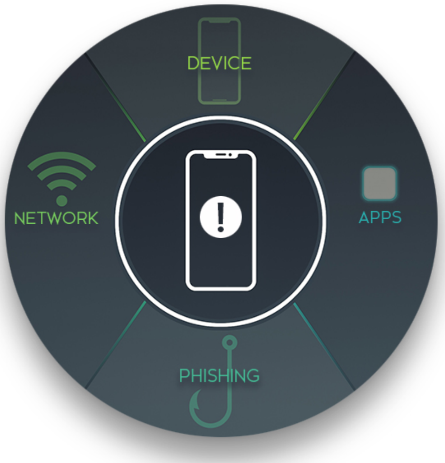
ZIMPERIUM®
MOBILE THREAT DEFENSE

MITRE ATT&CK FOR MOBILE MATRIX

MITRE ATT&CK FOR MOBILE MATRIX

MITRE ATT&CK is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

Initially, MITRE provided their ATT&CK Matrices specifically for desktops and laptops. Now, MITRE offers their ATT&CK Mobile Matrices, which describes the 13 tactical techniques and over 100 methods of exploitation that hackers employ against your mobile devices.



When examining the matrix - which reads like a periodic table - MDMs alone don't address the overwhelming majority of tactics and techniques (again, MDMs are not designed to do so). Together with an MTD, it's a much better protective posture.

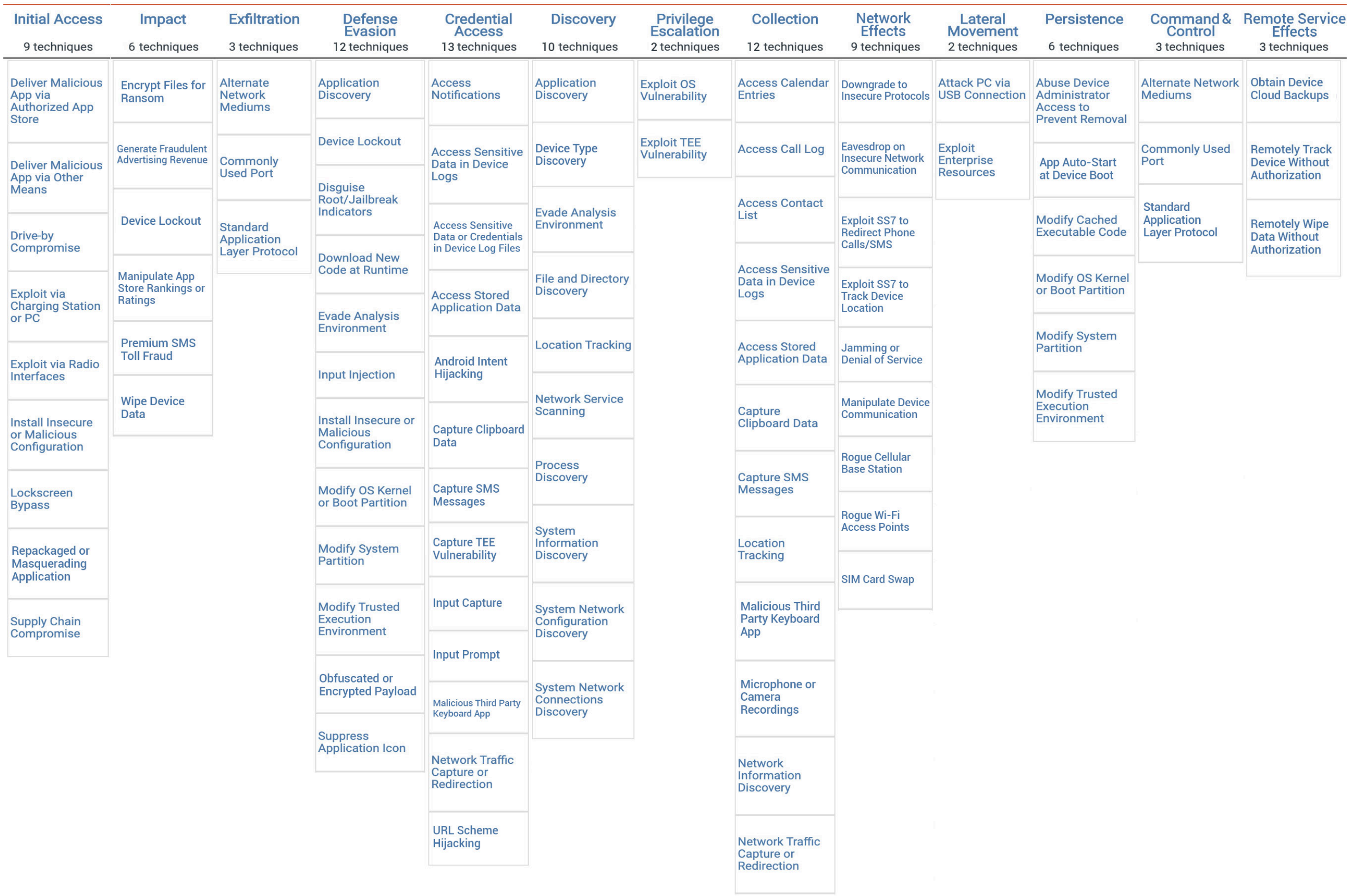
We've taken the "periodic table" and provided a thorough breakdown of each tactic and technique, including definitions and the specific solutions protecting/addressing each tactic and technique. We also include the list of exploitations and details, impacted operating systems, mitigation recommendations and the associated solutions. Possible solutions include:

