Dynamic Analysis Methods of IOS Application Security

Zi-qiang YIN*

School of Electronic Information and Electronic Engineering, Shanghai Jiao Tong University, China
*Corresponding author

Keywords: IOS security, Dynamic analysis, Keychain access, Encryption, UI web view.

Abstract. There are increasing numbers of malicious applications in iOS platform, which is a severe threat to the iPhone users. The static analysis and dynamic analysis both play important roles in application security assessment. However, there are a lot of challenges in dynamic analysis technology for iOS applications now. We did some research about the characteristics of the malicious applications and studied the key technologies of the iOS platform. In this paper, we provided some dynamic analysis methods about Keychain access monitoring, encryption and decryption monitoring and UI Web View security monitoring. These methods can discover some vulnerabilities for the iOS applications.

Introduction

With the rapid development of mobile Internet, smart phones have become an indispensable part to us. iOS is one of the dominating smart mobile platforms. By the end of September 2016, more than 140 billion applications had been downloaded on App Store. To ensure the quality and security, every application should be scrutinized by Apple before it is published to App Store. However, this assessment process is not always effective. More and more flaws had been found in iOS applications, which do harm to information security of the user. So the study for the analysis methods of iOS Application is necessary.

In recent years, the research for the static analysis of iOS application security is deep and comprehensive, however, static security detection is only for code analysis, and runtime environment variables should be taken into account when it comes to the application security. application security assessment based on the dynamic analysis can greatly enhance the overall and authenticity for the security detection.

However, because of the characteristics of iOS system, there are a lot of challenges in dynamic analysis technology for iOS applications now. The academic technology research based on dynamic analysis is relatively scarce. This paper presents some key technologies to implement the method of dynamic analysis, which may monitor the key security risks for the iOS application, and it can provide technical support for future researchers to design an integrated dynamic detection system.

Dynamic Analysis

Dynamic Analysis Technology

Dynamic analysis technology refers to the process of the implementation of the program, through the control of input variables and the operating environment of the program to analyze, to detect whether there are security risks in the applications [1].

Dynamic analysis makes it possible to gain an overview of the behavior of the application. So the analysis methods can greatly enhance the overall and authenticity for the security detection.

Hooking Technology

Hooking technology plays an important part in dynamic analysis. We can duplicate the aimed instructions of the dispatcher, like some function declaration instructions, before replacing them to
transfer the control flow to a special hook function. And after the executing of the hook function, control flow can be diverted to the original aimed dispatch function. Therefore, hook function makes it possible to monitor what functions are called by a program, which is the core of dynamic analysis.

So if we want to monitor the initial implementations, we should find the key classes and functions and design an appropriate hooking function.

**Dynamic Analysis Methods of iOS Application Security**

In order to efficiently monitor high-risk security risks of iOS applications, we focus on designing three important security detection modules: Keychain access monitoring, encryption and decryption monitoring, UI Web View Security monitoring.

**Keychain Access Monitoring**

Keychain is a security storage container provided by iOS equipment, which can be used to keep sensitive information such as user names, passwords, authentication tokens. Hence it is important to monitor the access control of Keychain.

We designed the keychain access monitoring module as the Figure 1. IOS uses a class named Keychain Item Wrapper to save data into keychain. When we make a Keychain Item Wrapper, we will create an identifier and an access group. Different applications can share the data in a keychain item if they are assigned to the same access group in entitlement.

We can focus on the Keychain Item Wrapper to know whether a keychain is accessed by other applications. The attacker may forge the name of access group the same to the targeted keychain. So we should determine whether the application has the real qualification to access for the keychain data security.

![Figure 1. Keychain Access Monitoring Module.](image-url)
Encryption and Decryption Monitoring

Although some developers realize to make the sensitive data encrypted, an improper choice of encryption algorithm or the storage of algorithm’s key data will still cause serious security risks. We can monitor encryption to assess whether the encryption is safe and monitor the decryption to see whether the application has the authority.
IOS provides the API, *Cryptographic Message Syntax Services*, to implement CMS digital signatures and encryption for S/MIME messages. *The Certificate, Key, and Trust Services* is another API used to trust validation and support functions for cryptography [7]. If we want to monitor the encryption process, we have to pay more attention to these two APIs.

And most of the encryption functions are from these header files: *Common Cryptor .h, Common Digest. h, Common Key Derivation. h, Common Symmetric Key wrap. h*. So we should concern about the function calls from these header files.

Through these two APIs and the header files, we can list the function names when they are called. We can make a security assessment when we get the function names. If the unsafe functions are used, we should be on the alert. *RC4, random and srand* are all unsafe encryption algorithms, which may cause security risks. Meanwhile, we should care about the identity of the user of encryption and decryption users.

**UI Web View Security Monitoring**

UI Web View is a kind of control in iOS development, which makes it possible to browse web pages in App application. iOS applications and network applications are able to interact due to the UI Web View. However, the insecurity of the web page is easy to pose a threat to the Application itself.

As the Figure 4. shows, When we find a URL request we can make a series of detection before loading the web page. First, we can use *data With Contents Of URL of NSdata* to detect the contents which may be loaded to the UI Web View. And it can make sure that there are no illegal scripts loaded by UI Web View. The program is as Figure 5. shows. Then, we can make a security assessment about whether the protocol is https or not, Whether the encryption algorithm for SSL/TLS is safe and verify the certificate for SSL/TLS.

![UIWebView Security Monitoring](image_url)

**Figure 4. UI Web View Security Monitoring Module.**
Summary

More and more malicious applications have been found in the market, and the users of iPhone have concerned more about their information security. The static analysis can’t make a full-scale security assessment for iOS application. Hence it’s necessary to do a deep research about dynamic analysis technology.

Because of the characteristics of iOS system, there are a lot of challenges in dynamic analysis technology for iOS applications security now. In this paper, we provide some dynamic analysis methods about Keychain access monitoring, encryption and decryption monitoring and UI Web View Security monitoring. These will help to discover the key security risks for the iOS application.

References


