A-SIT Technology
E-Government Innovation Center

23 July 2024 Analysis · Mobile Security · 16 min read

Security Analysis of new Sideloading Possibilities on iOS 17.4 / iPadOS 18

Florian Draschbacher



Authors	Florian Draschbacher
Version	2024-07-22
Source	https://technology2.a-sit.at/en/publications/security-analysis-of-new-sideloading-possibilities-on-ios-17-4-ipados-18/
Note	Machine translation.

Key findings

- iOS 17.4 allows installing apps from sources outside the App Store for the first time, but every app must still be reviewed by Apple (notarization).
- Apps are still signed and encrypted by Apple before delivery; Apple has not changed the security architecture of iOS.
- Jailbreaking therefore remains an important tool for security research; no new research opportunities have arisen.
- The new distribution channels require a separate developer agreement, including a Core Technology Fee of EUR 0.5 per download beyond 1 million per year.

> - In June 2024 the EU preliminarily found the developer agreement impermissible and is examining whether the Core Technology Fee breaches the DMA.

The Digital Markets Act (DMA) of the European Union forced Apple to relax its position as the gatekeeper of the iOS and iPadOS operating systems over the course of 2024. Among other things, the DMA stipulates that users should be able to obtain applications from sources not under Apple's control. Since some key security mechanisms (such as code signing) are based on the fact that apps have so far been signed by Apple, extensive adjustments to the security architecture of the platform were to be expected.In addition to the expanded possibilities for end-users, the anticipated changes also created new opportunities for security research on the platform. In particular, it was expected that research questions already examined under the competing Android system could now also be addressed under iOS.

However, after the release of iOS version 17.4, which was supposed to bring DMA compliance to at least the iPhone operating system, it became apparent that Apple only half-heartedly implemented some of the requirements. This project investigated to what extent the implemented changes affected the security architecture of the platform and what new research opportunities have emerged.

1. Introduction

When Steve Jobs introduced the iPhone in 2006, it was probably impossible to overestimate how much this product would change the world. Similar products from other manufacturers soon followed in the newly created device category of smartphones (those running the Android operating system deserve particular mention). Users quickly learned to appreciate the benefits of these mobile companions. Mobile telecommunication in the form of the phone call almost faded into the background. Ubiquitous mobile internet access made it possible to benefit from this vast store of knowledge on the move and to stay in touch with the world from anywhere. The built-in camera made it possible to share snapshots with the world instantly and soon made carrying a separate digital camera unnecessary. The previously booming market for mobile audio devices also soon had to concede defeat to the new competition. A remarkable new branch of industry was created, however, when the App Store was launched.

Software companies quickly recognised the enormous potential of smartphones. Through apps, the mobile devices could be turned into ideal tools for a wide variety of areas of life. The newly created app stores of Apple and Google (Play Store) provided distribution channels that allowed developers to exploit the full reach of the mobile platforms. They made it easy to make software visible to all potential users and to generate profits through paid content and advertising. Over the next 15 years, the app stores of Apple and Google developed into markets worth billions. According to current data, Google Play alone generated almost 50 billion dollars in revenue in 2021 [1]. Apple reports more than 1.1 trillion US dollars in revenue generated through apps in 2023 [2].

Since the App Store on iOS/iPadOS and the Google Play Store on Android are the main sources of software for their respective platforms, considerable market power falls to their operators, Apple and Google. Every app that is to be distributed in one of the two stores must comply with the rules of its operator. Among other things, this means that a share of every transaction (purchase, in-app purchase, subscription) must be passed on to the operator. In addition, the rules also prohibit transactions outside the app stores, so there is no way around the commissions. Apple and Google thus earn a considerable share of all revenue in their own app stores. Through the rules of their app stores, they also have the ability to intervene widely in the market. In the past, for example, developer licences were revoked arbitrarily, which meant the loss of the only distribution channel and thus economic ruin for the company concerned.

The power position of Google and Apple is particularly problematic for providers of apps or services (such as music streaming) that are in direct competition with corresponding products of Google or Apple. Here the market is distorted, because the products of Google and Apple do not have to comply with the rules of the company's own app stores, while the competing products must also hand over a share of their revenue to their direct competitor.

To tackle this distortion of competition, the EU adopted the Digital Markets Act (DMA) in 2022 after lengthy negotiations [3]. It legally regulates how the power of so-called gatekeepers, that is, quasi-monopolists in new (digital) markets, is to be broken in order to ensure fair competition (in particular for European companies).