- MTD - Mobile threat defense solutions which detect and prevent mobile device, network, phishing and malicious app attacks.

- MDM - Mobile device management solutions which are a management tool. MDMs allow compliant devices to access corporate email, apps via the corporate app store, and data, and it secures data-in-transit between the mobile device and the corporate network.

- MAM - Mobile application management describes software and services responsible for provisioning and controlling access to internally developed and commercially available mobile apps used in business settings on both company-provided and bring your own smartphones and tablet computers.

ATT&CK MOBILE MATRIX



Initial Access	Impact	Exfiltration	Defense Evasion	Credential Access	Discovery	Privilege Escalation	Collection	Network Effects	Lateral Movement	Persistence	Command & Control	Remote Service Effects
9 techniques	6 techniques	3 techniques	12 techniques	13 techniques	10 techniques	2 techniques	12 techniques	9 techniques	2 techniques	6 techniques	3 techniques	3 techniques
Deliver Malicious App via Authorized App Store	Encrypt Files for Ransom	Alternate Network Mediums	Application Discovery	Access Notifications	Application Discovery	Exploit OS Vulnerability	Access Calendar Entries	Downgrade to Insecure Protocols	Attack PC via USB Connection	Abuse Device Administrator Access to Prevent Removal	Alternate Network Mediums	Obtain Device Cloud Backups
Deliver Malicious App via Other Means	Generate Fraudulent Advertising Revenue	Commonly Used Port	Device Lockout	Access Sensitive Data in Device Logs	Device Type Discovery	Exploit TEE Vulnerability	Access Call Log	Eavesdrop on Insecure Network Communication	Exploit Enterprise Resources	App Auto-Start at Device Boot	Commonly Used Port	Remotely Track Device Without Authorization
Drive-by Compromise	Device Lockout	Standard Application Layer Protocol	Disguise Root/Jailbreak Indicators	Access Sensitive Data or Credentials in Device Log Files	Evade Analysis Environment		Access Contact List	Exploit SS7 to Redirect Phone Calls/SMS		Modify Cached Executable Code	Standard Application Layer Protocol	Remotely Wipe Data Without Authorization
Exploit via Charging Station or PC	Manipulate App Store Rankings or Ratings		Download New Code at Runtime	Access Stored Application Data	File and Directory Discovery		Access Sensitive Data in Device Logs	Exploit SS7 to Track Device Location		Modify OS Kernel or Boot Partition		
Exploit via Radio Interfaces	Premium SMS Toll Fraud		Evade Analysis Environment	Android Intent Hijacking	Location Tracking		Access Stored Application Data	Jamming or Denial of Service		Modify System Partition		
Install Insecure or Malicious Configuration	Wipe Device Data		Input Injection	Capture Clipboard Data	Network Service Scanning		Capture Clipboard Data	Manipulate Device Communication		Modify Trusted Execution Environment		
Lockscreen Bypass			Install Insecure or Malicious Configuration	Capture SMS Messages	Process Discovery		Capture SMS Messages	Rogue Cellular Base Station				
Repackaged or Masquerading Application			Modify OS Kernel or Boot Partition	Capture TEE Vulnerability	System Information Discovery		Location Tracking	Rogue Wi-Fi Access Points				
Supply Chain Compromise			Modify System Partition	Input Capture	System Network Configuration Discovery		Malicious Third Party Keyboard App	SIM Card Swap				
			Modify Trusted Execution Environment	Input Prompt	System Network Connections Discovery		Microphone or Camera Recordings					
			Obfuscated or Encrypted Payload	Malicious Third Party Keyboard App			Network Information Discovery					
			Suppress Application Icon	Network Traffic Capture or Redirection			Network Traffic Capture or Redirection					
				URL Scheme Hijacking								

