OFF-GRID APPS™

Common Privacy and Security Vulnerabilities of Mobile Devices

October 2021

Author: The APE (Advanced Privacy Enforcer)

Contents

Overview

Mobile device applications are at the center of today's current development trends. Many of these applications are intentionally built using a client–server centric architecture. The client runs on the mobile devices operating system, which is most frequently iOS or Android. The application that runs on the client is typically downloaded to the mobile device from the devices official app store, where developers publish their registered software apps. From the user's perspective, the client installed on the mobile device is the downloaded application. This is what the user interacts with to read emails, make online purchases, perform online banking or perhaps even pay bills. What is often forgotten by the end user of a mobile device application is that there is also another component involved the server, which is usually hosted by the application developer. Often this part of the client-server model is performed by the same software that is responsible for generating and processing the web content on that site. Typically, we have found that most often the server-side component is a web application that interacts with the mobile client application over the Internet by use of some type of application programming interface (API). So, from a security perspective, we can look at the server as the more important component as this is where information is being stored and processed.

Modern mobile device operating systems come with different security mechanisms. By default, an installed app can access only files in its own "sandbox" directory area, and user permissions do not allow a user to edit system files. The designing and writing of code for mobile applications done by some application developers, particularly those interested in target marketing individuals through access to ones, camera, microphone, bluetooth or location services will cause gaps in a user's privacy protection as well as allow for attack vectors that can often be abused by attackers.

- Many cyberattacks and target marketing campaigns rely on a user not paying attention to the permissions they are given to an app during installation or by a user simply clicking thru a license agreement without actually reading it in its entirety.
- High-risk vulnerabilities were found in 38 percent of mobile applications for iOS and in 43 percent of Android applications.
- Most security issues are found on both the iOS and Android platforms. Insecure data storage is the most common issue, found in 76 percent of mobile applications. Passwords, financial information, personal data, email and text messages are all at risk.
- Most cases are caused by weaknesses in security mechanisms (74% and 57% for iOS and Android apps, respectively, and 42% for server-side components).
- Hackers seldom need physical access to a smartphone to steal data: 89 percent of vulnerabilities can be exploited using malware.

The APE says: ***"Beware of the spies in your pocket..."***

Top Privacy Vulnerabilities of Mobile Devices

- **Geo tracking** - (aka mobile positioning and geotagging) - a key feature of a smartphone is being able to locate itself, via triangulation and "pinging" to cell towers, or via the integrated GPS chip. Originally known as "multilateration" which determines an objects position based on measurement of the times of arrival (TOAs) of energy waves, and is used to enable features such as tracking distances during walking, running or exercising and even map navigation. This geolocation information can be very useful, and also used by law enforcement to track a suspect via their phone. Do you think that disabling the GPS on the phone means you can't be tracked? Guess again, there are known ways and some published reports of locating phones via their other sensors, including the accelerometer, barometer and magnetometer. While disclosing location data may seem innocuous, it is still an invasion of privacy. This data can easily be used to build a profile on a user, which can then subsequently be used for an attacker to perform what is known as a "phishing attack" to gain unauthorized access to your personal identity information credentials.
- **Activity tracking** - apps also track users, and apps can also use that information for many different purposes. For example, to see which retailers the owner of the phone visits, and the time spent there. That location data, just like other data on your phone, is a hot commodity for internet marketers in today's digital economy. In fact, "targeted advertising" is one of the biggest enterprises on the web. Companies want to serve you ads for products you're likely to buy, and that data helps them hit their goal. Some companies have even made this their primary business model. These tactics are legal because the companies behind them give you a choice to opt-in or out, but it is not that easy to permanently change these settings and/or keep the app that you opt-into from changing them back after you turn them off.
- **Microphone is eavesdropping** - every smartphone has a microphone, and it's yet another security risk. While the main concern for many of us may be someone eavesdropping on private conversations, microphones also can be used for data collection. It happens to everyone. You're talking about something you want to buy, like a new set of audio speakers. Then you open your phone and there are ads on social media for speakers. How did this happen? For starters, there are companies out there that use someone's smartphone mic to record the ambient noise of that persons' environments, and then create a database of TV shows that a phone's owner has watched, and sells that data to advertisers to target market advertisements to those users. This practice of using voice data for marketing is actually legal.

