A-SIT

Zentrum für sichere Informationstechnologie - Austria

Sicherheitsanalyse der neuen Sideloading-Möglichkeiten von iOS 17.4 / iPadOS 18

A-SIT

Sicherheitsanalyse der neuen Sideloading-Möglichkeiten von iOS 17.4 / iPadOS 18

Autor:
Florian Draschbacher:
florian.draschbacher@iaik.tugraz.at

Datum: 22.07.2024

Abstract/Zusammenfassung:
Der Digital Markets Act (DMA) der Europäischen Union zwang Apple dazu, im Laufe des Jahres 2024 seine Position als Gatekeeper der iOS- und iPadOS-Betriebssysteme aufzulockern. Unter anderem sieht der DMA vor, dass es Anwendern möglich sein soll, Applikationen aus Quellen zu beziehen, die nicht unter der Kontrolle von Apple stehen. Da einige zentrale Sicherheitsmechanismen (Code Signing) darauf aufbauen, dass Apps bisher von Apple signiert wurden, waren weitreichende Anpassungen der Sicherheitsarchitektur der Plattform zu erwarten.

Neben den erweiterten Möglichkeiten für Endnutzer, ergaben sich durch die antizipierten Änderungen auch neue Gelegenheiten für die Sicherheitsforschung auf der Plattform. Insbesondere wurde erwartet, dass Forschungsfragen, die unter dem konkurrierenden Android-System bereits untersucht wurden, nun auch unter iOS behandelt hätten werden können.

Nach der Veröffentlichung von iOS-Version 17.4, mit der zumindest das iPhone-Betriebssystem DMA-Konformität erhalten sollte, zeigte sich allerdings, dass Apple einige der Vorgaben nur halbherzig umsetzte. Im Rahmen dieses Projektes wurde eruiert, inwieweit die umgesetzten Änderungen die Sicherheitsarchitektur der Plattform beeinflussen, bzw. welche neuen Forschungsmöglichkeiten sich aufgetan haben.

Inhalt

1. Einleitung

Als Steve Jobs 2006 das iPhone vorstellte, konnte wohl nicht überschätzt werden, wie sehr dieses Produkt die Welt verändern würde. Schon bald folgten in der neu geschaffenen Gerätekategorie Smartphone ähnliche Produkte anderer Hersteller (erwähnenswert insbesondere solche mit dem Betriebssystem Android). Schnell lernten Nutzer die Vorzüge der mobilen Begleiter zu schätzen. Die mobile Telekommunikation in Form des Telefonanrufs trat dabei fast in den Hintergrund. Die Möglichkeit des allgegenwärtigen mobilen Internet-Zugriffs erlaubte es, unterwegs von diesem gewaltigen Wissensspeicher zu profitieren und von überall mit der Welt im Austausch zu bleiben. Die im Gerät verbaute Kamera erlaubte es, Schnappschüsse sofort mit der Welt zu teilen, und machte bald das separate Mitführen von Digitalkameras überflüssig. Auch der bis dahin boomende Markt mobiler Audiogeräte musste bald eine Niederlage gegen die neue Konkurrenz eingestehen. Ein bemerkenswerter neuer Wirtschaftszweig wurde aber dafür ins Leben gerufen, als der App Store geschaffen wurde.

Schnell erkannten Software-Unternehmen das riesige Potential von Smartphones. Die mobilen Geräte konnten mittels Apps zu idealen Werkzeugen in verschiedensten Lebensbereichen gemacht werden. Durch die neu geschaffenen App-Stores von Apple und Google (Play Store) standen Distributions-Kanäle zur Verfügung, die es den Entwicklern erlaubten, die volle Reichweite der mobilen Plattformen auszuschöpfen. Sie ermöglichten es, Software einfach für alle potentielle Nutzer sichtbar zu machen und über kostenpflichtige Inhalte und Werbeanzeigen Gewinne zu erwirtschaften. Im Laufe der nächsten 15 Jahre entwickelten sich die App-Stores von Apple und Google zu milliardenschweren Märkten. Aktuellen Daten zufolge erzeugte allein Google Play im Jahr 2021 knapp 50 Milliarden Dollar Gewinn [1]. Apple vermeldet über 1.1 Billionen US-Dollar an über Apps generierten Umsätzen im Jahr 2023 [2].

