Audrey Long
JHU WEB SEC
Mobile Applications Security Assignment
04/06/2021

Please submit responses to the following six sections as deliverables in a PDF or Word Doc. Be sure to cite all sources!

A. Ransomware

1. What is ransomware?

Ransomware is a part of the malware family which threatens to publish data belonging to a victim or hold the victims data hostage until some money has been paid to release the lock. While some simple ransomware may lock the system so that it is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called cryptoviral extortion. [1]

Through the use of techniques called phishing, a threat actor sends the ransomware file to an unknowing victim. If the file is opened it will execute the virus payload, which is malicious code. The ransomware runs the code that encrypts user data on the infected computer or host. [2]

2. How does ransomware work cryptographically?

Generally speaking, once the ransomware gets released on your computer the program to encrypt your drive will be executed to target your file system and apply an encryption algorithm like RSA to make the files inaccessible. The attacker will generate a key pair and place the public key into the malware. Then the malware will generate a random symmetric key and encrypt the victims file system then uses a hybrid encryption model to encrypt the symmetric key which results in a small asymmetric ciphertext as well as symmetric ciphertext of the victim data. Once the attacker receives payment for the ransomware they will decipher the asymmetric ciphertext with the private key and send the symmetric key to the victim. [2]

3. Given that we are all security minded, do you think you can successfully fight off a ransomware attack on your own?

I personally don't think I could successfully fight off a ransomware attack if the encryption has already been done. But i know it would be hard for this software to ever end up on my computer since i am very vigilant and aware of phishing attacks and downloading suspicious software. I could use a binary analysis program like Ida pro to analyze the malicious binary and piece together what kind of encryption is being used, but other than that I think it would be hard to get the computer back to normal, unless you could set the version back on the computer itself.

4. Can ransomware be extended to mobile devices?

Yes, ransomware can be extended on mobile devices with the same techniques used for computer ransomware. Mobile ransomware is a form of malware that affects mobile devices. A cybercriminal can use mobile malware to steal sensitive data from a smartphone or lock a device, before demanding payment to return the data to the user or unlock the device. Sometimes people are tricked into accidentally downloading mobile ransomware through social networking schemes, because they think they are downloading innocent content or critical software. [3]

5. What are the defenses that can be employed to defend against ransomware?

I think one of the best defence mechanisms to defend against ransomware is to educate your users to be vigilant of how ransomware can end up on your computer. Phishing and downloading training can prevent such software from ever entering your environment. Windows and other operating systems can also detect malicious software entering your environment, so ensuring that all of those systems are updated and turned on will prevent such attacks from ever getting too far.

B. Mobile Application Scanning

In Module 5 and 6, we talked about static and dynamic analysis.

1. What are the 2 most popular static and dynamic tools for mobile applications?

Owasp ZAP is a popular static code analysis tool to find vulnerabilities and test mobile security. ImmuniWeb is another popular and also covers owasp top 10, DAST and SAST testing as well.

2. With respect to cost, is there any difference between the two?

ImmuniWeb costs from $199 - $995 per month depending on the package. OWASP ZAP looks to be a free and open source scanner which accepts donations.

3. Do any cloud solutions exist for performing this type of analysis?

Qualys is a cloud mobile scanning solution which contains an agent which is installed on the device and provides real time visibility and real time assessment of the mobile device, OS, apps, network vulnerabilities, and checks patches and updates for security concerns.

