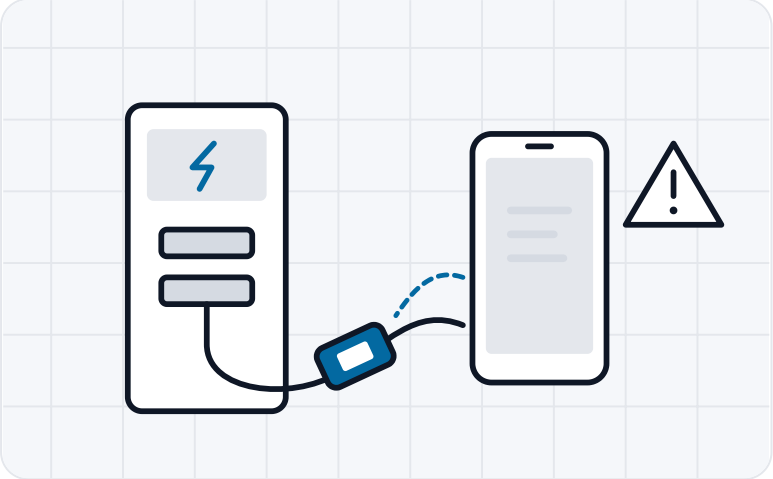
A-SIT Technology
E-Government Innovationszentrum

25. Jänner 2024 Überblick · Mobile Sicherheit · 20 Min. Lesezeit

Aktuelle Juice-Jacking-Angriffe und Gegenmaßnahmen für Mobilgeräte

Florian Draschbacher



Autorinnen und Autoren	Florian Draschbacher
Stand	2024-01-17
Quelle	https://technology2.a-sit.at/veroeffentlichungen/aktuelle-juice-jacking-angriffe-und-gegenmassnahmen-fuer-mobilgeraete/

Kernaussagen

- Seit iOS 7 bzw. Android 4.2 muss der Nutzer USB-Datenverbindungen bestätigen; dennoch sind abgewandelte Juice-Jacking-Formen weiter möglich.
- Die Angriffe nutzen USB-OTG-Funktionen (Eingabe, Video, Audio) oder den Power-Line-Seitenkanal, also Schwankungen im Ladestrom.
- Der Power-Line-Seitenkanal braucht keine Datenverbindung, daher helfen USB Data Blocker nicht; die Angriffe laufen meist nur unter kontrollierten Bedingungen.
- USB Data Blocker sind nur noch eingeschränkt zu empfehlen, etwa weil sie bei Angriffen im Kabel nutzlos sind.

- Am wirksamsten gilt eine Nutzerbestätigung im Betriebssystem auch für den USB-Host-Modus; öffentliche Ladestationen nur im Notfall nutzen.

Juice-Jacking bezeichnet eine Familie von Angriffen auf Mobilgeräte, in denen ein manipuliertes Ladekabel dazu genutzt wird, Daten zu extrahieren oder Malware zu installieren. Anfällig für diese Attacke sind Nutzer insbesondere überall dort, wo anstelle eines eigenen Ladegeräts bestehende Infrastruktur genutzt wird, etwa in Form von Ladestationen an Flughäfen. Zwar ist der generelle Angriffsmechanismus schon seit mehreren Jahren bekannt, doch werden immer neue Möglichkeiten gefunden, Gegenmaßnahmen zu umgehen.

Im Rahmen dieses Projektes wurde ein Überblick über verschiedene Möglichkeiten zum Juice-Jacking erarbeitet. Zusätzlich zu einer Literaturrecherche bezüglich bestehender Ansätze wurden Überlegungen angestellt, wie neuartige Angriffe technologische Änderungen an den Ladeschnittstellen von Mobilgeräten so ausnutzen können, dass bestehende Gegenmaßnahmen umgangen werden.

1. Einleitung

Im Gegensatz zu traditionellen Computersystemen sind die physischen Geräteabmessungen bei mobilen Endgeräten wie Smartphones oder Tablets entscheidende Verkaufsargumente. Um bei Wahrung geringer Geräteabmessungen trotzdem kabelgebundene Interkonnektivität mit Zubehör und Computern bereitzustellen, verfügen mobile Geräte über einen einzigen Anschluss, der sowohl zur Stromversorgung als auch zur Datenübertragung genutzt werden kann.

Die Funktionsfülle dieses Anschlusses wurde bald nach der Einführung der ersten Smartphones auch als Schwachstelle erkannt. Für den Nutzer ist häufig die Funktionsweise eines an das Smartphone angesteckten Gerätes nur anhand dessen äußerer Erscheinung ablesbar. Verhält sich aber ein verbundenes Gerät nicht so, wie dessen Erscheinung vermuten lässt, so hat ein durchschnittlicher Endanwender keine Möglichkeit, diese Täuschung zu erkennen.

Die bekannteste Form eines Angriffes, der auf einer solchen Täuschung basiert, sind Juice-Jacking-Attacken. Dabei werden über eine manipulierte Ladebuchse oder ein manipuliertes Ladekabel Daten vom Mobiltelefon extrahiert. Während für den Endanwender kein Unterschied zum normalen Ladevorgang besteht, erhält der Angreifer Zugriff etwa auf die am Telefon gespeicherten Fotos, Passwörter, Dokumente, uvm. Teilweise ist selbst die Installation von Apps am Gerät möglich, sodass der Angreifer auch nach dem Lösen der physischen Verbindung noch Zugriff auf Nutzerdaten hat.

