Top 5 Ways Hackers Attack Your App

Authentication Attacks

Authorization Attacks

Spoofing and Tampering Attacks

Racing Resources Attacks

Information Leakage Attacks

Authentication Attacks

Static Reverse Engineering

Credentials Phishing

Information Gathering

Poor Coding

Static Reverse Engineering

Hacker attempts to gain information about an app via its source code without necessarily running the app.

Uncover algorithms to replicate or abuse

Discover embedded credentials

Bypass security checks

Frida, Xposed, Substrate, QBDI, scriptable debuggers, CaptainHook, MobileSubstrate, Cycript, Cynject, IDA, Ghidra, BinaryNinja, Hopper, Radare2, JEB, jadx, apktool; dextra, jtool,joker

Bank TESCO

bitfi

Credentials Phishing

Here, the hacker attempts to acquire sensitive information (the credentials) by appearing to be a trustworthy entity, such as the user's employer.

Gain user credentials, e.g. user/password combinations that may also be usable in other sites.

Fraudulent sites trying to imitate the legit sites. Tools for massive mail/SMS distribution. Malicious apps aiming to steal two-factor authentication tokens.

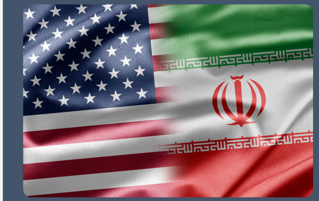
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Information Gathering

This attack seeks to gather private information usually intended for strategic or other importance to a business, government or other entity in order to achieve a competitive advantage.

Gain vital information such as email addresses, passwords, phone numbers, bank account details, etc. Attackers may use the stolen information or social engineering to impersonate the victim (e.g. by sending fraudulent emails under the victim's name).

Spear phishing seeks to gather information from an individual or to trigger the password recovery "protocol" on the victim's account and then attempt to replace the legitimate password with one from the attacker.



Poor Coding

This attack aims to exploit an app that can be both legitimate and non-malicious but whose coding is poor, such that the app incorporates identifiable vulnerabilities.

Gain personal or sensitive information about the victim via mobile app or communication methods.

Because this approach exploits design and security errors, hackers may attempt to guess credentials; for example, if security is dependent on knowing a user's email address, the hacker can make educated guesses as to what the user's email address may be.

Authorization Attacks

Botnets

Root Detection Bypass

App Vulnerabilities

Protection Bypass

Botnets

A botnet attack leverages the distributed computing power of a group of devices for tasks such as infiltrating a network to which one of the infected devices has access.

The aim is to access private network services and resources. Even though services may not be exposed to the Internet, a device connected to the same network (and connected to the Internet) acts as an entry point for the attacker, shifting the attack surface from mobile to server.

The primary vehicles are trojan applications that embed code to scan networks that devices are connected to.

Root Detection Bypass

This attack aims to enable a rooted device to run an application and bypass root detection. Bypass tools enable this by falsifying root detection and publishing a false reading.

Bypass the restrictions hindering the usability of root-based and instrumentation tools.

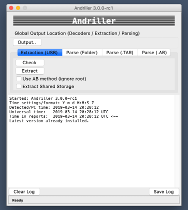
Frida and anti-anti-root detection mechanisms like Magisk are used to bypass root detection. Magisk includes a module called MagiskHide to hide falsify root detection.

App Vulnerabilities

This attack seeks to identify and then exploit inadvertent vulnerabilities in legitimate apps from legitimate vendors.

Gather sensitive and/or valuable information, or where possible to execute malicious actions.

Automated tools to scan for vulnerable or misused APIs (e.g. Hackode, Andriller).



Global Output Location (Decoders / Extraction / Parsing)

□ Use AB method (ignore root)

□ Extract Shared Storage

```
Started: Andriller 3.0.0-rc1
Time settings/format: Y-m-d H:M:S Z
Detected/PC time: 2019-03-14 20:28:12
Universal time:   2019-03-14 20:28:12 UTC
Time in reports:  2019-03-14 20:28:12 UTC <--
Latest version already installed.
```

Protection Bypass

The approach of this attack is to defeat the security measures put in place by app developers; specifically, the aim is to defeat attempts to obfuscate an app's source code and thereby make the app harder to reverse engineer.

Gain access to the actual code of the application or to reverse engineer the implementation of a specific algorithm.