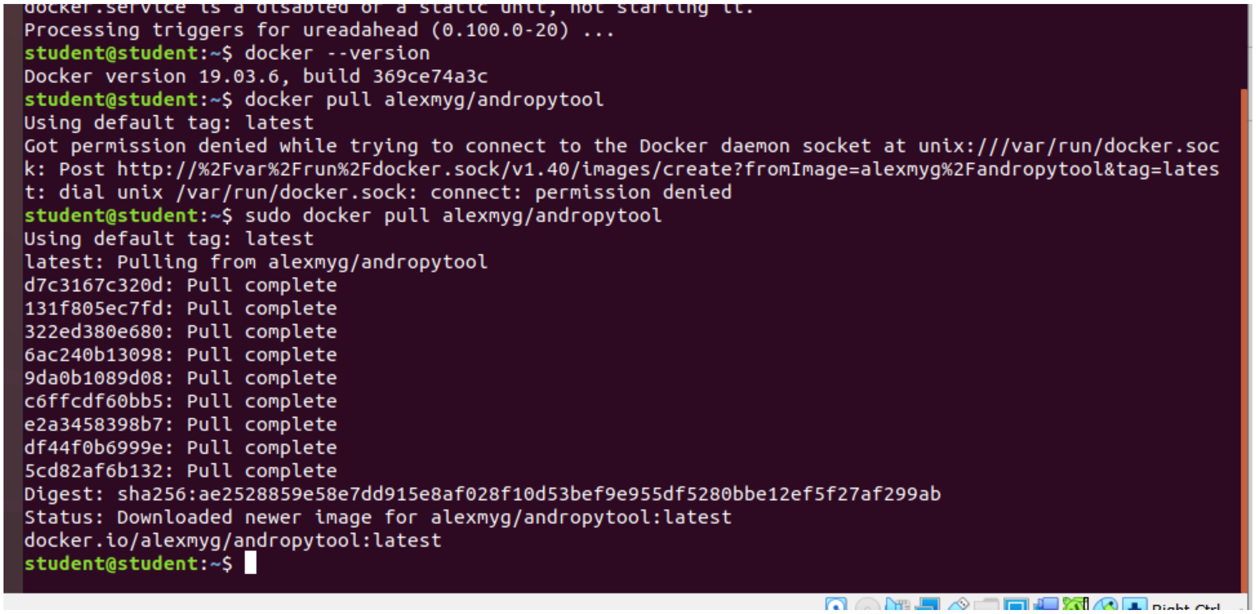
C. AndroPyTools: DroidBox

AndroPyTools can extract static and dynamic features from Android Application Packages (APKs). It encompasses many different Android scanning tools, of which we'll be focusing on DroidBox, a dynamic analysis tool.
Remember to provide screenshots of the installation and results.

• It is recommended to complete this assignment within a VM and it will also require docker installed.

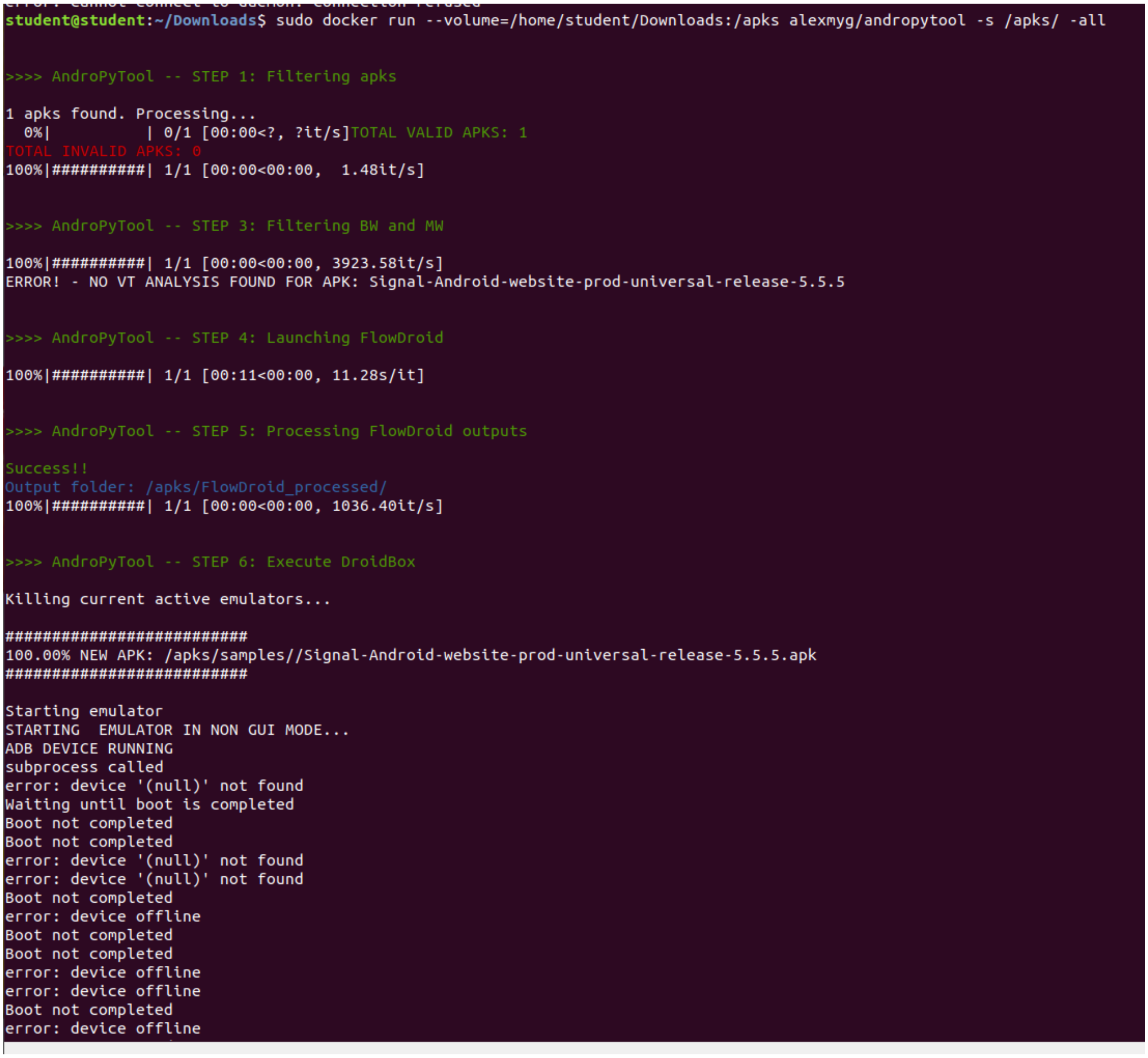
• Navigate to https://github.com/alexMyG/AndroPyTool scroll down, and follow the instructions for installing AndroPyTools via Docker. (Should you prefer to install via Source Code, you are welcome to do that, as well.)