Die ursprüngliche Form dieses Angriffes wurde vor etwa 10 Jahren öffentlich diskutiert und führte rasch zu Gegenmaßnahmen, die in die mobilen Betriebssysteme Android und iOS integriert wurden. Dennoch sind verschiedene abgewandelte Formen des Angriffs noch immer möglich.

Wiewohl noch keine bösartigen Juice-Jacking-Angriffe auf Endanwender dokumentiert wurden, warnen öffentliche Stellen in regelmäßigen Abständen vor der Gefahr, die von potentiell manipulierter frei zugänglicher Handy-Lade-Infrastruktur an Flughäfen oder Einkaufszentren ausgeht. So warnten 2023 die

US-Sicherheitsbehörde FBI [1] sowie die US-Behörde für Kommunikationstechnologie FCC [2] erneut insbesondere Reisende, öffentliche Ladeinfrastruktur soweit als möglich zu meiden. Kurz danach entbrannte auf verschiedenen IT-Nachrichten-Websites eine Diskussion über die Sinnhaftigkeit dieser Warnungen [1], [2]. Kritiker warfen den Behörden vor, dass die Gefahr durch die Änderungen im Betriebssystem schon lange gebannt worden war.

In diesem Bericht soll die Sachlage bezüglich Juice-Jacking eingehend untersucht werden. Dazu erläutern wir die Grundlagen der beteiligten Steckverbindungen und fassen verschiedene aktuelle Angriffe aus wissenschaftlichen Quellen zusammen. Zusätzlich diskutieren wir die Effektivität vorhandener Gegenmaßnahmen gegen Juice Jacking und bieten einen Ausblick auf neue Entwicklungen.

2. Hintergrund

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

2.1. USB

Bei USB, dem Universal Serial Bus, handelt es sich um eine Schnittstelle, mit der Peripheriegeräte an einen Computer angeschlossen werden können. Bei dem Standard handelt es sich um den ersten erfolgreichen Versuch, die vielen proprietären Konnektoren, die bis dahin von verschiedenen Herstellern für die unterschiedlichsten Ein- und Ausgabegeräte genutzt wurden, zu vereinheitlichen. Seit der Einführung Mitte der 1990er-Jahre hat sich USB im Endnutzer-Bereich für nahezu jede Art von Peripheriegerät durchgesetzt. Es gibt USB-Mäuse und -Tastaturen, Festplatten, DVD-Laufwerke und andere Speichermedien, die den Anschluss ebenso nutzen wie Drucker, Kameras, und viele mehr. Die weite Verbreitung des USB-Standards und entsprechender Buchsen führte nach wenigen Jahren schon soweit, dass viele Geräte USB-Anschlüsse zur Stromversorgung verwenden, selbst wenn sie gar keine Ein- oder Ausgabegeräte sind. So gibt es mittlerweile Fahrradlichter oder Ventilatoren, die am USB-Anschluss geladen bzw. betrieben werden können.

Jede Kommunikation findet bei USB zwischen einem USB-Host und einem USB-Device statt. Der USB-Host ist hier das Gerät, das die Kontrolle über die Verbindung hat und im Wesentlichen Funktionalität oder Daten vom USB-Device anfordern kann. In umgekehrter Richtung fließen Daten nur dann, wenn dies vom USB-Host veranlasst wurde. Es kann also von einer gerichteten Kommunikation gesprochen werden.

Konzeptionell werden Daten bei der Nutzung von USB immer nur zwischen einem USB-Host und einem USB-Device übertragen (nicht also zwischen mehreren USB-Hosts oder mehreren USB-Devices). Es besteht allerdings die Möglichkeit, an einem USB-Host mehrere USB-Devices zu betreiben. Realisiert wird diese Bus-Topografie mittels USB-Hubs, die Kommunikations-Pakete vom Host an mehrere verschiedene Devices weiterleiten können. Man kann bei USB also von einer baumförmigen Bus-Architektur sprechen.

Wird ein USB-Device an einen Host angesteckt, so beginnt der Host die Kommunikation, indem er das Device nach dessen Deskriptoren befragt. Es handelt sich dabei um Datenstrukturen, die Aufschluss über die Eigenschaften des USB-Geräts geben. Übertragen werden hier zum Beispiel der Hersteller- und Produktname des Geräts, ebenso wie die zur Verfügung gestellte Funktionalität des Geräts in Form von Interface-Deskriptoren. Mittels dieser Deskriptoren ist es dem Host möglich, den Typ des angeschlossenen Geräts zu ermitteln und einen entsprechenden Gerätetreiber zu laden.

2.2. USB-Anschlüsse und -Versionen

Seit der ersten Veröffentlichung des USB-Standards Mitte der 1990er-Jahre [3] wurden mehrere Überarbeitungen publiziert. Im Wesentlichen unterschieden sich die Überarbeitungen von ihren jeweiligen Vorgängern durch die Möglichkeit zu höherer Datenübertragungsrate. Während weitgehende Rückwärtskompatibilität zu älteren USB-Standards besteht, wurden auch neue Funktionalitäten eingeführt, die Hardware-Änderungen benötigten.

