CRAB-Droid

AJ Arnold, Matthew Berthoud, Justin Cresent, Ada Rigsby

May 12, 2024

Abstract

Analyzing Android applications for security practices related to permission misuse, SSL API misuse, and potential interface vulnerabilities is a challenging task. This paper presents our tool CRAB-Droid, a python script that builds upon Androguard to carry out a static analysis to identify potential security vulnerabilities in Android applications. We analyzed 100 apps from the Google Play Store with the objective of identifying potential security vulnerabilities. We created 5 experiments to test on our 7 research questions we had outlined in the planning stage of our analysis. This project shows the significance of developers following best practices when creating Android apps, and the abilities to develop tools to help guide and educate engineers to them. Implementing tools like Androguard and CRAB-Droid to be used in the development process can help to identify potential security vulnerabilities before putting apps into deployment onto the app stores. This can help to save time, money, and most of all, user privacy.

1 Introduction

Currently, Android is the most used smartphone operating system in the world, with a market share of 48% and over 400,000 applications (apps) available in the Google Play Market [4]. The Google Play Market is also mostly open and unrestricted, allotting developers more freedom, but many times at the cost of security. The ability to identify vulnerablities within Android applications is vital to the safety of users and their information. Showcasing these vulnerabilities then helps to educate developers to carry-out best security practices when creating an app and to take vulnerable apps off the app store to be secured. This project investigates a variety of Android applications and vulnerabilities that potentially exist within them.

With technological enhancements to smartphone devices over the past two decades, users have been downloading more and more apps to their phones. This rise of phone apps results in a greater chance for users to download malicious ones that may contain malware, such as trojans [3]. This spike has also lead to many new developers entering the ever expanding market, with many potential bad security practices in their apps along with them. For reasons mentioned previously, it is important to identify these vulnerabilities in order to educate developers and protect users.

For this project, we analyzed a set of 100 Android apps from the Google Play Store. We then established seven research questions to hypothesize about pontential vulnerabilites we believed we would find in the apps. We organized them into three domains: permission misuse, SSL API misue, and interface vulnerabilites. These domains were chosen to cover a broad attack vector of the Android applications such as the use of permissions that may violate user privacy, the use of SSL APIs that may not be secure, and the use of interfaces that may be vulnerable to attacks. Five experiments were then developed and tested on our set of apps.

The five experiments were tested on each app as follows: test apps for whether they use all the permissions they request and if they use any dangerous permission combinations, examine for overridden trust manager and error handler methods, test for implementation of the AllowAllHostnameVerifier class, see if apps contain mixed use of HTTP and HTTPS (mixed SSL), and finally test apps for incorrect use of the addJavascriptInterface method.

Using the Androguard library [1] and referencing Mallodroid [4], we completed a thorough analysis of the apps. The results showed that a significant number of Android applications contained the vulnerabilities that we originally hypothesized.

Overall, the significance of this project is seen in its use of static analysis and its applications in the discipline of Android mobile app security. This practice has the potential to be utilized in real-world applications to help secure the Google Play Store and protect users from malicious apps.

2 Methodology

This section outlines the methodology we will use for our five experiments. We will use a set of ninety-seven applications during testing, using automated experiments to

analyze each and every one. Finally, the results of these experiments will be analyzed for any true and/or false vulnerabilites present within each app.

2.1 Set of Apps

We have been given a set of a hundred Android applications to test (we tested on 97), many of which contain different purposes, uses, and features. There are applications ranging from "Live Earth Map" to "Universal TV Remote Control". This variety and quantity of applications gives us a broad scope to test and is more representative of the population of all applications you can find on Google Play.

2.2 Experiment Design

Our experiments use lightweight static analysis to parse through each application and find vulnerabilites. We utilize Androguard libraries within our CRAB-droid script to help with the decompilation and searching of the 97 applications.

Androguard is a python-based tool used for the reverse engineering of Android applications. It takes raw Android Packages (.apk) files and breaks them down, making them easier to analyze. The capabilities of the library make it a great tool for testing the existence of vulnerabilites within applications.

After our script finished, we then developed another script to parse through the output files and identify trends within the applications.

2.3 Results Generation

Our initial script (that scrapes the Android Packages) outputs results into a text file, which is subsequently analyzed by another script. The purpose of the second script is to collect and organize our findings by displaying different trends and statistics.