ATT&CK MOBILE MATRIX EXPLAINED

Initial Access

MITRE ATT&CK for Mobile Framework	Attack Details	O/S Type	MITRE Mitigation Recommendation	Solution
Deliver Malicious App via Authorized App Store	Malicious applications are a common attack vector used by adversaries to gain a presence on mobile devices. Mobile devices often are configured to allow application installation only from an authorized app store. An adversary may seek to place a malicious application in an authorized app store, enabling the application to be installed onto targeted devices.	🤖 🍎	App Vetting	MTD
Deliver Malicious App via Other Means	Malicious applications are a common attack vector used by adversaries to gain a presence on mobile devices. This technique describes installing a malicious application on targeted mobile devices without involving an authorized app store. Adversaries may wish to avoid placing malicious applications in an authorized app store due to increased potential risk of detection or other reasons. However, mobile devices often are configured to allow application installation only from an authorized app store which would prevent this technique from working.	🤖 🍎	MDM for iOS including configuration profile restrictions can be used to prevent users from installing apps signed using enterprise distribution keys	MTD & MAM
Drive-by Compromise	A drive-by compromise is when an adversary gains access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is targeted for exploitation. For example, a website may contain malicious media content intended to exploit vulnerabilities in media parsers as demonstrated by the Android Stagefright vulnerability.	🤖 🍎	O/S & Security Updates	MTD
Exploit via Charging Station or PC	If the mobile device is connected (typically via USB) to a charging station or a PC, for example to charge the device's battery, then a compromised or malicious charging station or PC could attempt to exploit the mobile device via the connection.	🤖 🍎	MDM, O/S Update	MTD
Exploit via Radio Interfaces	The mobile device may be targeted for exploitation through its interface to cellular networks or other radio interfaces.	🤖 🍎	O/S & Security Updates	MTD & MDM
Install Insecure or Malicious Configuration	An adversary could attempt to install insecure or malicious configuration settings on the mobile device, through means such as phishing emails or text messages either directly containing the configuration settings as an attachment, or containing a web link to the configuration settings. The device user may be tricked into installing the configuration settings through social engineering techniques.	🤖 🍎	O/S & Security Updates	MTD & MDM
Lockscreen Bypass	An adversary with physical access to a mobile device may seek to bypass the device's lockscreen by biometric spoofing, code guessing, brute force or exploiting other device lockscreen vulnerabilities.	🤖 🍎	Device Policy enforcement for pin/password	MTD & MDM
Repackaged or Masquerading Application	An adversary could distribute developed malware by masquerading the malware as a legitimate application. This can be done in two different ways: by embedding the malware in a legitimate application, or by pretending to be a legitimate application.	🤖 🍎	User Training	MTD
Supply Chain Compromise	Supply chain compromise is the manipulation of products or product delivery mechanisms prior to receipt by a final consumer for the purpose of data or system compromise.	🤖 🍎	N/A	MTD

Impact

MITRE ATT&CK for Mobile Framework	Attack Details	O/S Type	MITRE Mitigation Recommendation	Solution
Encrypt Files for Ransom	An adversary may encrypt files stored on the mobile device to prevent the user from accessing them, for example, with the intent of only unlocking access to the files after a ransom is paid.	🤖	App Vetting	**MTD**
Generate Fraudulent Advertising Revenue	An adversary could seek to generate fraudulent advertising revenue from mobile devices, for example, by triggering automatic clicks of advertising links without user involvement.	🤖 🍎	App Vetting	**MTD**
Device Lockout	An adversary may seek to lock the legitimate user out of the device, for example, to inhibit user interaction or to obtain a ransom payment.	🤖 🍎	App Vetting, Device Ent Policy & O/S Update	**MTD & MDM**
Manipulate App Store Rankings or Ratings	An adversary could use access to a compromised device's credentials to attempt to manipulate app store rankings or ratings by triggering app downloads or posting fake reviews of apps.	🤖 🍎	N/A	**MTD**
Premium SMS Toll Fraud	A malicious app could use standard Android APIs to send SMS messages. SMS messages could potentially be sent to premium numbers that charge the device owner and generate revenue for an adversary.	🤖	App Vetting, O/S Update	**MTD & MDM**
Wipe Device Data	An adversary could wipe the entire device contents or delete specific files. A malicious app could obtain and abuse Android device admin access to wipe the entire device.	🤖	Device Ent Policy	**MTD & MDM**

