THREAT INTELLIGENCE (POC)

NAME : SIDDHI SUNIL BENSEKAR.

INTERN ID : 344

MITRE ATT&CK Mobile Matrix:

The MITRE ATT&CK Mobile Matrix is a framework that details the tactics, techniques, and procedures (TTPs) used by adversaries targeting mobile devices (Android and iOS). It is based on the NIST Mobile Threat Catalog and aims to provide a comprehensive understanding of mobile-based attacks. This detailed Proof of Concept (PoC) explores how these tactics can be leveraged and how organizations can detect and mitigate them.

Summary flow of a mobile attack

A typical mobile attack can follow a flow similar to the Enterprise ATT&CK framework, but with nuances specific to the mobile environment:

1. Reconnaissance: The adversary gathers information about the target mobile device, user, or organization.
2. Resource Development: The adversary creates resources (e.g., malicious apps, exploit infrastructure) to facilitate the attack.
3. Initial Access: The adversary gains initial access to the mobile device, often through user interaction or exploiting a vulnerability.
4. Execution: The adversary executes malicious code or commands on the device.
5. Persistence: The adversary maintains access to the device even after restarts or updates.
6. Privilege Escalation: The adversary attempts to gain higher-level permissions (e.g., root access).
7. Defense Evasion: The adversary tries to avoid detection by security software or user vigilance.
8. Credential Access: The adversary steals user credentials (e.g., passwords, tokens).

9. Discovery: The adversary explores the compromised device and environment to identify valuable data or further vulnerabilities.
10. Lateral Movement: The adversary moves to other devices or systems accessible from the compromised mobile device.
11. Collection: The adversary gathers data of interest (e.g., photos, messages, call logs).
12. Command and Control: The adversary establishes and maintains communication with the compromised device to control it remotely.
13. Exfiltration: The adversary extracts collected data from the device to an external location.
14. Impact: The adversary takes actions to manipulate, interrupt, or destroy systems and data.

Detailed PoC for each tactic

Here are examples of techniques and procedures within each tactic, suitable for a controlled environment (with ethical considerations):

1. Reconnaissance

- Tactic: Reconnaissance (TA0043)
- Techniques:
    - Searching Open Websites/Domains (T1593):
        - Procedure 1: Searching for publicly available employee names on social media platforms like LinkedIn to identify potential targets or gather information about the organization's structure.
        - Procedure 2: Analyzing public app store listings for the target organization's applications to identify potential vulnerabilities, developer information, or exposed API endpoints.
        - Procedure 3: Utilizing search engines and OSINT tools to uncover email addresses, contact details, or public records associated with the organization or its employees.
    - Phishing for Information (T1598):

        - Procedure 1: Crafting a deceptive email pretending to be from a legitimate service (e.g., IT support) and sending it to employees to gather information about their devices or network environment.
        - Procedure 2: Creating a fake survey or questionnaire to trick users into providing details about their mobile device usage patterns, installed applications, or security awareness.
    - Traffic Light Analysis (T1595.002):
        - Procedure 1: Analyzing network traffic patterns from public Wi-Fi access points near the target organization's premises to infer the type of mobile devices, operating systems, and applications commonly used.
        - Procedure 2: Observing application usage patterns and frequently visited domains by employees on public networks to identify potential targets or common vulnerabilities.

2. Resource Development

- Tactic: Resource Development (TA0042)
- Techniques:
    - Develop Capabilities (T1588):
        - Procedure 1: Creating a malicious Android application (APK) that mimics a legitimate one (e.g., a banking app) to be used for phishing or malware distribution.
        - Procedure 2: Developing a custom exploit for a known mobile OS vulnerability to gain device access or elevate privileges.
        - Procedure 3: Building a toolkit for exploiting specific mobile application vulnerabilities (e.g., insecure data storage).
    - Acquire Infrastructure (T1583):
        - Procedure 1: Setting up a Command and Control (C2) server on a compromised cloud instance or virtual private server (VPS) to manage the compromised mobile device(s).
        - Procedure 2: Registering a domain name that closely resembles a legitimate service (e.g., a mobile carrier or app store) for phishing or C2 operations.