- Frida, Xposed, Substrate, QBDI, scriptable debuggers such as GDB/LLVM/IDA,CaptainHook, MobileSubstrate, Cycript, Cynject

- Privately developed tools, Emulators, or hardware devices

Spoofing and Tampering Attacks

Bank Impersonations

Payment Scams

Malvertising

Repackaging Legitimate Apps

Dynamic Analysis

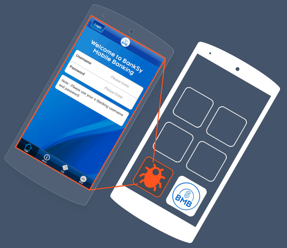
Bank Impersonations

These attacks leverage malicious mobile apps designed in such a way as to trick users into thinking they are from a legitimate financial institution.

Criminals seek to gain account credentials and/or credit card numbers. Once an account is breached, criminals can execute transfers or payments after logging into the account or can sell the credentials to another party.

Specially crafted apps for graphically and behaviorally imitating legitimate banking apps

Trojans running services and displaying overlays on top of legitimate banking apps mimicking legitimate banking applications


Login
BMB
Welcome to BankSy Mobile Banking
Username
Please Enter
Password
Please Enter
Note : Please use your e-Banking username and password.
BMB

Payment Scams

This attack focuses on hijacking data in motion. It is possible to gather data from a device from the pasteboard or received via SMS.

Criminals seek to obtain bitcoin and other cryptocurrencies addresses and identify e-wallet apps installed on the device. Once identified, criminals will monitor the app activities like notifications, SMS, emails in order to steal information and funds.

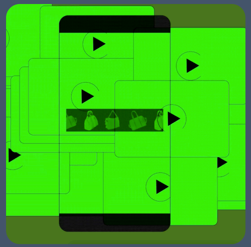
Specially crafted apps that monitor the clipboard, SMS inbox or user’s emails and notifications.

Malvertising

This attack displays advertisements on mobile devices through malicious, rather than legitimate, methods as a path to monetization.

Criminals see to collect human clicks on ads and also load hidden scripts to automatically click ads that are invisible to users since they run in the background.

Rogue ad SDKs that act maliciously based on GPS location, usage of the phone or other conditions.



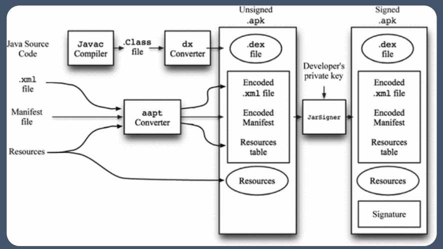
Repackaging Legitimate Apps

In this attack, the hacker repackages a legitimate application to include malicious code and then resigns the app using a different certificate.

Embed malware in a legitimate application.

Distribute paid applications for free, specifically cracked to bypass the protection mechanism and with embedded malicious code.

On Android, apktool, and in rare cases custom-made injection utilities.



Dynamic Analysis and Instrumentation

This attack seeks to reverse engineer an app by running it in a virtual environment so that its inputs and outputs can be observed and analyzed.

Obtain loaded/written files, allocated memory buffers, encrypted/decrypted information, and/or received/sent network packets; dynamically bypass security checks, forcing the call of specific functions with particular inputs.

Frida, Xposed, Substrate, QBDI, scriptable debuggers such as GDB/LLVM/IDA

For hooking and swizzling: Frida, CaptainHook, MobileSubstrate, Cycript, Cynject.

Racing Resources Attacks

Malicious Payload Injection

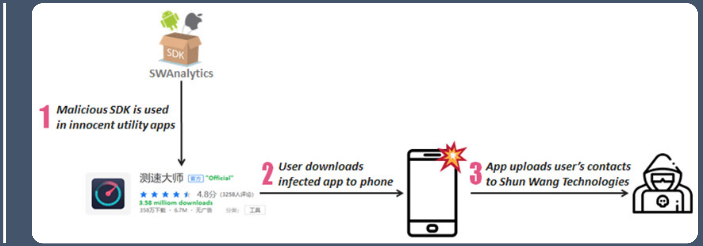
Crypto Mining

Malicious Payload Injection

This attack takes advantage of careless storage protocols in third-party applications in order to crash a victim's Android mobile device.

