A-SIT

Zentrum für sichere Informationstechnologie - Austria

Power-Side-Channels auf Mobilen Geräten









Power-Side-Channels auf Mobilen Geräten

Autor:
Florian Draschbacher:
florian.draschbacher@a-sit.at

Datum: 05.10.2026

Abstract/Zusammenfassung:
Seitenkanäle rücken seit einigen Jahren immer mehr in den Fokus der Forschung. Dabei handelt es sich um Attacken, die Informationen aus einem Computersystem extrahieren, indem indirekt durch die Verarbeitung dieser Informationen entstehende (meist physikalische) Effekte beobachtet werden. Auch auf Mobilgeräten sind solche Seitenkanäle vorhanden, und können zur Extraktion verschiedener Informationen benützt werden.

Im Rahmen dieser Arbeit wurde zunächst ein Überblick über bestehende wissenschaftliche Literatur zu Seitenkanälen auf mobilen Geräten geschaffen. Der Fokus wurde hier auf physikalische Seitenkanäle, und innerhalb dieses Bereichs insbesondere auf Seitenkanäle auf Basis von Fluktuationen im Stromverbrauch (Power Line Side Channels), gerichtet. Anschließend wurde eine eigene Evaluierungsplattform geschaffen und für ein konkretes Mobilgerät ein Seitenkanal auf Basis des Ladestromverbrauchs implementiert.

Inhalt

1. Einleitung 2
2. Hintergrund 3
2.1. Seitenkanäle 3
2.2. Ursachen von Seitenkanälen 3
2.3. Physikalische Grundlagen von Power Side Channels 3
3. Seitenkanäle auf Mobilen Geräten 4
3.1. Software-Seitenkanäle 4
3.2. Hardware-Seitenkanäle und Power Line Side Channels 5
4. Implementierung und Evaluierung 5
4.1. Angriffsszenario 6
4.2. Implementierung 6
4.3. Evaluierung 8
5. Ausblick 9
6. Zusammenfassung 10
Referenzen 10

1. Einleitung

Innerhalb der Forschung zu Problemstellungen der IT-Sicherheit sind Seitenkanäle ein relativ junges Forschungsfeld. Zwar war bereits in den Jahrzehnten zuvor bekannt, dass elektronische Geräte über ungewollte Abstrahlungen Informationen preisgeben können, doch erst Mitte der 1990er-Jahre rückten Seitenkanäle in den Fokus der akademischen Kryptographie. Den Ausgangspunkt bildeten Arbeiten, die zeigten, dass sich aus der Laufzeit kryptographischer Operationen Rückschlüsse auf geheime Schlüssel ziehen lassen. Kurz darauf folgte die Erkenntnis, dass auch der Stromverbrauch eines Geräts während einer Berechnung mit den verarbeiteten Daten korreliert. Das Grundprinzip ist dabei stets dasselbe: Ein Angreifer greift nicht den Algorithmus selbst an, der mathematisch als sicher gelten mag, sondern beobachtet physikalische oder systemseitige Nebeneffekte seiner konkreten Implementierung. In den folgenden Jahren wurde das Feld erheblich erweitert. Neben Laufzeit und Stromverbrauch wurden elektromagnetische Abstrahlung, akustische Emissionen und schließlich das Verhalten von Prozessor-Caches als Informationsquellen identifiziert. Spätestens mit der Veröffentlichung von Spectre und Meltdown im Jahr 2018 wurde auch einer breiten Öffentlichkeit bewusst, dass Seitenkanäle kein rein theoretisches Problem darstellen, sondern grundlegende Sicherheitsannahmen moderner Computersysteme untergraben können.

Mobilgeräte stellen in diesem Zusammenhang ein besonders interessantes Angriffsziel dar. Smartphones begleiten ihre Nutzer nahezu permanent und verarbeiten eine Vielzahl sensibler Informationen, von privater Kommunikation über Standortdaten bis hin zu Zugangsdaten für Bank- und Behördendienste. Gleichzeitig verfügen sie über zahlreiche Sensoren und Schnittstellen, die für Angreifer potentiell nutzbare Nebeneffekte erzeugen. Entsprechend konzentrierte sich ein großer Teil der bisherigen Forschung auf softwarebasierte Seitenkanäle. So konnte etwa gezeigt werden, dass Apps ohne besondere Berechtigungen über Bewegungssensoren Tastatureingaben rekonstruieren oder über öffentlich zugängliche Systemstatistiken auf die Aktivitäten anderer Apps schließen können. Die Betriebssystemhersteller haben auf solche Erkenntnisse reagiert und den Zugriff auf viele dieser Informationsquellen in den vergangenen Jahren schrittweise eingeschränkt.