Often, false positives can be found within our tests; our script identifies potential vulnerable patterns, but it does not guarentee that each individual finding is a true positive. In this way, our script may generate false positives.

3 Experiments

3.1 Permissions Misuse

Many Android applications misuse permissions that they allow their applications to possess. Often, certain permissions are granted to an app that doesn't use them in the first place. This practice is dangerous as it can leave vulnerabilities within the application that should not be possible based on the actual functionality of the application. For example, it would be easy for a developer to add functionality to an app that requires a certain permission, and then leave the permission in after reverting their previous changes.

Another common theme seen within applications is the combination of two permissions that can create a dangerous combination. For example, a malicious application with the permission combination of CAMERA and RECORD_AUDIO would allow the application to have access to a device's camera and microphone, tools that would be able to perform serious invasions of privacy. Another example could be seen with INTERNET and ACCESS_FINE_LOCATION, which would grant an application the ability to track a device's physical location (and subsequently serve as a tool for stalking).

The ability of permissions to allow an application within reach of sensitive data means that users should be prompted whether they wish to allow certain permissions to be enabled. However, many applications do not give users the chance to make this decision; this choice is a significant breach of trust between an application and its users.

All of these developer mistakes constitute permission vulnerabilities within Android applications. For our first experiment, we tested these common misuses of permissions. First, the experiment tests whether apps utilize all of the permissions that they request. Second, the experiment searches for the use of dangerous permission combinations implemented in the app. Finally, the experiment tests whether users are prompted to explicity give their consent to every permission used.

Setup: For this experiment, we first looked into whether the app abided by the principle of least privilege. Out of all permissions that the app asked for, we checked how many were used and how many were unused. We used Androguard's get_permissions() method on our apps' associated APK objects to find the overall permissions, and the get_permission_usage() method on the Analysis objects to evaluate if the permissions were actually used. When permissions were found to be requested, but never used throughout the app, this signified that the app did not follow the principle of least privilege, as unnecessary permissions were included in the app.

We also checked to make sure that all permissions that were included in the app were requested, providing transparency about the permissions that the app utilized. In order to check this, we focused on the apps' Androguard Analysis objects, calling multiple methods related to permission requests.

Finally, we checked for dangerous permission combinations in the applications. We specificially looked for combinations of RECORD_AUDIO and INTERNET, ACCESS_FINE_LOCATION and RECEIVE_BOOT_COMPLETED, CAMERA and INTER-

NET, as well as SEND_SMS and WRITE_SMS.

3.2 Trust Managers and Error Handlers

Trust Managers are put in place to verify the authenticity of a remote server. To do this, many Android built-in trust managers are implemented to securely verify a server's certificate. However, the built-in X509TrustManager class allows the complete override of the server verification process, potentially endangering an application if implemented incorrectly.

Many times, developers will avoid the built-in trust manager in an effort to take shortcuts around the correct implementation (whether this be for convenience or lack of experience). This practice is often carried out by implementing the checkServerTrusted() function in a way that configures the hostname verifier to trust all X.509 certificates. By doing this, developers expose their application to danger; third parties may attempt a Man-in-the-Middle attack on network traffic from the application, compromising a user's network data if successful.

Hand-in-hand with avoiding the proper trust manager, many developers also seek to override built-in error handlers for various reasons. When a possibly dangerous error is thrown during the certificate verification process, the developer instructs the system to follow their code to handle it. This is often used in a way that simply disregards any errors thrown, a dangerous shortcut to the problem.

This experiment tests whether or not an app overrides a built-in trust manager or error handler to forgo methods intended purpose of correctly verifying certificates.

Setup: For this experiment, we utilized Androguard's ClassAnalysis and MethodAnalysis classes, and aspects of Mallodroid to check if built-in trust manager or error handler methods were overridden. We focused on the checkServerTrusted() and onReceivedSslError() methods.

3.3 AllowAllHostnameVerifier

The HostnameVerifier interface is responsible for the verification of the hostname within the server being connected to, making sure the hostname within the server's certificate matches the one seen in the server the client it is attempting to connect to.