From the very start of the DMA, Apple's situation in the App Store on iOS (on iPhones) was classified as that of a gatekeeper, so Apple was forced to grant third parties extensive rights to run apps on the platform from March 2024. Apple presented corresponding changes with iOS 17.4 [4]. In this project, the details of the implementation of the DMA are explained and discussed, in particular with regard to the effects on security research.

2. Background

This section explains the technologies that are necessary for understanding the later discussion.

2.1. Security Architecture and Code Signing on iOS

iOS is essentially based on Apple's macOS operating system for desktop computers. The XNU kernel used [5] combines components of the Mach microkernel with those of the monolithic FreeBSD. The latter in particular provides compatibility with the POSIX programming interface, so that software for other Unix variants can be quickly adapted to XNU. Although the iOS userspace also inherits some low-level components from macOS, these were supplemented by further components created specifically for the requirements of mobile environments. Among others, the libraries and services that provide the user interface deserve mention here. Many of the security mechanisms of iOS were likewise taken over from macOS or extended for the mobile platform. Although Apple's operating system for the iPad tablet line is now marketed separately as iPadOS, it has considerable technological overlap with iOS. For example, it is possible to run iOS applications under iPadOS.

With few exceptions, iOS only allows the execution of signed software [6]. This means that, for each executable memory page, the presence of a valid signature is checked at the time it is mapped into the virtual memory of the process. As a rule, iOS only accepts signatures issued by Apple. In practice, this

means that software must first be reviewed and approved by Apple before it can be run by end users. The only exception worth mentioning for consumers is the option to run software signed by a developer who holds a corresponding permission from Apple. For this, however, a so-called provisioning profile issued by Apple must be installed on the device. It restricts on which devices the software signed by the developer may be run and which operating system functionality the app may access. It can therefore be stated that Apple holds a central position of control here already from a technological point of view.

The regular publication process for apps for iOS and iPadOS includes a review by Apple [7]. Strict rules must be observed, which aim at a consistent user experience (e.g. no crashes) and at avoiding security vulnerabilities or malicious software. To this end, software submitted to Apple for publication is both executed automatically in a test environment and checked manually by Apple employees. In addition, rules must be observed that are intended to ensure that there is no way to carry out transactions outside Apple's infrastructure. Apple receives a commission of 30% on these (15% for apps with lower revenue). In addition, every developer needs a licence that must be renewed annually (at least $99 per year [8]), as well as Apple devices on which the development tools can be run and pre-release versions of the software can be tested.

2.2. Comparison: Security Architecture of Android and Research Opportunities

Android is the most widely used operating system for mobile devices such as smartphones and tablets. Android is based on the Linux kernel. All components above it in the software stack ("userspace") were developed for the Android operating system specifically for the requirements of mobile devices (low power consumption, touch display, ...). These userspace components are available under the Apache 2.0 licence. The licence permits arbitrary modifications without requiring the source code of the derivative to be published under the same licence.

With regard to the execution of third-party software, Android is designed to be significantly more open than iOS/iPadOS. Apps do have to be signed before they can be run on a device, but the origin of the signature is not checked. Each developer generates their own certificate for this. When the app is installed, the validity of the signature is checked once. Later, it is only checked whether updates for the app were signed by the same developer. Otherwise, an attacker could use a malicious app update to steal the data that the app has stored in its internal storage area.

The fact that the app signature carries no information about the origin of an app makes it possible for third parties to modify existing apps and distribute them re-signed. In the past, attackers exploited this possibility for so-called app repackaging attacks. In these, a legitimate app was maliciously modified and delivered to unsuspecting users as the supposed original app. A banking app manipulated in this way allowed an attacker, for example, to redirect all transactions to their own account without the user being informed of the redirection. To prevent repackaging attacks on sensitive apps, app attestation was eventually found to be an effective measure [9]. At the start of communication with the backend, an independent system component determines the signature of the app and transmits it to the backend. The backend thus has information about the integrity of the app and can stop communication if manipulation is detected.

Besides the potential for abuse, the ability to adapt compiled apps also offers considerable opportunities for security research. To determine, for example, whether an app contains malicious or vulnerable components, dynamic analysis is often used [10]. For this purpose, method calls are redirected, for example, so that the analyst can trace the calls and the parameters passed. Based on this information, it can be determined, for example, whether a certain method is called with insecure parameters. This

strategy also allows, for example, the reverse engineering of proprietary and encrypted communication protocols. Finally, this method can also be used to fix security vulnerabilities in compiled apps automatically [11].