Weniger Beachtung fanden bislang Hardware-Seitenkanäle, die ohne jegliche Software auf dem Zielgerät auskommen. Klassische Angriffe dieser Art, etwa die Leistungsanalyse, setzen üblicherweise physischen Zugang zum Gerät und aufwendige Messaufbauten voraus. Bei Smartphones ergibt sich jedoch eine Besonderheit: Aufgrund der begrenzten Akkukapazität müssen sie regelmäßig geladen werden, und zwar zunehmend auch an fremder Infrastruktur, etwa an öffentlichen USB-Ladestationen in Flughäfen, Zügen oder Cafés. Das Ladekabel stellt damit eine direkte elektrische Verbindung zwischen dem Gerät und einer potentiell nicht vertrauenswürdigen Gegenstelle her. Da der aufgenommene Ladestrom nicht nur vom Ladezustand des Akkus, sondern auch vom momentanen Energiebedarf der Hardware abhängt, spiegeln sich Aktivitäten des Geräts in diesem Strom wider. Ein solcher Power Line Side Channel erfordert vom Angreifer weder die Installation einer App noch eine Interaktion mit dem Nutzer, sondern lediglich eine manipulierte Ladestation, und ist für den Nutzer praktisch nicht erkennbar.

Im Rahmen dieses Projektes wurde daher eine Evaluierungsplattform entwickelt und umgesetzt, mit der sich der Ladestrom von Mobilgeräten präzise aufzeichnen und systematisch auf Informationslecks untersuchen lässt. Auf Basis dieser Plattform konnte ein Seitenkanal identifiziert werden, der es erlaubt, allein anhand des Ladestroms zu erkennen, wann ein Nutzer telefoniert. Das Ziel dieses Berichts ist es, den Aufbau der Plattform, die durchgeführten Messungen sowie den gefundenen Seitenkanal im Detail darzustellen und dessen Praxisrelevanz zu bewerten. Abschließend werden mögliche Gegenmaßnahmen diskutiert, sowohl auf Seiten der Hardware- und Betriebssystemhersteller als auch in Form von Empfehlungen an Endanwender.

2. Hintergrund

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

2.1. Seitenkanäle

Ein Seitenkanal ist ein unbeabsichtigter Informationsfluss. Er entsteht nicht durch die eigentliche Funktion eines Systems, sondern durch beobachtbare Nebeneffekte seiner Ausführung. Ein Angreifer liest dabei keine geschützten Daten direkt aus. Stattdessen beobachtet er physikalische oder logische Größen, die mit diesen Daten zusammenhängen, und zieht daraus Rückschlüsse.

Seitenkanäle gibt es auch im Alltag. Ein Einbrecher muss nicht ins Haus sehen, um zu wissen, ob die Bewohner verreist sind: Ein überquellender Briefkasten oder tagelang geschlossene Rollläden verraten es ihm. Ein bekanntes Beispiel ist auch der Tresorknacker, der das Klicken des Zahlenschlosses abhört, statt die Kombination zu kennen. In beiden Fällen ist das eigentliche Geheimnis gut geschützt. Es wird jedoch über einen Kanal preisgegeben, den der Verteidiger nicht bedacht hat.

Bei Computern kommen als solche Kanäle unter anderem die Ausführungszeit, die Belegung gemeinsam genutzter Ressourcen wie Caches, elektromagnetische Abstrahlung, Schall und der Stromverbrauch in Frage.

2.2. Ursachen von Seitenkanälen

Viele Seitenkanäle sind eine direkte Folge von Optimierungen. Ein System, das jede Aufgabe immer gleich lange und mit gleichem Energieaufwand ausführt, verrät wenig über die verarbeiteten Daten. Effizient ist das jedoch nicht. Moderne Software und Hardware sparen deshalb überall dort Zeit und Energie, wo es möglich ist. Als Nebenprodukt wird dadurch ihr Verhalten abhängig von Eingaben und Zustand.

Auf Software-Ebene bricht beispielsweise ein naiver Passwortvergleich ab, sobald das erste falsche Zeichen gefunden ist. Die Laufzeit verrät damit, wie viele Zeichen korrekt waren. Caches halten insbesondere auf Betriebssystem-Ebene häufig genutzte Daten vor, sodass ein Zugriff je nach Vorgeschichte unterschiedlich schnell ist. Für mobile Geräte besonders relevant sind Energiesparmechanismen: Prozessoren passen Takt und Spannung dynamisch an die Last an (Dynamic Voltage and Frequency Scaling, DVFS), nicht benötigte Schaltungsteile werden abgeschaltet, und Funkmodule wechseln zwischen Schlaf- und Sendezuständen. Solche Mechanismen sind notwendig, damit ein Smartphone mit einer Akkuladung einen Tag lang durchhält. Gleichzeitig führen sie dazu, dass sich der Stromverbrauch eng an der tatsächlichen Aktivität des Geräts orientiert, und genau das macht ihn als Seitenkanal so aussagekräftig.