• Next, you'll have to find an .apk file to perform a scan on. You are welcome to choose any application to download and scan (always double check the download source and scan it, VirusTotal is an example tool you can use to do this.)



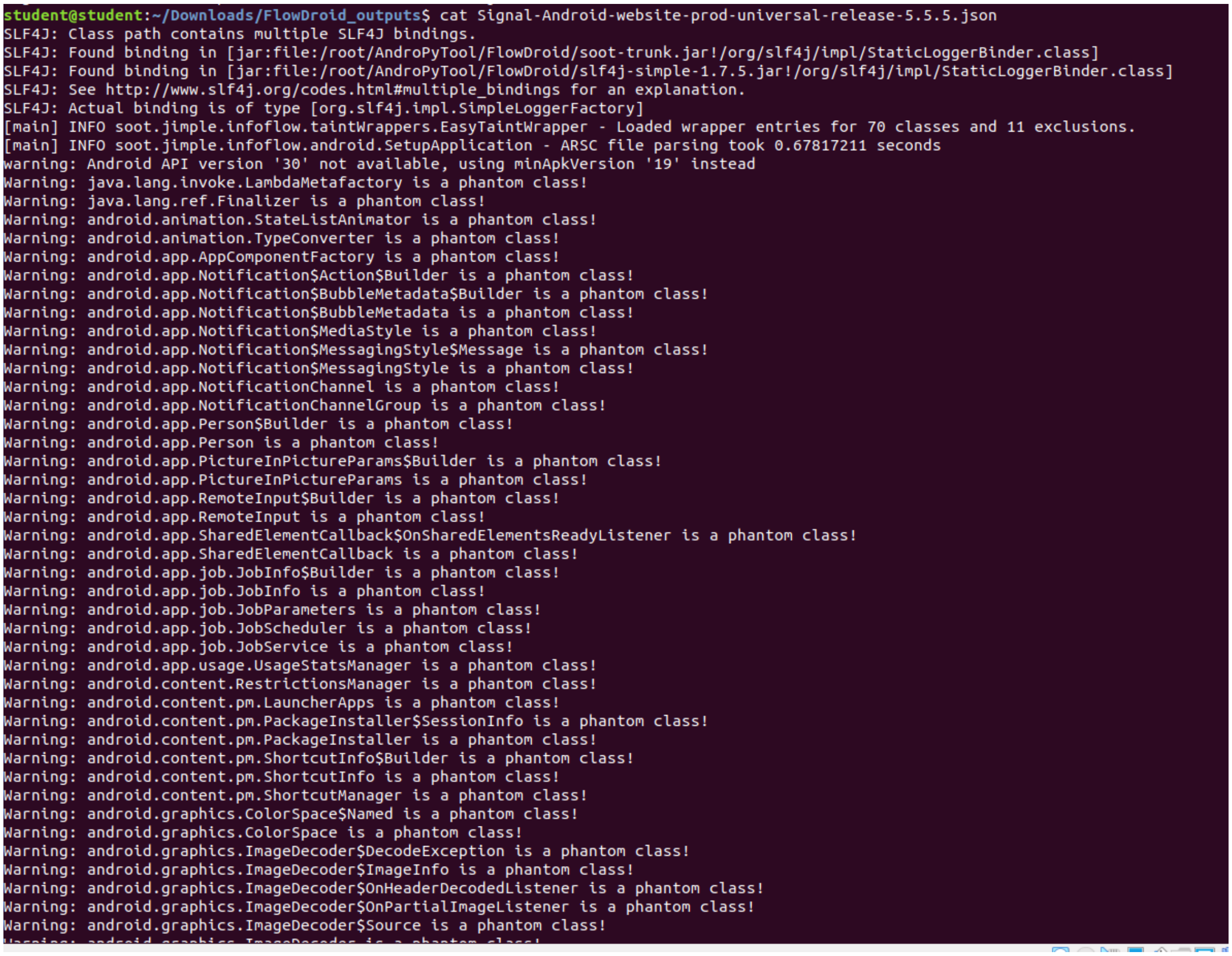
```
docker.service is a disabled or a static unit, not starting it.
Processing triggers for ureadahead (0.100.0-20) ...
student@student:~$ docker --version
Docker version 19.03.6, build 369ce74a3c
student@student:~$ docker pull alexmyg/andropytool
Using default tag: latest
Got permission denied while trying to connect to the Docker daemon socket at unix:///var/run/docker.soc
k: Post http://%2Fvar%2Frun%2Fdocker.sock/v1.40/images/create?fromImage=alexmyg%2Fandropytool&tag=lates
t: dial unix /var/run/docker.sock: connect: permission denied
student@student:~$ sudo docker pull alexmyg/andropytool
Using default tag: latest
latest: Pulling from alexmyg/andropytool
d7c3167c320d: Pull complete
131f805ec7fd: Pull complete
322ed380e680: Pull complete
6ac240b13098: Pull complete
9da0b1089d08: Pull complete
c6ffcdf60bb5: Pull complete
e2a3458398b7: Pull complete
df44f0b6999e: Pull complete
5cd82af6b132: Pull complete
Digest: sha256:ae2528859e58e7dd915e8af028f10d53bef9e955df5280bbe12ef5f27af299ab
Status: Downloaded newer image for alexmyg/andropytool:latest
docker.io/alexmyg/andropytool:latest
student@student:~$
```