A vulnerability arises when the developer attempts to shortcut the hostname verification process (similar to Experiment 2), resulting in an improper verification process. Specifically, many developers use the AllowAllHostnameVerifier class; this class essentially turns hostname verification off (by allowing all hostnames) and instructs the process to never throw an SSL Exception.

This vulnerability, similar to avoiding trust managers, creates the opportunity for a Man-in-the-Middle attack. If the host cannot be verified, a third-party has the opportunity to impersonate a legitimate server and trick the application into sending sensitive data to it.

This experiment tests whether or not an application implements the AllowAllHostnameVerifier class, which allows all hostnames to be accepted for a certificate.

Setup: For this experiment, we made use of Androguard to analyze an app's method instructions, checking if the AllowAllHostnameVerifier class was ever implemented. Specifically we looked for AllowAllHostnameVerifier and SsLSocketFactory - ALLOW_ALL_HOSTNAME_VERIFIER, similar to Mallodroid.

3.4 Mixed use SSL

When an application is connected to the internet, it is not good practice to use both HTTPS and HTTP. HTTPS connections are more secure since they use Secure Sockets Layer (SSL) to encrypt normal HTTP requests and responses, which consist of only plaintext messages. When HTTP content is loaded by an HTTPS page, attackers have the opportunity to read and/or modify HTTP traffic. This results in a mixed-use SSL vulnerability.

Developers create this vulnerability when they do not ensure that every resource on their page is loaded over HTTPS, and this can prove tricky; modern websites often load several different resources from various places, making it hard to keep track of where HTTPS and HTTP is used. The consequence of this vulnerability is the potential for an attacker to perform a SSL Stripping attack, which can lead into a Man-in-the-Middle attack.

In this experiment, we test whether or not an application is using a mixture of HTTP and HTTPS protocol when loading content.

Setup: For this experiment, we used Androguard to parse through the apps' files, locating instances of the strings "http://" and "https://". More specifically, we utilized the find_strings() method on the Androguard Analysis object associated with each app. If "http://" was found in an app, but not "https://", this signified that the app only used HTTP, which is not secure. If both were found, this signified mixed-use SSL. Lastly, if "http://" was never found, but the app was found to include URLs, the app likely only uses HTTPS connections.

3.5 addJavascriptInterface Method

Many applications use WebViews as a way to display web pages as a part of their activity layout. The addJavascriptInterface() method is subsequently used to inject a supplied Java object into a WebView. This process allows JavaScript to control the host application, but presents a

significant security threat if a developer is not using the interface only where necessary.

The vulnerability arises when a malicious third party seeks to use the webview as a bridge into the user's system. If a webview were to contain untrusted content, an attacker could use it to manipulate the host application in unintended ways. This is done by injecting JavaScript into a user's system and running the malicious code.

By using the @JavascriptInterface annotation, developers can use the interface only where necessary and avoid allowing untrusted content within webviews.

This experiment tests whether or not the application is being exposed to potentially dangerous outside sources, depending on if the application is using a webview.

Setup: For this experiment, we first utilized Androguard's MethodAnalysis class to check if the apps implemented the addJavascriptInterface() method. If this method was found to be used, we then checked if the @JavascriptInterface annotation was included for methods within the same class as the addJavascriptInterface() method, confirming whether or not the developer used the method responsibly. To check if the annotation was included, we called various annotation related methods on the apps' DalvikVMFormat objects.

4 Evaluation

This section comprehensively evaluates the performance of our proposed and tested experiments. It determines which experiements performed the best on criteria of most true positive matches and least false positive matches.

5 Results

1. Experiment: Permission Misuse

   90 of the 97 apps contained permissions that were unused (and thus unnecessarily added). The average number of unused permissions used within all apps was 6.01, and when only considering apps with at least one unused permission, this number rises to 6.48.

   62 of the 97 apps were identified to be using a potentially dangerous combination of permissions. The average number of dangerous permission combinations within all apps totaled 1.21, with the number rising to 1.89 when only considering apps with at least one instance of a dangerous permission combination.

   All of the apps requested every permission they included, as is expected by Android applications.

2. Experiment: Trust Managers and Error Handlers

   66 of the 97 apps contained overriden trust managers. The average number of overridden trust managers within the apps totaled 3.06, with the number rising to 4.50 when only considering apps with at least one instance of an overridden trust manager.