In den ersten beiden Version 1.0 und 1.1 [4] sieht der USB-Standard Anschlüsse ausschließlich mit 4 Verbindungen vor. Dabei sind 2 Verbindungen (Pins) für die Stromversorgung des USB-Devices in Verwendung (5V bzw. Masse/Ground), sowie ein differenzielles Leitungspaar der Datenübertragung gewidmet.

Es wurden verschiedene USB-Buchsen bzw. -Stecker spezifiziert, die die Rolle des jeweiligen Anschlusses in der USB-Verbindung festlegen. Hier wird zwischen den folgenden Anschlüssen unterschieden:

- USB-A: Es handelt sich hier um den gängigen USB-Anschluss, wie er etwa von USB-Sticks bekannt ist. USB-Host ist immer jenes Gerät, das über die USB-A-Buchse verfügt.
- USB-B: Bei USB-Devices, die kein fix verbautes Kabel (oder keinen fix verbauten USB-A-Stecker) haben, kommt eine USB-B-Buchse zum Einsatz. Geräte, die über eine USB-B-Buchse (nach USB 1.0 bzw. 1.1) verfügen, arbeiten stets in der Rolle als USB-Device (sind also niemals Host).

Eine wesentliche Änderung in Version 2.0 des USB-Standards [5] in Bezug auf Juice-Jacking-Angriffe war die Einführung von USB On-The-Go [6]. Es handelt sich dabei um die Möglichkeit, ein USB-fähiges Gerät sowohl als Device als auch als Host nutzen zu können. Umgesetzt wurde diese Möglichkeit, indem die neu eingeführten verkleinerten Varianten der USB-A- und USB-B-Verbindungen (Mini USB sowie Micro USB) mit einem zusätzlichen Pin ausgestattet wurden. Verschiedene Belegungen dieses Pins signalisieren die Rolle des verbundenen Geräts in der USB-Verbindung. OTG-fähige Geräte prüfen nach Herstellung der physischen Verbindung den Status dieses sogenannten ID- oder Sense-Pins, um ihren USB-Stack in den jeweils passenden Modus zu schalten. Die Regelung, welcher Kommunikationspartner die Rolle als Host bzw. Device übernimmt, wird hier also immer noch in Hardware fixiert. Es stehen verschiedene Kabel zur Verfügung, in denen die Beschaltung des ID-Pins am Micro-USB-B-Konnektor entweder den Anschluss von USB-Peripheriegeräten (wie Mäuse, Tastaturen, etc.) an eine USB-OTG-Buchse erlaubt, oder eine Verbindung des OTG-fähigen Gerätes an einen Computer.

Micro-USB-Anschlüsse (häufig auch OTG-fähig) fanden vor der Einführung von USB Type-C weite Verbreitung bei Smartphones und Tablets, insbesondere solchen, die mit Android betrieben wurden.

Version 3.0 des USB-Standards [7] führte zusätzliche Pins im USB-A-Konnektor sowie neue abwärtskompatible Micro- bzw. Mini-Anschlüsse ein. Die zusätzlichen Pins erlauben durch zwei parallele Datenpaare schnellere Übertragungsgeschwindigkeiten.

2.3. Lightning

Im Unterschied zu Geräten mit dem Betriebssystem Android stattete Apple seine Geräte nicht mit einer Micro-USB-Schnittstelle aus, sondern setzte in der Vergangenheit stets auf proprietäre Anschlüsse. Frühe iPhones und iPads verfügten über einen 30-Pin-Anschluss, der dedizierte Verbindungen für alle

verfügbaren Zubehörarten enthielt. So trugen einige der Pins etwa analoge Audio-Signale oder USB-Signale für den Anschluss von USB-Sticks.

Um die Abmessungen der Geräte und das Nutzererlebnis weiter zu optimieren ersetzte Apple den 30-Pin-Anschluss 2012 durch den immer noch proprietären aber zeitgemäßeren Lightning-Anschluss. Dieser verfügt auf jeder Seite über eine Reihe von 8 Pins. Das damit verbundene Mobilgerät kann erkennen, welche Art von Kabel in welcher Orientierung verbunden wurde, und beschaltet die 16 Pins entsprechend mit Signalen. Zur Verwirklichung dieses Verfahrens kommuniziert das iPhone oder iPad mit einem im Kabel verbauten Chip. Das Gegenstück im iPhone schaltet dann mittels Multiplexing die benötigten Signale frei.

2.4. USB Type-C

Seit etwa fünf Jahren setzt sich unter Mobilgeräten immer mehr der USB Type-C Standard [8] durch. Es handelt sich um einen neuen USB-Konnektor, der einige Vorteile gegenüber Micro-USB (Typ B) hat:

- Umdrehbar Der Stecker kann in beiden Orientierungen in die Buchse gesteckt werden.
- Höhere Datenraten Durch höhere Anzahl an Pins können Datenraten von mehreren Gbit/s erreicht werden.
- Höherer Ladestrom Der Konnektor wurde für mindestens 15 Watt Leistung ausgelegt.