Figure 1: installing andropy tool



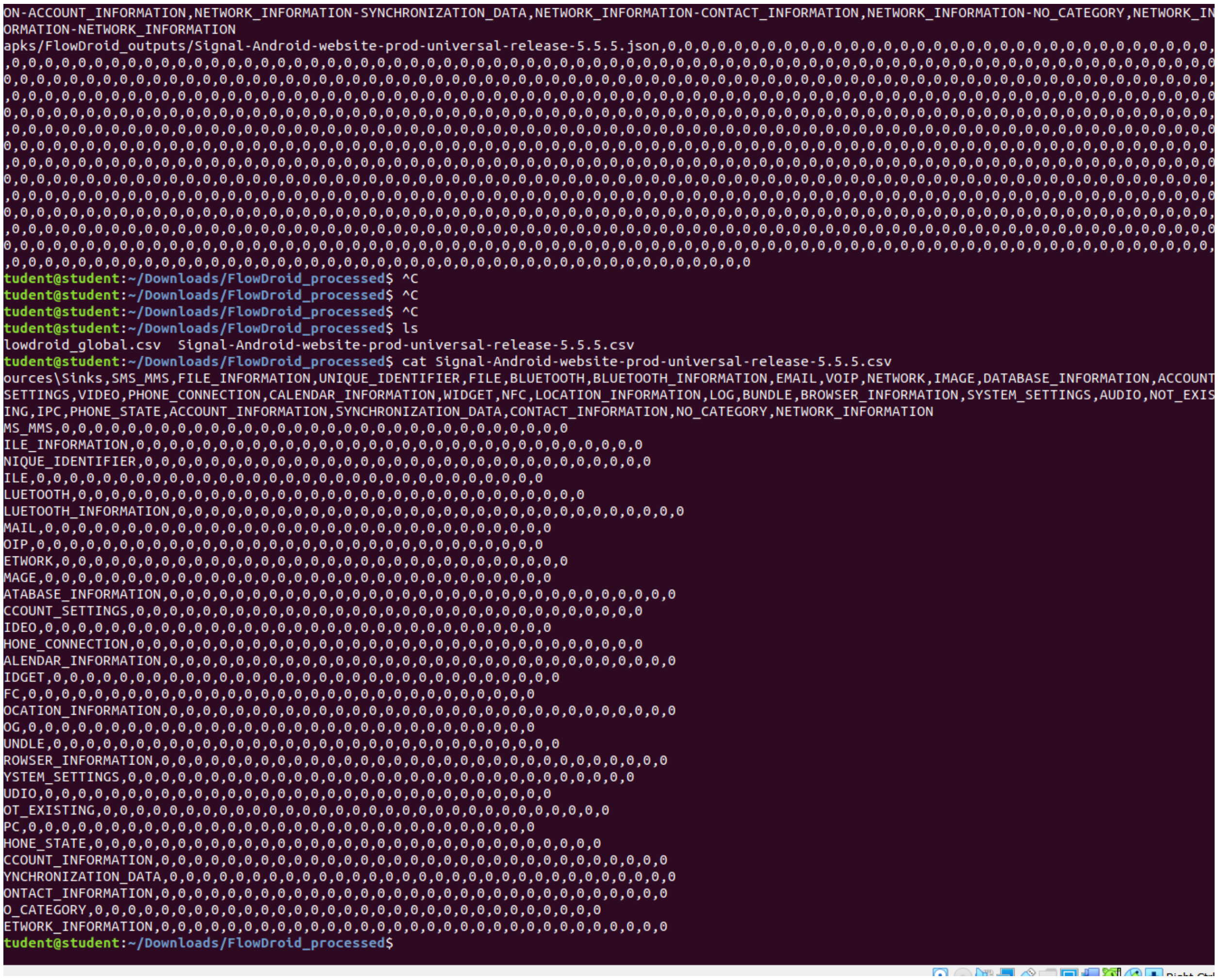
```
error: cannot connect to daemon: connection refused
student@student:~/Downloads$ sudo docker run --volume=/home/student/Downloads:/apks alexmyg/andropytool -s /apks/ -all


>>>> AndroPyTool -- STEP 1: Filtering apks

1 apks found. Processing...
  0%|          | 0/1 [00:00<?, ?it/s]TOTAL VALID APKS: 1
TOTAL INVALID APKS: 0
100%|##########| 1/1 [00:00<00:00,  1.48it/s]


>>>> AndroPyTool -- STEP 3: Filtering BW and MW

100%|##########| 1/1 [00:00<00:00, 3923.58it/s]
ERROR! - NO VT ANALYSIS FOUND FOR APK: Signal-Android-website-prod-universal-release-5.5.5


>>>> AndroPyTool -- STEP 4: Launching FlowDroid

100%|##########| 1/1 [00:11<00:00, 11.28s/it]


>>>> AndroPyTool -- STEP 5: Processing FlowDroid outputs

Success!!
Output folder: /apks/FlowDroid_processed/
100%|##########| 1/1 [00:00<00:00, 1036.40it/s]


>>>> AndroPyTool -- STEP 6: Execute DroidBox

Killing current active emulators...

##########################
100.00% NEW APK: /apks/samples//Signal-Android-website-prod-universal-release-5.5.5.apk
##########################

Starting emulator
STARTING  EMULATOR IN NON GUI MODE...
ADB DEVICE RUNNING
subprocess called
error: device '(null)' not found
Waiting until boot is completed
Boot not completed
Boot not completed
error: device '(null)' not found
error: device '(null)' not found
Boot not completed
error: device offline
Boot not completed
Boot not completed
error: device offline
error: device offline
Boot not completed
error: device offline
```