2.3. Physikalische Grundlagen von Power Side Channels

Digitale Schaltungen bestehen heute fast ausschließlich aus CMOS-Transistoren. Ein CMOS-Gatter verbraucht zwar im Ruhezustand nur wenig Strom, für jeden Zustandswechsel wird allerdings ein etwas höherer Strom benötigt. Je mehr Rechenarbeit anfällt, desto mehr Gatter schalten, und desto höher ist also auch der Stromverbrauch. So lässt sich erklären, wie die auf einem Prozessor ausgeführten Berechnungen messbare Spuren im Stromverbrauch hinterlassen.

Bei einem Smartphone kommen weitere große Verbraucher hinzu, deren Leistungsaufnahme unmittelbar vom Nutzungsverhalten abhängt. Bei OLED-Displays hängt der Verbrauch von Helligkeit und Farbe jedes

einzelnen Pixels ab. Das Mobilfunkmodem benötigt beim Senden deutlich mehr Energie als im Ruhezustand. Lautsprecherverstärker und Vibrationsmotor verbrauchen Strom proportional zu ihrer Ausgabe. Ein Telefonat etwa versetzt Modem, Audiopfad und Prozessor gleichzeitig in einen charakteristischen Betriebszustand, der sich deutlich von anderen Nutzungsarten unterscheiden kann. Während bei diesen Seiteneffekten meist von Energieverbrauch als Messgröße, die Aufschluss über die Nutzeraktivität verrät, die Rede ist, wird in der Praxis der Einfachheit halber meist eher die Stärke des fließenden Stroms gemessen, und davon ausgegangen, dass die Spannung relativ konstant bleibt.

3. Seitenkanäle auf Mobilen Geräten

Seitenkanalangriffe nutzen nicht die eigentliche Funktion eines Systems aus, sondern unbeabsichtigte Nebeneffekte seiner Ausführung. Dazu gehören etwa das Zeitverhalten, die Nutzung gemeinsamer Ressourcen, elektromagnetische Abstrahlung oder der Stromverbrauch. Ursprünglich richteten sich solche Angriffe vor allem gegen kryptografische Implementierungen auf Smartcards [1]. Inzwischen gehören Smartphones zu den am intensivsten untersuchten Zielen: Sie verarbeiten eine Vielzahl sensibler Daten, sind mit zahlreichen Sensoren ausgestattet und werden regelmäßig an fremde Infrastruktur wie öffentliche Ladestationen angeschlossen. Spreitzer et al. geben einen systematischen Überblick über Seitenkanäle auf mobilen Geräten. Sie unterscheiden dabei unter anderem zwischen Angriffen, die physischen Zugang zum Gerät oder Nähe zu ihm erfordern, und Angriffen, die rein aus Software heraus möglich sind [2]. Im Folgenden geben wir zunächst einen kurzen Überblick über Software-Seitenkanäle. Danach gehen wir ausführlicher auf Hardware-Seitenkanäle ein, insbesondere auf Power Line Side Channels.

3.1. Software-Seitenkanäle

Software-Seitenkanäle werden von einer bösartigen App ausgenutzt, die bereits auf dem Gerät installiert ist. Sie wertet, häufig ohne besondere Berechtigungen, öffentlich zugängliche Informationen des Betriebssystems aus. Frühe Arbeiten zeigten, dass die im procfs-Dateisystem einsehbaren Speicherstatistiken fremder Prozesse Rückschlüsse auf besuchte Webseiten zulassen [3]. Zhou et al. leiteten aus öffentlichen Ressourcen wie Datennutzungsstatistiken die Identität, den Aufenthaltsort und sogar Erkrankungen von Nutzern ab [4]. Chen et al. erkannten anhand von Shared-Memory-Zählern den aktuellen UI-Zustand fremder Apps und konnten so gezielt Phishing-Angriffe durchführen [5]. Mit ProcHarvester wurde die Suche nach solchen Informationslecks schließlich automatisiert [6].

