UNIVERSITÉ Concordia UNIVERSITY

INSE 6610
Foundations of Cryptography

PRIVACY & SECURITY ANALYSIS OF ANDROID APPLICATIONS

Submitted to Dr. Amr Youssef

Submitted By:
Ashwin Anandakumar - 40229182
Chris Regy Vallikunnathu - 40232485
Harleen Kaur - 40232489
Mukul Prabhu - 40257131
Ragavi Subramonia Pillai - 40238915

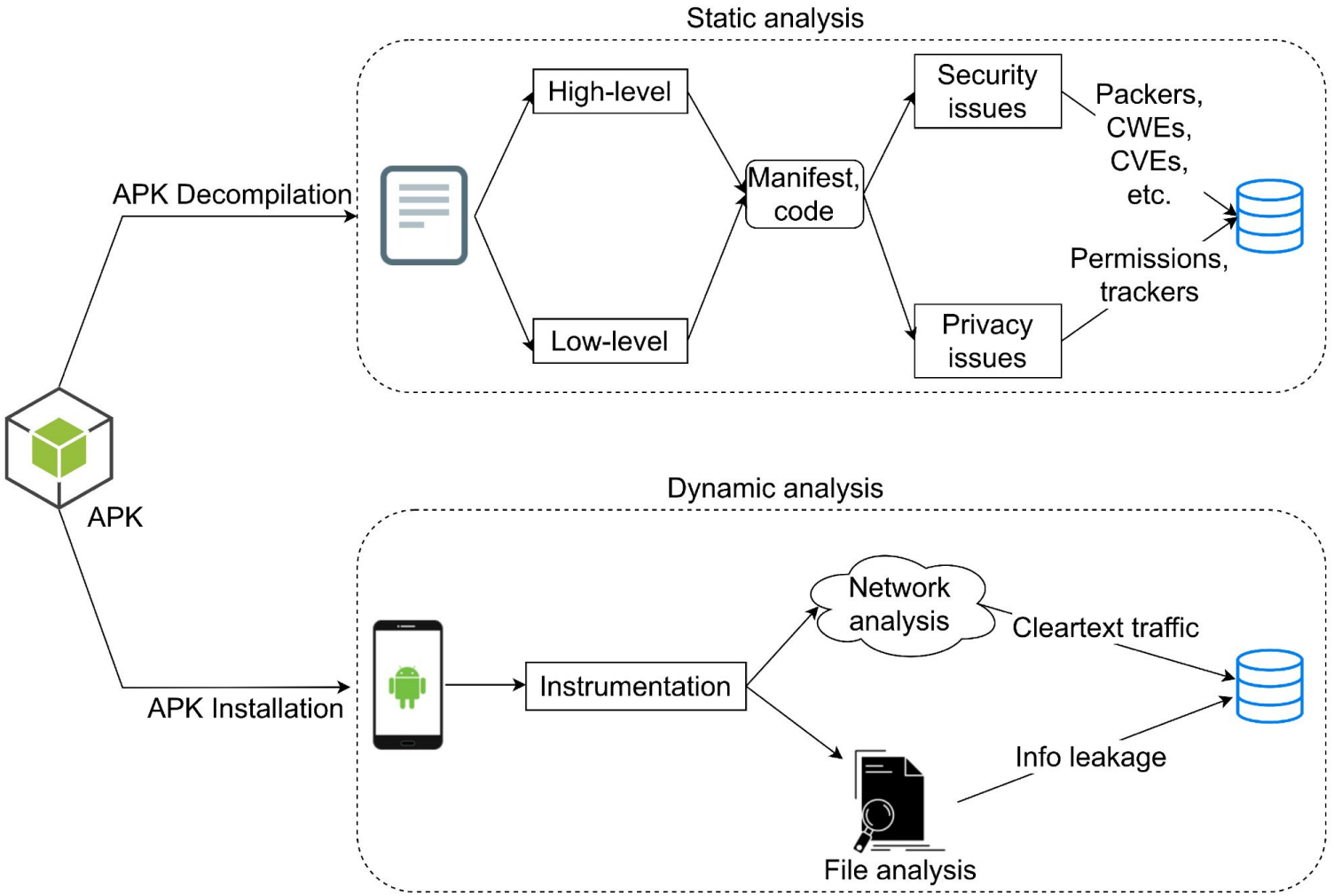
Tools Used

- ***Genymotion*** - Android emulator which includes a complete set of sensors and features in order to interact with a virtual Android environment.
- ***VirtualBox*** - VirtualBox (which allows us to run the Android OS on our operating systems)
- ***Mobsf*** - Using MobSF,an automated mobile pen-testing framework, we conduct static analysis of 13 elderly apps to detect vulnerabilities related to sensitive information, SQLite databases, SSL, and WebView implementation. We also review the Manifest file of each app to obtain their permissions.
- ***LiteRadar*** - Third-Party Library Analysis: Using LiteRadar and a custom Python script, we analyze the permissions and purpose of third-party libraries used in elderly apps to identify potential security issues.
- ***Firebase Scanner*** - Firebase Analysis: We use Firebase Scanner to automatically analyze the Firebase configuration of elderly apps for critical misconfigurations that may lead to data breaches, similar to Appthority work.
- ***APK Extractor*** - APK Extractor which extracts APK that are installed on your android device. Extracts almost all application,including system applications.
- ***APKtool*** - A tool for reverse engineering 3rd party, closed, binary Android apps.

List of Analyzed Applications

• **The Home Depot**	• **Target**
• **Wayfair**	• **Sephora**
• **AR Watches**	• **Goodstyle**
• **Wanna Kicks**	• **Nike**
• **Amazon**	• **Warby Parker**
• **Houzz**	• **Ikea Place**
• **Myntra**	• **Augmenty**
• **IPSY**	• **Sephora**

Analysis Methodology



Dangerous Permissions

- Using the MobSF tool, we analysed some of the dangerous permissions used by these Android applications.
- Location tracking and camera access are among the most commonly used permissions. ACCESS_FINE_LOCATION could potentially be used for targeted advertising or even stalking. ACCESS_BACKGROUND_LOCATION can also be misused as this permission allows location tracking even when the application is not in use.
- READ_EXTERNAL_STORAGE AND WRITE_EXTERNAL_STROAGE are very commonly requested permissions. These permissions can be easily misused by malicious actors as they offer the ability to access and modify data on the user's device.
- Amazon and Houzz applications use READ_CONTACTS permission which might be used for phishing attacks and other fraudulent activities. This could potentially lead to constant tracking and monitoring of the user's movements.