   51 of the 97 apps contained overridden error handlers. The average number of overridden error handlers within the apps totaled 1.34, with the number rising to 2.55 when only considering apps with at least one instance of an overriden error handler.

3. Experiment: AllowAllHostnameVerifier

   20 of the 97 apps contained the AllowAllHostnameVerifier class. The average number of AllowAllHostnameVerifier uses within all apps totaled to 0.25, with the number rising to 1.26 when only considering apps with at least one instance of the class.

4. Experiment: Mixed use SSL

   90 of the 97 apps contained mixed use SSL. None of the apps contained only HTTPS or HTTP usage, and 5 of the apps used no URLs at all. The average number of HTTP URLs within the apps totaled to 49.51, with this number rising to 52.77 when only considering apps with at least one HTTP URL being used.

5. Experiment: addJavascriptInterface Method

   80 of the 97 apps contained improper handling of the addJavascriptInterface method. The average number of javascript vulnerabilites totaled to 3.67 per app, with the number rising to 4.75 when only considering apps with at least one vulnerability of this kind.

6 Findings and Future Work

6.1 Analysis of Results

Through our experiments, we see that the majority of applications (out of the 97 we analyzed) contain vulnerabilities within their code. This indicates improper security practices are at play for most of the apps we analyzed.

When considering our sample size as representative of all applications on the Google Play store, the rate at which vulnerabilites are found is quite alarming. Many applications available on the market, according to our study, have a significant chance of containing a vulnerability that allows for a third-party malicious attack.

For evaluating our results, we chose to invesitgate how each experiment potentially would produce false positives.

Experiment 1 False positives within the permissions experiment are not exactly an issue. Unused permissions

Vulnerability	# of Apps	Avg. #	Avg. # min. 1
Unused Permissions	90	6.01	6.48
Dangerous Permission Combinations	62	1.21	1.89
Unrequested Permissions	0	0	0
Overridden Trust Manager	66	3.06	4.50
Overridden Error Handler	51	1.34	2.55
Allow All Hostname Verifier	20	0.25	1.26
Mixed-Use SSL	90	49.51	52.77
Improper Handling of addJavascriptInterface	80	3.67	4.75

Table 1: Shows the number of apps that each vulnerability was found in, the average number of instances found of each vulnerability overall, and the average number of instances in apps where at least one instance was found.

would have a 100% true positive rate (granted the Androguard library works as intended). This is due to the fact that all unsued permissions are a potentially vulnerable exploit that can always be avoided with developers checking and seeing what permissions are actually needed within the app.

Dangerous permission combinations are not exactly evaluated the same as the other experiments (and other parts of this experiment). This is a test to simply see if any potentially dangerous combinations exist between the ones used within the app.

Experiment 2 False positives would occur for similar reasons in this experiment. Since the experiment looks for reimplementation of trust managers and error handlers, if the developer rewrites one of these important methods, it's crucial for them to do so in a safe way. That involves actually checking for the security of a connection.

In order to check the validity of a positive, we selected a random sample of 10 apps that supposedly contained overridden trust managers, and 10 apps that supposedly contained overridden error handlers. From these 10 apps each, we selected one instance of the vulnerability to investigate further. We then manually checked the smali code of each vulnerability's file location to see if the overridden methods were implemented in a safe way.

For trust managers, 4 out of the 10 apps contained an unsafe implementation. This indicates a false positive rate of 60% for trust managers. For error handlers, 1 out of the 10 apps contained an unsafe implementation. This indicates a false positive rate of 90% for error handlers.

These are high false positive rates, which indicate that the experiment is not as accurate as we would desire.

Experiment 3 False positives for the AllowAllHostnameVerifier experiment may arise if an instance of the AllowAllHostnameVerifier class is found within an app, but is located in dead code. Manually verifying if an instance of a vulnerability is located in dead code, however, is not in the scope of this project. We assume that anytime this class is found to be implemented, the hostname verification process is not being carried out as intended, and thus the hostname within the server's certificate is not properly matched to that in the relevant server.

Experiment 4 For the Mixed-Use SSL experiment, false positives may arise in situations where HTTP content being loaded by an HTTPS page is known and trusted by a developer. Additionally, there can be false positives if there exist strings that contain "http://" but never are used for a network call, or if HTTP is used within a local, secure environment. Within the scope of this project, it is difficult to identify these false positives, as we do not have knowledge of the application's network structure and therefore what would be within the scope of a local, secure environment.