An dieser Stelle muss festgehalten werden, dass der USB Type-C-Anschluss weitgehend unabhängig von der USB-Spezifikation genutzt werden kann, die die Datenübertragung regelt. Konkret bedeutet das, dass Geräte mit USB Type-C teils nur USB 2.0-Geschwindigkeiten zur Datenübertragung unterstützen. Für den neuesten USB 4.0-Standard wird allerdings verpflichtend die Nutzung des Type-C-Anschlusses vorgeschrieben. Damit wird die Unterscheidung zwischen Host und Device auf Anschluss-Ebene, die bis USB 3.0 noch immer in Teilen vorhanden war, abgeschafft.

Während frühe Anwender von Type-C diesen einfach als physische Steckverbindung für einen USB 2.0-Anschluss nutzten, bietet heutzutage nahezu jedes mobile Endgerät auch Unterstützung für Power Delivery [9]. Es handelt sich dabei um ein zusätzliches Kommunikationsprotokoll, mit dem zwei per USB Type-C verbundene Geräte Details über ihren Daten- und Strom-Austausch vereinbaren können. Diese Kommunikation findet über ein separates Pin-Paar im USB-Type-C-Konnektor statt. Neben einigen standardisierten Nachrichten erlaubt Power Delivery es Geräteherstellern auch, das Protokoll durch proprietäre Nachrichten zu erweitern.

3. Juice Jacking

Juice-Jacking-Angriffe sind in der Literatur immer nur von Forschungsprojekten dokumentiert, die zum Ziel hatten, die Öffentlichkeit vor der technischen Möglichkeit solcher Angriffe zu warnen. Es stehen keine Berichte über tatsächlich durchgeführte Angriffe abseits von Forschungsumgebungen zur Verfügung, was dennoch nicht bedeutet, dass solche nicht stattgefunden haben können.

Die geistigen Geschwister von Juice-Jacking-Angriffen können in Bad-USB-Angriffen für klassische Computersysteme gefunden werden. Bei diesen kommen Geräte zum Einsatz, die optisch den Eindruck eines Massenspeichers im USB-Stick-Format erwecken, aber tatsächlich auf technischer Ebene wie USB-Eingabegeräte (etwa Maus oder Tastatur) operieren. Der Angriff sieht vor, dass unbedarfte Nutzer eines

dieser Geräte vorfinden und aus Neugierde auf die am scheinbar harmlosen USB-Stick abgespeicherten Inhalte an ihren Computer stecken. Dort kann das simulierte Eingabegerät dann etwa dazu genutzt werden, eine Abfolge an Input-Events zu generieren, die zum Beispiel Malware am Computer installiert. Angriffe dieser Art wurden in der Vergangenheit von Hacker-Gruppen benutzt, um etwa Zugang zu internen Computernetzwerken großer Unternehmen zu erhalten [3] [4].

Juice Jacking selbst wurde erstmals 2011 auf der Computer-Sicherheitskonferenz Defcon gezeigt [10]. Es handelte sich bei der ursprünglichen Umsetzung um eine scheinbar harmlose Ladestation für Mobilgeräte. Tatsächlich wurden angesteckte Geräte allerdings nicht nur mit Strom versorgt. Stattdessen bauten in die Ladestation integrierte Computer eine Datenverbindung zum Mobilgerät auf, über die dann Daten vom Gerät kopiert werden konnten. Hier wurde die Tatsache ausgenutzt, dass Android- und iPhone-Geräte zur damaligen Zeit jedem angeschlossenen Computer standardmäßig vertrauten. Das Betriebssystem nahm an, dass die Verbindung zum Computer vom Nutzer bewusst initiiert worden war, und stellte daher ohne weitere Rücksprache mit dem Nutzer eine Datenverbindung her.

2013 präsentierten Lau et al. auf der Computer-Sicherheitskonferenz Black Hat erneut einen Angriff namens Mactans [11], der den Zugriff auf den Geräte-Anschluss während des Ladens dazu nutzte, über die Debugging-Schnittstelle Apps auf einem iPhone zu installieren.

Nachdem die Schwachstelle ausführlich öffentlich demonstriert worden war, reagierten Google und Apple mit Änderungen an ihren mobilen Betriebssystemen. Seit iOS 7 bzw. Android 4.2 müssen USB-Datenverbindungen zwischen einem Computer (als Host) und dem Mobilgerät (als Device) vom Nutzer über einen Dialog bestätigt werden, bevor der Zugriff auf Dateien oder die Debugging-Schnittstelle gewährt wird.

4. Aktuelle Juice-Jacking-Varianten

Als Teil dieses Forschungsprojekts wurde untersucht, in welcher Form Juice-Jacking noch heute möglich ist. Dazu wurden Publikationen analysiert, die die physische Verbindung beim Laden dazu benutzen, entweder Daten vom Mobilgerät zu extrahieren, oder dessen Zustand zu manipulieren.