APE NOTE: "Smartphones are equipped with the perfect array of surveilance monitoring equipment, equipped with microphones, cameras and motion sensors designed to pick up and transmit clear audio and video. While these tools may be useful for you as the device owner, they can also serve as a far more effective means for advertisers to target market you."

- **Camera is watching** - smartphone cameras are a great convenience and for a lot of us, the best camera we have is the one that we have on our smartphone. However, smartphone cameras are also a security risk, as they can be activated and used to spy on the owner. This can be done by an opt-in app policy allowing it access to use your camera. Or even by installing software on the phone via physical access, or by using the attacker method of a remote exploitation of the security services already running and enabled on your smartphone.
- **Bluetooth interception and hi-jacking (aka bluesnarfing and bluejacking)** – the bluetooth device on your smartphone can allow access to your calendars, contact lists, emails and text messages, and on some smartphones, users can copy pictures and private videos thru bluetooth. Both "bluesnarfing" and "bluejacking" exploit another person's bluetooth connections without their knowledge. Although bluejacking is somewhat benign and mostly harmless since it only transmits data to the target device, bluesnarfing on the other hand is a bit more dangerous as it is the theft of information from the target device. If an attacker is nearby and sends an invalid public key to your bluetooth device, it's highly probable he or she can determine your current session key. Once that's done, the attacker can intercept and decrypt all data that passes between the bluetooth device very easily. This type of attack combined with a few other techniques to intercept a mobile device International Mobile Equipment Identity (IMEI) number can also be used to clone a user's mobile device.
- **Potential backdoors** – a lot of privacy and security minded individuals worry about what the government could do if they had a "backdoor" into our smartphone, and could access all of our data whenever it wanted to, this issue actually became a heated battle when the FBI demanded that Apple help it circumvent an iPhone's security[1] due to the attack in 2016 by the terrorist attacker known as Syed Farook. In 2018, there was concern that the Chinese Government had engineered a backdoor into smartphones from two manufacturers: Huawei and ZTE. That bit of growing uncertainty led the directors of six US intelligence agencies (CIA, NGA, FBI, NSA, NRO, and DIA) to recommend that Americans do not purchase smartphones from these manufacturers during official testimony before the US Senate Intelligence Committee. The concern was and still is that users' data could be shared with a foreign government via a backdoor.
- **Malicious apps –** certainly**,** a great feature about a smartphone is that its functionality can be expanded by installing apps, allowing you to build a device platform with a personalized feature set of useful applications to fit your lifestyle over time. However, those apps are sometimes not from the most reputable sources (even though they may be registered in your smartphone's application store) and many of them can and will help themselves to more information than is required. The interesting and somewhat frightening thing about this is that we as the unsuspecting user willingly provide this ability to them when we agree to the app permissions and will typically just "click through" its End User Licensing Agreement (EULA) without actually reading it in it's entirety.

APE NOTE: "We should at least be a little more suspicious why that new app you just installed needs access to our contacts, GPS, microphone and camera."

- **Wi-Fi tracking –** many retailers and even airports have offered free Wi-Fi to their customers and many of us will just click to accept the terms of service (without actually reading them) since we are thankful for the connection and assume nothing nefarious is intended. This convenient free Wi-Fi connection is in many cases an actual invasion of your privacy. Several years ago two major US chain stores made headline news when it was revealed that they were using a service known as "Euclid Analytics" to track shoppers[2]. Thru the free Wi-Fi, Euclid can determine which departments the shoppers have visited and how long they spent there. While these particular retailers reportedly no longer use Euclid after much shopper backlash when the tracking came to light, Forbes reports that more than 100 other retailers use the Euclid Analytics service. Please visit the URL in footnote #2 below for more details on this incident as reported by Forbes magazine.

Footnotes:

[1] https://www.techradar.com/news/phone-and-communications/mobile-phones/apple-reveals-critical-new-detail-in-its-encryption-battle-with-the-government-1315336

[2] https://www.forbes.com/sites/petercohan/2013/05/09/how-nordstrom-and-home-depot-use-wifi-to-spy-on-shoppers

Top 10 Security Vulnerabilities of Mobile Devices

1. **Data leakage** - mobile device apps are often the cause of unintentional data leakage. For example, for mobile users who grant apps broad permissions, but don't always check security this poses a real problem and is often referred to as "riskware" apps. These are typically free apps found in official app stores that work as advertised, but also send personal and potentially corporate data to a remote server, where it is mined by advertisers, and sometimes, by attackers and organized cybercriminals. Data leakage can also happen through hostile enterprise-signed mobile apps. These mobile malware programs use distribution code native to popular mobile operating systems like iOS and Android to move valuable data across corporate networks without raising red flags. To avoid these problems, the latest updates for Android and Apple iOS both added protocols to make users more aware of it and why apps collect users' location data.