Figure 2: running scan on apk



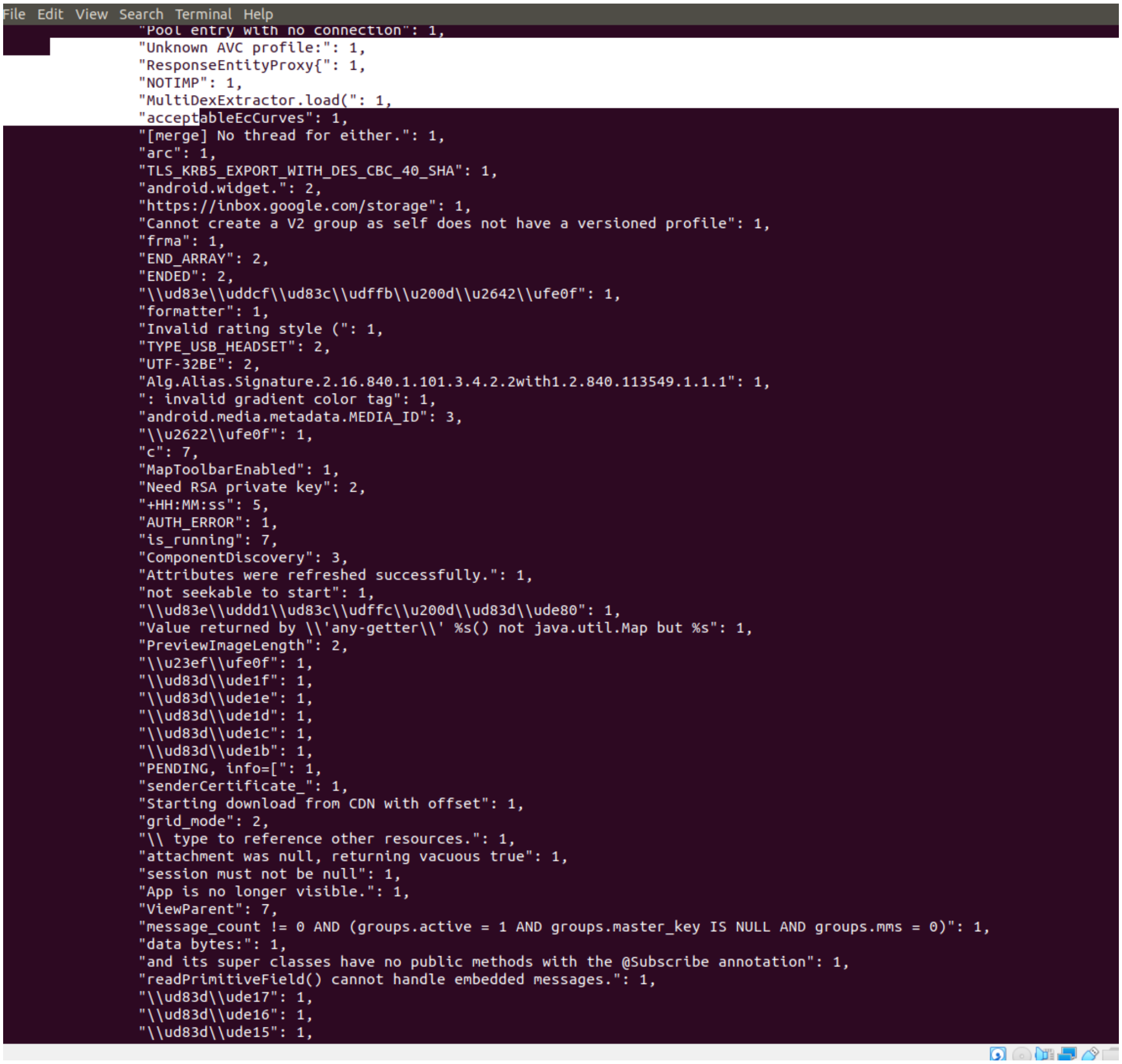
```
student@student:~/Downloads/FlowDroid_outputs$ cat Signal-Android-website-prod-universal-release-5.5.5.json
SLF4J: Class path contains multiple SLF4J bindings.
SLF4J: Found binding in [jar:file:/root/AndroPyTool/FlowDroid/soot-trunk.jar!/org/slf4j/impl/StaticLoggerBinder.class]
SLF4J: Found binding in [jar:file:/root/AndroPyTool/FlowDroid/slf4j-simple-1.7.5.jar!/org/slf4j/impl/StaticLoggerBinder.class]
SLF4J: See http://www.slf4j.org/codes.html#multiple_bindings for an explanation.
SLF4J: Actual binding is of type [org.slf4j.impl.SimpleLoggerFactory]
[main] INFO soot.jimple.infoflow.taintWrappers.EasyTaintWrapper - Loaded wrapper entries for 70 classes and 11 exclusions.
[main] INFO soot.jimple.infoflow.android.SetupApplication - ARSC file parsing took 0.67817211 seconds
warning: Android API version '30' not available, using minApkVersion '19' instead
Warning: java.lang.invoke.LambdaMetafactory is a phantom class!
Warning: java.lang.ref.Finalizer is a phantom class!
Warning: android.animation.StateListAnimator is a phantom class!
Warning: android.animation.TypeConverter is a phantom class!
Warning: android.app.AppComponentFactory is a phantom class!
Warning: android.app.Notification$Action$Builder is a phantom class!
Warning: android.app.Notification$BubbleMetadata$Builder is a phantom class!
Warning: android.app.Notification$BubbleMetadata is a phantom class!
Warning: android.app.Notification$MediaStyle is a phantom class!
Warning: android.app.Notification$MessagingStyle$Message is a phantom class!
Warning: android.app.Notification$MessagingStyle is a phantom class!
Warning: android.app.NotificationChannel is a phantom class!
Warning: android.app.NotificationChannelGroup is a phantom class!
Warning: android.app.Person$Builder is a phantom class!