Da der App Store unter iOS/iPadOS und der Google Play-Store unter Android die Hauptbezugsquelle von Software für die jeweilige Plattform darstellen, fällt den Betreibern Apple und Google beträchtliche Marktmacht zu. Jede App, die in einem der beiden Stores vertrieben werden soll, muss sich den Regeln dessen Betreibers beugen. Dazu gehört etwa, dass ein Anteil jeder Transaktion (Kauf, In-App-Kauf, Abo) an den Betreiber abgegeben werden muss. Außerdem werden über Regeln auch Transaktionen außerhalb der App-Stores verboten, sodass kein Weg um die Kommissionen führt. Apple und Google erwirtschaften also einen erheblichen Teil aller Umsätze in den eigenen App-Stores. Zusätzlich haben sie über die Regeln ihrer App-Stores die Möglichkeit, weiträumig in den Markt einzugreifen. In der Vergangenheit wurden etwa willkürlich Entwicklerlizenzen entzogen, die für das betroffene Unternehmen den Wegfall des einzigen Distributionskanals und somit den wirtschaftlichen Ruin bedeutete.

Besonders problematisch wird die Machtposition von Google und Apple für Anbieter von Apps bzw. Services (etwa Musik-Streamen), die in direkter Konkurrenz zu entsprechenden Produkten von Google oder Apple stehen. Hier wird der Markt verzerrt, weil die Produkte von Google und Apple sich nicht an die Regelwerke der firmeneigenen App-Stores halten müssen, während die Konkurrenzprodukte auch noch einen Anteil ihrer Umsätze an ihren direkten Konkurrenten abtreten müssen.

Um dieser Wettbewerbsverzerrung Herr zu werden, beschloss die EU 2022 nach langen Verhandlungen den Digital Markets Act (DMA) [3]. Hier wird gesetzlich geregelt, wie die Macht von sogenannten Gatekeepern, also Quasi-Monopolisten in neuen (digitalen) Märkten gebrochen werden soll, um fairen Wettbewerb (insbesondere für europäische Unternehmen) zu gewährleisten.

Schon mit Beginn des DMA wurde die Situation Apples im App-Store unter iOS (auf iPhones) als Gatekeeper erfasst, sodass Apple dazu gezwungen wurde, mit März 2024 Dritten weitreichende Rechte zur App-Ausführung auf der Plattform einzuräumen. Apple präsentierte entsprechende Änderungen mit iOS 17.4 [4]. Im Rahmen dieses Projekts werden die Details zur Umsetzung des DMA erläutert, und insbesondere im Hinblick auf die Auswirkungen auf die Sicherheits-Forschung diskutiert.

2. Hintergrund

In diesem Abschnitt sollen jene Technologien erklärt werden, die für das weitere Verständnis der späteren Ausführungen notwendig sind.

2.1. Sicherheitsarchitektur und Code-Signing unter iOS

iOS basiert im Wesentlichen auf Apples macOS-Betriebssystem für Desktop-Computer. Der verwendete XNU-Kernel [5] vereint Bestandteile des Microkernels Mach mit solchen vom monolithischen FreeBSD. Letzterer stellt insbesondere Kompatibilität mit der POSIX-Programmierschnittstelle her, sodass Software für andere Unix-Varianten schnell an XNU angepasst werden kann. Auch wenn der Userspace von iOS auch einige Low-Level-Komponenten von macOS erbt, so wurden diese durch weitere Bestandteile ergänzt, die speziell für die Anforderungen von mobilen Umgebungen geschaffen wurden. Erwähnenswert sind hier unter anderem die Bibliotheken und Services, die die Benutzeroberfläche zur Verfügung stellen. Viele der Sicherheitsmechanismen von iOS wurden ebenso von macOS übernommen bzw. für die mobile Plattform erweitert. Obwohl Apples Betriebssystem für die iPad-Tablet-Modellreihe mittlerweile als iPadOS separat vermarktet wird, verfügt es technologisch über erhebliche Überschneidungen mit iOS. So ist es etwa möglich, iOS-Anwendungen unter iPadOS auszuführen.