 **APE NOTE:** "Only give apps the permissions that they absolutely need in order to properly function and stay clear of any apps that asks for more permissions than necessary."

2. **Unsecured Wi-Fi** – given that wireless hot spots are often readily available and no one wants to burn through their cellular data plan, why not just connect to that free Wi-Fi available? Most free Wi-Fi networks are usually unsecured or not very well secured. For example, three British politicians who agreed to be part of a free wireless security experiment were easily hacked by the technology experts running the experiment. Their social media, PayPal and even their VoIP conversations were compromised.

 **APE NOTE:** "To be safe, use free Wi-Fi sparingly on your mobile device and never use it to access confidential or personal services, like banking or credit card information."

3. **Network spoofing -** when attackers set up fake Wireless Access Points (WAP) which are connections that look like Wi-Fi networks, but are typically traps. These are often seen in high-traffic public locations such as coffee shops, libraries and airports. Attackers and/or Organized Cybercriminals give the access points common names like "Free Airport Wi-Fi" or "Coffeehouse" to encourage users to connect. In some cases, attackers require users to create an "account" to access these free services, complete with asking for a password. Now, given many users will use the same email and password combination for multiple services, attackers are then able to potentially compromise a users' email, online banking, online shopping accounts and other secure information which might be using the same email and password combination. In addition to using caution when connecting to any free Wi-Fi, never provide personal information.

 **APE NOTE:** "Whenever you are asked to create a login, whether for Wi-Fi or any application, always create it with a unique password."

4. **Phishing attacks** - mobile devices are typically always powered-on, and due to this they are usually the front lines of most phishing attacks. Mobile users are more vulnerable because they often monitor their email in real-time, opening and reading emails when they are received. Mobile device users are also more susceptible because email apps display less information to accommodate the smaller screen sizes. For example, even when opened, an email may only display the sender's name unless you expand the header information bar. And if the matter isn't urgent, then let the response or action items wait until you're at your computer.

5. **Spyware -** many mobile users worry about malware sending data streams back to attackers or would be organized cybercriminals. However, there's a big threat a lot closer to home that is known as "spyware" which in most cases, it's not malware from unknown attackers that users install but rather an app installed by spouses, coworkers or employers to keep track of a users whereabouts and activity. Sometimes called "stalkerware" a lot of these types of apps are designed to be loaded on the target user's device without their consent or knowledge. A good up-to-date comprehensive antivirus and malware detection application suite should use scanning techniques designed to detect this type of program, which requires slightly different handling than does other malware as to how it gets onto your device and its real purpose.

6. **Broken cryptography -** broken cryptography can happen when app developers use weak encryption algorithms, or fail to properly implement strong encryption techniques. Developers may use familiar encryption algorithms despite their known vulnerabilities in order to speed up the app development process. As a result, any slightly motivated attacker can exploit those known vulnerabilities to break/crack passwords and gain access. Other app developers may use highly secure algorithms, but then leave other "backdoors" open that limit the effectiveness of what should be a secure encryption algorithm. For example, it may not be possible for attackers to break/crack the passwords, but if developers leave flaws in the code that allow attackers to modify high-level app functions, such as sending or receiving text message then an attacker does not not need passwords to cause problems, they will just exploit the known flaw. It is very important that developers and organizations enforce strong encryption standards before apps are deployed.

7. **Improper session handling -** for ease of use and mobile device transaction access, many apps make use of a common technology implementation known as "tokens," which will allow users to perform multiple actions without being forced to re-authenticate their identity for each action. Similar to user passwords, tokens are used to identify and validate devices but are typically generated by the application program code. Secure apps generate new tokens with each access attempt or "session" and they should remain confidential. Improper session handling occurs when apps unintentionally share session tokens with what we call "bad actors" allowing those malicious attackers to impersonate legitimate users. Often this is the result of a session that remains open after the user has navigated away from the app or website. For example, if you logged into an online shopping application, entered your credit card information and made a purchase on your home network from your laptop or tablet and neglected to log out when you finished the task, by remaining open, a potential attacker or organized cybercriminal could be free to explore that website and other connected parts of your home network if they were able to gain access to that session token thru your browser and/or device.