In der Literatur ergeben sich hier die folgenden Kategorien von Angriffen:

4.1. Ausnutzung der USB-OTG-Funktion

Seit der Version 3.1 (Tablets) bzw. 4.0 (Smartphones) unterstützt das Android-Betriebssystem USB OTG, also den Betrieb von USB-Eingabe- und Ausgabegeräten wie Mäuse, Tastaturen und Massenspeichergeräten am USB-Anschluss. Die meisten aktuellen Android-Geräte unterstützen den Anschluss solcher Geräte noch immer, allerdings wird hierzu nun nicht mehr USB OTG verwendet, sondern USB-Type-C. Aus Gründen der einfacheren Nutzbarkeit ist für den Betrieb dieses Zubehörs keine Bestätigung des Nutzers erforderlich. Mittels Power Delivery ist es hier einfach möglich, das Android-Gerät gleichzeitig mit Strom zu versorgen und dennoch in den USB-Host-Modus zu versetzen. Bei Geräten mit Micro-USB-Anschluss ist hierfür eine spezielle Beschaltung des ID-Pins nötig, die nicht mit allen Gerätemodellen kompatibel ist.

Auch aktuelle Versionen von iOS und iPadOS unterstützen die Verbindung von USB-Peripheriegeräten. Bei Geräten, die noch den Lightning-Anschluss benutzen (iPhones bis Modell 14), ist dazu ein proprietärer Adapter nötig, der den entsprechenden Apple-Chip enthält, um das iPhone zur Freischaltung des USB-Host-Modus am Lightning-Anschluss zu bewegen. Bei neueren Geräten (iPhone ab Modell 15) kann ein Standard-USB-C-Kabel verwendet werden. Das Laden im USB-Host-Modus ist bei beiden Anschlüssen möglich. Es ist darüber hinaus erwähnenswert, dass aktuelle iOS-Versionen verbundenen USB-Peripheriegeräten nur vertrauen, wenn sie angesteckt werden, während das Mobilgerät entsperrt ist.

Die verschiedenen Angriffe unterscheiden sich im Wesentlichen im USB-Peripheriegerät, das sie verwenden, um Daten abzuschöpfen.

Input-basierte Angriffe (BadUSB) Ähnlich der oben genannten Attacke gegen klassische Computersysteme werden hier von der bösartigen Ladestation mittels Simulation einer Tastatur oder Maus Input-Events injiziert. Mittlerweile stehen hier sogar schon kommerzielle Produkte wie das O.M.G.-Kabel von Hak5 [5] zur Verfügung, die die komplette Hardware, die für den Angriff notwendig ist, im Ladekabel verstecken. Dadurch werden simple Gegenmaßnahme wie USB Data Blockers, die die Datenleitungen an der USB-Buchse des Ladegeräts kappen, umgangen.

Angriffe dieser Kategorie haben aber den entscheidenden Nachteil, dass sie unmittelbar keine Extraktion von Daten erlauben (da sie lediglich Eingabegeräte simulieren). Erst durch automatisierte Interaktion mit der Benutzeroberfläche des Mobilgeräts können Daten über einen separaten Kanal (etwa Internet) geteilt werden. Diese Interaktion bleibt aber aller Wahrscheinlichkeit nach nicht vor dem Nutzer verborgen.

Video-basierte Angriffe (Video Jacking / Juice Filming) Hier wird im bösartigen Ladegerät ein HDMI-Adapter eingebettet oder simuliert, der sonst dazu dient, den Bildschirminhalt des Mobilgeräts an einen Fernseher oder Beamer zu übertragen. Mit diesem Angriff können sensible Informationen, die am Display sichtbar sind, vom Gerät extrahiert werden. Es kann sich hierbei zum Beispiel um Login-Informationen oder Emails handeln.

Der Angriff wurde im wissenschaftlichen Kontext erstmalig 2015 von Meng et al. vorgestellt [12]. In einer späteren Publikation erweiterten sie den Ansatz um ein System für automatische Buchstabenerkennung [13], mit dem textuelle Daten automatisiert aus der Benutzeroberfläche extrahiert werden konnten.

Angriffe dieser Kategorie leiden unter einigen Einschränkungen:

- Sie benötigen Hardware-Support. Während Apple-Geräte mithilfe eines proprietären Adapters und Protokolls schon länger die Bildausgabe über 30-Pin- oder Lightning-Anschluss unterstützten, war dies nur auf wenigen Android-Geräten mit Micro-USB möglich, für die je nach Hersteller unterschiedliche Adapter (etwa. MHL) nötig waren. Der USB-C-Anschluss bietet mit DisplayPort AltMode zwar einen einheitlichen Standard für die kabelgebundene Bildübertragung, allerdings wird auch dieser nur verlässlich von Apple-Geräten mit USB-Type-C unterstützt. Bei Android-Geräten hängt die Unterstützung vom jeweiligen Geräte-Hersteller ab. Samsung etwa verbaut die notwendige Hardware nur bei den teuren Flagship-Modellen, während Google bei der Vorzeige-Serie Pixel sogar gänzlich auf die Unterstützung von USB-C DP AltMode verzichtet.
- Die Eingabe des Geräte-Pins wird (bei aktuellem OS) nicht auf das externe Display übertragen. Der Angriff kann also nicht dazu benutzt werden, die Gerätesperre zu umgehen.