Bis auf wenige Ausnahmen erlaubt iOS lediglich das Ausführen von signierter Software [6]. Das bedeutet, dass für jede ausführbare Speicherseite zum Zeitpunkt des Mappens in den virtuellen Speicher des Prozesses überprüft wird, dass eine gültige Signatur vorliegt. iOS erlaubt hier in der Regel nur Signaturen, die von Apple ausgestellt wurden. In der Praxis bedeutet das, dass Software erst von Apple begutachtet und freigegeben werden muss, bevor sie von Endanwendern ausgeführt werden kann. Als einzige für den Endverbraucher erwähnenswerter Ausnahme besteht die Möglichkeit, Software auszuführen, die von einem Entwickler signiert wurde, der über eine entsprechende Erlaubnis von Apple verfügt. Dazu muss allerdings am Gerät ein von Apple ausgestelltes sogenanntes Provisioning Profile installiert werden. Dieses schränkt ein, auf welchen Geräten die vom Entwickler signierte Software ausgeführt werden darf, sowie auf welche Betriebssystem-Funktionalität die App zugreifen darf. Es kann also festgehalten werden, dass Apple hier schon aus technologischer Sicht eine zentrale Kontrollposition innehält.

Der reguläre Veröffentlichungsprozess von Apps für iOS und iPadOS sieht eine Überprüfung („Review“) durch Apple vor [7]. Es müssen strikte Regeln eingehalten werden, die ein konsistentes Nutzererlebnis (z.B. keine Abstürze) und das Vermeiden von Sicherheitslücken oder bösartiger Software zum Ziel haben. Dazu wird an Apple zur Veröffentlichung übermittelte Software sowohl automatisiert in einer Testumgebung ausgeführt, als auch manuell von Apple-Angestellten überprüft. Zusätzlich müssen Regeln eingehalten werden, die sicherstellen sollen, dass es keine Möglichkeit gibt, Transaktionen außerhalb von Apples Infrastruktur durchzuführen. Von diesen erhält Apple nämlich eine Provision in Höhe von 30% (15 % für Apps mit niedrigeren Umsätzen). Zusätzlich benötigt jeder Entwickler eine jährlich zu erneuernde Lizenz (mindestens 99$ im Jahr [8]), sowie Apple-Geräte, auf denen die Entwicklungswerkzeuge ausgeführt und Vorabversionen der Software getestet werden können.

2.2. Vergleich: Sicherheitsarchitektur von Android und Forschungs-Möglichkeiten

Android ist das am weitesten verbreitete Betriebssystem für mobile Endgeräte wie Smartphones und Tablets. Die Basis von Android bildet der Linux-Kernel. Alle im Software-Stack darüberliegenden Komponenten („Userspace") wurden für das Android-Betriebssystem speziell für die Anforderungen von mobilen Geräten (geringer Stromverbrauch, Touch-Display, …) entwickelt. Diese Userspace-Komponenten stehen unter der Apache-2.0-Lizenz zur Verfügung. Die Lizenz erlaubt beliebige Modifikationen, ohne dass der Quellcode des Derivats unter der gleichen Lizenz veröffentlicht werden muss.

Im Hinblick auf die Ausführung von Drittanbieter-Software ist Android deutlich offener gestaltet als iOS/iPadOS. Zwar müssen Apps signiert werden, bevor sie auf einem Endgerät ausgeführt werden können, allerdings wird die Herkunft der Signatur nicht überprüft. Jeder Entwickler generiert dazu ein eigenes Zertifikat. Wird die App installiert, wird die Gültigkeit der Signatur für die App einmalig überprüft. Später wird lediglich überprüft, ob Updates für die App vom selben Entwickler signiert wurden. Andernfalls wäre es einem Angreifer möglich, über ein bösartiges App-Update jene Daten zu stehlen, die die App in ihrem internen Speicherbereich abgelegt hat.