Experiment 5 For the addJavascriptInterface() Method experiment, false positives can occur if the addJavascriptInterface() method is implemented without any @JavascriptInterface annotations in the class, but the developer trusts the source of the content being used within the webview. Once again, it is difficult to identify this type of false positive for this project, as we do not know which webviews are trusted by the developer.

6.2 Future Work

If we were to continue this research in the future, we would want to explore some of the following areas.

First and foremost, we would like to have more thorough experiments. Our experiments currently utilize the Androguard library in order to parse the apk files and find simple string matches. One example is from experiment two, where we search for overridden built-in methods. This experiment is fairly simplistic and could be expanded upon into something where the method internals are also automatically checked to view if they are forgoing original intended use, making the user vulnerable.

Additionally, we would like to expand our set of Android applications to test on. If we were able to test on a larger set of apps, this would allow us to draw more accurate conclusions and notice more common trends in regards to vulnerabilities. This would allow us to develop a more comprehensive tool and experiments.

Finally, instead of just utilizing static analysis, breaking into the domain of dynamic analysis could prove to be beneficial in seeing how these vulnerabilities can be exploited in real time. This would give us a chance to see how our predictions of vulnerabilities holds in a test environment of the application running. The results could

prove valuable to enforce our findings and potentially find more vulnerabilities that were not found in static analysis.

7 Conclusion

This project explored developing and evaluating experiments intended to find potential vulnerabilities within a set of Android applications. After downloading the apps, we then developed a set of five experiments to cover three domains: permission misuse, SSL API misue, and interface vulnerabilites.

Our work shows the importance of understanding the permissions that an app requests along with their implications to be used or used together potentially by attackers. Another factor is the importance of understanding the SSL API calls that an app makes. Communicating securely over the internet with the use of SSL is vital to the privacy and security of users' data and personal information. Our tool developed in this project showcases the implications of scanning Android applications for potential vulnerabilities before entering or while on the market, or to catch in the early stages of development. Tools like this could help aid developers and security professionals alike.

Main takeaways include:

1. Static analysis is a powerful baseline in order to target specific sectors within an app in order to identify potential vulnerabilities and attack vectors.

2. This project's result signifies the importance of best security practices when developing and publishing Android applications.

3. The table and statistics help to visualize the data and results to see trends and potentially repeated bad practices and vulnerabilities.

Overall, this project serves as a stepping stone for an ever growing field of work. With mobile phone technology improving each year, the need for secure applications is more important than ever. Tools like CRAB-Droid can quickly and effectively aid developers and security professionals to identify potential vulnerabilities within applications and minimize the threats awaiting their users.

References

[1] Sebastian Bachmann Anthony Desnos, Geoffroy Gueguen. Androguard. `https://github.com/androguard/androguard`, 2018.

[2] Erika Chin, Adrienne Porter Felt, Kate Greenwood, and David Wagner. Analyzing inter-application communication in android. In *Proceedings of the 9th International Conference on Mobile Systems, Applications, and Services*, MobiSys '11, page 239–252, New York, NY, USA, 2011. Association for Computing Machinery. ISBN 9781450306430. doi: 10.1145/1999995.2000018. URL `https://doi.org/10.1145/1999995.2000018`.

[3] William Enck, Machigar Ongtang, and Patrick McDaniel. On lightweight mobile phone application certification. In *Proceedings of the 16th ACM Conference on Computer and Communications Security*, CCS '09, page 235–245, New York, NY, USA, 2009. Association for Computing Machinery. ISBN 9781605588940. doi: 10.1145/1653662.1653691. URL `https://doi.org/10.1145/1653662.1653691`.

[4] Sascha Fahl, Marian Harbach, Thomas Muders, Lars Baumgärtner, Bernd Freisleben, and Matthew Smith. Why eve and mallory love android: an analysis of android ssl (in)security. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, CCS '12, page 50–61, New York, NY, USA, 2012. Association for Computing Machinery. ISBN 9781450316514. doi: 10.1145/2382196.2382205. URL `https://doi.org/10.1145/2382196.2382205`.

[4] [1] [2] [3]