Warning: android.app.Person is a phantom class!
Warning: android.app.PictureInPictureParams$Builder is a phantom class!
Warning: android.app.PictureInPictureParams is a phantom class!
Warning: android.app.RemoteInput$Builder is a phantom class!
Warning: android.app.RemoteInput is a phantom class!
Warning: android.app.SharedElementCallback$OnSharedElementsReadyListener is a phantom class!
Warning: android.app.SharedElementCallback is a phantom class!
Warning: android.app.job.JobInfo$Builder is a phantom class!
Warning: android.app.job.JobInfo is a phantom class!
Warning: android.app.job.JobParameters is a phantom class!
Warning: android.app.job.JobScheduler is a phantom class!
Warning: android.app.job.JobService is a phantom class!
Warning: android.app.usage.UsageStatsManager is a phantom class!
Warning: android.content.RestrictionsManager is a phantom class!
Warning: android.content.pm.LauncherApps is a phantom class!
Warning: android.content.pm.PackageInstaller$SessionInfo is a phantom class!
Warning: android.content.pm.PackageInstaller is a phantom class!
Warning: android.content.pm.ShortcutInfo$Builder is a phantom class!
Warning: android.content.pm.ShortcutInfo is a phantom class!
Warning: android.content.pm.ShortcutManager is a phantom class!
Warning: android.graphics.ColorSpace$Named is a phantom class!
Warning: android.graphics.ColorSpace is a phantom class!
Warning: android.graphics.ImageDecoder$DecodeException is a phantom class!
Warning: android.graphics.ImageDecoder$ImageInfo is a phantom class!
Warning: android.graphics.ImageDecoder$OnHeaderDecodedListener is a phantom class!
Warning: android.graphics.ImageDecoder$OnPartialImageListener is a phantom class!
Warning: android.graphics.ImageDecoder$Source is a phantom class!
Warning: android.graphics.ImageDecoder is a phantom class!
```