- Acquire Accounts (T1586):
    - Procedure 1: Purchasing or stealing credentials for online services (e.g., social media, email) that might be used on target mobile devices.
    - Procedure 2: Creating fake developer accounts on app stores (e.g., Google Play, Apple App Store) to distribute malicious applications.

3. Initial Access

- Tactic: Initial Access (TA0001)
- Techniques:
    - Phishing (T1566):
        - Procedure 1: Sending a spearphishing email with a malicious link (e.g., to a fake app store or website) designed to install malware or steal credentials when accessed from a mobile device.
        - Procedure 2: Distributing malicious apps through social media platforms or messaging apps, disguised as popular games or utility tools, enticing users to install them.
        - Procedure 3: Sending a SMS message (smishing) with a link to a fake login page for a banking application, attempting to steal banking credentials.
    - Drive-by Compromise (T1187):
        - Procedure 1: Embedding a malicious JavaScript snippet on a compromised website that exploits vulnerabilities in mobile browsers when visited by the victim.
        - Procedure 2: Exploiting a vulnerability in a public-facing web application that is also accessed by mobile users to deliver a malicious payload.
    - Supply Chain Compromise (T1195):
        - Procedure 1: Injecting malicious code into a legitimate mobile application during its development or distribution process, resulting in the spread of malware upon app installation.
        - Procedure 2: Compromising a third-party library or SDK used in a mobile application, leading to the distribution of malware to the app's users.

4. Execution

- Tactic: Execution (TA0002)
- Techniques:
    - Malicious Application (T1470):
        - Procedure 1: Developing a malicious Android APK that executes arbitrary code upon installation, potentially establishing a backdoor or stealing data.
        - Procedure 2: Embedding malicious code within an iOS application to execute specific functions or collect sensitive data without user consent.
        - Procedure 3: Exploiting vulnerabilities within a legitimate application to execute unauthorized commands or processes on the device.
    - Network Effects (T1471):
        - Procedure 1: Launching a denial-of-service (DoS) attack against the target mobile device via network-based protocols, potentially disrupting communication or service availability.
        - Procedure 2: Using DNS poisoning or man-in-the-middle attacks to redirect mobile traffic to malicious servers for data interception or malware delivery.
    - Scheduled Task/Job (T1053.005): (While traditionally for enterprise, can have mobile analogues like alarms or recurring events).
        - Procedure 1: Exploiting a vulnerability to create a hidden scheduled task or alarm event that automatically triggers a malicious script or action on **the mobile device.**

5. Persistence

- Tactic: Persistence (TA0003)
- Techniques:
    - Modify System Configuration (T1407):
        - Procedure 1: Modifying a legitimate application's configuration files to enable unauthorized functionality or to launch at startup, maintaining presence on the device.

        - Procedure 2: Modifying system settings (e.g., accessibility services, default keyboard) to grant a malicious app persistent access and control.
        - Procedure 3: Creating a new user account with elevated privileges or modifying an existing one to ensure continuous access to the compromised mobile device.
    - Boot or Reinstall (T1409):
        - Procedure 1: Planting malicious code in the bootloader or firmware of the mobile device to ensure re-installation upon factory reset or system update.
        - Procedure 2: Bundling the malicious application within a system update package, ensuring its persistence even after the device is wiped and restored.
    - Install Root Certificate (T1408):
        - Procedure 1: Tricking the user into installing a malicious root certificate that allows the adversary to decrypt encrypted traffic and intercept sensitive data.
        - Procedure 2: Exploiting a vulnerability to install a malicious root certificate without user interaction, enabling pervasive surveillance of network communications.

6. Privilege Escalation

- Tactic: Privilege Escalation (TA0004)
- Techniques:
    - Exploitation for Privilege Escalation (T1068):
        - Procedure 1: Exploiting a vulnerability in the Android or iOS operating system (kernel or system services) to gain root or administrator privileges.
        - Procedure 2: Leveraging a vulnerability in a third-party application with elevated permissions to compromise the system and achieve privilege escalation.