Gather sensitive and/or valuable information, or where possible to execute malicious actions.

```
Malicious SDKs (e.g.
SWAnalytics).
```

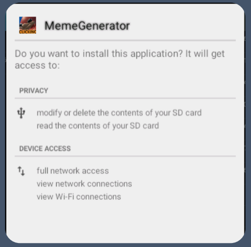

SDK
SWAnalytics
1 Malicious SDK is used in innocent utility apps
测速大师 官方 "Official"
4.8分
3.58 milliom downloads
358万下载 · 6.7M · 无广告
工具
2 User downloads infected app to phone
3 App uploads user's contacts to Shun Wang Technologies

Crypto Mining

This attack makes unauthorized use of computing resources on the victim's device to assist the bad actor in cryptocurrency mining.

Using the computational power someone else's device to mine cryptocurrencies.

Hackers will inject malicious JavaScript payloads by embedding (and usually hidden) WebViews in a legitimate application.



MemeGenerator

Do you want to install this application? It will get access to:

PRIVACY

modify or delete the contents of your SD card
read the contents of your SD card

DEVICE ACCESS

full network access
view network connections
view Wi-Fi connections

Information Leakage Attacks

Stealing Information

Data Leakage

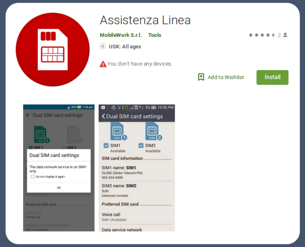
Monitoring Network Traffic

Stealing Information

This attack method is to exploit vulnerabilities on a device such as bad communications, weak or missing encryption, and side-channel leakages (logs, files, backups, cloud). This attack seeks to gather information from sources such as the device’s microphone, camera and messaging/SMS apps.

Obtain unique device identifiers, geolocation information, photos, emails, SMS/MMS, contacts, IM messages.

Spyware installed on the victim's device; network monitoring tools that detect information leaks.



Assistenza Linea

MobileWork S.r.l. Tools

★★★★½ 2

USK: All ages

You don't have any devices.

Add to Wishlist

Install

Dual SIM card settings

SIM 1 SIM 2

Dual SIM card settings

The data network service is on SIM1 only.

□ Do not display it again

OK

Preferred SIM card

Voice call

Always ask

Redial for Bluetooth headset

SIM 1 (Available)

Dual SIM card settings

☑ SIM1 Available ☑ SIM2 Available

SIM card information

SIM1 name: SIM1

GLOBE (Globe Telecom-PH)

905-204-5088

SIM2 name: SIM2

SUN

Unknown number

Preferred SIM card

Voice call

SIM1 (Available)

Data service network

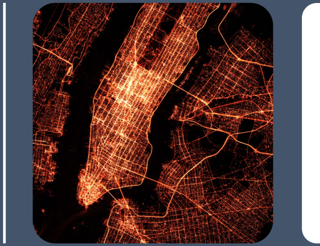
ZIMPERIUM®

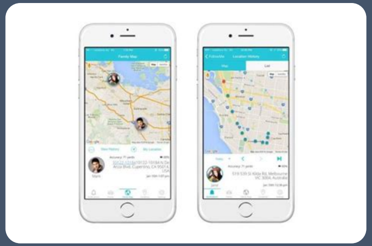
Data Leakage

This attack exploits back-end databases used to store data from mobile apps. An un-protected or inadequately-protected database can leak inadvertently expose user data and violate privacy laws.

Obtain location data for specific devices and individuals.

Hackers will sniff and intercept data using Bettercap, BurpSuite, CharlesProxy, Fiddler, or custom scripts.





Monitoring Network Traffic

This is a network-based attack that intercepts data (including potentially unencrypted data) sent and received by a mobile device across a network.

The goal of monitoring a mobile device’s network communication is to obtain sensitive data (encrypted or unencrypted) shared over the network, such as passwords, emails, links to private resources, or sensitive binary data such as photos or OTA updates.

- Wireshark, BurpSuite, Fiddler;

- Sniffing and interception: Bettercap, BurpSuite, CharlesProxy, Fiddler

Questions?

Scott King

Director Embedded Security

Scott has over 20 years experience providing customized software solutions to enterprise customers in mobile, supply chain and DevOps. Scott invests his time researching mobile app security and worldwide mobile threat events.

1. How do I defend against these attacks?
2. How can we view attacks to our apps?
3. How do we configure remediation?
4. How can we measure improvements?
5. What examples can I provide to my colleagues?

Paper: https://get.zimperium.com/top-5-ways-hackers-attack-your-apps/

Need more: king@zimperium.com

Top 5 Ways Hackers Attack Your App