Die Tatsache, dass die App-Signatur keine Aussagekraft zur Herkunft einer App hat, ermöglicht es Dritten, bestehende Apps zu modifizieren und neu signiert in Umlauf zu bringen. In der Vergangenheit wurde diese Möglichkeit von Angreifern zu sogenannten App-Repackaging-Attacken ausgenutzt. Dabei wurde eine legitime App bösartig verändert und als die vermeintliche Original-App an unbedarfte Nutzer ausgeliefert. Eine auf diese Art manipulierte Banking-App erlaubte es einem Angreifer zum Beispiel, alle Transaktionen an einen eigenen Account umzuleiten, ohne dass der Nutzer über diese Umleitung informiert wurde. Um Repackaging-Attacken für sensible Apps zu unterbinden, wurde schließlich mit App Attestation ein wirksames Mittel gefunden [9]. Dabei wird zu Beginn der Kommunikation mit dem Backend durch eine unabhängige Systemkomponente die Signatur der App ermittelt und an das Backend übermittelt. Das Backend verfügt so über Informationen zur Integrität der App und kann bei erkannter Manipulation die Kommunikation einstellen.

Die Möglichkeit zur Adaption von kompilierten Apps birgt neben dem Potential für Missbrauch auch erhebliche Chancen für die Sicherheitsforschung. Um etwa festzustellen, ob eine App bösartige oder anfällige Komponenten enthält, wird häufig auf dynamische Analyse zurückgegriffen [10]. Dazu werden zum Beispiel Methoden-Aufrufe so umgeleitet, dass der Analyst die Aufrufe und übergebenen Parameter nachvollziehen kann. Anhand dieser Informationen kann zum Beispiel festgestellt werden, ob eine bestimmte Methode mit unsicheren Parametern aufgerufen wird. Auch erlaubt diese Strategie zum Beispiel das Reverse-Engineering von proprietären und verschlüsselten Kommunikations-Protokollen. Schließlich kann diese Methode auch dazu genutzt werden, Sicherheitslücken in kompilierten Apps automatisiert zu beheben [11].

Um ähnliche Forschungsvorhaben unter iOS umzusetzen, müssen 2 zentrale Sicherheitsmechanismen umgangen werden. Auf Code Signing wurde hier schon im Detail eingegangen. Zusätzlich werden iOS-Apps beim Download vom App Store für das jeweilige Zielgerät mit dem proprietären FairPlay-Digital-Rights-Management-System (DRM) verschlüsselt. Entschlüsselt werden kann die App nur mit einem Schlüssel, der im separaten Sicherheits-Chip (Secure Enclave) des Geräts liegt und diesen nie verlässt. In der Vergangenheit gab es zwar Lösungen, um beide Sicherheitsmechanismen zu umgehen. Allerdings benötigten diese einen Jailbreak, also das weiträumige Ausschalten der Sicherheitsarchitektur des Geräts durch Ausnutzung mehrere Schwachstellen im Betriebssystem. Ein Jailbreak ist immer mit erheblich erhöhtem Sicherheitsrisiko verbunden und daher für Endanwender nicht zu empfehlen. Außerdem besteht die Möglichkeit, dass Apps erkennen, wenn sie auf einem gejailbreakten Gerät ausgeführt werden, und den Dienst in einer solchen Umgebung verweigern.

3. Digital Markets Act

Mit dem Digital Markets Act (DMA) [3] hat sich die EU zum Ziel gesetzt, für faire Voraussetzungen für alle Beteiligten in neu entstandenen digitale Markplätzen zu sorgen. Das Gesetz wurde im September 2022 beschlossen und trat im November desselben Jahres in Kraft. Seit Mai 2023 wurden dann Gatekeeper identifiziert und dazu aufgefordert, ihre Plattformen DMA-konform umzugestalten.