Exfiltration

Alternate Network Mediums	Adversaries can communicate using cellular networks rather than enterprise Wi-Fi in order to bypass enterprise network monitoring systems. Adversaries may also communicate using other non-Internet Protocol mediums such as SMS, NFC, or Bluetooth to bypass network monitoring systems.	🤖 🍎	N/A	**MTD**
Commonly Used Port	Adversaries may communicate over a commonly used port to bypass firewalls or network detection systems and to blend with normal network activity to avoid more detailed inspection. They may use commonly open ports such as: • TCP:80 (HTTP) • TCP:443 (HTTPS) • TCP:25 (SMTP) • TCP/UDP:53 (DNS) They may use the protocol associated with the port or a completely different protocol.)	🤖 🍎	N/A	**MTD**
Standard Application Layer Protocol	Adversaries may communicate using a common, standardized application layer protocol such as HTTP, HTTPS, SMTP, or DNS to avoid detection by blending in with existing traffic.	🤖 🍎	N/A	**MTD**

Defensive Evasion

MITRE ATT&CK for Mobile Framework	Attack Details	O/S Type	MITRE Mitigation Recommendation	Solution
Application Discovery	Adversaries may seek to identify all applications installed on the device. One use case for doing so is to identify the presence of endpoint security applications that may increase the adversary's risk of detection. Another use case is to identify the presence of applications that the adversary may wish to target.	🤖	App Vetting	MTD & MDM
Device Lockout	Adversary may seek to lock the legitimate user out of the device, for example, to inhibit user interaction or to obtain a ransom payment.	🤖	App Vetting, O/S & Security Updates	MTD & MDM
Disguise Root/Jailbreak Indicators	An adversary could use knowledge of the techniques used by security software to evade detection. For example, some mobile security products perform compromised device detection by searching for particular artifacts such as an installed "su" binary, but that check could be evaded by naming the binary something else. Similarly, polymorphic code techniques could be used to evade signature-based detection.	🤖	O/S & Security Updates	MTD
Download New Code at Runtime	An app could download and execute dynamic code (not included in the original application package) after installation to evade static analysis techniques (and potentially dynamic analysis techniques) used for application vetting or application store review.	🤖	App Vetting & O/S Update	MTD & MDM
Evade Analysis Environment	Malicious applications may attempt to detect their operating environment prior to fully executing their payloads. These checks are often used to ensure the application is not running within an analysis environment such as a sandbox used for application vetting, security research, or reverse engineering. Adversaries may use many different checks such as physical sensors, location, and system properties to fingerprint emulators and sandbox environments.	🤖	App Vetting	MTD
Input Injection	A malicious application can inject input to the user interface to mimic user interaction through the abuse of Android's accessibility APIs.	🤖	App Vetting & Device Ent Policy	MTD & MAM
Install Insecure or Malicious Configuration	An adversary could attempt to install insecure or malicious configuration settings on the mobile device, through means such as phishing emails or text messages either directly containing the configuration settings as an attachment, or containing a web link to the configuration settings. The device user may be tricked into installing the configuration settings through social engineering techniques.	🤖	O/S Update	MTD & MDM
Modify OS Kernel or Boot Partition	If an adversary can escalate privileges, he or she may be able to use those privileges to place malicious code in the device kernel or other boot partition components, where the code may evade detection, may persist after device resets, and may not be removable by the device user. In some cases, the attack may be detected but could result in the device being placed in a state that no longer allows certain functionality.	🤖	O/S & Security Updates, Attestation	MTD & MDM
Modify System Partition	If an adversary can escalate privileges, he or she may be able to use those privileges to place malicious code in the device system partition, where it may persist after device resets and may not be easily removed by the device user.	🤖	O/S & Security Updates, Attestation	MTD & MDM

Defensive Evasion (cont.)

