PERMISSION BASED MALWARE DETECTION (MOBILE PHISHING) USING SIDE ATTACKER

Vinod Shete[1], Dattatray Dukare[2], Abhishek Waghmare[3], Saurabh Jagtap[4], Chinmay Shejole[5]

Computer Engineering DY Patil College of Engineering Akurdi Pune-44.(SPPU Pune)
Prof. Rahul Y. Pawar , Dept. of Computer Engineering, D.Y.Patil college, MH, India.

Abstract - *Many of attacks are increased on mobile platform because android operating system is popular among users and these attacks are used to theft passwords, credit card numbers, text messages, etc. Current versions of Android are susceptible to these attacks. Phishing attacks are increasing on android platform from last few year because of security issues and attacker can manipulate algorithm easily. Many organization have implemented effective defense scheme for phishing attack but they are not effective and can be easily manipulated. We are implementing side channel attack to prevent phishing attacks on android applications. First we will try to attack original application and we will also detect this attack. In side channel attack we are comparing login page of original application and fake login page created by attacker. After user enters his credentials this credentials are save to attacker server and message will be displayed on UI. The feasible solution this problem has a significant side channel phishing also susceptibility to click jacking that allow non-privileged malware to totally compromise the privacy of the system, and successfully theft passwords or other keyboard input. We discuss the flaws found in the system, propose possible defense mechanism, and then evaluate our security system against different types of UI deception attacks.*

Key Words: Image comparison, side channel , server ,mysql.

1. INTRODUCTION

User interface attacks are increasing threat to smartphone users. In these type of attacks, malicious application is created which replaces original login page with the fake one. User Interface attacks are erious attack as they collect information at the losest server to the user. Once a malicious application is installed on a mobile device, it is possible for the attacker it to rob credentials and can force the user to grant additional permission, totally compromising the device security. One type of such attacks is app-based phishing. Svpeng is a malicious mobile app that collects the users sensitive information like bank credentials and credit & debit card numbers, to a server that the attacker controls. User Interface deception attacks are possible due to two reasons:

(a) The smartphone GUI environment is critical to handle and provide intricate interactions between GUIs to support a multitude of use cases.

(b) Users cannot verify the fake window they are interacting with. A few defense mechanism have been used to defend against these attacks, for eg DECAF uses dynamic application exploration to find UI fraud .OCR techniques are used to automatically detect spoofed keyboards. However, these techniques are limited to specific User Interface and are not dependable solution.

1.1 Existing System

Effective Defence scheme has been a topic for phishing attack. And multiple architectural solution for this attack are available. Different research work are done for prevent such type of attack. Mobifish method are used for prevent this attack and it is used in desktop system.

1.1.1 Mobifish

Mobifish come to development action in 2015. It solved the problem of various phishing attacks. Mobifish are used to detect the url phishing and hijacking also they are used for prevent the android application problem. Mobifish method work on security on desktop and android system.

1.1.2 User habits

Many of the users are unaware of mobile security they are not known about attacks. Now a day touchscreen and high compatibility smartphones are increased. In mobile many of work done by user such as email, chat, online payment but they all are not secure. Phishing attack is success because of user enters to the unauthorised zone but user isn't aware of this and attacker can theft the database and guess the password and other login related information.

2. Related Work

The field of Malware Detection has been through a lot of research. In Component Traversal named for a novel dynamic analysis method is proposed which can automatically execute the code schedules of each a vailable Androd Application(app) as completely as possible. Depending on the extracted system calls of Linux kernel, the weighted directed graphs are further constructed and a deep learning framework is then applied resting on the graph based features for Android malware detection which are newly unknown. However, emulator executes the Android apps and from this data, extraction of system calls is done. In this scenario, some malware are able to detect whether they run on emulator or real device and their functionality is changed accordingly. As a result of which, from this method some malware cannot be detected.

