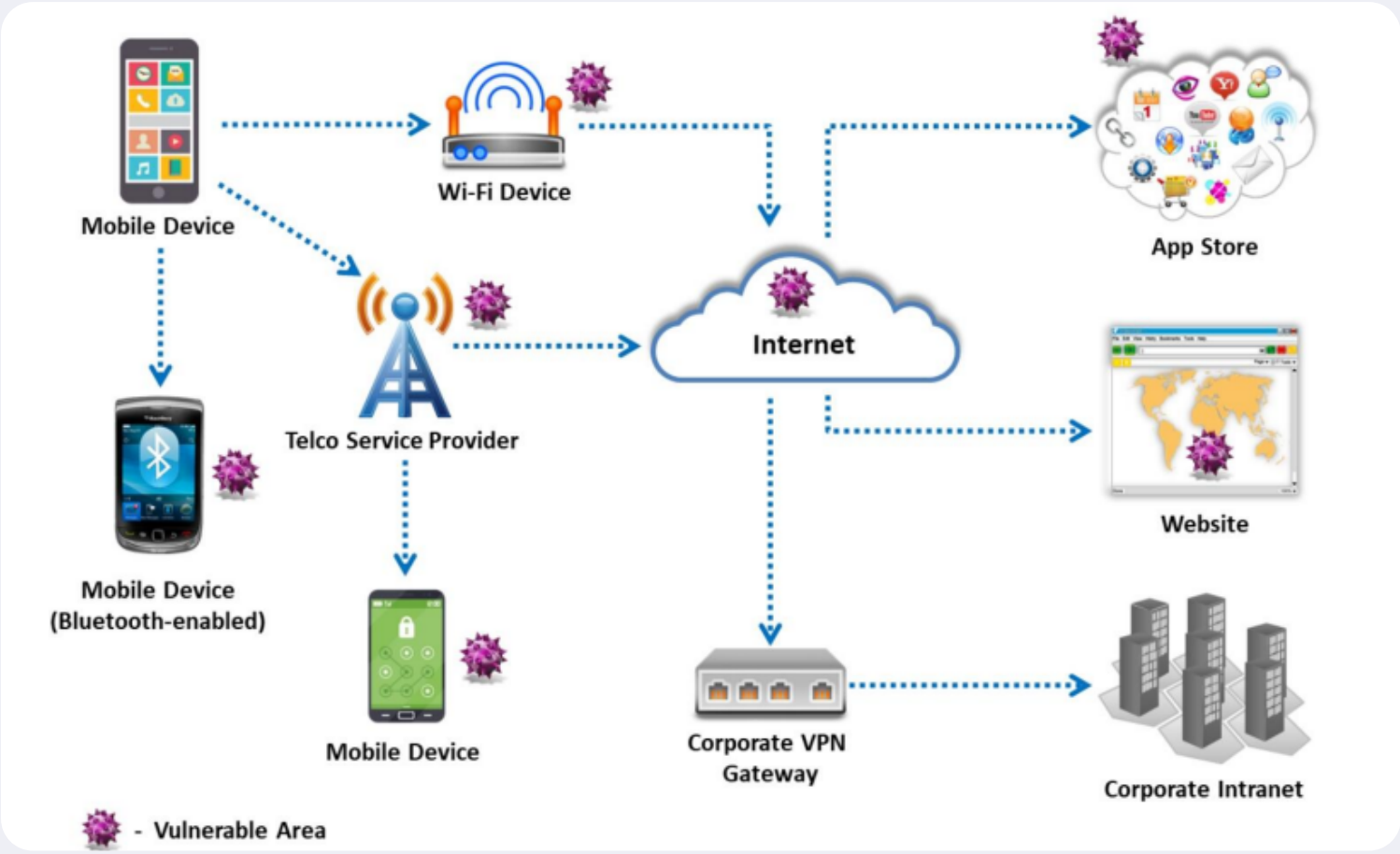
Hacking Mobile Platforms Module-17

by Dheera Thakare

Mobile Platform Attack Vectors



Smartphones offer broad Internet and network connectivity via different channels, such as 3G/4G/5G Bluetooth, Wi-Fi, and wired computer connections Security threats may arise in different places along these channels during data transmission

Malware	Data Exfiltration	Data Tampering	Data Loss
Virus and rootkit	Extracted from data streams and email	Modification by another application	Application vulnerabilities
Application modification	Print screen and screen scraping	Undetected tamper attempts	Unapproved physical access
OS modification	Copy to USB key and loss of backup	Jailbroken device	Loss of device

OWASP TOP 10 MOBILE RISKS

OWASP (Open Web Application Security Project) is a non-profit organization that provides guidance on application security. The OWASP Top 10 Mobile Risks is a list of the most critical mobile application security risks. It helps identify potential vulnerabilities in mobile applications and provides recommendations for mitigating them.

1 Improper Platform Usage

The first item among the OWASP top 10 is improper platform usage. Platforms such as iOS, Android, or Windows Phone provide different capabilities and features that you can use. If the app does not use an existing function or even uses it incorrectly, this is called improper use. This can be, for example, a violation of published guidelines that affects the security of the app. Unlike the other items in the OWASP Mobile Top Ten, this aspect is not aimed exclusively at app developers. The problem with violating common conventions is that it allows for unintended misuse.

2 Insecure Data Storage

Insecure data storage as well as unintentional data leaks also fall under the OWASP Mobile Top Ten. Mobile application penetration testing tools help uncover such grievances. However, it does not necessarily have to be your SQL database. Manifest and log files, cookie storage or cloud synchronisation can also be affected. By the way, this problem occurs so often that it should be an important part of your OWASP Mobile Security Checklist. The reason is almost always found in insufficiently documented or undocumented internal processes.

3 Insecure Communication

Your app transports data from point A to point B. If this transport is insecure, the risk increases. Here, too, the main mobile application penetration testing tools will help you. They support you in detecting faulty app-to-server or mobile-to-mobile communication. The biggest problem is the transfer of sensitive data from one device to another. This could be encryption, passwords, account details or private user information. If the necessary security measures are missing at this point, it is easy for hackers to access your data.

4 Insecure Authentication

Secure authentication adds another key security aspect to your OWASP Mobile Security Checklist. In fact, there are many different ways that the app can provide insecure authentication. A classic example is a back-end API service request that the mobile app executes anonymously without relying on an access token. Additionally, there are still apps that store passwords locally in clear text. To mitigate these potential risks, consider OWASP's recommendations.

5 Lack of Cryptography

The insecure use of cryptography can be observed in most app applications. This is almost always one of two problems: a fundamentally flawed process behind the encryption mechanisms or the implementation of a weak algorithm.

6 Insecure Authorization

Unlike authentication, authorization deals with the verification of an identified person. It verifies that the necessary authorizations are in place to perform certain actions. Of course, the two are closely related – yet both items belong separately on the OWASP Top 10 list. Both are mutually dependent, which is why a lack of authentication almost always leads to a lack of authorization. You need to secure these vulnerabilities as soon as possible to protect your sensitive corporate data from unwanted access.

7 Poor Client Code Quality

This item of the OWASP Top 10 refers to an explicit programming language. All vulnerabilities from code-level errors can provide attackers with a way inside. The main risk lies in the need to make localized changes to the code. In particular, insecure API usage or insecure language constructs are common problems that you need to fix directly at the code level.

8 Code Manipulation

From a technical perspective, any code on a mobile device is vulnerable to tampering. This is because the mobile code is running in a foreign environment. It is no longer under the control of your organization. Therefore, there are numerous ways to modify it at will. You should always consider these unauthorized changes in the context of business implications.

9 Reverse Engineering

Attackers who want to understand how your app works can use reverse-engineering to access all the information they need. Especially metadata, which is supposed to be a relief for your programmers, is a high risk. Basically, if you can clearly understand the string table of the binary or cross-functional analysis is possible, the app is considered at risk.

10 Extraneous Functionality

How a Hackers Can Profit From Mobile Devices That Are Successfully Compromised

Surveillance	Financial	Data Theft	Botnet Activity	Impersonation
Audio	Sending premium-rate SMS messages	Account details	Launching DDoS attacks	SMS redirection
Camera	Fake anti-virus	Contacts	Click fraud	Sending emails
Call logs	Making expensive calls	Call logs and phone number	Sending premium-rate SMS messages	Posting to social media
Location	Extortion via ransomware	Stealing data via app vulnerabilities		
SMS messages	Stealing Transaction Authentication Numbers (TANs)	Stealing International Mobile Equipment Identity Number (IMEI)		

Mobile Spam

Unsolicited text/email messages sent to mobile devices from known/unknown phone number and email IDs

Spam messages contain advertisements or malicious links that can trick users into revealing confidential information

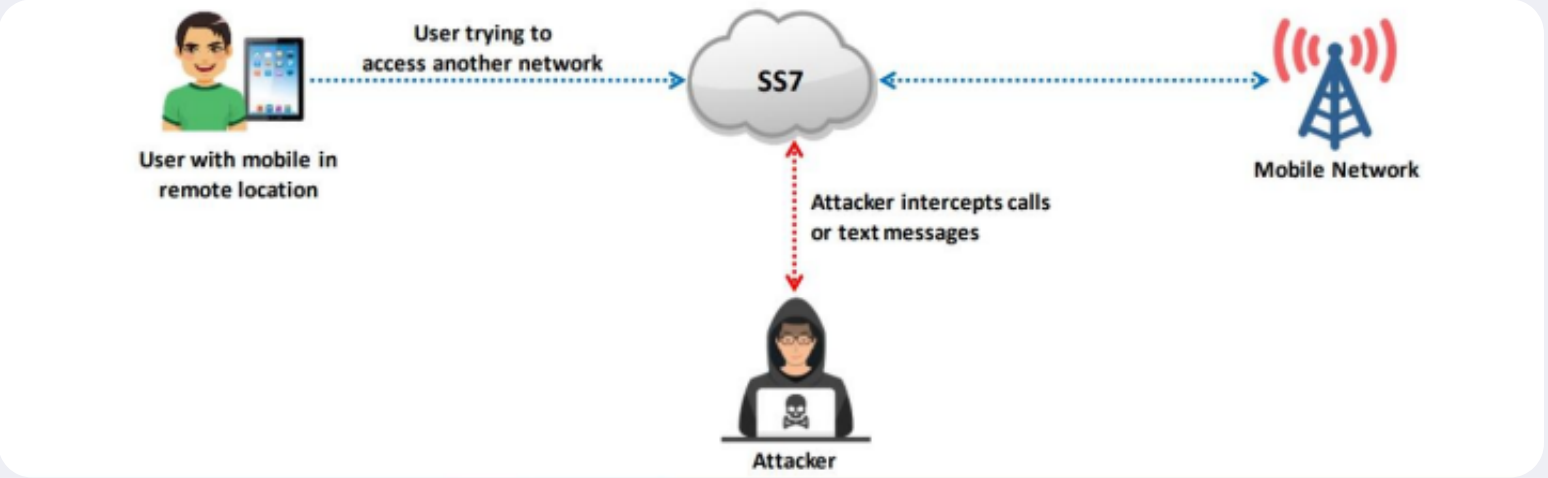
Significant amount of bandwidth is wasted by spam messages

Spam attacks are performed for financial gain

www.smscountry.com

SMS Marketing Solution Provider | SMS & Voice Marketing APIs - SMSCountry

SS7 Vulnerability

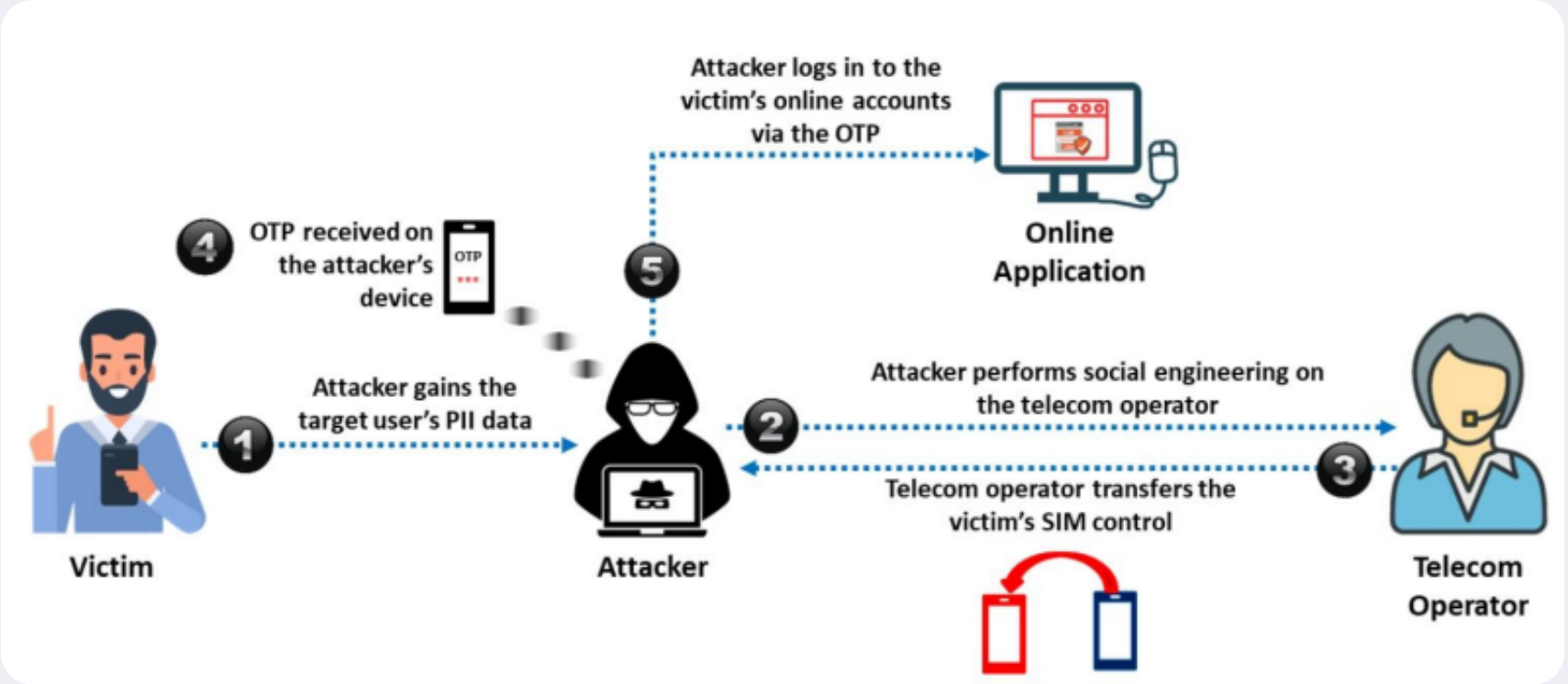


Signaling System 7 (557) is a communication protocol that allows mobile users to exchange communication through another cellular network

SS7 is operated depending on mutual trust between operators without any authentication

Attackers can exploit this vulnerability to perform a man-in-the-middle attack, impeding the texts and calls between communicating devices

OTP Hijacking



OTP Hijacking via Lock Screen Notifications Attackers physically steal SMS-based OTPs from the target user's mobile phone by monitoring the user's actions closely. They can view the notifications on the target user's lock screen when they request for an OTP. Attackers can hijack lock screen notifications using different methods such as eavesdropping

Camera/Microphone Capture Attacks

A camfecting attack is a webcam capturing attack that is performed to gain access to the camera of a target's computer or mobile device

An attacker infects the target device with a remote access Trojan (RAT) and compromises it to access the victim's camera and microphone

Using this method, the attacker can obtain sensitive data such as personal photos, recorded videos, and the location of the user

Android Rooting

Rooting allows Android users to attain privileged control (known as "root access") within Android's subsystem

Rooting process involves exploiting security vulnerabilities in the device firmware and copying the SU binary to a location in the current process's PATH (e.g., /system/xbin/su) and granting it executable permissions with the chmod command

Rooting enables all user-installed applications to run privileged commands, such as

Modifying or deleting system files, module, ROMs (stock firmware), and kernels

Removing carrier- or manufacturer-installed applications (bloatware)

Low-level access to the hardware that are typically unavailable to the devices in their default configuration

Wi-Fi and Bluetooth tethering

Rooting also comes with many security and other risks to your device, including

Voiding of your phone's warranty

Malware infection

Bricking of the device

ANDROID PHONE ROOTING

Step 1: Unlock Bootloader

Step 2: Install TWRP or PBRP Recovery

Step 3: Flash Magisk Manager

OR

Use kingoroot or Kingroot application (may not work for latest phone)

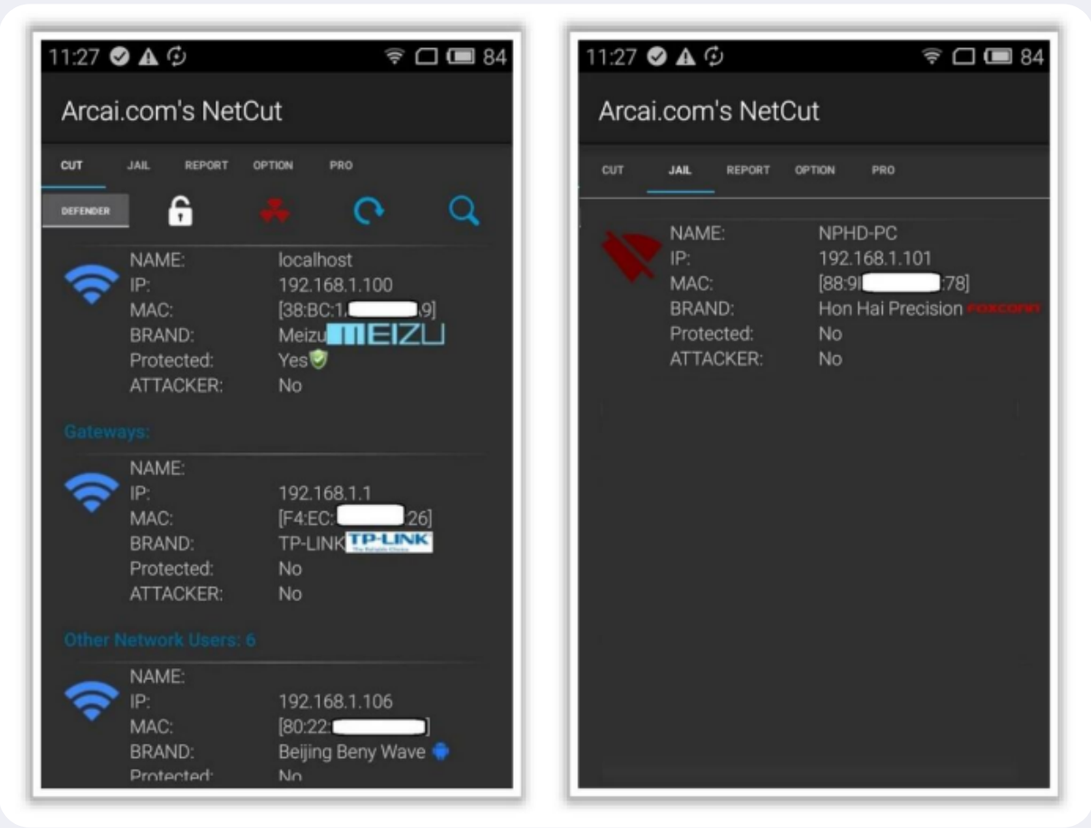
Blocking wi-fi Access Using NetCut

Step 1: Download and install NetCut Android application on your device.

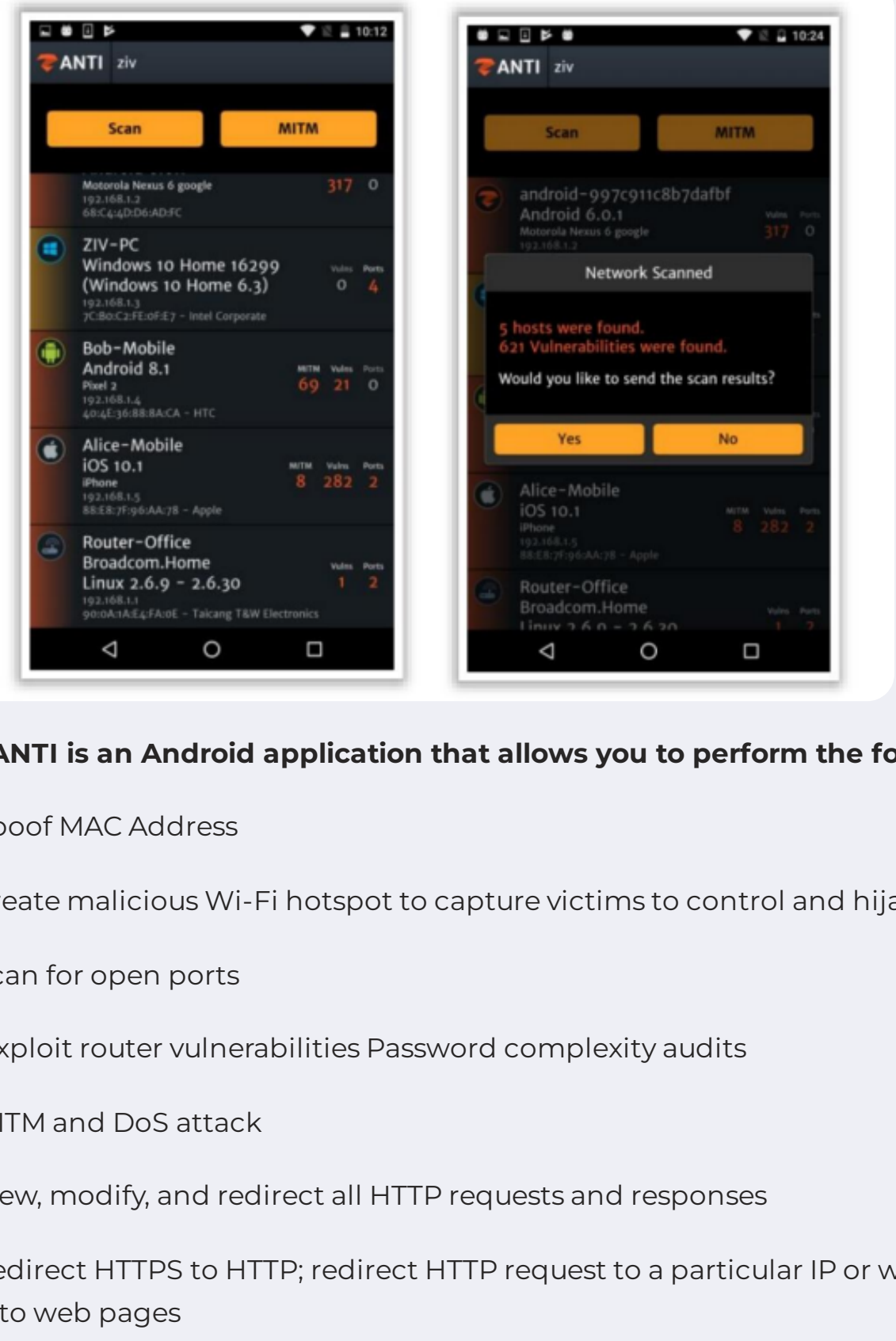
Step 2: Launch the NetCut app.

Step 3: It automatically scans all the devices accessing the Wi-Fi network and displays the list under the CUT tab on the interface.

Step 4: Identify the target device and tap on it to block Wi-Fi access to the device. The Wi-Fi propagation symbol on the left of the blocked device name turns from blue to red. You can confirm this by navigating to the JAIL tab on the interface, where the list of blocked devices will be displayed.



Zanti and NettworkSpoofer



ZANTI is an Android application that allows you to perform the following attacks:

Spoof MAC Address

Create malicious Wi-Fi hotspot to capture victims to control and hijack their device traffic

Scan for open ports

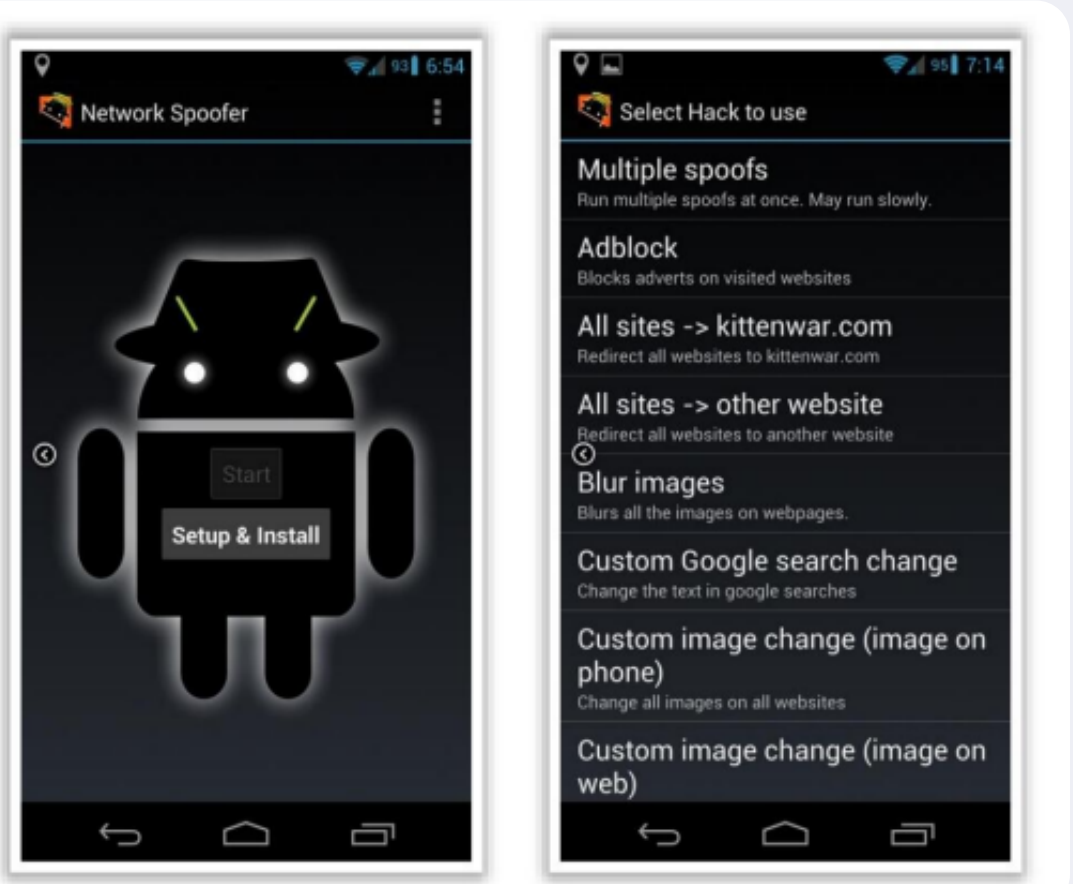
Exploit router vulnerabilities Password complexity audits

MITM and DoS attack

View, modify, and redirect all HTTP requests and responses

Redirect HTTPS to HTTP; redirect HTTP request to a particular IP or web page o Insert HTML code into web pages

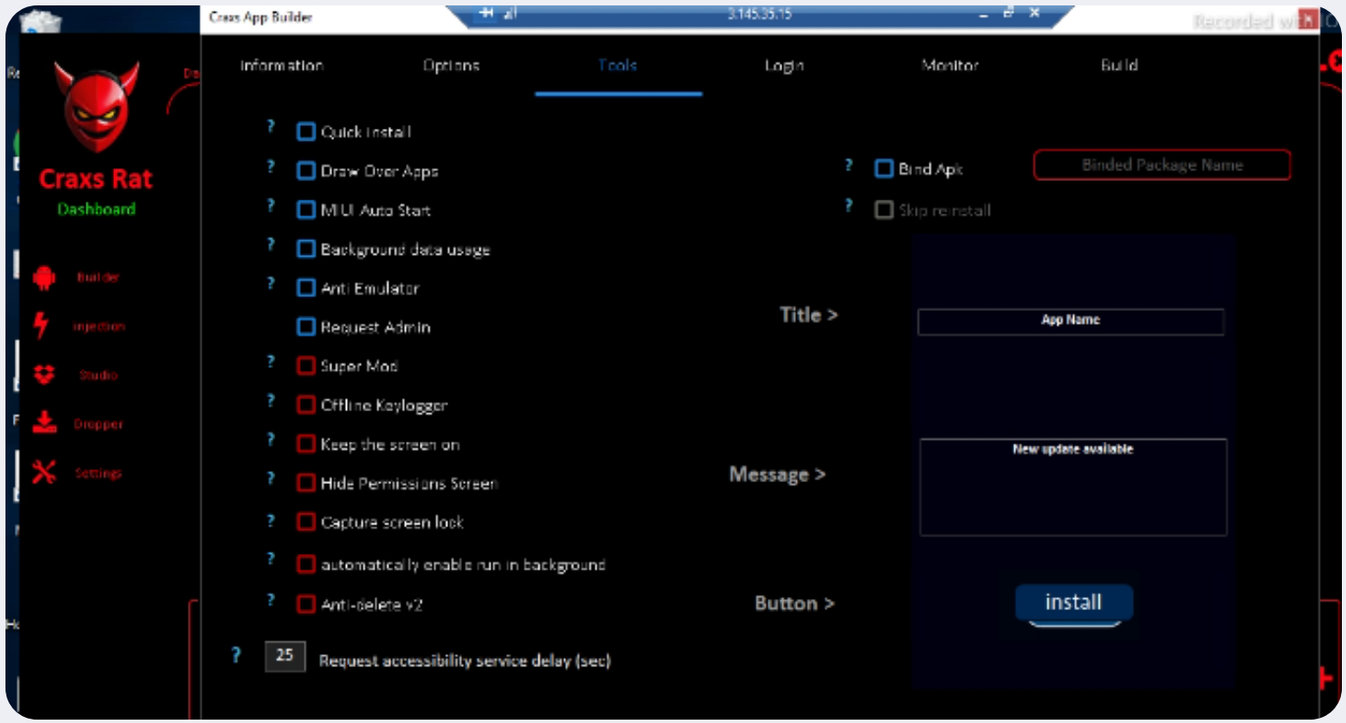
Hijack sessions o View and replace all images that are transmitted over the network o Capture and intercept downloads



Network Spoofer allows you to change websites on others' computers via an Android phone. It allows attackers to flip pictures and text upside down, make websites experience gravity, redirect websites to other pages, and delete or replace random words on websites

Hacking Android Using Trojan/Rat

A Trojan Horse Virus is a type of malware that downloads onto a Android Device disguised as a legitimate program. The delivery method typically sees an attacker use social engineering to hide malicious code within legitimate software to try and gain users' system access with their software.



Top Rat For Hacking Android Devices

CRAXRAT

METASPLOITE

SPYNOTE

RAFEL RAT

APPLE Ios Devices

Jailbreaking Ios

Jailbreaking is defined as the process of installing a modified set of kernel patches that allows users to run third-party applications not signed by the OS vendor

Jailbreaking provides root access to the operating system and permits downloading of third-party applications, themes, and extensions on iOS devices

Jailbreaking removes sandbox restrictions, which enables malicious apps to access restricted mobile resources and information

Types of Jailbreaking

Userland Exploit

Userland Exploit uses a loophole in the system application. It allows user-level access but does not allow iboot-level access. You cannot secure iOS devices against this exploit, as nothing can cause a recovery mode loop. Only firmware updates can patch such vulnerabilities.

iBoot Exploit This type of exploit can be semi-tethered if the device has a new bootrom. An iboot jailbreak allows user-level access and iboot-level access. This exploit takes advantage of a loophole in iBoot (iDevice's third bootloader) to delink the code-signing appliance. Firmware updates can patch such exploits.

Bootrom Exploit Bootrom Exploit uses a loophole in the SecureROM (iDevice's first bootloader) to disable signature checks, which can be used to load patch NOR firmware. Firmware updates cannot patch such exploits. A bootrom jailbreak allows user-level access and iboot-level access. Only a hardware update of bootrom by Apple can patch this exploit.

Step 1-Download the zJailbreak Pro app. Provide the device passcode for this step.

Step 2-Open the zJailbreak Pro app. Go to the Hexxa Plus app available under Most Popular by clicking on it.

Step 3-Click on the Download button for Hexxa Plus. A Hexxa Plus profile will be downloaded to the iOS 15.4 device settings.

Step 4-Go to Settings and then click on Profile Download.

Step 5-Enter the device passcode to complete the Hexxa Plus installation process.

Step 6-Once the installation process is completed, the Hexxa Plus icon will appear on the home screen.

Step 7-Open the Hexxa Plus app and select Get Repos.

Step 8-Choose a jailbreaker's repo and copy its URL from the given categories.

Step 9-Go to the Extract Repo option. Then, paste the copied URL.

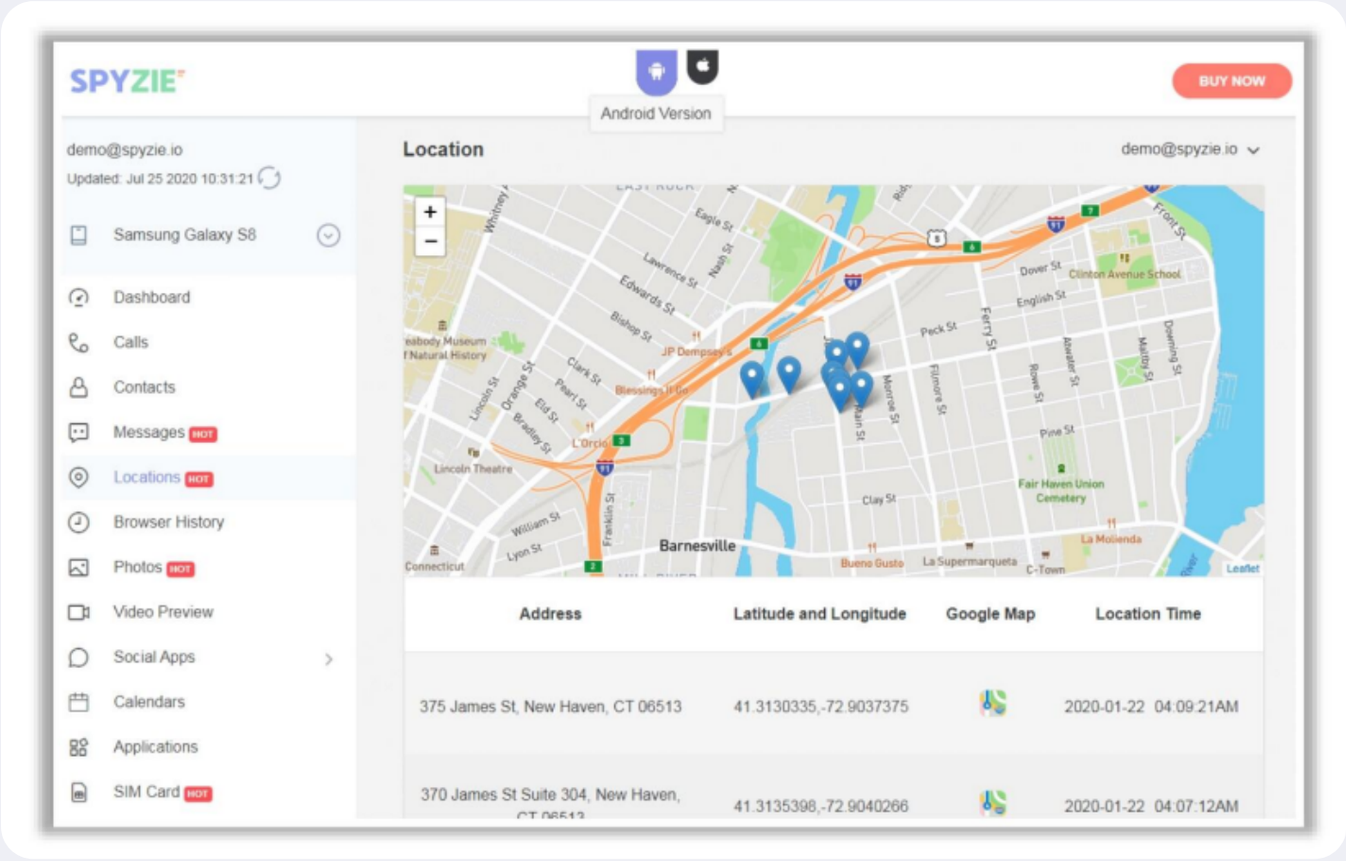
Step 10-Extract the repo by selecting the OK button. Tap the Install button to install the chosen jailbreaker.

Step 11-Finally, the selected jailbreaker app icon appears on the home screen.

Ios Jailbreaking Tools

Apricot,Checkra,Yuxigon,Sileo,Fugu14,Bregxi

Hacking Ios Devices



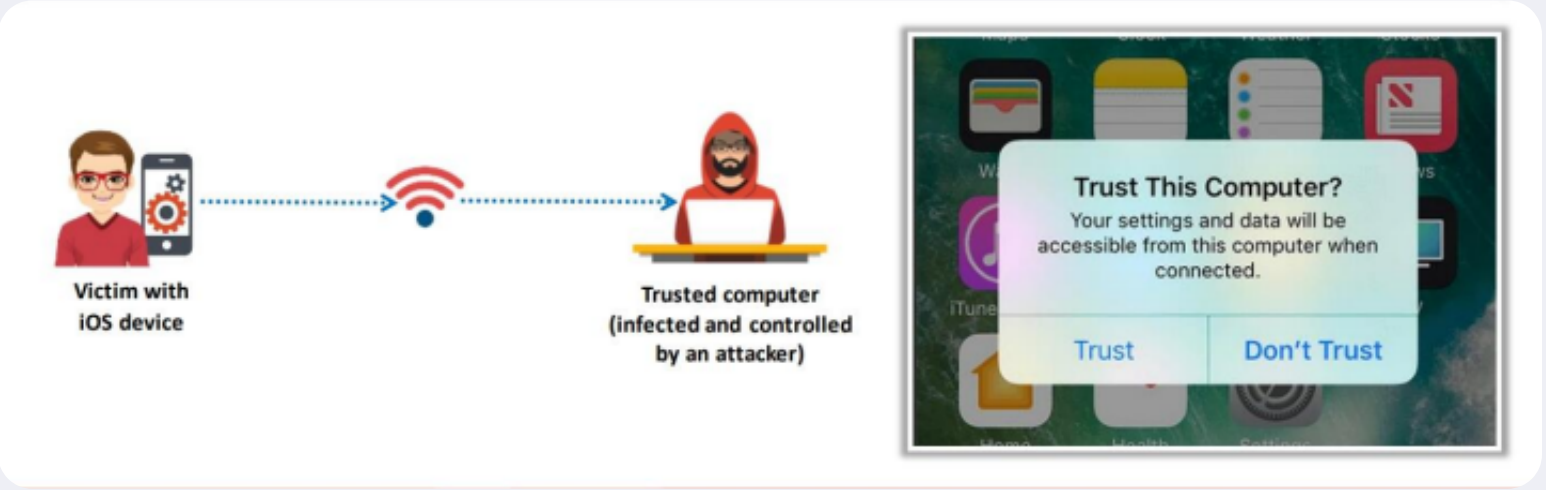
Hacking using Spyzie

Attackers use various online tools such as Spyzie to hack the target iOS mobile devices. Spyzie allows attackers to hack SMS, call logs, app chats, GPS, etc. This tool is compatible with all types of iOS devices such as iPhone, iPad, and iPod. Attackers hack the target device remotely in an invisible mode without jailbreaking the device

Ios Trustjacking

iOS Trustjacking is a vulnerability that can be exploited by an attacker to read messages and emails and capture sensitive information from a remote location without the victim's knowledge

This vulnerability exploits the "iTunes Wi-Fi Sync" feature, where the victim connects their phone to any trusted computer that is already infected by an attacker



IOS MALWARE

NoReboot,Pegasus,XcodeSpy,XCSSET,KeyRaider,PryntStealer,Cliker