MITRE ATT&CK for Mobile Framework	Attack Details	O/S Type	MITRE Mitigation Recommendation	Solution
Modify Trusted Execution Environment	If an adversary can escalate privileges, he or she may be able to use those privileges to place malicious code in the device's Trusted Execution Environment (TEE) or other similar isolated execution environment where the code can evade detection, may persist after device resets, and may not be removable by the device user. Running code within the TEE may provide an adversary with the ability to monitor or tamper with overall device behavior.	🤖	Security Updates	**MTD & MDM**
Obfuscated or Encrypted Payload	An app could contain malicious code in obfuscated or encrypted form, then deobfuscate or decrypt the code at runtime to evade many app vetting techniques.	🤖	App Vetting	**MTD**
Suppress Application Icon	A malicious application could suppress its icon from being displayed to the user in the application launcher to hide the fact that it is installed, and to make it more difficult for the user to uninstall the application. Hiding the application's icon programmatically does not require any special permissions. This behavior has been seen in the BankBot/Spy Banker family of malware.	🤖	N/A	**MTD**
Credential Access				
Access Notifications	A malicious application can read notifications sent by the operating system or other applications, which may contain sensitive data such as one-time authentication codes sent over SMS, email, or other mediums.	🤖	MDM	**MTD**
Access Sensitive Data in Device Logs	On versions of Android prior to 4.1, an adversary may use a malicious application that holds the READ_LOGS permission to obtain private keys, passwords, other credentials, or other sensitive data stored in the device's system log. On Android 4.1 and later, an adversary would need to attempt to perform an operating system privilege escalation attack to be able to access the log.	🤖	App Vetting, O/S & Security Updates	**MTD & MDM**
Access Sensitive Data or Credentials in Device Log Files	An adversary would need to attempt to perform an operating system privilege escalation attack to be able to access the log.	🤖	App Vetting, O/S Update	**MTD & MDM**
Access Stored Application Data	Adversaries may access and collect application data resident on the device. Adversaries often target popular applications such as Facebook, WeChat, and Gmail. This technique requires either escalated privileges or for the targeted app to have stored the data in an insecure manner (e.g., with insecure file permissions or in an insecure location such as an external storage directory).	🤖	App Vetting, O/S Update	**MTD & MDM**
Android Intent Hijacking	A malicious app can register to receive intents meant for other apps and may then be able to receive sensitive values such as OAuth auth codes.	🤖	App Vetting	**MTD**

Credential Access (cont.)

MITRE ATT&CK for Mobile Framework	Attack Details	O/S Type	MITRE Mitigation Recommendation	Solution
Capture Clipboard Data	Adversaries may abuse Clipboard Manager APIs to obtain sensitive information copied to the global clipboard. For example, passwords being copy-and-pasted from a password manager app could be captured by another application installed on the device.	🤖 🍎	App Vetting, O/S Update	MTD & MDM
Capture SMS Messages	A malicious application could capture sensitive data sent via SMS, including authentication credentials. SMS is frequently used to transmit codes used for multi-factor authentication.	🤖 🍎	App Vetting, O/S & Security Updates	MTD & MDM
Exploit TEE Vulnerability	A malicious app or other attack vector could be used to exploit vulnerabilities in code running within the Trusted Execution Environment (TEE). The adversary could then obtain privileges held by the TEE potentially including the ability to access cryptographic keys or other sensitive data. Escalated operating system privileges may be first required in order to have the ability to attack the TEE. If not, privileges within the TEE can potentially be used to exploit the operating system.	🤖	App Vetting, O/S & Security Updates	MTD
Input Capture	Adversaries may capture user input to obtain credentials or other information from the user through various methods. Malware may masquerade as a legitimate third-party keyboard to record user keystrokes. On both Android and iOS, users must explicitly authorize the use of third-party keyboard apps. Users should be advised to use extreme caution before granting this authorization when it is requested.	🤖 🍎	App Vetting & Device Ent Policy	MTD & MDM
Input Prompt	The operating system and installed applications often have legitimate needs to prompt the user for sensitive information such as account credentials, bank account information, or Personally Identifiable Information (PII). Adversaries may mimic this functionality to prompt users for sensitive information.	🤖 🍎	App Vetting & Device Ent Policy & O/S Update	MTD & MDM
Malicious Third Party Keyboard App	Malicious apps could be used to exploit vulnerabilities to escalate privileges to record keystrokes.	🤖 🍎	App Vetting	MTD
Network Traffic Capture or Redirection	An adversary may capture network traffic to and from the device to obtain credentials or other sensitive data, or redirect network traffic to flow through an adversary-controlled gateway to do the same.	🤖 🍎	App Vetting, O/S & Security Updates, Data-in-Transit Encryption	MTD & MDM
URL Scheme Hijacking	An iOS app may be able to maliciously claim a URL scheme, allowing it to intercept calls that are meant for a different application. This technique, for example, could be used to capture OAuth auth codes or to phish user credentials.	🍎	App Vetting	MTD