A detailed report on the risky permissions used by all the mobile applications analyzed by our team is available at the below link:

https://docs.google.com/document/d/1d7tlxdqRQVeYsgNZU6rzKwGGyoygDkHi/edit?usp=share_link&ouid=100463175969089847158&rtpof=true&sd=true

Trackers

We found a majority of the apps used Facebook and Google firebase Analytics trackers. Analysing trackers are essential for the privacy aspect of our research

Facebook trackers for cybersecurity and privacy can be significant, as they can be used to collect and analyze large amounts of personal and sensitive data about users.

- Profiling and targeted advertising: It collects information about users' interests, behaviors, and demographics, which can be used to create detailed profiles for targeted advertising
- Privacy violations: This data can be used to track users across different websites and online platforms, creating a detailed profile of their online activity.
- Data breaches: If Facebook trackers are compromised, either through a vulnerability or a hack, the sensitive data they collect can be exposed to malicious actors. This can lead to data breaches, identity theft, and other types of cyber attacks.

Google Firebase Analytics is a mobile and web analytics platform provided by Google as part of the Firebase suite of tools. It’s privacy concerns are:

- User engagement tracking: It tracks user interactions with their mobile and web applications
- Audience segmentation: Segments audience by location, language, app version, and device type.
- Conversion tracking: Tracks users through sign-ups, purchases, or app installs.
- Real-time data reporting: Allowing developers to monitor user behavior and engagement as it happens

A report on the list of Trackers used by all the mobile applications analyzed by our team is available at the below link:

https://docs.google.com/document/d/1slZR9P4_deuKJ_MOp9PDPMMgnuvabR3R/edit?usp=share_link&ouid=100463175969089847158&rtpof=true&sd=true

Third-Party Libraries

Some of the third party libraries used by the analyzed mobile applications could present possible security risks of they contain vulnerabilities that can be exploited by attackers.

- 'Joda Time' is a date and time handling library which can be possibly vulnerable to buffer overflow attacks. This can lead to denial-of-service (DOS) attackers.
- ZKing or 'Zebra Crossing' is a barcode scanning library used by Sephora and Nike. This third-party library has been known to be vulnerable to main-in-the-middle attacks.
- The 'Glide' library which is used by Amazon, Nike and Houzz applications are vulnerable to remote code executions attacks.
- Nike uses the 'Bouncy Castle' library for encryption and decryption and this might be vulnerable to cryptographic attacks.
- Also, the 'Apache Common' library used by Nike has been a victim of code injection attacks in the past.