- Die Bildschirm-Freigabe wird vom Betriebssystem kommuniziert. Je nach Gerät wird der Nutzer im Statusbalken des Betriebssystems darüber informiert, dass ein externer Monitor angesteckt ist. Er hat also eine Möglichkeit, den Angriff zu erkennen und zu unterbinden.
- Der Angreifer hat keine Kontrolle über das Gerät Er kann lediglich Daten extrahieren, die in der Benutzeroberfläche des Geräts sichtbar sind. Die Daten müssen dabei außerdem erst aus der visuellen Benutzeroberfläche getrennt werden.

Audio-basierte Angriffe Viele Mobilgeräte unterstützen die Audio-Ein- sowie Ausgabe über ihren Multifunktionsanschluss. Seit der Einführung von system-weiten Sprachassistenten in mobilen Betriebssystemen kann auch diese Funktionalität für einen Angriff missbraucht werden. Dieser Angriff wurde erstmals 2022 von Wang et al. beschrieben [14]. Die Forscher manipulierten ein Ladekabel so, dass der Angreifer Audio-Eingabe erzeugen kann (ein virtuelles Mikrofon anschließt), sowie die Audio-Ausgabe abfangen kann. Durch Interaktion mit dem Sprachassistenten kann so die komplette Input-Output-Schleife kontrolliert werden.

Der Ansatz hat dennoch einige Nachteile:

- Der Sprachassistent muss aktiviert sein.
- Eingeschränkter Datenzugriff. Es können lediglich jene textbasierten Inhalte extrahiert werden, die vom Sprachassistenten zugänglich gemacht werden. Jede Datenausgabe muss außerdem erst mittels Speech-To-Text in Daten rückumgewandelt werden, die vom Computer sinnvoll verarbeitet werden können.

4.2. Ausnutzung des Power-Line-Seitenkanals

Jedes elektronische Gerät benötigt Strom für seinen Betrieb. Eine Eigenschaft, die in jüngerer Vergangenheit für eine ganze Reihe an sicherheitstechnischen Forschungsarbeiten ausgenutzt wurde, ist die Tatsache, dass der Stromverbrauch einiger in Computersystemen verbauter Komponenten von den gerade verarbeiteten Daten bzw. Befehlen abhängt. Diese Eigenschaft ist besonders auch für Juice-Jacking-Angriffe sehr relevant. Während des Ladevorgangs speisen Mobilgeräte nämlich nicht nur ihren Akku mit dem Strom aus dem Ladegerät, sondern decken von dort auch ihren für den Betrieb anfallenden Verbrauch. Ein angeschlossenes Ladegerät kann also anhand des Ladestroms Rückschlüsse über die aktuell am Mobilgerät ausgeführten Operationen ziehen. Über elektromagnetische Effekte können außerdem durch bewusste Kontrolle der Stromversorgung Sensorwerte am Mobilgerät manipuliert werden. Alle diese Angriffe benötigen keine Datenverbindung zum Mobilgerät. Gängige Gegenmaßnahmen wie USB Data Blocker sind also gegen sie nicht effektiv. Es muss allerdings angemerkt werden, dass die meisten dieser Angriffe jeweils nur bei kontrollierten Bedingungen funktionieren. Die verwendeten mathematischen Modelle werden etwa anhand bestimmter Mobilgeräte optimiert, und funktionieren dann nur genau für diese.

Extraktion von Daten Yang et al. präsentierten 2016 einen Ansatz, der mittels Schwankungen im Ladeverbrauch eines Mobilgeräts Rückschlüsse auf die gleichzeitig im Browser am Gerät besuchten Websites ziehen kann [15]. Die Forscher konnten zeigen, dass selbst Faktoren wie der aktuelle Ladestand

des Akkus oder verschiedene Netzwerk-Verbindungen ihre Detektion kaum beeinflussen. Genkin et al. nutzten diesen Angriffsvektor 2016, um über die Ladeverbindung kryptografische Schlüssel vom Mobilgerät auszulesen [16].

Cronin et al. gelang es 2021, anhand des Stromverbrauchs beim Laden die Position von Änderungen des Bildschirminhalts zu erkennen [17]. Dies ist bei ausreichend hoher Messauflösung möglich, da moderne Bildschirme ihre Darstellung Pixel-für-Pixel sequentiell aufbauen und für jeden sich ändernden Bildpunkt einen erhöhten Strombedarf haben. Mittels dieses Ansatzes konnten die Forscher auf einer Anzahl an Testgeräten sogar Unlock-Pins bei der Eingabe mitlesen, da das visuelle Feedback beim Tastendruck die Position der gedrückten Taste verrät.

Übertragung von Daten Der Power-Line-Seitenkanal kann auch in umgekehrter Richtung zum Datenaustausch genutzt werden. Spolaor et al. schlagen eine Android-App vor, die die CPU des Geräts gezielt so auslastet, dass mittels Variationen im Stromverbrauch Daten an die ebenfalls vom Angreifer gestellte Ladeinfrastruktur übertragen werden können [18].

5. Mögliche Gegenmaßnahmen

Für die verschiedenen Arten der oben beschriebenen Angriffe stehen jeweils unterschiedliche Gegenmaßnahmen zur Verfügung.