3.1. Gatekeeper

Der DMA betrifft insbesondere Firmen, die als Gatekeeper eines neu geschaffenen digitalen Marktes auftreten. Diese Gatekeeper werden anhand klarer im Gesetzestext definierter Kriterien identifiziert. Zunächst muss ein Unternehmen in der Lage sein, bedeutenden Einfluss auf einen Markt zu nehmen (in Form eines sogenannten „Core Platform Service", der den Zugang Anderer zum Markt bestimmt. Außerdem muss der entsprechende Markt einen gewissen Maßstab erreichen. Hier wird der vom Unternehmen erwirtschaftete Umsatz herangezogen. Schließlich müssen auch zumindest 45 Millionen Endnutzer (Kunden) aus der EU am Markt beteiligt sein, sowie 10.000 Produkt-Anbieter aus der EU. Der Markt muss außerdem für zumindest 3 EU-Länder zugänglich sein.

Im September 2023 wurden von der EU die erste 6 Gatekeeper genannt: Es handelte sich um Alphabet, Amazon, Apple, ByteDance, Meta und Microsoft [12]. Apple war hier als Gatekeeper des iOS-Betriebssystems und des entsprechenden App Stores (sowie des Safari-Browsers) betrachtet worden. Zunächst bestand Apple darauf, dass nur der App Store für iOS (nicht aber der für iPadOS) die Gatekeeper-Kriterien erfülle, und setzte die Forderungen des DMA schließlich auch nur für diese Plattform fristgerecht um. Im April 2024 verkündete die EU allerdings, dass Apple auch in Bezug auf iPadOS als Gatekeeper auftritt [13]. Zwar waren hier die offiziell von Apple angegebenen Endnutzerzahlen etwas unter dem offiziellen Grenzwert, doch die Anzahl an Produkt-Anbieter aus der EU überstieg den Grenzwert bei weitem. Angesichts des prognostizierten Wachstums der Nutzerzahlen wurde entschieden, hier der Entwicklung schon etwas vorauszugreifen. Ab dem Zeitpunkt der offiziellen Ankündigung hatten die Unternehmen jeweils 6 Monate Zeit, um die Forderungen des DMA umzusetzen.

3.2. Forderungen

Der DMA sieht vor, dass jeder Gatekeeper sicherstellen muss, dass andere am Markt beteiligte Unternehmen („Drittanbieter") die gleichen Voraussetzungen haben wie der Gatekeeper selbst.

Beispielsweise nennt die EU hier folgende Pflichten von Gatekeepern (nach [14]):

- Drittanbietern erlauben, mit den eigenen Services des Gatekeepers in bestimmten Situationen zusammenzuarbeiten
- Drittanbietern erlauben, Daten einzusehen, die sie durch die Verwendung der Plattform des Gatekeepers generieren
- Firmen, die auf ihrer Plattform werben, mit den Werkzeugen und Informationen ausstatten, die notwendig sind, damit Werbeunternehmen und Publisher ihre eigenen unabhängigen Überprüfungen der vom Gatekeeper gehosteten Werbeanzeigen durchführen können
- Drittanbietern erlauben, Endnutzer über Angebote abseits der Plattform des Gatekeepers zu informieren, bzw. dort Verträge mit dem Endnutzer abzuschließen

Außerdem müssen Gatekeeper unter anderem die folgenden Wettbewerbsverzerrungen unterlassen (nach [14]):

- Services und Produkte des Gatekeepers in Rankings gegenüber ähnlichen Services oder Produkten anderer Anbieter bevorzugen
- Nutzer davon abhalten, vorinstallierte Software zu deinstallieren

4. Umsetzung des DMA durch Apple

4.1. Erwartungen

Zur Umsetzung des DMA wurde von Apple verlangt, die App-Installation von Quellen außerhalb des offiziellen App-Stores zu erlauben. Bei vorgabengetreuer Einhaltung des DMA hätte dies bedeutet, dass ähnlich wie unter Android die Installation von Apps ermöglicht worden wäre, die vom Entwickler selbst signiert wurden. Nachdem außerdem die App nie an Apple übermittelt worden wäre (und dort verschlüsselt werden hätte können), hätte die App wohl auch in unverschlüsselter Form installiert werden müssen. Damit wären beide Sicherheitsmechanismen deaktiviert werden müssen, die den unter 2.2 erwähnten Forschungsmöglichkeiten im Wege standen.