Eine zweite große Gruppe bilden Bewegungssensoren, die Apps lange Zeit ohne Berechtigung und mit hoher Abtastrate auslesen konnten. Über Gyroskop und Beschleunigungssensor lassen sich beispielsweise Sprachsignale rekonstruieren [7]. Mit AccelEve gelang das sogar für die Ausgabe des geräteeigenen Lautsprechers [8]. Darüber hinaus wurden mikroarchitektonische Angriffe wie Cache-Timing-Angriffe, die zunächst von Desktop- und Serversystemen bekannt waren, auf ARM-basierte Smartphones übertragen [9]. Bemerkenswert ist, dass sich auch der Stromverbrauch aus Software heraus beobachten lässt. PowerSpy nutzte die von Android bereitgestellten Batteriedaten, um den Aufenthaltsort eines Nutzers zu bestimmen [10]. Oberhuber et al. zeigten jüngst, dass die über das Android Sensor Framework zugänglichen Strom- und Leistungsmesswerte Power-Side-Channel-Angriffe ganz ohne physischen Zugang ermöglichen [11].

Als Reaktion auf diese Arbeiten haben die Plattformbetreiber den Zugriff auf viele der genannten Informationsquellen schrittweise eingeschränkt. Beispiele sind der eingeschränkte Zugriff auf procfs-Einträge fremder Prozesse und die Begrenzung der Abtastrate von Bewegungssensoren auf 200 Hz ab Android 12. Außerdem setzen Software-Seitenkanäle stets voraus, dass der Angreifer Code auf dem

Zielgerät ausführen kann. Hardware-Seitenkanäle umgehen diese Voraussetzung, da sie physikalische Größen außerhalb der Kontrolle des Betriebssystems messen.

3.2. Hardware-Seitenkanäle und Power Line Side Channels

Bei der klassischen Power Analysis wird der Stromverbrauch eines Geräts gemessen, um auf die verarbeiteten Daten zu schließen. Genkin et al. zeigten, dass dies auch bei komplexen Systemen wie Smartphones funktioniert. Sie extrahierten ECDSA-Schlüssel von iOS- und Android-Geräten, und zwar sowohl mit einer elektromagnetischen Sonde in Gerätenähe als auch über eine Messung am USB-Ladekabel [12]. Die meisten jüngeren Arbeiten zielen jedoch nicht auf kryptografische Schlüssel, sondern auf Nutzeraktivitäten ab. Das Bedrohungsmodell ist dabei meist ein manipuliertes Ladegerät oder eine manipulierte Ladestation, die unbemerkt den Stromverbrauch des angeschlossenen Smartphones aufzeichnet. Dieser Stromverbrauch hängt maßgeblich von Komponenten wie Display, Prozessor, Funkmodulen und Lautsprecher ab. Deren Aktivität wiederum wird unmittelbar durch die Nutzung des Geräts bestimmt.

Yang et al. zeigten 2017 als eine der ersten Arbeiten, dass eine USB-Ladestation am Stromverbrauch erkennen kann, welche Webseite auf einem ladenden Smartphone aufgerufen wird. In vielen Konfigurationen erreichten sie dabei eine Genauigkeit von über 90 % [13]. Matovu et al. demonstrierten weitere Angriffe auf Nutzeraktivitäten mit Strommessgeräten, die in Ladestationen integriert sind. Zugleich schlugen sie Gegenmaßnahmen vor, die den Stromverbrauch während des Ladevorgangs zufällig verrauschen [14]. Cronin et al. gingen mit Charger-Surfing einen Schritt weiter: Das visuelle Feedback beim Antippen einer Bildschirmtaste verändert den Stromverbrauch des Displays messbar. Darüber konnten sie mit einem bösartigen Ladegerät eingegebene Entsperr-PINs tastengenau rekonstruieren [15]. Lifshits et al. untersuchten ein verwandtes Szenario, in dem ein manipulierter Akku statt des Ladegeräts den Stromverbrauch aufzeichnet. Daraus konnten sie unter anderem Tastatureingaben, besuchte Webseiten und eingehende Anrufe ableiten [16]. Power Line Side Channels verraten außerdem akustische Signale. Wang et al. zeigten mit GhostTalk, dass sich über ein modifiziertes Ladekabel die Lautsprecherausgabe eines Smartphones abhören lässt, während gleichzeitig unhörbare Sprachbefehle eingeschleust werden [17].

Weitere Arbeiten erweitern das Bedrohungsmodell über das direkt angeschlossene Ladegerät hinaus. Ni et al. zeigten mit XPorter, dass in Mehrfach-Ladegeräten ein Angreifergerät am benachbarten Port die Aktivität eines Smartphones über Spannungsschwankungen beobachten kann. So lassen sich laufende Apps und Tastatureingaben erkennen [18]. Wie Oberhuber et al. gezeigt haben, lassen sich viele dieser Seitenkanäle zudem indirekt aus Software heraus ausnutzen [11]. Auch kabelloses Laden schützt nicht: La Cour et al. demonstrierten Website-Fingerprinting über den Stromverbrauch eines kabellosen Ladegeräts [19]. Ni et al. konnten mit BankSnoop sogar kontaktlos die laufende App und die Tastatureingaben eines Smartphones bestimmen, das an einer kabellosen Powerbank lädt. Dafür werteten sie das Spulenpfeifen und Störungen des Magnetfelds aus [20].