To implement similar research projects under iOS, two central security mechanisms must be bypassed. Code signing has already been discussed in detail. In addition, iOS apps downloaded from the App Store are encrypted for the respective target device with the proprietary FairPlay digital rights management (DRM) system. The app can only be decrypted with a key that resides in the device's separate security chip (Secure Enclave) and never leaves it. In the past, there were solutions to bypass both security mechanisms. However, these required a jailbreak, that is, the wholesale disabling of the device's security architecture by exploiting several vulnerabilities in the operating system. A jailbreak is always associated with a considerably increased security risk and is therefore not recommended for end users. In addition, apps may detect that they are being run on a jailbroken device and refuse service in such an environment.

3. Digital Markets Act

With the Digital Markets Act (DMA) [3], the EU has set itself the goal of ensuring fair conditions for all parties in newly emerged digital marketplaces. The law was adopted in September 2022 and entered into force in November of the same year. Since May 2023, gatekeepers have been identified and asked to redesign their platforms in compliance with the DMA.

3.1. Gatekeepers

The DMA concerns in particular companies that act as gatekeepers of a newly created digital market. These gatekeepers are identified on the basis of clear criteria defined in the text of the law. First, a company must be able to exert significant influence on a market (in the form of a so-called "core platform service" that determines the access of others to the market). In addition, the market in question must reach a certain scale. The revenue generated by the company is used for this. Finally, at least 45 million end users (customers) from the EU must also participate in the market, as well as 10,000 product providers from the EU. The market must also be accessible in at least 3 EU countries.

In September 2023, the EU named the first 6 gatekeepers: Alphabet, Amazon, Apple, ByteDance, Meta and Microsoft [12]. Apple was considered here as the gatekeeper of the iOS operating system and the corresponding App Store (as well as the Safari browser). Initially, Apple insisted that only the App Store for iOS (but not the one for iPadOS) met the gatekeeper criteria, and ultimately implemented the requirements of the DMA on time only for this platform. In April 2024, however, the EU announced that Apple also acts as a gatekeeper with regard to iPadOS [13]. The end-user numbers officially stated by Apple were somewhat below the official threshold here, but the number of product providers from the EU exceeded the threshold by far. In view of the forecast growth in user numbers, it was decided to anticipate the development somewhat. From the time of the official announcement, the companies each had 6 months to implement the requirements of the DMA.

3.2. Requirements

The DMA provides that every gatekeeper must ensure that other companies participating in the market ("third parties") have the same conditions as the gatekeeper itself.

For example, the EU lists the following obligations of gatekeepers (according to [14]):

- Allow third parties to interoperate with the gatekeeper's own services in certain situations
- Allow third parties to access the data that they generate through the use of the gatekeeper's platform
- Provide companies advertising on their platform with the tools and information necessary for advertisers and publishers to carry out their own independent verification of the advertisements hosted by the gatekeeper
- Allow third parties to inform end users about offers outside the gatekeeper's platform, or to conclude contracts with the end user there

In addition, gatekeepers must refrain from, among other things, the following distortions of competition (according to [14]):

- Ranking the gatekeeper's own services and products more favourably than similar services or products of other providers
- Preventing users from uninstalling pre-installed software

4. Implementation of the DMA by Apple

4.1. Expectations

To implement the DMA, Apple was required to allow app installation from sources outside the official App Store. Had the DMA been complied with as specified, this would have meant that, similar to Android, the installation of apps signed by the developer themselves would have been enabled. Since the app would also never have been submitted to Apple (and could not have been encrypted there), the app would presumably have had to be installable in unencrypted form as well. Both security mechanisms that stood in the way of the research opportunities mentioned under 2.2 would thus have had to be deactivated.

It would also have been expected that third-party applications would gain extensive access to advanced functionality of the iOS operating system that was previously reserved for Apple applications. One example worth mentioning here would be the ability to map dynamically allocated memory pages as executable.

4.2. Actual Implementation

Even during the negotiations with the EU on the DMA, Apple had repeatedly insisted that its implementation would involve considerable security risks for end users. Even when DMA compliance was finally announced with iOS 17.4, the official communication was characterised by an attempt to direct the public's focus to the security concerns rather than to the new opportunities for end users and entrepreneurs to participate in the platform on an equal footing.

iOS 17.4 does allow, for the first time, the installation of applications from sources other than the Apple App Store (more precisely, from websites or third-party app stores), but every app must still be reviewed by Apple before publication [4]. This review, now called "notarization", is intended according to Apple to ensure that no malware can reach end devices through installation from external sources. Only after notarization does Apple provide an encrypted version of the app, signed by Apple, that can be installed on devices.