Zusätzlich wäre auch zu erwarten gewesen, dass Drittanbieter-Anwendungen weitreichenden Zugriff auf fortgeschrittene Funktionalitäten des iOS-Betriebssystems erlangt hätten, die bislang Anwendungen von Apple vorbehalten waren. Erwähnenswert wäre hier etwa die Möglichkeit, dynamisch allozierte Speicherseiten als ausführbar zu mappen.

4.2. Tatsächliche Umsetzung

Schon während der Verhandlungen mit der EU zum DMA hatte Apple mehrmals darauf bestanden, dass deren Umsetzung mit erheblichen Sicherheitsrisiken für Endanwender verbunden wäre. Auch als mit iOS 17.4 schließlich DMA-Konformität bekannt gegeben wurde, war die offizielle Mitteilung geprägt vom Versuch, den Fokus der Öffentlichkeit auf die Sicherheitsbedenken zu lenken, statt auf die neuen Möglichkeiten für Endnutzer und Unternehmer, gleichberechtigt an der Plattform teilzuhaben.

Zwar erlaubt iOS 17.4 erstmals die Installation von Anwendungen aus Quellen abseits des Apple App Store (genauer von Websites oder aus Dritt-Anbieter-App-Stores), allerdings muss weiterhin jede App vor der Veröffentlichung von Apple geprüft werden [4]. Die nun „Notarization" genannte Prüfung soll laut Apple sicherstellen, dass im Wege der Installation aus externen Quellen keine Schadsoftware auf Endgeräte gelangen kann. Erst nach der Notarization stellt Apple eine verschlüsselte und durch Apple signierte Version der App zur Verfügung, die auf Endgeräten installiert werden kann.

Bevor Entwickler in der EU diese neuen Distributions-Möglichkeiten nutzen können, müssen sie ein gesondertes Abkommen mit Apple unterschreiben. Besonders erwähnenswert ist hier die sogenannte „Core Technology Fee". Dabei handelt es sich um eine Abgabe von 0,5€, die für jeden Download an Apple entrichtet werden muss, der über 1 Million Downloads pro Jahr hinausgeht. Für Anbieter von Dritt-Anbieter-App-Stores muss diese Abgabe für jeden Download (ab dem ersten Download) erfolgen.

4.3. Konsequenzen für die Sicherheitsforschung

Die Möglichkeiten für die Umsetzung der in 2.2 beschriebenen Forschungsprojekte unter iOS bleiben weiterhin stark eingeschränkt. Im Wesentlichen hat Apple entgegen den Erwartungen die Sicherheitsarchitektur von iOS nicht verändert. Da Apps noch immer von Apple signiert und verschlüsselt werden, bevor sie an Endkonsumenten ausgeliefert werden, bleibt Jailbreaking (mit allen damit verbundenen Konsequenzen) ein wichtiges Werkzeug in der Sicherheitsforschung.

4.4. Weitere Entwicklungen

Mehrere Untersuchungen zur DMA-Konformität von Apple sind derzeit anhängig. Im Juni 2024 veröffentlichte die EU einen ersten Zwischenbericht [15]., wonach das neue gesonderte Entwickler-Abkommen, das die Möglichkeit zur Information über externe Bezahlmethoden an andere Abrechnungsmodelle knüpft, unzulässig wäre. Außerdem teilte die EU mit, dass eine neue Untersuchung klären soll, ob Apple mit der „Core Technology Fee"-Abgabe gegen die Vorgaben des DMA verstößt.

5. Zusammenfassung

In diesem Projekt wurde untersucht, welche Auswirkungen der Digital Markets Act auf die Sicherheitsarchitektur des iOS-Betriebssystems hat, bzw. ob durch die Änderungen neue Möglichkeiten für die Sicherheitsforschung entstanden sind. Es zeigt sich, dass die bisherigen Anpassungen keine neuen Forschungsmöglichkeiten zulassen, da Apple in der Umsetzung des DMA sehr konservativ vorgegangen ist. Angesichts der laufenden Untersuchungen der EU bleiben die Entwicklungen der nächsten Monate abzuwarten.

Referenzen

[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/developers-generated-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/legal-content/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/app-store/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-ipados-under-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-for-gatekeepers. [Zugriff am 2024].

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