4. Implementierung und Evaluierung

In Anlehnung an den bisherigen State-of-the-Art wurde im Rahmen dieses Projekts eine eigene Evaluierungsplattform geschaffen, auf Basis deren Power-Line-Side-Channel-Angriffe an Smartphones im Detail analysiert werden können.

4.1. Angriffsszenario

Für unsere Evaluierung nahmen wir als Angriffsszenario ein bösartiges Ladegerät an, wie es auch schon von früheren Angriffen (etwa JuiceJacking) bekannt ist. Hierbei manipuliert ein Angreifer zum Beispiel ein Ladegerät im öffentlichen Raum (denkbar sind Flughäfen, Bahnhöfe, Museen, Cafés, …), indem er die Elektronik auswechselt. Von außen lässt sich die Manipulation nicht feststellen. Schließt ein Nutzer sein Gerät an das manipulierte Ladegerät an, so wird das Gerät noch immer mit Strom versorgt. Zusätzlich misst das Ladegerät allerdings heimlich den Stromverbrauch des Geräts, und kann so Rückschlüsse auf die vom Nutzer am Gerät ausgeführten Aktionen ziehen.

4.2. Implementierung

Um Power Line Side Channels im oben beschriebenen Szenario zu untersuchen, nutzen Forscher meist einen Versuchsaufbau im Labor auf Basis eines Oszilloskops. Dieses misst anhand des Spannungsabfalls an einem niederohmigen Widerstand den Stromverbrauch. Zwar erlaubt der Einsatz eines Oszilloskops sehr hohe Messauflösungen und -frequenzen, allerdings weichen so ausgeführte Experimente zwangsläufig von realen Angriffsumgebungen ab. Zum einen sind Oszilloskope teure Messinstrumente, und daher für einen Angriff ungeeignet, der vor allem über die Skalierung auf eine große Zahl manipulierter Ladegeräte tatsächlichen Impact erreicht. Zum anderen sind Oszilloskope aufgrund ihrer physischen Maße schwer in ein manipuliertes Ladegerät zu integrieren. Unabhängig davon ist der Einsatz eines Oszilloskops auch zur Erforschung von Power Line Side Channels schon allein aufgrund der Anschaffungskosten und physischen Abmessungen unpraktisch.

Für unsere Forschung haben wir daher eine eigene Evaluierungsplattform entworfen und umgesetzt, die in Form einer handlichen Platine ein bösartiges Ladegerät simuliert. Zwischen dem Smartphone als Verbraucher und der Masseleitung (Ground / GND) sitzt ein Shunt-Widerstand. Der Spannungsabfall über den Widerstand wird vom Analog-To-Digital-Converter (ADC) eines RP2040-Mikrokontrollers erfasst und bei Bedarf über USB an einen Computer weitergegeben. Dieser kann so aufwändige Echtzeitanalysen der Messwerte vornehmen, um mögliche Power Line Side Channels zu identifizieren. Für das Ausführen von bereits erfassten Angriffen kann die Platine auch eigenständig, nur mit dem Mikrokontroller als Recheneinheit, genutzt werden.

Der Shunt-Widerstand muss sehr niederohmig gewählt werden (konkret 15 Milliohm), um die Ladespannung für das Smartphone nicht wesentlich zu beeinflussen. Es ergibt sich allerdings auch nur ein sehr geringer Spannungsabfall über den Widerstand, der unterhalb des Messbereichs des ADC typischer Mikrokontroller liegt. Unsere Evaluierungsplattform enthält daher einen genau für solche Anwendungsfälle gedachten Verstärker vom Typ INA301A2, der den gemessenen Spannungsabfall um den Faktor 50 verstärkt. Der entsprechende Auszug aus dem Schaltplan ist in *Abbildung 1* zu sehen.

