TBA - OWASP Top Risks, Android Security

Yucheng Liu, MSINFS, GaTech, yliu3003@gmail.com
Eby John, MSINFS, GaTech, ebyjohn@gatech.edu

***Abstract*—Mobile security is critical as the number of people using smartphones are increasing by the day. Mobile platforms like Android and IOS go beyond providing solutions for just telephony needs but also manage a lot of personal information. OWASP Mobile top 10 risks project is an effort and a time proven industrial standard to classify the security pitfalls developers face during the creating the application. We analyze a collection of Android applications using static and dynamic analysis techniques to check if they correctly handle the OWASP mobile risks. Our goal is to develop techniques and procedures developers can use and follow to test their application for each of the risks. As new threats are emerging all the time, our method should be also improved to face new risks. We will conclude with our findings and offer directions for future analysis.**

I. Introduction

MOBILE phones have seen a tremendous growth in popularity in the recent years and its functions go beyond the traditional communication needs. By 2016, smartphones and tablets will put power in the pockets of a billion global consumers[1]. Hundreds of new applications are added to the app stores each day and are used at work and leisure. There is tremendous competition among developers to get their application to the app markets first and in this process security is often an afterthought. Todays mobile platforms deal with a lot of personal information like sms, location and contacts among others so it is imperative that the applications installed on the mobile device do not misuse this information. Apart from an application directly misusing this information it is also possible that security vulnerabilities in an application might allow an adversary access to private information. Android malware is a growing problem, with rogue apps making their way into the official Google Play store. Trend Micro [2] predicts that the number of malicious and high-risk Android apps will increase three-fold from about 350,000 in 2012 to more than 1 million in 2013. We plan to study the prevalence of these security threats in Android applications so that the average user who is generally oblivious to the security implications when installing an application can have a better idea of the risks involved.

Mobile applications are developed and deployed very quickly which can have an adverse effect on security [8]. As the number of entrepreneurs with creative ideas rise, security is not keeping up pace. The past year illustrated how the mobile threat landscape continually evolves, with new attacks and exploits being frequently discovered [9]. Over 100 million Android phones shipped in the second quarter of 2012 alone. In the U.S., a September 2012 survey of smartphone users gave Android a whopping 52.2% market share [3]. Given its dominance, the Android platform has naturally become the main target for active malware development, with a total of 238 new, unique variants found on the platform, which accounted for 79% of all new malware variants identified in 2012 [4]. A number of mobile apps also contain advertising, in-app purchasing ability, and links to social media. Some of these applications send private information to ad networks, analytics companies, or other third parties, without the consent of the user. The Federal Trade Commission (FTC) issued a staff report [5] showing the results of a survey of mobile apps for children. The results show that many mobile applications aimed for children share personal information like device ID, geolocation with third parties without the consent of the parent. The end user is mostly unaware of the risks in installing software which has not been properly vetted. It is our aim that by conducting a survey of a collection of Android applications we can present the risks and prevalence of such threats in applications used everyday to the user in a way that is meaningful and easy to understand.

There are not many mobile app developers specializing in mobile security unlike traditional web and network application security. OWASP Mobile Security Project is a centralized resource intended to give developers and security teams the resources they need to build and maintain secure mobile applications [6]. To the best of our knowledge, OWASP is the only effort made to classify the threats facing a mobile application. We intend to develop a framework which can be used to test Android applications for these common risks. This will be very helpful for individual developers as well as large mobile development shops. Many companies employ the Bring Your Own Device policy today, a framework to analyse the risks involved with installing a particular application can be very helpful for vetting mobile software on devices which contain sensitive business data.

Currently there is no checklist for securing all mobile apps. The FTC expects app developers to adopt and maintain reasonable data security practices and doesnt prescribe a one-size-fits-all approach. Different apps have different security needs. In order to build a standard for researchers and testers to certify whether an application is secure, OWASP started its own Mobile Security project. The OWASP top 10 mobile risks project tries to classify the common causes of security vulnerabilities on the mobile platform in order to equip developers with the knowledge to make correct design choices during development.

OWASP is not platform specific so we will choose the appropriate tools and techniques. Testing an application is broken up into three phases.

- **Information Gathering:** We build a solid understanding of what the application should do and shouldnt do, understand the functionality and workflow of this application. Network interfaces, protocols,

hardware components, sensors and system services the apps need to interact with are all factors which will affect our test procedure.

- **Static Analysis:** This is mainly about scanning compiled or "byte" code at the binary level rather than reviewing source code. There are abundant tools to do Android application static analysis such as ScanDroid, Klocwork, APK Analyzer, AndroGuard, etc. We will adjust our choice according to the specific app during the process of testing.
- **Dynamic Analysis:** This is conducted against the backend services and APIs and the type of tests varies depending on mobile application type. We will execute the analysis target in an instrumented emulator environment using tools like TaintDroid or DroidBox. Dynamic analysis can reveal the network and filesystem operations an app performs. Such information can be used to find out if the application stores or sends sensitive data in the clear text. Weaknesses in SSL implementation can also be tested [7]. Dynamic analysis is more precise compared with static analysis, but also takes more effort to do correctly but we plan to provide a set of procedures that developers can use in their own software development life cycle.

We wish to raise the awareness among both the users and the developers about common security risks as specified in the OWASP mobile top 10 risks and how to test and mitigate them. The techniques we used and test procedures we established will provide developers a reference during their development and help them avoid the OWASP top 10 mobile risks.

References

[1] Schadler, T., McCarthy , J. Mobile Is The New Face Of Engagement: CIOs Must Plan Now For New Systems Of Engagement

[2] TREND MICRO INC. http://www.trendmicro.com/us/indexnight.html.

[3] comScore, Inc, comScore Reports July 2012 U.S. Mobile Subscriber Market Share http://www.comscore.com/Insights/Press_Releases/2012/9/comScore_Reports_July_2012_US_Mobile_Subscriber_Market_Share.

[4] F-Secure Labs, F-Secure Threat Report H2 2012

[5] Federal Trade Commission, Mobile Apps for Kids: Current Privary Disclosures are Disappoiting, Feb 2012

[6] OWASP. OWASP Mobile Security Project: Top Ten Mobile Risks. https://www.owasp.org/index.php/Mobile, Sep, 2011.

[7] Fahl, S., Harbach, M., Muders, T., Smith, M., Baumgartner, L., Freisleben, B. Why Eve and Mallory Love Android: An Analysis of Android SSL (In)Security. In *CCS'12*. Oct, 2012.

[8] Raphael, J. Google: Android wallpaper apps were not security threats. http://blogs.computerworld.com/16666/google_android_wallpaper_apps, Aug, 2010.

[9] 2013: Mobile exploit kits, Apple App Store malware, cyberwar top the threatscape http://www.infosecurity-magazine.com/view/29908/2013-mobile-exploit-kits-apple-app-store-malware-newblockcyberwar-top-the-threatscape/, Dec, 2012.