        - Procedure 3: Exploiting race conditions or memory corruption vulnerabilities in system-level applications to elevate privileges on the device.
    - Process Injection (T1055):
        - Procedure 1: Injecting malicious code into a legitimate, privileged process running on the mobile device to execute actions with higher permissions.
        - Procedure 2: Using dynamic code loading or reflection techniques to bypass security restrictions and achieve privilege escalation within an application.
    - Bypass User Account Control (T1548.002): (Android/iOS specific mechanisms for user consent).
        - Procedure 1: Exploiting a vulnerability or using social engineering to trick the user into granting excessive permissions to a malicious application, bypassing the standard permission model.
        - Procedure 2: Creating a malicious application that exploits a flaw in the system's permission mechanism, allowing it to bypass user consent prompts.

7. Defense Evasion

- Tactic: Defense Evasion (TA0005)
- Techniques:
    - Obfuscated Files or Information (T1027):
        - Procedure 1: Employing code obfuscation techniques (e.g., using packed malware, string encryption) to make the malicious application harder to analyze and detect by security software.
        - Procedure 2: Packing the malicious application with legitimate code to mask its true purpose and evade static analysis tools.
        - Procedure 3: Using polymorphic code or code morphing to constantly change the malware signature, making it difficult for traditional antivirus to detect.
    - Hide Artifacts (T1564):

        - Procedure 1: Deleting or modifying system logs to remove traces of malicious activity on the device.
        - Procedure 2: Suppressing the application's icon from the launcher to prevent the user from easily locating and uninstalling it.
    - Install Root Certificate (T1408): (Also serves persistence and defense evasion).
        - Procedure 1: Installing a malicious root certificate that enables the adversary to intercept and decrypt network traffic, bypassing secure communication protocols (e.g., HTTPS).
        - Procedure 2: Using the installed root certificate to sign malicious applications, making them appear legitimate to the system and evading some security checks.

8. Credential Access

- Tactic: Credential Access (TA0006)
- Techniques:
    - Input Capture (T1056):
        - Procedure 1: Using a malicious application with keyboard accessibility permissions to capture keystrokes and steal login credentials or other sensitive input.
        - Procedure 2: Implementing a screen overlay or fake login page to capture user credentials when they attempt to log in to legitimate applications.
        - Procedure 3: Recording user interaction gestures (e.g., tap patterns) to infer PINs or unlock patterns.
    - Credential Dumping (T1003):
        - Procedure 1: Exploiting vulnerabilities to extract saved credentials from application data storage (e.g., plaintext passwords or authentication tokens).
        - Procedure 2: Leveraging root access to dump credentials or hashes from the device's memory or keychain.
    - Man-in-the-Middle (T1557):

        - Procedure 1: Setting up a rogue Wi-Fi access point or using DNS poisoning to intercept network traffic and steal credentials or session tokens.
        - Procedure 2: Exploiting vulnerabilities in Wi-Fi protocols or mobile network infrastructure to conduct man-in-the-middle attacks.

9. Discovery

- Tactic: Discovery (TA0007)
- Techniques:
    - Device Information (T1473):
        - Procedure 1: Collecting detailed device information, including IMEI, device model, OS version, and network configuration, to identify potential vulnerabilities or tailor attacks.
        - Procedure 2: Using legitimate APIs to enumerate installed applications, running processes, and available storage on the device.
        - Procedure 3: Accessing system logs and configuration files to gather information about device usage patterns and user activities.
    - Application Usage (T1474):
        - Procedure 1: Monitoring which applications are launched and used by the user to understand their interests and identify targets for further exploitation (e.g., banking apps, social media).
        - Procedure 2: Analyzing the permissions granted to installed applications to identify potential avenues for privilege escalation or data access.
    - Network Information (T1475):
        - Procedure 1: Scanning for nearby Wi-Fi networks and Bluetooth devices to gather information about the surrounding environment or identify potential targets for lateral movement.
        - Procedure 2: Accessing network connection details, including IP address, network type, and connected Wi-Fi networks, to gain insight into the device's network context.