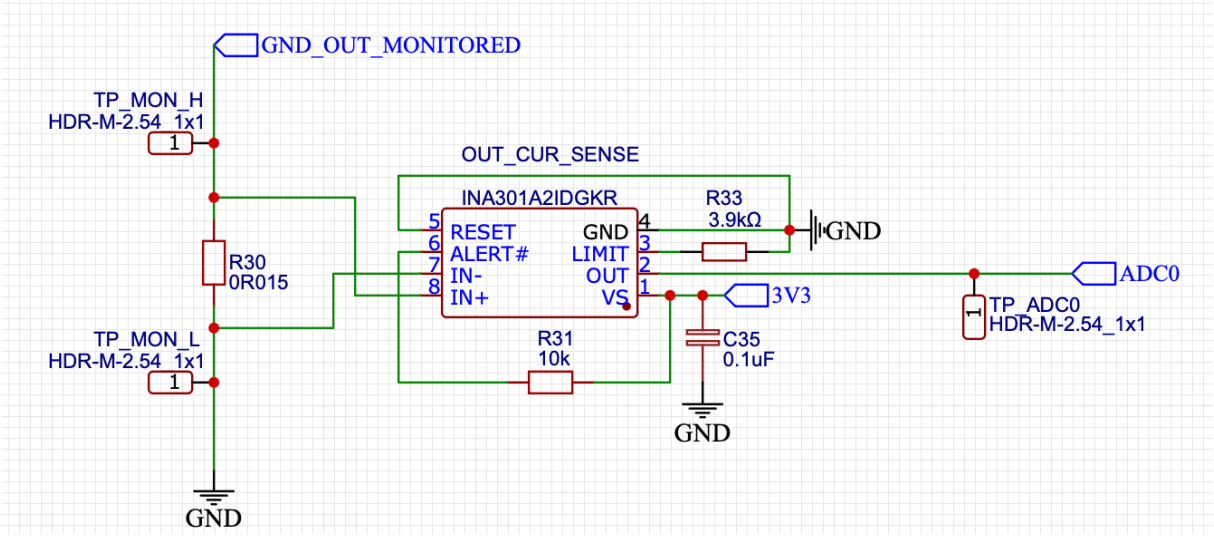


Abbildung 1: Ausschnitt des Schaltplans mit Shunt-Widerstand und Verstärker

Die Wahl für den verbauten Mikrocontroller fiel aus mehreren Gründen auf den RP2040. Zum einen verfügt er über einen ADC mit hoher Abtastrate (bis zu 1,2 Millionen Samples pro Sekunde) und relativ hoher Auflösung (12 bit). Zum anderen verfügt der Mikrocontroller über programmierbare Peripheriegeräte (PIO), mit denen sich verschiedene zusätzliche Schnittstellen implementieren lassen. So konnten wir die Platine mit 2 funktionierenden USB-Schnittstellen ausstatten, die die gleichzeitige Kommunikation sowohl mit einem Computer als auch mit einem Smartphone erlauben. Außerdem hat der Mikrocontroller der Marke Raspberry Pi in den letzten Jahren breite Verwendung gefunden, sodass eine Vielzahl an Bibliotheken und Tooling zur Verfügung stehen.

Zusätzlich zur reinen Strommessung verhält sich unsere Platine auch wie ein modernes Smartphone-Ladegerät. Es kommuniziert mittels USB-Power-Delivery-Controllern über den Control Channel (CC) mit dem Smartphone, um sich auf ein Profil aus Ladestrom und Ladespannung zu einigen. Hierfür wurde ein Controller vom Typ FUSB302 verbaut, der über I2C vom RP2040-Mikrocontroller gesteuert wird. Die vollständige Platine ist in *Abbildung 2* zu sehen.

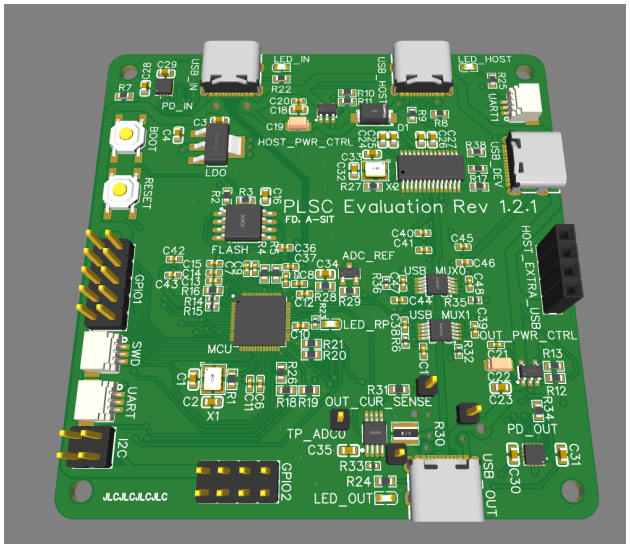


Abbildung 2: Rendering der Platine unserer Evaluierungs-Plattform

Die Firmware am Mikrocontroller konfiguriert, sobald die Platine mit Strom versorgt wird, den USB-PD-Controller und startet die USB-Schnittstelle. Falls die Platine über USB an einen Computer angeschlossen wird, kann dieser über ein virtuelles Serial-Interface zum Beispiel einige Einstellungen setzen. Informiert der Controller über den Anschluss eines Smartphones, beginnt der Mikrocontroller, in einem vom Computer vorgegebenen Intervall den ADC auszulesen und die Messwerte an den Computer weiterzureichen.