A detailed report on the list of third party libraries used by all the mobile applications analyzed by our team is available at

https://docs.google.com/document/d/1zWcwcAQ3C4TzesIznjjvm94srCMuH9OL/edit?usp=share_link&ouid=100463175969089847158&rtpof=true&sd=true

Firebase Scan Results

- Using the Firebase Scan tool, we tried to scan for any misconfigurations in the android applications and we inferred the following
- The Applications which had “Secure Firebase Instance found” as output are said to have no vulnerabilities or misconfigurations that could potentially compromise the confidentiality, integrity, or availability of the application’s data or functionality.
- The Applications which had “Unable to identify misconfiguration” as output could not detect obvious misconfigurations or vulnerabilities.
- However it is not conclusive that these applications are completely secure or free of vulnerabilities.
- Automated scans could not detect vulnerabilities in this case, and further manual testing or analysis is required

Security Analysis of ‘Augmenty’

Augmenty is a white-label application which Augmented Reality technology for home furniture and decor companies.

- Through dynamic analysis, we were able to identify that the backend services used by Augmenty included services from Yandex, a Russian multinational technology company. Yandex has been accused of harvesting information from millions of people by embedding code into mobile apps before transferring the data to servers in Russia, raising significant security concerns.

an.yandex.ru	**IP:** 93.158.134.90 **Country:** Russian Federation **Region:** Moskva **City:** Moscow **Latitude:** 55.752220 **Longitude:** 37.615559 **View:** Google Map
dr.yandex.net	**IP:** 93.158.134.242 **Country:** Russian Federation **Region:** Moskva **City:** Moscow **Latitude:** 55.752220 **Longitude:** 37.615559 **View:** Google Map

- It was also found that Augmenty captures location information of users without explicitly obtaining permission to do so. Location information was stored in ‘metrica_data.db’ file.

LOCATION_TRACKING_ENABLED	true

- The Augmenty mobile application also fails the TLS Pinning/Certificate Transparency test. This might make it possible to perform man-in-the-middle attacks. It also indicates that the certificate used by the server might not be trusted.

TLS Pinning/Certificate Transparency Test	✗

Security Analysis of 'Ipsy'

The 'Ipsy' application offers personalized beauty products on monthly subscriptions. It uses Augmented Reality to help its customers get personalised suggestions of beauty products.

- By scanning through the error logs of the application, we found that it is attempting to use the **'getConfiguredNetworks'** method. This method of the WifiService can present a possible security threat as it provides information about the configured WiFi networks. This might include sensitive information such as network names and passwords.

```
WifiService: Permission violation - getConfiguredNetworks not allowed for uid=10062, packageName=com.ipsy.mobile.production, reason=java.lang.SecurityException: UID 10062 has no location permission\n'
```

- Also, the code shown below appears to be a string representation of a JSON object that contains sensitive information, such as an email address and device information. If this code is transmitted over an insecure channel, such as an unencrypted HTTP connection, it could potentially be intercepted by an attacker and used for malicious purposes, such as identity theft or account takeover.


```
b'{"email":"harleen9780355479@gmail.com","device":{"token":"cyyjTv5ORDioJx0yc0P4bN:APA91bEBY-pcIN-lnlgr8ysM_E3uBgtptNI8f5TKs_jHhlC3bRWHsY7YKVXUk-saGy4GSBYCl4N_XpnYz-ANMbSMWmTNqcPy-
wE3nKSsjuymHFjiyB6ecFDOUPQ7aLkG9JLET2eD_sKf","platform":"GCM","applicationName":"androidPushIntegration","dataFields":
{"tokenRegistrationType":"FCM","firebaseCompatible":true,"brand":"Custom","manufacturer":"Genymobile","advertisingId":"5269be4b-d090-4397-b1ae-
12af58beb695","systemName":"genymotion","systemVersion":"10","model":"Phone","sdkVersion":29,"deviceId":"1b3b5aed-f095-46bc-8d58-
972cbf35cac6","appPackageName":"com.ipsy.mobile.production","appVersion":"3.21.3","appBuild":"361","iterableSdkVersion":"3.2.1","notificationsEnabled":true}}}'
=========
```


- Static analysis through MobSF also revealed that the launch mode of activity (com.ipsy.mobile.MainActivity) is not standard. An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.