10. Lateral Movement

- Tactic: Lateral Movement (TA0008)

- Techniques:
    - Remote Services (T1021): (If the device is connected to a network with other accessible systems).
        - Procedure 1: Using stolen credentials or exploiting vulnerabilities to access other devices on the same Wi-Fi network (e.g., smart home devices, computers).
        - Procedure 2: Leveraging a compromised mobile device as a jump point to pivot into a corporate network via VPN or other remote access services.
    - Application Exploitation (T1485):
        - Procedure 1: Exploiting vulnerabilities in applications on other connected devices (e.g., shared files on a network drive) to gain access and propagate malware.
    - Side-loading (T1484): (If the adversary can install apps on another device)
        - Procedure 1: Remotely installing a malicious application on another connected device (e.g., via a compromised Bluetooth connection or a vulnerable file sharing service).

11. Collection (TA0009)

What it is about: Adversaries gather data relevant to their objectives from the compromised mobile device.

PoC example: Extracting sensitive data from apps

- Technique: Data from Local System (T1005)
- Procedure: An attacker uses malware to access and copy sensitive data stored by legitimate apps (e.g., photos, contacts, location data, documents, chat logs) from the device's storage.
- Why this PoC works: Mobile devices often store a wealth of personal and corporate data, making them attractive targets.

12. Command and control (TA0011)

What it is about: Adversaries establish communication channels to control the compromised mobile device.

PoC example: SMS-based C2

- Technique: Standard Application Layer Protocol: SMS (T1071.004)
- Procedure: An attacker sets up a C2 server that communicates with the mobile malware via SMS messages. The malware receives commands and exfiltrates data through encoded SMS messages.
- Why this PoC works: SMS messages can be used as a covert channel for C2, especially when network traffic is monitored.

13. Exfiltration (TA0010)

What it is about: Adversaries steal data from the compromised mobile device.

PoC example: Exfiltrating data via the Command and Control channel

- Technique: Exfiltration Over C2 Channel (T1041)
- Procedure: The collected data is encrypted and transferred from the mobile device to the attacker's C2 server using the established SMS-based communication channel (or another covert channel like DNS tunneling).
- Why this PoC works: Using the C2 channel blends the data exfiltration with normal communication, making it harder to detect.

14. Impact (TA0040)

What it is about: Adversaries aim to disrupt, damage, or destroy the mobile device or data.

PoC example: Mobile ransomware

- Technique: Data Encrypted for Impact (T1486)
- Procedure: Malware encrypts the data on the mobile device (e.g., photos, documents) and displays a ransom message, demanding payment for decryption.
- Why this PoC works: Encryption renders data unusable, forcing victims to pay to regain access to their information.

Summary flow of a mobile attack

A typical mobile attack flow, following the MITRE ATT&CK Mobile matrix, might involve:

- Reconnaissance: Gathering information about the target's device, applications, and habits.
- Resource Development: Acquiring or creating malicious apps, exploits, or C2 infrastructure.
- Initial Access: Gaining initial access through social engineering (e.g., phishing for credentials or tricking the user into sideloading a malicious app).
- Execution: Executing the malicious payload on the device.
- Persistence: Ensuring continued access by modifying system settings or processes.
- Privilege Escalation: Gaining higher privileges (e.g., root access) to bypass security controls.
- Defense Evasion: Disabling security features or obscuring code to avoid detection.
- Discovery: Mapping the network or the device's capabilities to identify valuable data or further targets.
- Lateral Movement: Accessing other systems or accounts through the compromised device.
- Collection: Gathering sensitive data from the device or linked accounts.
- Command and Control: Establishing a covert channel to control the malware and exfiltrate data.
- Exfiltration: Transferring the stolen data from the device.
- Impact: Disrupting the device or encrypting data (e.g., ransomware)