Zur weiteren Analyse haben wir am Computer ein Python-Framework implementiert, das die Kommunikation mit der Platine abstrahiert. Die gelesenen ADC-Werte können hier zusätzlich abgespeichert und zur späteren Analyse ohne angeschlossene Platine eingelesen werden. Außerdem können sie als Echtzeit-Plot ausgegeben werden, um erste visuelle Ansatzpunkte für Power Line Side Channels zu identifizieren.

4.3. Evaluierung

Ziel der Evaluierung unserer Plattform war es, einen Seitenkanal zu identifizieren, mit dem Rückschlüsse zum Aktivitätsprofil des angeschlossenen Smartphones gezogen werden können. Als anschauliches Beispiel dient hier die Erkennung von Momenten, in denen der Nutzer das Smartphone zum Telefonieren verwendet. Da hier besonders energiehungrige Mobilfunkkommunikation verwendet wird, vermuteten wir besonders große Chancen auf einen eindeutigen Power-Line-Side-Channel. Als Testgerät diente ein Xiaomi 12. Wir wählten die niedrige Abtastrate von 1 kHz, da hier die Datenmenge überschaubar bleibt und grobe Muster auch visuell einfach zu erfassen sind.

In diesem Setup schlossen wir das Testgerät an unsere Evaluierungsplattform an und beobachteten mittels Echtzeitplot den Stromverbrauch, während wir am Gerät einen Anruf starteten. Wie erhofft zeichnete sich hier ein Muster ab. Wie in *Abbildung 3* zu sehen, sind Beginn und Ende des Anrufs durch charakteristische Verbrauchsspitzen und ein etwas erhöhtes Mittel gekennzeichnet.

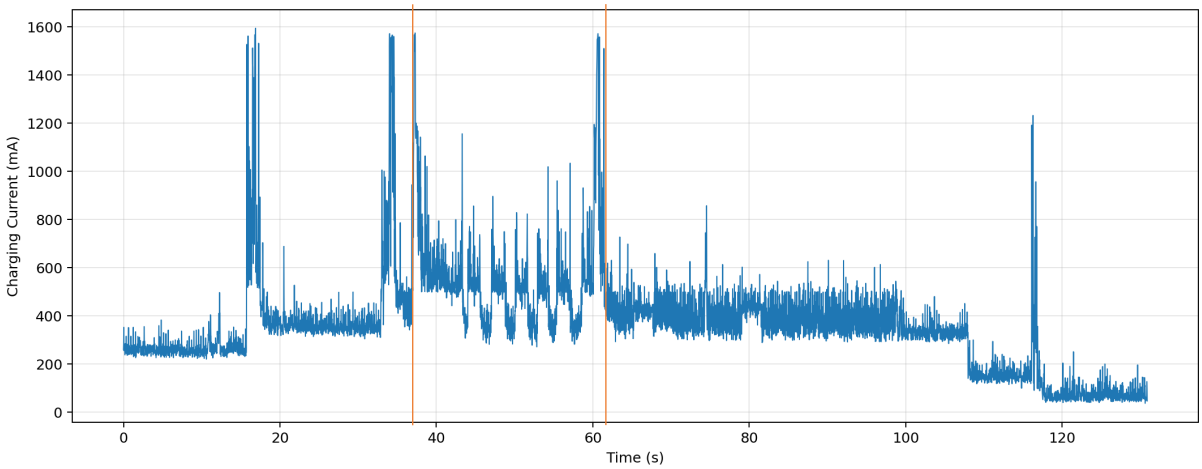


Abbildung 3: Stromverbrauch eines Xiaomi 12. Die roten Linien markieren Beginn und Ende des Anrufs.

Im nächsten Schritt trainierten wir ein Machine-Learning-Modell (konkret ein Convolutional Neural Net; CNN), um automatisiert anhand des Stromverbrauchs zu erkennen, wann sich das Smartphone in einem Anruf befindet. Zunächst mussten wir dazu zusätzliche Aufzeichnungen von alternativen Aktivitäten am Smartphone sammeln, um sicherzugehen, dass keine ähnlichen Muster im Stromverbrauch zu erkennen sind. Konkret sammelten wir automatisiert Stromverbrauchs-Aufzeichnung von 16 typischen Nutzeraktivitäten, unter anderem:

- Webbrowsen (mittels Google Chrome)
- Online-Shopping (auf Amazon)
- Musik-Hören (Spotify)
- Video-Streaming (Youtube)
- Social Media (Facebook, Snapchat, TikTok)
- Taschenrechner
- Datei-Management (via OneDrive)