Security Analysis of ‘Good Style’

Good Style is an app that is used as an Outfit maker, planner of a wardrobe - shopping fashion design clothes. With its augmented reality technology, one can try on any clothes and shoes without going to stores

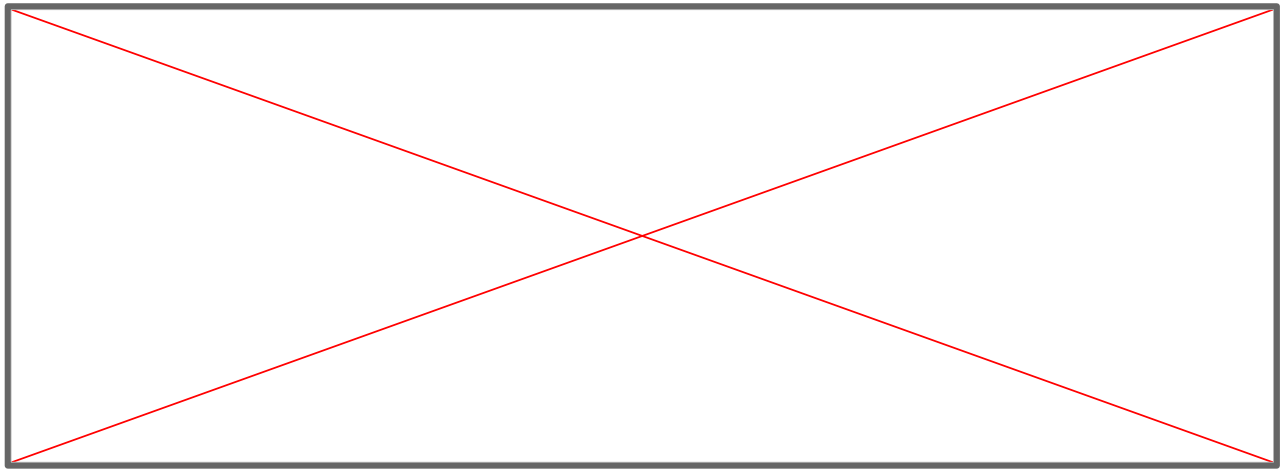
- It was also found that Augmenty captures location information of users without explicitly obtaining permission to do so

LOCATION_TRACKING_ENABLED	true

- The application uses SHA-1, which is prone to collision attack

CERTIFICATES_SHA1_FINGERPRINTS	["76:C5:8B:61:8E:E2:29:8F:D8:22:8B:27:8A:28:5E:03:E8:AF:52:5B"]

- The application is vulnerable to bypassing TLS pinning and certificate transparency checks. This test checks if an application can connect to a server that does not have a valid certificate or if it is possible to bypass TLS pinning and connect to a different server



References

“Silver Surfers on the Tech Wave: Privacy Analysis of Android Apps for the Elderly”, by Pranay Kapoor, Rohan Pagey, Mohammad Mannan, and Amr Youssef

https://www.indigo9digital.com/blog/how-six-leading-retailers-use-augmented-reality-apps-to-disrupt-the-shopping-experience

https://github.com/MobSF/Mobile-Security-Framework-MobSF

What is Broken Authentication and How to Prevent it | LoginRadius Blog

Session management: What it is and why your security depends on it (clerk.com)

Security Misconfiguration| Balbix

Important Links

Due to restriction on the number of slides that can be presented we have provided links to the reports of all the apps we have analysed.

Dynamic Analysis: https://drive.google.com/drive/folders/1V0gYS3IbQ3MTKY0a2CS1cPSnNAZPJmJh?usp=share_link

Dangerous Permissions:
https://docs.google.com/document/d/1d7tlxdqRQVeYsgNZU6rzKwGGyoygDkHi/edit?usp=share_link&ouid=100463175969089847158&rtpof=true&sd=true

Trackers:
https://docs.google.com/document/d/1slZR9P4_deuKJ_MOp9PDPMMgnuvabR3R/edit?usp=share_link&ouid=100463175969089847158&rtpof=true&sd=true

Third Party Libraries:
https://docs.google.com/document/d/1zWcwcAQ3C4TzesIznjjvm94srCMuH9OL/edit?usp=share_link&ouid=100463175969089847158&rtpof=true&sd=true