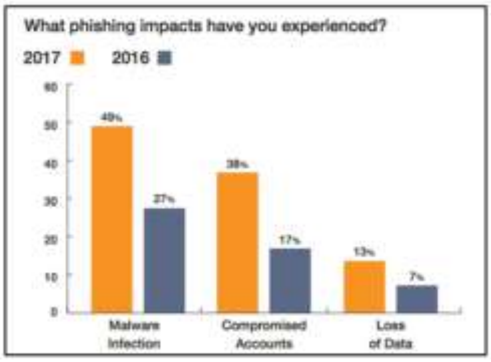

Fig -1: Report Of Phishing attack

2.1 Literature survey

In android, permission checks are used for security for certain resources but if applications are granted more permissions than needed it gives scope of malicious activities. This analysis requires accurate mapping between API method of the framework and the permission they require. It is shown that the native static analysis fails when applied with off shelf components on android framework. By advanced class hierarchy and field sensitive set of analysis to extract this mapping are capable of analysing the android framework.

In permission based security model.

1) Each application is associated with a set of permissions that allows accessing certain resources.

2) Permissions are explicitly accepted by users during installation process.

Permissions are checked at runtime when resources are requested. In android permission model is embedded into the android framework. Missing a permission causes the application to crash and adding too many of them is not secure.

3. Proposed System Architecture:

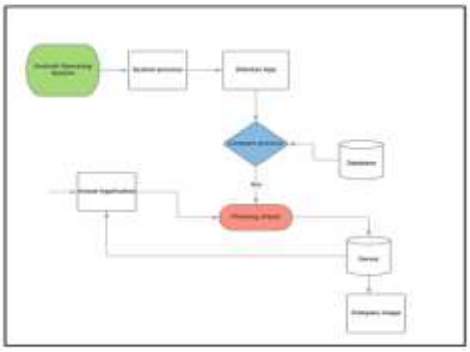

Fig-2: System Architecture

An android application is designed so as to attack the android applications installed on the mobile device. An android mobile device with android operating system installed is needed for the phishing attack of the desired applications.

Android Operating System: It provides various permissions, security privileges to the attacker application. Also, It provides the access of root files and permissions, application compatibility and hardware, software compatibility is also provided.

System process: In computer science, a process is an object of a computer program that is being executed. It contains the its current activity and program code. System process can validate the attacker application and also provide some authentication services related to services

Attacker app: side channel attack is used to extract system processes from the android operating system in which a fake login page is created and then the login credentials of users are stored on the database.

Compare process: It will compare the original application page with the attacker application page. The fake pages are stored in the databases. The comparison is done when attacker app is starting and running in background.

Database: In the database the fake images are stored in database which is set by default.

Phishing Attack: If comparison process is successfully done then the fake page go to the actual application

Server: The user credentials are stored in server also they provide the alert message to actual application. When an actual application is running and also the attacker application is running in the background, the fake login page and the original login page of the application will be compared in the compare process. Then by using the phishing attack is done and the user credentials are stole and stored on the server.

3. CONCLUSIONS

A wide range of UI attacks are vulnerable for Android platform. The standard solution to handling UI attacks is to use security indicators to assist users in identifying the attacks and recent solutions have proposed security indicators inspired by HTTPS lock icons for Android. We studied the security properties determined that it remains vulnerable to side-channel-enhanced.

REFERENCES

1. Android UI Deception PoC Code. https://github.com/earlence/AndroidUIDeceptionRevisitedFC16, Accessed: Oct 2015.
2. Apple XCodeGhost Attack. http://www.apple.com/cn/xcodeghost/#english, Accessed: Oct 2015.
3. Activity hijacking pattern for Android. http://capec.mitre.org/data/definitions/501. html, Accessed: Oct2015.

4. C. Karlof, J. D. Tygar, D. Wagner, "Conditioned-safe ceremonies and a user study of an application to web authentication", Proc. 5th SOUPS, 2009.

5. Y. Niu, F. Hsu, H. Chen, "iPhish: Phishing vulnerabilities on consumer electronics", Proc. 1st Conf. Usability Psychol. Security, pp. 10:1-10:8, 2008.

6. S. Afroz, R. Greenstadt, "PhishZoo: Detecting phishing websites by looking at them", Proc. 5th IEEE ICSC, pp.368-375, 2011.

7. M. Dunlop, S. Groat, D. Shelly, "GoldPhish: Using images for content-based phishing analysis", Proc. 5th ICIMP, pp. 123-128, 2010.

8. "How Android Users Interact With Their Phones", Yahoo Aviate, 2014, [online] Available: http://yahooaviate.tumblr.com/image/95795838933.