Discovery

MITRE ATT&CK for Mobile Framework	Attack Details	O/S Type	MITRE Mitigation Recommendation	Solution
Application Discovery	Adversaries may seek to identify all applications installed on the device. One use case for doing so is to identify the presence of endpoint security applications that may increase the adversary's risk of detection. Another use case is to identify the presence of applications that the adversary may wish to target.	🤖 🍎	App Vetting	**MTD & MDM**
Device Type Discovery	Apps looking in Build Class (ex Device Info).	🤖	App Vetting	**MTD**
Evade Analysis Environment	Malicious applications may attempt to detect their operating environment prior to fully executing their payloads. These checks are often used to ensure the application is not running within an analysis environment such as a sandbox used for application vetting, security research, or reverse engineering. Adversaries may use many different checks such as physical sensors, location, and system properties to fingerprint emulators and sandbox environments.	🤖 🍎	App Vetting	**MTD**
File and Directory Discovery	On Android, command line tools or the Java file APIs can be used to enumerate file system contents. However, Linux file permissions and SELinux policies generally strongly restrict what can be accessed by apps (without taking advantage of a privilege escalation exploit). The contents of the external storage directory are generally visible, which could present concern if sensitive data is inappropriately stored there. iOS's security architecture generally restricts the ability to perform file and directory discovery without use of escalated privileges.	🤖	O/S Update	**MTD & MDM**
Location Tracking	An adversary could use a malicious or exploited application to surreptitiously track the device's physical location through use of standard operating system APIs.	🤖	App Vetting	**MTD**
Network Service Scanning	Adversaries may attempt to get a listing of services running on remote hosts, including those that may be vulnerable to remote software exploitation. Methods to acquire this information include port scans and vulnerability scans from the mobile device. This technique may take advantage of the mobile device's access to an internal enterprise network either through local connectivity or through a Virtual Private Network (VPN).	🤖 🍎	N/A	**MTD**
Process Discovery	On Android versions prior to 5, applications can observe information about other processes that are running through methods in the ActivityManager class. On Android versions prior to 7, applications can obtain this information by executing the ps command, or by examining the /proc directory. Starting in Android version 7, use of the Linux kernel's hidepid feature prevents applications (without escalated privileges) from accessing this information.	🤖	App Vetting, O/S Update	**MTD & MDM**
System Information Discovery	An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, and architecture.	🤖 🍎	App Vetting	**MTD & MDM**
System Network Configuration Discovery	On Android, details of onboard network interfaces are accessible to apps through the java.net.NetworkInterface class.	🤖	App Vetting, O/S Update	**MTD & MDM**
System Network Connections Discovery	On Android, applications can use standard APIs to gather a list of network connections to and from the device.	🤖	App Vetting	**MTD**

Privilege Escalation

MITRE ATT&CK for Mobile Framework	Attack Details	O/S Type	MITRE Mitigation Recommendation	Solution
Exploit OS Vulnerability	Malicious app can exploit unpatched vulnerabilities in the operating system to obtain escalated privileges.	🤖 🍎	App Vetting, O/S & Security Updates	MTD
Exploit TEE Vulnerability	A malicious app or other attack vector could be used to exploit vulnerabilities in code running within the Trusted Execution Environment (TEE). The adversary could then obtain privileges held by the TEE potentially including the ability to access cryptographic keys or other sensitive data. Escalated operating system privileges may be first required in order to have the ability to attack the TEE. If not, privileges within the TEE can potentially be used to exploit the operating system.	🤖	App Vetting, O/S & Security Updates	MTD

Collection

Access Calendar Entries	An adversary could call standard operating system APIs from a malicious application to gather calendar entry data, or with escalated privileges could directly access files containing calendar data.	🤖 🍎	App Vetting	MTD
Access Call Log	On Android, an adversary could call standard operating system APIs from a malicious application to gather call log data, or with escalated privileges could directly access files containing call log data. On iOS, applications do not have access to the call log, so privilege escalation would be required in order to access the data.	🤖 🍎	App Vetting, O/S & Security Updates	MTD & MDM
Access Contact List	An adversary could call standard operating system APIs from a malicious application to gather contact list (i.e., address book) data, or with escalated privileges could directly access files containing contact list data.	🤖 🍎	App Vetting	MTD
Access Sensitive Data in Device Logs	On versions of Android prior to 4.1, an adversary may use a malicious application that holds the READ_LOGS permission to obtain private keys, passwords, other credentials, or other sensitive data stored in the device's system log. On Android 4.1 and later, an adversary would need to attempt to perform an operating system privilege escalation attack to be able to access the log.	🤖	App Vetting, O/S & Security Updates	MTD & MDM
Access Stored Application Data	Adversaries may access and collect application data resident on the device. Adversaries often target popular applications such as Facebook, WeChat, and Gmail. This technique requires either escalated privileges or for the targeted app to have stored the data in an insecure manner (e.g., with insecure file permissions or in an insecure location such as an external storage directory).	🤖 🍎	App Vetting, O/S & Security Updates	MTD & MDM
Capture Clipboard Data	Adversaries may abuse Clipboard Manager APIs to obtain sensitive information copied to the global clipboard. For example, passwords being copy-and-pasted from a password manager app could be captured by another application installed on the device.	🤖 🍎	App Vetting, O/S Update	MTD & MDM
Capture SMS Messages	A malicious application could capture sensitive data sent via SMS, including authentication credentials. SMS is frequently used to transmit codes used for multi-factor authentication.	🤖 🍎	App Vetting, O/S & Security Updates	MTD & MDM

Collection (cont.)