Lange Zeit wurden gegen Angriffe, die die USB-Datenverbindung ausnutzen (etwa USB OTG) USB-Data-Blocker empfohlen. Diese können zwischen die USB-Buchse der Ladestation und das Ladekabel gesteckt werden und unterbrechen an dieser Stelle die Datenleitungen. Aufgrund neuerer Entwicklungen sind diese Lösungen allerdings nur noch eingeschränkt zu empfehlen:

- Sie sind nutzlos, wenn der Angriff im Kabel verbaut ist.
- Einige Hersteller nutzen proprietäre Lösungen, mit denen das Ladegerät dem Mobilgerät den erlaubten Ladestrom kommuniziert. Einige davon benutzen dazu die Datenleitungen. Werden diese gekappt, kann das Gerät nur langsam laden.
- iPhones und iPads mit Lightning-Anschluss beginnen den Ladeprozess erst nachdem sie Informationen über das benutzte Kabel eingeholt haben. Dies passiert über den sogenannten IDBUS-Pin. Derselbe Pin wird auch dazu verwendet, um JTAG (Hardware-Debugging) zu realisieren. Jedes funktionsfähige Ladegerät hat hier also zwangsläufig die Möglichkeit zum Hardware-Debugging.
- Mobilgeräte mit USB-C-Anschluss laden nur dann mit voller Geschwindigkeit, wenn die Kommunikation mit dem Ladegerät über Power Delivery möglich ist. Dazu werden die CC-Leitungen im Anschluss verwendet, die bei einigen Geräten ebenso dazu benutzt werden können, die Firmware des USB-Type-C-Controllers zu überschreiben.

Außerdem setzen diese Maßnahmen voraus, dass der Nutzer ein Bewusstsein für das Potential eines Angriffs hat. Es lässt sich hier also keine Massenwirksamkeit erreichen.

Die effektivste und weitreichendste Möglichkeit gegen Missbrauch der Datenverbindung im Ladeanschluss ist daher in einem Mechanismus im Betriebssystem zu sehen, der auch für den Anschluss von Peripheriegeräten (USB-Host-Modus) nach expliziter Bestätigung des Nutzers fragt. Ein äquivalenter Schutzmechanismus gegen Angriffe, die den USB-Device-Modus ausnutzen, hat sich in der Vergangenheit bewährt.

Aufgrund der Spezifizität der aktuellen Power-Line-Seitenkanal-Angriffe stellen diese für durchschnittliche Endanwender keine realistische Gefahr dar. Da die ausgenutzten Effekte teils bauartbedingt von der Hardware erzeugt werden, stehen für Endanwender keine Gegenmaßnahmen zur Verfügung.

Als einfache Gegenmaßnahme für Endanwender empfiehlt es sich, öffentliche Ladeinfrastruktur nur im Notfall zu verwenden und Vorsicht walten zu lassen. Erscheint nach dem Anschluss des Ladegeräts eine unerwartete Meldung am Gerät, so sollte die Verbindung umgehend gelöst werden.

6. Zukünftige Forschung

Aufgrund der breiten Nutzung von mobilen Geräten und der Sensibilität der häufig darauf verarbeiteten Daten werden auch Juice-Jacking-Angriffe ein aktives Forschungsfeld bleiben. Besonders in der Kombination mit USB-C, zu dessen Unterstützung die EU vor kurzem alle Gerätehersteller gezwungen hat, ergeben sich spannende Fragestellungen. So gibt es etwa noch keine Forschungen zu hybriden Juice-Jacking-Angriffen, oder zur Verbreitung und Anfälligkeit von Firmware Updates via USB Power Deliver.

Als Quelle spannender Forschungsfragen haben sich in der Vergangenheit insbesondere proprietäre Lösungen erwiesen. Beispiele mit Relevanz für Juice-Jacking waren hier beispielsweise die Erforschung proprietärer AT-Schnittstellen, die über USB angesprochen werden können durch Tian et al. [19] oder die Untersuchung von Vendor Defined Messages für USB Power Delivery durch Alendal et al. [20].

7. Zusammenfassung

In diesem Bericht beleuchteten wir Juice-Jacking-Angriffe auf Mobilgeräte. Nach der Erläuterung notwendiger Informationen zum USB-Standard und involvierter Konnektoren haben wir einen Überblick über die Entstehung von frühen Juice-Jacking-Angriffen geboten. Schließlich diskutierten wir verschiedene Ansätze für aktuelle Angriffe und entsprechende Gegenmaßnahmen.

Obwohl auf technischer Ebene nach wie vor das Potential für Angriffe besteht, sind aktuelle Angriffe entweder nur stark eingeschränkt zur Datenextraktion fähig oder müssen an ein konkretes Zielgerät angepasst werden.

Referenzen

[1] D. Goodin, „Ars Technica: Those scary warnings of juice jacking in airports and hotels? They're mostly nonsense," 05 2023. [Online]. Available: https://arstechnica.com/informationtechnology/2023/05/fearmongering-over-public-charging-stations-needs-to-stop-heres-why/. [Zugriff am 01 2024].

[2] B. Krebs, „Krebs on Security: Why is ‘Juice Jacking‘ Suddenly Back in the News?,“ 04 2023. [Online]. Available: https://krebsonsecurity.com/2023/04/why-is-juice-jacking-suddenly-back-in-thenews/. [Zugriff am 01 2024].