Figure3: FlowDroid Output



```
ON-ACCOUNT_INFORMATION,NETWORK_INFORMATION-SYNCHRONIZATION_DATA,NETWORK_INFORMATION-CONTACT_INFORMATION,NETWORK_INFORMATION-NO_CATEGORY,NETWORK_IN
ORMATION-NETWORK_INFORMATION
apks/FlowDroid_outputs/Signal-Android-website-prod-universal-release-5.5.5.json,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
tudent@student:~/Downloads/FlowDroid_processed$ ^C
tudent@student:~/Downloads/FlowDroid_processed$ ^C
tudent@student:~/Downloads/FlowDroid_processed$ ^C
tudent@student:~/Downloads/FlowDroid_processed$ ls
lowdroid_global.csv  Signal-Android-website-prod-universal-release-5.5.5.csv
tudent@student:~/Downloads/FlowDroid_processed$ cat Signal-Android-website-prod-universal-release-5.5.5.csv
ources\Sinks,SMS_MMS,FILE_INFORMATION,UNIQUE_IDENTIFIER,FILE,BLUETOOTH,BLUETOOTH_INFORMATION,EMAIL,VOIP,NETWORK,IMAGE,DATABASE_INFORMATION,ACCOUNT
SETTINGS,VIDEO,PHONE_CONNECTION,CALENDAR_INFORMATION,WIDGET,NFC,LOCATION_INFORMATION,LOG,BUNDLE,BROWSER_INFORMATION,SYSTEM_SETTINGS,AUDIO,NOT_EXIS
ING,IPC,PHONE_STATE,ACCOUNT_INFORMATION,SYNCHRONIZATION_DATA,CONTACT_INFORMATION,NO_CATEGORY,NETWORK_INFORMATION
MS_MMS,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
ILE_INFORMATION,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
NIQUE_IDENTIFIER,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
ILE,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
LUETOOTH,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
LUETOOTH_INFORMATION,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
MAIL,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
OIP,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
ETWORK,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
MAGE,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
ATABASE_INFORMATION,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
CCOUNT_SETTINGS,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
IDEO,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
HONE_CONNECTION,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
ALENDAR_INFORMATION,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
IDGET,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
FC,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
OCATION_INFORMATION,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
OG,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
UNDLE,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
ROWSER_INFORMATION,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
YSTEM_SETTINGS,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
UDIO,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
OT_EXISTING,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
PC,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
HONE_STATE,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
CCOUNT_INFORMATION,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
YNCHRONIZATION_DATA,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
ONTACT_INFORMATION,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
O_CATEGORY,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
ETWORK_INFORMATION,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
tudent@student:~/Downloads/FlowDroid_processed$
```

Figure 4: Flowdroid processed output



```
            "Pool entry with no connection": 1,
            "Unknown AVC profile:": 1,
            "ResponseEntityProxy{": 1,
            "NOTIMP": 1,
            "MultiDexExtractor.load(": 1,
            "acceptableEcCurves": 1,
            "[merge] No thread for either.": 1,
            "arc": 1,
            "TLS_KRB5_EXPORT_WITH_DES_CBC_40_SHA": 1,
            "android.widget.": 2,
            "https://inbox.google.com/storage": 1,
            "Cannot create a V2 group as self does not have a versioned profile": 1,
            "frma": 1,
            "END_ARRAY": 2,
            "ENDED": 2,
            "\\ud83e\\uddcf\\ud83c\\udffb\\u200d\\u2642\\ufe0f": 1,
            "formatter": 1,
            "Invalid rating style (": 1,
            "TYPE_USB_HEADSET": 2,
            "UTF-32BE": 2,
            "Alg.Alias.Signature.2.16.840.1.101.3.4.2.2with1.2.840.113549.1.1.1": 1,
            ": invalid gradient color tag": 1,
            "android.media.metadata.MEDIA_ID": 3,
            "\\u2622\\ufe0f": 1,
            "c": 7,
            "MapToolbarEnabled": 1,
            "Need RSA private key": 2,
            "+HH:MM:ss": 5,
            "AUTH_ERROR": 1,
            "is_running": 7,
            "ComponentDiscovery": 3,
            "Attributes were refreshed successfully.": 1,
            "not seekable to start": 1,
            "\\ud83e\\uddd1\\ud83c\\udffc\\u200d\\ud83d\\ude80": 1,
            "Value returned by \\'any-getter\\' %s() not java.util.Map but %s": 1,
            "PreviewImageLength": 2,
            "\\u23ef\\ufe0f": 1,
            "\\ud83d\\ude1f": 1,
            "\\ud83d\\ude1e": 1,
            "\\ud83d\\ude1d": 1,
            "\\ud83d\\ude1c": 1,
            "\\ud83d\\ude1b": 1,
            "PENDING, info=[": 1,
            "senderCertificate_": 1,
            "Starting download from CDN with offset": 1,
            "grid_mode": 2,
            "\\ type to reference other resources.": 1,
            "attachment was null, returning vacuous true": 1,
            "session must not be null": 1,
            "App is no longer visible.": 1,
            "ViewParent": 7,
            "message_count != 0 AND (groups.active = 1 AND groups.master_key IS NULL AND groups.mms = 0)": 1,
            "data bytes:": 1,
            "and its super classes have no public methods with the @Subscribe annotation": 1,
            "readPrimitiveField() cannot handle embedded messages.": 1,
            "\\ud83d\\ude17": 1,
            "\\ud83d\\ude16": 1,
            "\\ud83d\\ude15": 1,
```

Figure 5: output from Feature Files

Above contain some of the findings from the mobile scanning tool. It contains both static and dynamic information from a provided APK. The tool also outputs all of its findings in multiple output files with multiple extensions for an easier to analyze user experience. Any insights on what you app is doing in a runtime environment and statically will provide developers with values insights into their applications to ensure security is at the forefront.