MITRE ATT&CK for Mobile Framework	Attack Details	O/S Type	MITRE Mitigation Recommendation	Solution
Location Tracking	An adversary could use a malicious or exploited application to surreptitiously track the device's physical location through use of standard operating system APIs.	🤖 🍎	App Vetting	MTD
Malicious Third Party Keyboard App	Malicious apps could be used to exploit vulnerabilities to escalate privileges to record keystrokes.	🤖 🍎	App Vetting	MTD
Microphone or Camera Recordings	Adversaries may utilize the camera to capture information about the user, their surroundings, or other physical identifiers. Adversaries may use the physical camera devices on a mobile device to capture images/video/audio.	🤖 🍎	App Vetting, O/S & Security Updates	MTD & MDM
Network Information Discovery	Adversaries may use device sensors to collect information about nearby networks, such as Wi-Fi and Bluetooth.	🤖	N/A	MTD
Network Traffic Capture or Redirection	An adversary may capture network traffic to and from the device to obtain credentials or other sensitive data, or redirect network traffic to flow through an adversary-controlled gateway to do the same.	🤖 🍎	App Vetting, O/S & Security Updates, Data-in-Transit Encryption	MTD & MDM

Network Effects

Downgrade to Insecure Protocols	An adversary could cause the mobile device to use less secure protocols, for example by jamming frequencies used by newer protocols such as LTE and only allowing older protocols such as GSM to communicate. Use of less secure protocols may make communication easier to eavesdrop upon or manipulate.	🤖 🍎	IPsec VPN Tunnel	MTD & MDM
Eavesdrop on Insecure Network Communication	If network traffic between the mobile device and remote servers is unencrypted or is encrypted in an insecure manner, then an adversary positioned on the network can eavesdrop on communication.	🤖 🍎	IPsec VPN Tunnel	MTD & MDM
Exploit SS7 to Redirect Phone Calls/SMS	An adversary could exploit signaling system vulnerabilities to redirect calls or SMS to a phone # under the attacker's control. The adversary could then act as a man-in-the-middle to intercept or manipulate the communication.	🤖 🍎	IPsec VPN, Interconnection Filtering	Telco
Exploit SS7 to Track Device Location	An adversary could exploit signaling system vulnerabilities to redirect calls or text messages (SMS) to a phone number under the attacker's control. The adversary could then act as a man-in-the-middle to intercept or manipulate the communication. Interception of SMS messages could enable adversaries to obtain authentication codes used for multi-factor authentication.	🤖 🍎	Carrier IPS/IDS/FW	Telco
Jamming or Denial of Service	An attacker could jam radio signals (e.g. Wi-Fi, cellular, GPS) to prevent the mobile device from communicating.	🤖 🍎	N/A	Telco
Manipulate Device Communication	If network traffic between the mobile device and a remote server is not securely protected, then an attacker positioned on the network may be able to manipulate network communication without being detected.	🤖 🍎	IPsec VPN Tunnel & App Vetting	MTD & MDM

Network Effects (cont.)