[3] Compaq, Digital Equipment Corporation, IBM PC Company, Intel, Microsoft, NEC, Northern Telecom, „Universal Serial Bus Specification,“ 01 1996. [Online]. Available: https://web.archive.org/web/20180130144424/https://fl.hw.cz/docs/usb/usb10doc.pdf. [Zugriff am 01 2024].

[4] Compaq, Digital Equipment Corporation, IBM PC Company, Intel, Microsoft, NEC, Northern Telecom, „Universal Serial Bus Specification Revision 1.1,“ 09 1998. [Online]. Available: https://fabiensanglard.net/usbcheat/usb1.1.pdf. [Zugriff am 01 2024].

[5] Compaq, Hewlett-Packard, Intel, Lucent, Microsoft, NEC, Philips, „Universal Serial Bus Specification Revision 2.0,“ 04 2000. [Online]. Available: http://sdpha2.ucsd.edu/Lab_Equip_Manuals/usb_20.pdf. [Zugriff am 01 2024].

[6] USB Implementers Forum, Inc, „On-The-Go Supplement to USB 2.0 Specification,“ 12 2001. [Online]. Available: https://www.rockbox.org/wiki/pub/Main/DataSheets/OTG1_0a.pdf. [Zugriff am 01 2024].

[7] Hewlett-Packard Company, Intel Corporation, Microsoft Corporation, NEC Corporation, ST-NXP Wireless, Texas Instruments, „Universal Serial Bus 3.0 Specification,“ 11 2008. [Online]. Available: http://www.softelectro.ru/usb30.pdf. [Zugriff am 01 2024].

[8] USB 3.0 Promoter Group, „Universal Serial Bus Type-C Cable and Connector Specification,“ 08 2014. [Online]. Available: https://www.usb.org/sites/default/files/USB%20Type-C%20Spec%20R2.0%20-%20August%202019.pdf. [Zugriff am 01 2024].

[9] USB 3.0 Promoter Group, „Universal Serial Bus Power Delivery Specification,“ 07 2012. [Online]. Available: https://www.usb.org/document-library/usb-power-delivery. [Zugriff am 01 2024].

[10] B. Krebs, „Krebs on Security: Beware of Juice-Jacking,“ 08 2011. [Online]. Available: https://krebsonsecurity.com/2011/08/beware-of-juice-jacking/. [Zugriff am 01 2024].

[11] Y. J. C. S. T. W. P. H. C. P. R. Billy Lau, „Mactans: Injecting Malware into iOS devices via malicious chargers,“ in BlackHat, 2013.

[12] W. H. L. S. M. S. K. Weizhi Meng, „Charging Me and I Know Your Secrets!: Towards Juice Filming Attacks on Smartphones,“ in CPSS ‘15: Proceedings of the 1st ACM Workshop on Cyber-Physical System Security, 2015.

[13] W. H. L. S. M. S. K. Weizhi Meng, „JuiceCaster: Towards automatic juice filming attacks on smartphones,“ Journal of Network and Computer Applications, Bd. 68, 2016.

[14] H. G. Q. Y. Yuanda Wang, „GhostTalk: Interactive Attack on Smartphone Voice System Through Power Line,“ in Network and Distributed Systems Security (NDSS) Symposium, 2022.

[15] P. G. G. Z. A. F. K. S. B. Qing Yang, „On Inferring Browsing Activity on Smartphones via USB Power Analysis Side-Channel,“ IEEE Transactions on Information Forensics and Security, Bd. 12, Nr. 5, 2017.

[16] L. P. I. P. E. T. Y. Y. Daniel Genkin, „ECDSA Key Extraction from Mobile Devices via Nonintrusive Physical Side Channels,“ in CCS ‘16: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016.

[17] X. G. C. Y. Patrick Cronin, „Charger-Surfing: Exploiting a Power Line Side-Channel for Smartphone Information Leakag,“ in Proceedings of the 30th USENIX Security Symposium, 2021.

[18] L. A. V. M. M. C. Riccardo Spolaor, „No Free Charge Theorem: A Covert Channel via USB Charging Cable on Mobile Devices,“ Lecture Notes in Computer Science, 2017.

[19] G. H. J. C. V. F. C. R. P. T. H. V. L. H. A. R. M. G. K. B. Dave Tian, „ATtention Spanned: Comprehensive Vulnerability Analysis of AT Commands Within the Android Ecosystem,“ in Proceedings of the 27th USENIX Security Symposium, 2018.

[20] S. A. G. O. D. Gunnar Alendal, „Exploiting Vendor-Defined Messages in the USB Power Delivery Protocol,“ in IFIP International Conference on Digital Forensics, 2019.

---

1. https://twitter.com/FBIDenver/status/1643947117650538498 ↩
2. https://twitter.com/FCC/status/1645849934728511494 ↩
3. https://www.bleepingcomputer.com/news/security/fbi-hackers-sending-malicious-usb-drives-and- teddy-bears-via-usps/ ↩
4. https://www.zdnet.com/article/fbi-cybercriminals-are-mailing-out-usb-drives-that-will-install- ransomware/. ↩
5. https://shop.hak5.org/products/omg-cable ↩