Before developers in the EU can use these new distribution options, they must sign a separate agreement with Apple. The so-called "Core Technology Fee" deserves particular mention here. This is a fee of €0.5 that must be paid to Apple for every download beyond 1 million downloads per year. For providers of third-party app stores, this fee must be paid for every download (from the first download onwards).

4.3. Consequences for Security Research

The possibilities for implementing the research projects described in 2.2 under iOS remain severely limited. Essentially, contrary to expectations, Apple has not changed the security architecture of iOS. Since apps are still signed and encrypted by Apple before they are delivered to end consumers, jailbreaking (with all the associated consequences) remains an important tool in security research.

4.4. Further Developments

Several investigations into Apple's DMA compliance are currently pending. In June 2024, the EU published a first interim report [15], according to which the new separate developer agreement, which ties the possibility of informing about external payment methods to other billing models, would be impermissible. The EU also announced that a new investigation is to clarify whether Apple violates the requirements of the DMA with the "Core Technology Fee".

5. Summary

This project investigated what effects the Digital Markets Act has on the security architecture of the iOS operating system, and whether the changes have created new opportunities for security research. It shows that the adjustments made so far do not allow any new research opportunities, since Apple has been very conservative in implementing the DMA. In view of the EU's ongoing investigations, the developments of the coming months remain to be seen.

References

[1] statista, „Worldwide gross app revenue of Google Play from 2016 to 2021," 13 02 2024. [Online]. Available: https://www.statista.com/statistics/444476/google-play-annual-revenue/. [Zugriff am 2024].

[2] Apple, „App Store developers generated $1.1 trillion in total billings and sales in the App Store ecosystem in 2022," 31 05 2023. [Online]. Available: https://www.apple.com/newsroom/2023/05/developersgenerated-one-point-one-trillion-in-the-app-store-ecosystem-in-2022/. [Zugriff am 2024].

[3] Official Journal of the European Union, „REGULATION (EU) 2022/1925 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL," 12 10 2022. [Online]. Available: https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=uriserv%3AOJ.L_.2022.265.01.0001.01.ENG&toc=OJ%3AL%3A2022%3A265%3ATOC. [Zugriff am 2024].

[4] Apple, „Update on apps distributed in the European Union," 03 2024. [Online]. Available: https://developer.apple.com/support/dma-and-apps-in-the-eu/. [Zugriff am 2024].

[5] Apple, „xnu," [Online]. Available: https://github.com/apple-oss-distributions/xnu. [Zugriff am 2024].

[6] Apple, „App code signing process in iOS and iPadOS,“ 18 02 2021. [Online]. Available: https://support.apple.com/en-gb/guide/security/sec7c917bf14/web. [Zugriff am 2024].

[7] Apple, „App Review Guidelines,“ 10 06 2024. [Online]. Available: https://developer.apple.com/appstore/review/guidelines/. [Zugriff am 2024].

[8] Apple, „Choosing a Membership,“ [Online]. Available: https://developer.apple.com/support/compare memberships/. [Zugriff am 2024].

[9] G. Palfinger, B. Prünster und D. J. Ziegler, „AndroTIME: Identifying Timing Side Channels in the Android API,“ in IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2020.

[10] F. Draschbacher, „A2P2 - An Android Application Patching Pipeline Based On Generic Changesets,“ in ARES ‘23: Proceedings of the 18th International Conference on Availability, Reliability and Security, 2023.

[11] F. Draschbacher, „CryptoShield - Automatic On-Device Mitigation for Crypto API Misuse in Android Applications,“ in ASIA CCS ‘23: Proceedings of the 2023 ACM Asia Conference on Computer and Communications Security, 2023.

[12] European Commission, „Digital Markets Act: Commission designates six gatekeepers,“ 06 09 2023. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/IP_23_4328. [Zugriff am 2024].

[13] European Commission, „Commission designates Apple’s iPadOS under the Digital Markets Act,“ 29 04 2024. [Online]. Available: https://digital-markets-act.ec.europa.eu/commission-designates-apples-ipadosunder-digital-markets-act-2024-04-29_en. [Zugriff am 2024].

[14] European Commission, „About the Digital Markets Act: What does this mean for gatekeepers?,“ [Online]. Available: https://digital-markets-act.ec.europa.eu/about-dma_en#what-does-this-mean-forgatekeepers. [Zugriff am 2024].

[15] European Commission, „Commission sends preliminary findings to Apple and opens additional noncompliance investigation against Apple,“ 24 06 2024. [Online]. Available: https://digital-marketsact.ec.europa.eu/commission-sends-preliminary-findings-apple-and-opens-additional-non-complianceinvestigation-2024-06-24_en. [Zugriff am 2024].