8. **Communication channels may be poorly secured -** Having communication channels, such as bluetooth communications, "open" or in "discovery" mode (which allows the device to be seen by other bluetooth-enabled devices so that connections can be made) could allow an attacker to install malware through that connection, or covertly activate a microphone or camera to eavesdrop on the user. In addition, as we previously mentioned in vulnerabilities #2 and #3 using unsecured public wireless networks or Wi-Fi hotspots could allow an attacker to connect to your mobile device and view sensitive information. Connecting to any unsecured Wi-Fi network could also let an attacker access your personal information from that device, putting you at further risk for data and identity theft. One type of attack that exploits the Wi-Fi network is known as “Man-In-The-Middle” (MITM) where an attacker inserts him or herself in the middle of the communication stream and steals information. An attacker could access your mobile device through a port that is not secured. A good firewall should secure these ports and allow you to choose what connections you want to allow into your mobile device. Without a firewall, your mobile device may be open to intrusion through an unsecured communications port, and an attacker can probably obtain sensitive information on your device and then proceed to misuse it in various ways described earlier in this document.

9. **Two-factor authentication is not always used** - users generally use static passwords instead of two-factor authentication when conducting online sensitive transactions while using mobile devices. Using static passwords for authentication has a large security concern. Passwords can be guessed, forgotten, written down and stolen, or even eavesdropped. Two-factor authentication albeit not the end all or be all solution does generally provide for a higher level of security than traditional passwords and PINs, and this higher level is important for sensitive transactions. Two-factor authentication (often referred to as 2FA) refers to an authentication system in which users are required to authenticate using at least two different "factor" types, either something you know, something you have, or something you are (knowledge, possession or inheritance) before being granted access. Mobile devices can be used as a second factor in some two-factor authentication schemes. The mobile device can generate pass codes, or the codes can be sent via a text message to the phone. Without two-factor authentication, increased risk exists that unauthorized users could gain access to sensitive information and misuse mobile devices.

10. **Mobile devices may have unauthorized modifications -** modifying a mobile device to remove its limitations so consumers can add features (known as "jailbreaking" or "rooting") changes how security for the device is managed and will increase your security risks. Jailbreaking allows users to gain access to the operating system of a device so as to permit the installation of unauthorized software functions and applications and/or to not be tied to a particular wireless carrier. While some users may jailbreak or root their mobile devices specifically to install security enhancements such as firewalls, others may simply be looking for a less expensive or easier way to install desirable applications. In the latter case, users face increased security risks, because they are bypassing the application registration and vetting process established by the manufacturer and thus have less protection against inadvertently installing malware. Also, jailbroken devices may not receive notifications of security updates from the manufacturer and may require extra effort from the user to maintain up-to-date software.

So What Can Be Done To Secure Mobile Devices?

The APE says: ***"Here are a number of ideas..."***

Personal and Organizational

1. **Install P3 Personal Privacy Protection software to provide you with secure access and master control over who and what has access to your:**
    - Camera
    - Microphone
    - Bluetooth
    - Location Services
    - Activity Tracking and Activity Data
2. **Verify the authenticity of downloaded applications** - procedures can be implemented for assessing the digital signatures of downloaded applications to ensure that they have not been tampered with during transit.
3. **Remotely disable lost or stolen devices** - remote disabling is a feature for lost or stolen devices that either locks the device or completely erases its contents remotely. Locked devices can be unlocked subsequently by the user if they are recovered.
4. **Enable encryption for data stored on device or memory card** - file encryption protects sensitive data stored on mobile devices and memory cards. Devices can have built-in encryption capabilities or use commercially available encryption tools.
5. **Install anti-malware capability -** anti-malware protection can be installed to protect against malicious applications, viruses, spyware, infected secure digital cards and malware-based attacks. In addition, such capabilities can protect against unwanted spam of voice messages, text messages, and e-mail attachments.
6. **Install a firewall with allow listing (formerly known as "whitelisting") capabilities** - a personal firewall can protect against unauthorized connections by intercepting both incoming and outgoing connection attempts and blocking or permitting them based on a list of rules. Enable the allow listing (whitelisting) software control that permits only known safe applications to execute commands on your mobile device.
7. **Install security updates in a timely manner** - software updates can be automatically transferred from the manufacturer or cellular carrier directly to a mobile device. Procedures can be implemented to ensure these updates are transmitted promptly and in a secure fashion.
8. **Enable user authentication** – mobile devices can be configured to require passwords or PINs to gain access. In addition, the password field can be masked to prevent it from being observed, and the devices can activate idle-time screen locking to prevent unauthorized access.

