig. 2.

The detection and reporting model of the Android platform based on log analysis mainly consists of three parts: (1) the system operation log information record collection part, (2) the application information and log information index library part, and (3) the log matching analysis module. The log information collection and recording module mainly uses the broadcast monitoring and daemon processes to stay in the system memory, record the log information generated by the system, and periodically clear the records according to the data volume of the system log information. The file for the log information. The function of the application information and log information indexing module is to store related information of the installed system application and user application under the Android system into the monitor application database. At the same time, the log information string corresponding to the behavior of the system is stored in the log information index library to provide data for the log information analysis module to analyze the system log. Finally, the log information analysis module queries the application database and the log information index library to match the log information by means of the Aho-Corasick automata algorithm, identify the behavior of the software, and report the malicious behavior according to the judgment standard defined by the model and report it to the server through the network.

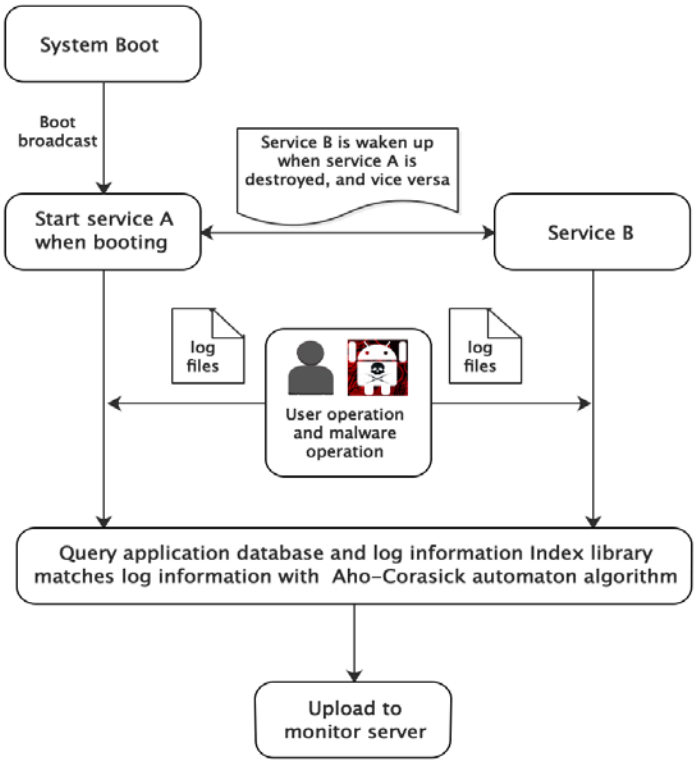

Figure 2. Detection and reporting model overall processing flow.

If the current behavior is identified as malicious, the automatic report process is initiated. When reporting, it will be packaged into a blockchain malicious application message according to the information about the malicious application identified this time, and then sent to the server side of the monitoring malicious application. The data structure of the detected malicious information related content is as follows shown in Fig. 3.

Malware Info ID	Application Signature	App Market Signature	Device ID (IMIE)	Malicious Action Log Message	Timestamp	Malware APK Hash

Figure 3. Malicious behavior report data structure.

When this feedback transaction is successfully written to the blockchain, it indicates that our malicious message has been confirmed. When the server synchronizes the message, it will send the message to the device with the specified application installed. The user is at risk and needs to be processed in a timely manner. Such malicious applications that have been certified by the consortium blockchain can effectively reduce the error rate.

3. Experimental Results

Based on the detection model proposed in this paper, the detection software is designed and implemented. Software behavior detection for the test environment is performed with Android 6.0 platform. Testing software samples come from the mainstream Android application market. The sample software consists of the following: 100 benign software and 400 software containing malicious behaviors.

Through the inspection software, the 500 samples of software collected were tested and found to contain the following malicious behaviors: running unknown software, accessing remote servers, sending text message, etc. The test results are shown in Table 1.

Table 1. Experimental results.

Malicious behaviour	Normal sample	Abnormal sample	Detection quantity	Detection rate	Error rate
Running unknown software	45	150	134	89.3%	4.2%
Access remote server	45	150	137	91.3%	3.1%
Send messages	10	50	45	90.0%	4.0%
Others	10	50	41	82.0%	6.3%
Total	100	400	357	89.3%	4.4%

The experimental data and test results in Table 1 it proves that the detection model proposed in this paper can effectively detect the malicious behavior of Android system, and verify the validity and feasibility of the detection model for malicious behavior detection.

4. Conclusion

We have implemented a detection and control technology scheme based on the consortium blockchain for malicious applications. Through the means of the consortium blockchain, the authenticated application markets are chained into the blockchain, through the consensus mechanism of the consortium blockchain and the value circulation system that is easy to be supervised, we can effectively curb the generation of malicious applications from the source. In addition, facing the problem of the inability to synchronize data online and the limited computing power in the mobile platform in the consortium blockchain, we put forward the mobile-based log monitoring and reporting framework to detect and report malicious behaviors on the mobile terminal, this model not only effectively solves the problem that the mobile terminal cannot access the blockchain, but also solves the problem that the user cannot perceive most of the malicious behaviors. However, our system still has some defects, such as the problem of weak real-time authentication of the consortium blockchain and the problem of the excessive memory consumption. We hope to solve these problems in future research work.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (Grant No.U1536112) and Special Funds for Public Industry Research Projects of State Administration of Grain of China (Grant No.201513002).

References

[1] Shabtai A, Fledel Y, Kanonov U, et al. Google Android: A Comprehensive Security Assessment. J.IEEE Security & Privacy. 8.2(2010):35-44.
[2] Information on https://www.kantarworldpanel.com/global/smartphone-os-market-share/
[3] K. Chen, P. Wang, Y. Lee, et al. Finding unknown malice in 10 seconds: mass vetting for new threats at the Google-play scale. Usenix Conference on Security Symposium USENIX, 2015, pp.659-674.
[4] X. Xiao, X. Xiao, Y. Jiang and R. Ye. Identifying Android malware with system call co-occurrence matrices. J.Transactions on Emerging Telecommunications Technologies. 27.5 (2016) 675-684.
[5] Burguera, Iker, U. Zurutuza, and S. Nadjm-Tehrani. "Crowdroid:behavior-based malware detection system for Android." ACM Workshop on Security and Privacy in Smartphones and Mobile Devices ACM, 2011, pp.15-26.
[6] Nofer, Michael, et al. "Blockchain." Business & Information Systems Engineering. 59.3 (2017) 183-187.