• **Deliverable: Take a screenshot of the results, annotate and provide an analysis of your findings.**

D. OWASP Mobile Vulnerabilities

In Module 5 and 6 we also talked about the OWASP Top 10 vulnerabilities. Please respond to the following questions. Be sure to cite all sources!

1. Is there a Top 10 list for mobile vulnerabilities?

Yes the Mobile top 10 includes:

M1: Improper Platform Usage
M2: Insecure Data Storage
M3: Insecure Communication
M4: Insecure Authentication
M5: Insufficient Cryptography
M6: Insecure Authorization
M7: Client Code Quality
M8: Code Tampering
M9: Reverse Engineering
M10: Extraneous Functionality

2. How do they differ from typical web application vulnerabilities?

Some of the top 10 concepts both for mobile and web apps are similar, but the mobile device has a larger attack surface which also focuses on the physical device security, and anti-tamper techniques that can be mitigated for reverse engineers. This also focuses on platform usage, and extraneous functionality.

3. In your mind, which 3 mobile vulnerabilities are the most significant and how can they be guarded against?

I used to be an anti-tamper software engineer so i definitely see the value in securing your devices against reverse engineers. Reverse engineering can be combated by installing software to check device sensors and react to a threshold being tripped which is unusual. Improper platform usage can be very important to implement security controls which can mitigate potential issues by users, following security best practices to enable these controls is ideal. Insecure communication could potentially leak a lot of sensitive data and must be hardened. Ensuring data is encrypted in transit and at rest along with using up to date protocols will prevent a lot of future vulnerabilities.

4. Which mobile OS are attacks more successful against: Android or iOS?

After doing some light research it looks like Android is more susceptible to attacks because Androids rely on open source code for a majority of its stack and adversaries can study up on some of these modules to perform attacks on devices they know carries certain tech stacks. A majority of mobile device owners carry androids as well, this makes the device more appealing for attackers.

E. “Bring Your Own Device” Policy

We touched on BYOD device policies in the lecture notes. In practice, this is a difficult thing to get right. Pretend you’re the CIO of an IT company. Outline a 4-5 point plan you

think would help enhance the security of BYOD devices that can be used both on company premises and at home.

If I was a CIO of a company and i needed to implement a BYOD device policy i would outline the following plan to enhance the security on premises and at home:

1.) Create security controls plan
    a.) Creating a plan of patches, OS, versions, and security monitoring tools can be very valuable in securing the network and limiting the attack surface of BYODs. I think this is the first and most fundamental step that can be taken to start hardening security best practices.
2.) Define a policy of allowed apps to be downloaded on the device
    a.) Users will always download what they want on their own devices without doing any security research beforehand. If a company website contains information about trusted download sources or applications that are only allowed on the users BYOD VPN for download then we can ensure no worms or malware will penetrate company networks.
3.) Enable VPN usage
    a.) Ensuring an employee can use their own device can come with backdoors and leakage of critical company data, and creating a plan for an employee to only be able to work on the company VPN can mitigate some unwanted internet traffic and safeguard company data.
4.) Define user usage plan
    a.) In order for employees to use their own devices for work usage a plan will need to be implemented to ensure no malicious software can access company data. This is important because we are trying to limit the attack surface and openings adversaries can exploit.

References

https://en.wikipedia.org/wiki/Ransomware [1]
https://hackernoon.com/cryptography-malware-ransomware-36a8ae9eb0b9 [2]
https://us.norton.com/internetsecurity-mobile-what-is-mobile-ransomware.html [3]
https://www.softwaretestinghelp.com/mobile-app-security-testing-tools/ [4]
https://www.immuniweb.com/pricing/ [5]
https://owasp.org/www-project-zap/ [6]
https://www.qualys.com/apps/vulnerability-management-detection-response/mobile-devices/ [7]
https://owasp.org/www-project-mobile-top-10/ [8]
https://us.norton.com/internetsecurity-mobile-android-vs-ios-which-is-more-secure.html#:~:text=iOS%3A%20The%20threat%20level,of%20the%20two%20operating%20systems.&text=Android%20is%20more%20often%20targeted,so%20many%20mobile%20devices%20today. [9]
https://www.ontrack.com/en-gb/blog/6-tips-improving-byod-security [10]