9. **Enable two-factor authentication for sensitive transactions -** two-factor authentication (2FA) can be used when conducting sensitive transactions on mobile devices. 2FA provides a higher level of security than traditional passwords. Two-factor refers to an authentication system in which users are required to authenticate using at least two different "factors" consisting of; something you know, something you have, or something you are, before being granted access. Mobile devices themselves can be used as a second factor in some 2FA schemes used for remote access. The mobile device can generate pass codes, or the codes can be sent via a text message or email to the phone. 2FA may be important when sensitive transactions occur, such as for mobile banking or conducting financial transactions.
10. **Do NOT jailbreak or root your mobile device to install security enhancements** – any reputable security or privacy software should not require you to jailbreak or root your phone, even if the application is only available from outside your mobile device's official app store.

Additional Steps for Organizations and Enterprises

- Establish a mobile device security policy - security policies define the rules, principles, and practices that determine how an organization treats mobile devices, whether they are issued by the organization or owned by individuals. Policies should cover areas such as roles and responsibilities, infrastructure security, device security, and security assessments. By establishing policies that address these areas, agencies can create a framework for applying practices, tools, and training to help support the security of mobile devices and the wireless networks they connect to.
- Provide mobile device security training - training employees in your organization's mobile security policies can help to ensure that mobile devices are configured, operated, and used in a secure and appropriate manner.
- Establish a deployment plan - following a well-designed deployment plan helps to ensure that your security objectives are met and security policies are enforced.
- Perform risk assessments - risk analysis identifies vulnerabilities and threats, enumerates potential attacks, assesses the likelihood of the success of such attacks and estimates the potential damage from successful attacks on mobile devices.
- Perform configuration control and management - configuration management ensures that mobile devices are protected against the introduction of improper modifications before, during, and after deployment.

About Our Data

“Common Vulnerabilities and Exposures” - Mitre 2021

“Mobile Phone Tracking” - Wikipedia 2021

“Guidelines for Managing the Security of Mobile Devices in the Enterprise”
SP 800-124 Rev. 2, NIST Computer Security Resource Center - 2020

“Understanding Mobile Device and WiFi Traffic Analysis”
Erik Choron, SANS Institute - 2018

"ECDSA Key Extraction from Mobile Devices via Nonintrusive Physical Side Channels"
International Association for Cryptologic Research - August 2016

“Mobile Positioning Using Wireless Networks”
Fredrik Gustafsson and Fredrik Gunnarsson – July 2005

Additional Resources

New York Times
https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html

CSO Magazine
https://www.csoonline.com/article/2157785/five-new-threats-to-your-mobile-security.html

https://www.csoonline.com/article/3241727/8-mobile-security-threats-you-should-take-seriously.html

Network World Magazine
https://www.networkworld.com/article/2160011/the-10-most-common-mobile-security-problems-and-how-you-can-fight-them.html

Computer Weekly Magazine
https://www.computerweekly.com/tip/Stop-phone-tracking-and-GPS-data-leakage

Kim Komando Community OnDemand

https://www.komando.com/smartphones-gadgets/stop-your-phone-from-tracking-you/543526/

https://www.komando.com/smartphones-gadgets/phone-listening-how-to-make-it-stop/693020/

BGR Mobile Electronics News
https://bgr.com/2018/02/14/iphone-encryption-backdoor-us-government-huawei-zte/

Positive Technologies Security Solutions
https://www.ptsecurity.com/ww-en/analytics/mobile-application-security-threats-and-vulnerabilities-2019/

https://positive-tech.com/knowledge-base/research/epc-research/

Kaspersky Labs

https://usa.kaspersky.com/resource-center/preemptive-safety/public-wifi-risks

https://usa.kaspersky.com/resource-center/threats/spam-phishing

This page intentionally left blank

NOTES:

OFF-GRID APPS™

APE Says: