Parul® University

Mobile Application Security

Rakshith

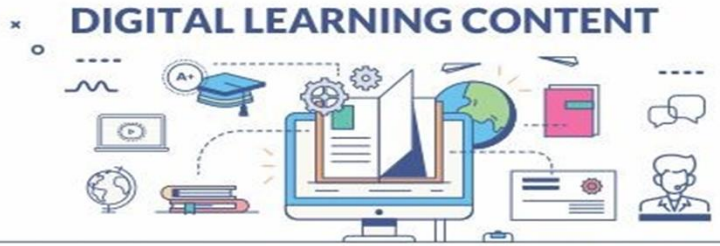
Cyber security Trainer

Parul® University

UNIT 2

IOS & IPA ARCHITECTURE

Parul® University

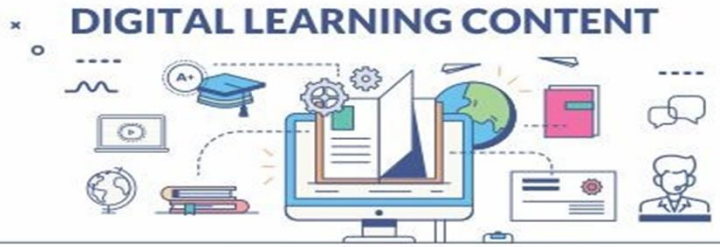


IOS HISTORY

Overview of iOS and iPadOS versions

Version	Initial release date	Latest version	Release date	Device end-of-life		
				iPad	iPhone	iPod Touch
iPhone OS 1	June 29, 2007	1.1.5	July 15, 2008	—	—	—
iPhone OS 2	July 11, 2008	2.2.1	January 27, 2009	—	—	—
iPhone OS 3	June 17, 2009	3.2.2	February 2, 2010	—	1st[a]	1st[a]
iOS 4	June 21, 2010	4.3.5[b]	July 25, 2011	—	3G[c]	2nd[c]
iOS 5	October 12, 2011	5.1.1	May 7, 2012	1st	—	3rd
iOS 6	September 19, 2012	6.1.6	February 21, 2014	—	3GS	4th
iOS 7	September 18, 2013	7.1.2	June 30, 2014	—	4	—
iOS 8	September 17, 2014	8.4.1	August 13, 2015	—	—	—
iOS 9	September 16, 2015	9.3.6	July 22, 2019	2, 3rd, Mini[d]	4S	5th[d]
iOS 10	September 13, 2016	10.3.4	July 22, 2019	4th[e]	5, 5C[e]	—
iOS 11	September 19, 2017	11.4.1	July 9, 2018	—	—	—
iOS 12	September 17, 2018	12.5.7	January 23, 2023	Air (1st), Mini 2, Mini 3	5S, 6	6th
iOS 13 / iPadOS 13	September 19, 2019 (iOS) September 24, 2019 (iPadOS)	13.7	September 1, 2020	—	—	—
iOS 14 / iPadOS 14	September 16, 2020	14.8.1	October 26, 2021	—	—	—
iOS 15 / iPadOS 15	September 20, 2021	15.8	October 25, 2023	Air 2, Mini 4	6S, SE (1st), 7	7th
iOS 16 / iPadOS 16	September 12, 2022 (iOS) October 24, 2022 (iPadOS)	16.7.4	December 19, 2023	Pro (1st), 5th	8, X	—
iOS 17 / iPadOS 17	September 18, 2023	17.2.1	December 19, 2023	—	—	—

Parul® University



IOS HISTORY

- The iPhone was first released in June 2007 and on September 5, 2007, Apple released the iPod Touch which had most of the non-phone abilities of the iPhone.
- In June 2010 Apple rebranded iPhone Os as iOS. iPad first generation iPad was released in April 2010 and the iPad Mini was released in November 2012
- IOS stands for iPhone operating system. It is a proprietary mobile operating system of Apple for its handheld.
- It supports Objective-C, C, C++, and Swift programming languages. It is based on the Macintosh OS X.

Parul® University

iOS 17

Apple announced iOS 17 at the June 2023 WWDC, with a public rollout to take place in Fall 2023.

One of the most notable updates to iOS 17 is the change from, "Hey Siri!" to, "Siri," as well as the ability to give Siri back-to-back commands,

iOS 17 includes upgrades to Phone, FaceTime, and Messages, which also features an all-new Stickers experience.

AirDrop has been upgraded to include NameDrop to allow for easy contact sharing.

Parul® University

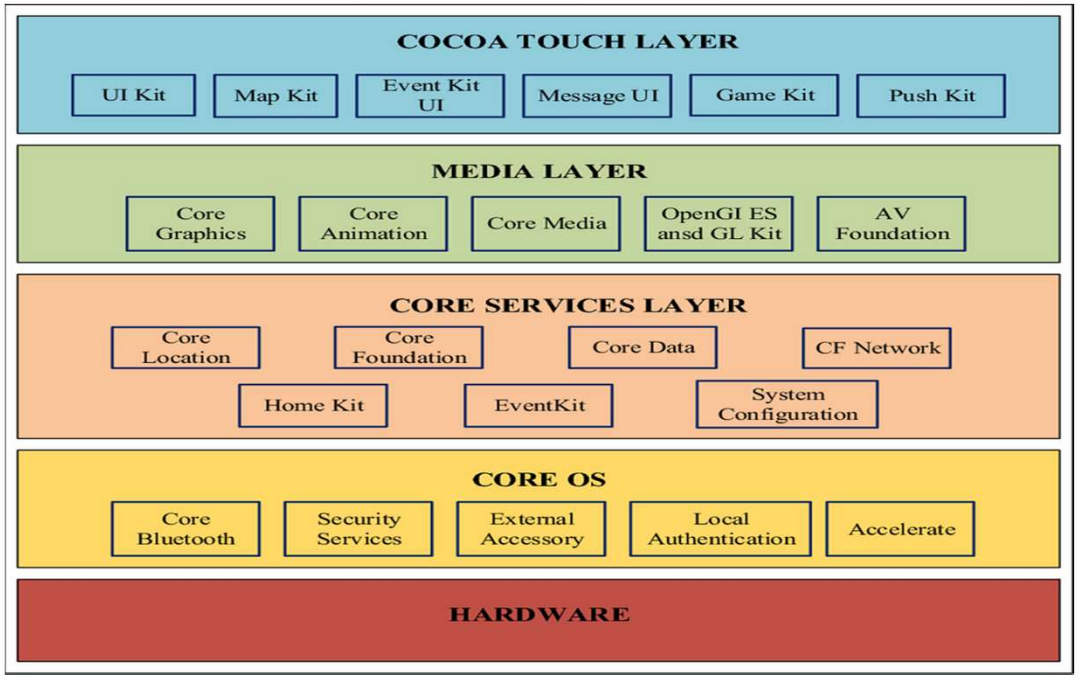
IOS Architecture

- IOS (iPhone Operating System) is a Mobile Operating System that was developed by Apple Inc. for iPhones, iPads, and other Apple mobile devices
- IOS is the second most popular and most used Mobile Operating System after Android.
- The Structure of the IOS is layer based. Its communication doesn't occur directly. The layer's between the Application Layer and the Hardware layer will help for communication.
- The lower level gives basic services on which all applications rely and the higher-level layers provide graphics and interface-related services.
- Most of the system interfaces come with a special package called a framework.

Parul® University

DIGITAL LEARNING CONTENT

IOS Architecture



Parul®
University

DIGITAL LEARNING CONTENT

Layer Name	Description	Framework Names
COCOA TOUCH:	is also known as the application layer which acts as an interface for the user to work with the iOS Operating system. It supports touch and motion events and many more features. The COCOA TOUCH layer provides the following frameworks :	EvenKit Framework,GameKit Framework,MapKit Framework,PushKit Framework,iAd Framework,UIKit Framework
MEDIA Layer	With the help of the media layer, we will enable all graphics video, and audio technology of the system. This is the second layer in the architecture. The different frameworks of MEDIA layers are:	ULKit Graphics, Core Graphics Framework, Core Animation,Media Player Framework,AV Kit,Open AL, Core Images,GL Kit
CORE SERVICES Layer	Some important frameworks are present in the CORE SERVICES Layer which helps the iOS operating system to cure itself and provide better functionality. It is the 2nd lowest layer in the Architecture as shown above. The different frameworks of CORE SERVICES layers are:	Address Book Framework,Cloud Kit Framework,Core Data Framework,Core Location Framework,Core Motion Framework,HomeKit Framework, StoreKit Framework
CORE OS Layer	All the IOS technologies are built under the lowest level layer i.e. Core OS layer. These technologies include:	Core Bluetooth Framework External Accessories Framework Accelerate Framework

Parul® University

Key points to remember

COCOA TOUCH (APPLICATION LAYER)	acts as an interface for the user to work with the iOSsupports touch and motion events and many more features.
MEDIA LAYER	With the help of the media layer, we will enable all graphics video, and audio technology of the system.
CORE SERVICES	helps the iOS operating system to cure itself and provide better functionality.
CORE OS	All the IOS technologies are built under this layer.

Parul® University

CORE OS LAYER

- All the IOS technologies are built under the lowest level layer i.e. Core OS layer.

- These technologies include:

1. Core Bluetooth Framework
2. External Accessories Framework
3. Accelerate Framework
4. Security Services Framework
5. Local Authorization Framework etc.

- It supports 64 bit which enables the application to run faster.

Parul® University

CORE SERVICE LAYER

- Some important frameworks are present in the CORE SERVICES Layer which helps the iOS operating system to cure itself and provide better functionality.
- Below are some important frameworks present in this layer:

1.Address Book Framework-
The Address Book Framework provides access to the contact details of the user.
2.Cloud Kit Framework-
This framework provides a medium for moving data between your app and iCloud.
3.Core Data Framework-
This is the technology that is used for managing the data model of a Model View Controller app.
4.Core Foundation Framework-
This framework provides data management and service features for iOS applications.

5.Core Location Framework-
This framework helps to provide the location and heading information to the application.
6.Core Motion Framework-
All the motion-based data on the device is accessed with the help of the Core Motion Framework.
7.Foundation Framework-
Objective bbcovering too many of the features found in the Core Foundation framework.
8.HealthKit Framework-
This framework handles the health-related information of the user.
9.HomeKit Framework-
This framework is used for talking with and controlling connected devices with the user's home.
10.Social Framework-
It is simply an interface that will access users' social media accounts.
11.StoreKit Framework-
This framework supports for buying of contents and services from inside iOS apps.

Parul® University

MEDIA

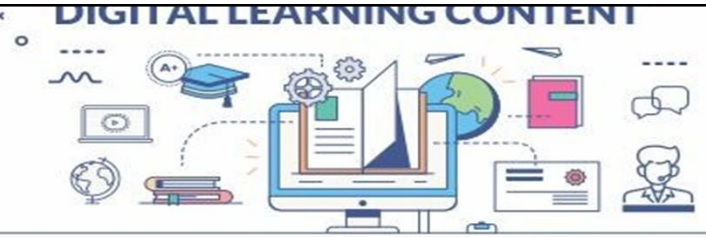
- With the help of the media layer, we will enable all graphics video, and audio technology of the system.

- The different frameworks of MEDIA layers are,

1.ULKit Graphics-
This framework provides support for designing images and animating the view content.

2.Core Graphics Framework-
This framework support 2D vector and image-based rendering and it is a native drawing engine for iOS.

3.Core Animation-
This framework helps in optimizing the animation experience of the apps in iOS.



4.Media Player Framework-
This framework provides support for playing the playlist and enables the user to use their iTunes library.

5.AV Kit-
This framework provides various easy-to-use interfaces for video presentation, recording, and playback of audio and video.

6.Open AL-
This framework is an Industry Standard Technology for providing Audio.

7.Core Images-
This framework provides advanced support for motionless images.

8.GL Kit-
This framework manages advanced 2D and 3D rendering by hardware-accelerated interfaces.

Parul® University

COCOA TOUCH LAYER

- COCOA Touc his also known as the application layer which acts as an interface for the user to work with the iOS Operating system. It supports touch and motion events and many more features.

- The COCOA TOUCH layer provides the following frameworks :

1.EvenKit Framework-
This framework shows a standard system interface using view controllers for viewing and changing events.
2.GameKit Framework-
This framework provides support for users to share their game-related data online using a Game Center.
3.MapKit Framework-
This framework gives a scrollable map that one can include in your user interface of the app.
4.PushKit Framework-
This framework provides registration support.

Parul® University

Understanding iOS Security Model

- iOS provides security right from the hardware level. It extends to System Security maximizing security of OS. Data security safe guards user data with encryption. Moving further App Security guarantees apps are free of known malware.

- Here we'll talk about iOS security categorizing it into below 3 sections.

1. System Security
2. Data Security
3. App Security

Parul® University

1.System Security

- ios system security is having 5 security processes

1. iOS secure boot chain
2. System software authorization
3. SEP (secure enclave processor)
4. Touch ID
5. Face ID

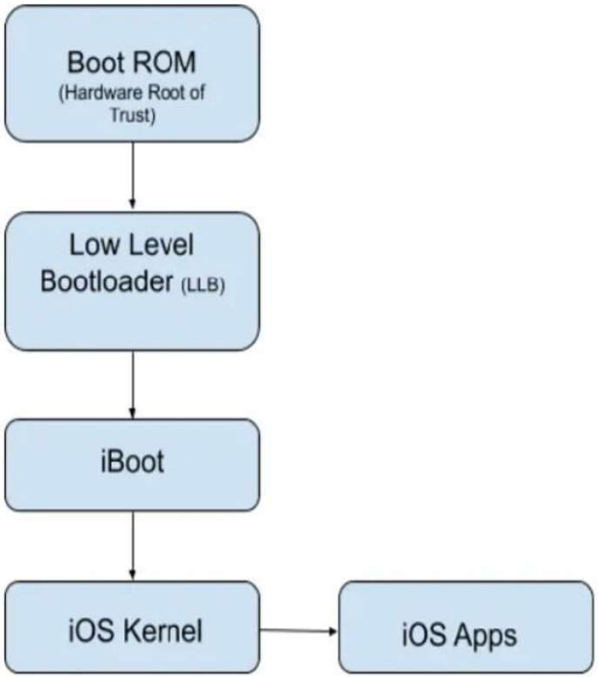
Parul® University

DIGITAL LEARNING CONTENT

1. iOS secure boot chain:-

- when an iOS device is turned on, it immediately executes code from BOOT ROM which is a read-only memory, known as Hardware Root of trust, is laid down during chip fabrication, and is implicitly trusted. This also contains the Apple root certificate with public key and uses it to verify that the low-level boot loader is properly signed and has not been tampered before loading. LLB verifies the iBoot and iBoot verifies iOS kernel before starting it.

- This process ensures lowest levels of software are not tampered and iOS running only on valid Apple devices.



2. system software authorization:-

- Apple regularly releases software updates to address emerging security concerns and prevents devices being downgraded to older versions that lacks latest security updates.

3. SEP (secure enclave processor):-

- Secure Enclave Processor is a co-processor fabricated within the system on chip. It runs its own OS, undergoes secure boot process separate from the rest of the device and receives its system updates independent of the other CPU components. The purpose of the SEP is to handle keys and other info such as bio-metrics and prevents main processor from gaining direct access to sensitive data.

4. Touch ID:-

- Scans fingerprint and store mathematical representation of it in SEP.

5. Face ID:-

- Uses True Depth camera system to accurately map the geometry of the face, use neural networks for determining attention, matching, and anti-spoofing. Data are digitally signed and sent to the SEP.

Parul® University

2. Data Security

- There are 3 main methods of Data security in iOS.

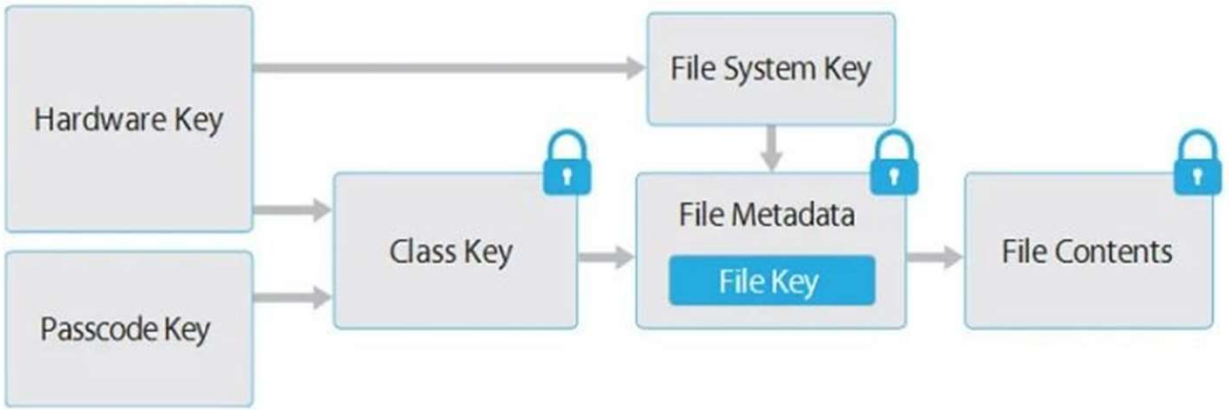
1. Device ID and Group ID
2. File level protection
3. Key chain data protection

1. Device ID and Group ID

- Each device has its unique ID(UID) and a device group ID(GID) which are AES 256-bit keys compiled in to the application processor and SEP during manufacturing. No Software or hardware can access them directly. UID allows data to be tied to a particular device, hence if the memory chip is physically moved to another device, the encrypted files will not be accessible.

2. File level protection

- iOS protects the file data by constructing and managing a hierarchy of keys in conjunction with hardware encryption engine. All keys are stored in SEP.



3. Key chain data protection

- The iOS Keychain can be used to securely store short, sensitive bits of data. eg: encryption keys and session tokens.
- Secure storage for sensitive information, such as passwords, keys, and certificates
- Uses encryption to protect data form unauthorized access.
- Accessible by authorized apps and services.

Parul® University

3.App Security

- There are 5 methods of application security in the iOS.

1. App code signing
2. App updates
3. App sandbox
4. Run time process security
5. App store review

1. App code signing

- App code signing ensures that code is coming from a specific legitimate source/ developer (ensures authenticity) and code has not been altered since it was signed.

2. App updates

- App updates are available to supported devices for security fixes and functionality enhancements.

Parul® University

sandboxing

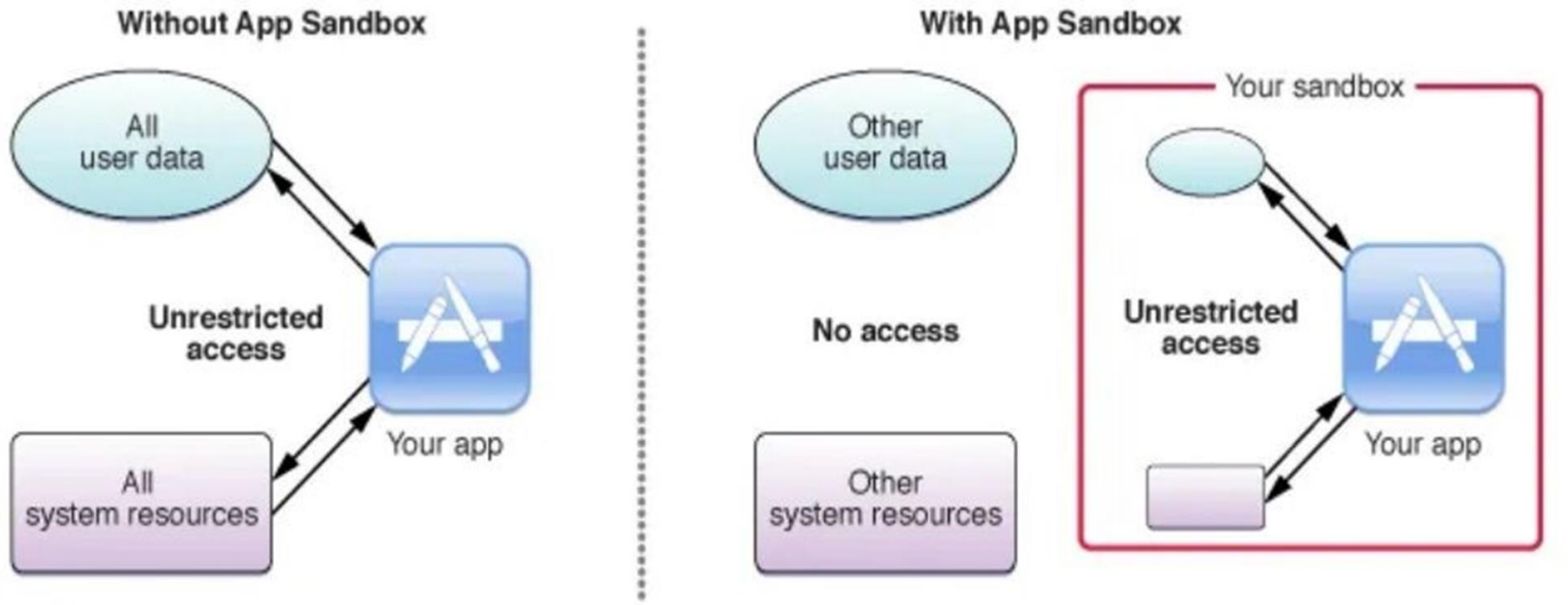
App sandboxing

- All third party apps are “sandboxed” and restricted from accessing files stored by other apps and making any changes to the device. Each app has got a “unique home directory” for its files and it is randomly assigned when app is installed.

- Based on iOS 9.3,

□ third party apps are located in
/private/var/containers/Bundle/Application/<unique id>
/private/var/mobile/Containers/Data/Application/<unique id>

□ Apple apps are located in
/Application


Without App Sandbox
All
user data
Unrestricted
access
Your app
All
system resources
With App Sandbox
Other
user data
No access
Other
system resources
Your sandbox
Unrestricted
access
Your app

4. Run time process security

- **iOS Address Space Layout Randomization(ASLR)**

Primarily used to protect against buffer overflow attacks. Buffer overflows require an attacker to know where each part of the program is located in memory. ASLR randomizes the locations of different parts of the program in memory. Every time the program is run, components are moved to a different address in virtual memory. So attackers can no longer learn where their target is to inject malicious data in to the payload.

- **iOS Data Execution Prevention (DEP)**

All pages in memory are marked as writable or executable but not both.

- **Stack Smashing Protection**

Canary value is placed after the local variables to detect buffer overflows

- **Automatic Reference Counting**

ARC keeps track of class instances and decides when it's safe to deallocate the class instances it monitors. It does this by counting the references of each class instance.

5. App store review

Apple reviews apps before publish them in app store for users to download to ensure that apps are free of known malware and haven't been tampered with.

Parul® University

- **key considerations for developers by iOS sec model**

implementing secure codeing
practices using secure frameworks
and libraries.
Validating user input and handling errors gracefully

- **Security Enhancement**

Data protection
secure communication protocols
Regular software updates

Parul® University

Understanding iOS

- The iOS permission model is quite different compared to the Android platform, Apple has mandated that every single app accessing any class must request user permission, since all data is extremely segregated.

- iOS helps prevent apps from accessing a user's personal information without permission. Additionally, in Settings, users can see which apps they have permitted to access certain information, as well as grant or revoke any future access. This includes access to:

Contacts
Photos
Motion activity and fitness
Location Services
Microphone
Camera

Parul® University

- **Purpose of the permission model**

Empower user to control how apps access their personal information and device resources.

Protect user privacy and prevent unauthorized data access.

Enhance app security by limiting potential attack surfaces.

- **permission granting process**

Apps request when accessing sensitive resources.

Users are presented with clear explanations of the requested access. Users can grant permision, deny it, or grant temporary access.

- **impact on application development**

Developers must carefully consider thte permissions their apps require.

justify and explain permission requests to users.

Minimizing data collection and access to sensitive resources.

Parul® University

Jail Breaking

Definition of jailbreaking

- Modifying an iOS device to bypass Apple's restrictions and gain root access
- Allowing users to install third-party apps and customizations not allowed by Apple
- Potentially compromising device security and stability.

Parul® University

Jail Breaking

1. Tethered jailbreaking

- Although tethered jailbreaks are challenging for Apple to patch, they're not as popular as the untethered jailbroken variety due to their limitations. The limitation, and it's a big one, is that a tethered jailbreak requires an iOS device to connect to a computer to boot.

- The limitation is inconvenient because a jailbroken iPhone can have a shorter battery life and may be more prone to freezes and crashes. Bringing a tethered jailbroken iPhone home every time for a reboot after a glitch can be bothersome.

2. Untethered jailbreaking

- Untethered jailbreaks contrast sharply with tethered jailbreaks. While untethered iOS devices need to connect to a computer for jailbreaks or patches, they can reboot without connecting to a computer.

Parul® University

Jail Breaking

3**. Semi-tethered jailbreaking**

- Semi-tethered jailbreaks require computers for the activation of a jailbreak or modified code. But you can still reboot your semi-tethered iPhone without a computer connection. You just won't have access to jailbreak features without a computer in a semi-tethered jailbreak.

4. Semi-untethered jailbreaking

- Like an untethered jailbreak, an iPhone with a semi-untethered jailbreak can reboot without a computer connection. However, users must redo the jailbreak through the software on the iPhone after a reboot.

Reasons for jailbreaking

- Access to a wider range of apps and customizations.
- Freedom to modify system settings and behavior.
- Ability to run emulators and older version of iOS.

Parul® University

Risks of jailbreaking

Vulnerability to malware and security threats.

Potentioal for device instability and bricking.

Voiding device warranty and losing technical support.

Parul® University

Understanding of IPA

IPA file overview

- File format for packing iOS applications.
- Contains the app's executable code, resources, and metadata.
- Distributed through the App Store or other sources.

IPA file Structure

- Payload folder: Contains the app's executable and resources.
- iTunesArtwork: App icon image for display in iTunes and App Store.
- iTunesMetadata.plist : Metadata about the app, such as name, version and description.

Purpose of IPA Files

- Distributing apps to users for installation.
- Maintaining app integrity and authenticity.
- Enabling app deployment and management.

Parul® University

Understanding Directories and Files on an

Payload folder

- Contains the app's executable file (main.app) and other resources.
- Organized into subfolders for different types of resources, such as images, sounds, and data files.
- Essential for app execution and functionality.

Parul® University

iTunesArtwork

- 512x512 PNG image representing the app's icon.
- Displayed in iTunes and App Store listings.
- Essential for app recognition and user experience.

iTunesMetadata.plist

- XML-based file containing metadata about the app.
- Provide information such as name, version, description, developer, and copyright.
- Used for app identification and display in app stores and device settings.

Parul® University

Additional Files

- Resource files (images, sound,fonts,etc.)
- Configuration files (plist files)
- Third-party libraries or SDKs.
- Documentation and support files.

Parul®
University

Parul® University

www.paruluniversity.ac.in