MITRE ATT&CK for Mobile Framework	Attack Details	O/S Type	MITRE Mitigation Recommendation	Solution
Rogue Cellular Base Station	An adversary could set up a rogue cellular base station and then use it to eavesdrop on or manipulate cellular device communication. A compromised cellular femtocell could be used to carry out this technique.	🤖 🍎	VPN	Telco & MDM
Rogue Wi-Fi Access Points	An adversary could set up unauthorized Wi-Fi access points or compromise existing access points and, if the device connects to them, carry out network-based attacks such as eavesdropping on or modifying network communication.	🤖 🍎	VPN & Enterprise Policy	MTD & MDM
SIM Card Swap	An adversary could convince the mobile network operator (e.g. through social networking, forged identification, or insider attacks performed by trusted employees) to issue a new SIM card and associate it with an existing phone number and account. The adversary could then obtain SMS messages or hijack phone calls intended for someone else.	🤖 🍎	N/A	Telco
Lateral Movement				
Attack PC via USB Connection	With escalated privileges, an adversary could program the mobile device to impersonate USB devices such as input devices (keyboard and mouse), storage devices, and/or networking devices in order to attack a physically connected PC.	🤖	MDM, O/S Update	MTD & MDM
Exploit Enterprise Resources	Adversaries may attempt to exploit enterprise servers, workstations, or other resources over the network. This technique may take advantage of the mobile device's access to an internal enterprise network either through local connectivity or through a Virtual Private Network (VPN).	🤖 🍎	N/A	MTD
Persistence				
Abuse Device Administrator Access to Prevent Removal	A malicious application can request Device Administrator privileges. If the user grants the privileges, the application can take steps to make its removal more difficult.	🤖	App Vetting, O/S Update	MTD
App Auto-Start at Device Boot	Android apps can listen for the BOOT_COMPLETED broadcast, ensuring that the app's functionality will be activated every time the device starts up without having to wait for the device user to manually start the app.	🤖	App Vetting	MTD
Modify Cached Executable Code	ART (the Android Runtime) compiles optimized code on the device itself to improve performance. An adversary may be able to use escalated privileges to modify the cached code in order to hide malicious behavior. Since the code is compiled on the device, it may not receive the same level of integrity checks that are provided to code running in the system partition.	🤖	O/S & Security Updates	MTD
Modify OS Kernel or Boot Partition	If an adversary can escalate privileges, he or she may be able to use those privileges to place malicious code in the device kernel or other boot partition components, where the code may evade detection, may persist after device resets, and may not be removable by the device user.	🤖 🍎	O/S & Security Updates & Attestation, lock bootloader	MTD

Persistence (cont.)

MITRE ATT&CK for Mobile Framework	Attack Details	O/S Type	MITRE Mitigation Recommendation	Solution
Modify System Partition	If an adversary can escalate privileges, he or she may be able to use those privileges to place malicious code in the device system partition, where it may persist after device resets and may not be easily removed by the device user.	🤖	Security Updates & System Partition Integrity & lock bootloader	MTD
Modify Trusted Execution Environment	If an adversary can escalate privileges, he or she may be able to use those privileges to place malicious code in the device's Trusted Execution Environment (TEE) or other similar isolated execution environment where the code can evade detection, may persist after device resets, and may not be removable by the device user. Running code within the TEE may provide an adversary with the ability to monitor or tamper with overall device behavior.	🤖	O/S & Security Updates	MTD

Command & Control

Alternate Network Mediums	Adversaries can communicate using cellular networks rather than enterprise Wi-Fi in order to bypass enterprise network monitoring systems. Adversaries may also communicate using other non-Internet Protocol mediums such as SMS, NFC, or Bluetooth to bypass network monitoring systems.	🤖	N/A	MTD
Commonly Used Port	Adversaries may communicate over a commonly used port to bypass firewalls or network detection systems and to blend with normal network activity to avoid more detailed inspection. They may use commonly open ports such as: • TCP:80 (HTTP) • TCP:443 (HTTPS) • TCP:25 (SMTP) • TCP/UDP:53 (DNS) They may use the protocol associated with the port or a completely different protocol.	🤖	N/A	MTD
Standard Application Layer Protocol	Adversaries may communicate using a common, standardized application layer protocol such as HTTP, HTTPS, SMTP, or DNS to avoid detection by blending in with existing traffic. In the mobile environment, the Google Cloud Messaging (GCM; two-way) and Apple Push Notification Service (APNS; one-way server-to-device) are commonly used protocols on Android and iOS respectively that would blend in with routine device traffic and are difficult for enterprises to inspect. Google reportedly responds to reports of abuse by blocking access to GCM.	🤖	N/A	MTD

Remote Service Effects

MITRE ATT&CK for Mobile Framework	Attack Details	O/S Type	MITRE Mitigation Recommendation	Solution
Obtain Device Cloud Backups	An adversary who is able to obtain unauthorized access to or misuse authorized access to cloud backup services (e.g. Google's Android backup service or Apple's iCloud) could use that access to obtain sensitive data stored in device backups.	🤖	User Training	O/S Platform OEM
Remotely Track Device Without Authorization	An adversary who is able to obtain unauthorized access to or misuse authorized access to cloud services (e.g. Google's Android Device Manager or Apple iCloud's Find my iPhone) or to an enterprise mobility management (EMM)/mobile device management (MDM) server console could use that access to track mobile devices.	🤖	User Training	MDM
Remotely Wipe Data Without Authorization	An adversary who is able to obtain unauthorized access to or misuse authorized access to cloud services (e.g. Google's Android Device Manager or Apple iCloud's Find my iPhone) or to an EMM console could use that access to wipe enrolled devices.	🤖	User Training	MDM

CONTACT US

If you are interested in learning more, please contact us.

ZIMPERIUM®