Für jede der ausgeführten Aktivitäten sammelten wir mindestens 15 Aufzeichnungen, die wir zusammen mit derselben Menge an Aufzeichnungen zu Anruf-Beginn und Anruf-Ende zum Training des CNN verwendeten. Anschließend evaluierten wir den Classifier anhand von 10 neuen Aufzeichnungen je oben genannter Aktivität. Hier ergab sich für das Modell eine Genauigkeit von knapp 93%. Zwar wurde Beginn und Ende von Anrufen stets korrekt erkannt, doch gab es einzelne andere Aktivitäten, die in einzelnen Fällen fälschlicherweise ebenfalls als Anruf-Ende erkannt wurden. Wir gehen davon aus, dass die Genauigkeit durch komplexere Modelle und ausführlicheres Training noch gesteigert werden kann. Dennoch konnte das Experiment bereits zeigen, dass anhand des Stromverbrauchs eines ladenden Smartphones zwischen verschiedenen typischen Aktivitäten unterschieden werden kann.

5. Ausblick

In diesem Projekt konnten wir zeigen, dass Power Line Side Channels als konkretes Beispiel eines hardwarebasierten Side-Channels aktuelle Android-Geräte betreffen. In der Tat sind aktuelle Geräte nicht nur betroffen, ein Ausblick auf aktuelle Entwicklungen zeigt auch, dass derartige Seitenkanäle immer interessanter für Angreifer werden:

Breites Bewusstsein zu JuiceJacking. In der jüngeren Vergangenheit wurde immer wieder auch in den Massenmedien über die Gefahr berichtet, die von öffentlichen Ladestationen ausgeht. Nicht zuletzt durch die neuartigen ChoiceJacking-Attacken, die wir im letzten Jahr gefunden haben, konnte das öffentliche Bewusstsein über diese Angriffe erneuert und vertieft werden, sodass zumindest besonders gefährdete Nutzer auf zusätzliche Schutzmaßnahmen wie die Verwendung von USB Data Blockern setzen. Diese blockieren die USB-Datenleitungen, sodass hardwareseitig die USB-Verbindung nur noch zum Laden verwendet werden kann.

Immer mehr technische Maßnahmen gegen klassische USB-Daten-Angriffe. Nicht zuletzt durch unsere Forschung zu ChoiceJacking haben alle namhaften Smartphone-Hersteller mittlerweile auch weitere softwareseitige Schutzmaßnahmen integriert, die verhindern sollen, dass bösartige Ladegeräte über USB Zugriff auf Nutzerdaten erhalten können. Sowohl iOS als auch Android verfügen mittlerweile über optionale Lockdown-Modi für besonders gefährdete Nutzer, die die USB-Kommunikation schon auf niedriger Software-Ebene deaktivieren.

Allgegenwärtige Verfügbarkeit von Ladeinfrastruktur. Gleichzeitig ist weiterhin eine starke Zunahme an Smartphone-Lademöglichkeiten im öffentlichen Raum zu verzeichnen. Mittlerweile bieten etwa sogar schon Busse oder Museen Ladebuchsen oder mietbare Powerbanks an. Es ist davon auszugehen, dass aufgrund dieser starken Exposition in Summe auch die Nutzung von öffentlicher Ladeinfrastruktur zunimmt. Nicht zuletzt sorgen die oben genannten USB-Data-Blocker und Lockdown-Modi dafür, dass

sich selbst besonders gefährdete Anwender im Glauben an die Wirksamkeit der Schutzmaßnahmen zur Nutzung des Ladeangebots hinreißen lassen.

Pass-Through Charging. Immer mehr Smartphone-Hersteller integrieren Pass-Through Charging in ihre Geräte. Ist Pass-Through Charging aktiviert, so wird das Smartphone vereinfacht gesagt direkt aus dem Ladestrom versorgt. Üblich war bisher grob gesagt, dass mit dem Ladestrom der Akku im Smartphone geladen wird und dieser wiederum die anderen Komponenten im Smartphone mit Strom versorgt. Die Verbraucher im Smartphone verlangsamen hier das Laden, weil sie dem Akku währenddessen laufend Strom entziehen. Zunächst hat dies negative Konsequenzen auf die Lebensdauer des Akkus. Außerdem führt diese ineffiziente Vorgehensweise zu Wärmeentwicklung, die besonders während der Ausführung von rechenintensiven Anwendungen zur Drosselung der CPU-Geschwindigkeit führen kann. Pass-Through Charging hat Konsequenzen für Power Side Channels, wie wir sie in diesem Projekt gezeigt haben: Zwar konnten frühere Studien und auch unsere Experimente schon zeigen, dass solche Angriffe unabhängig vom genauen Ladezustand funktionieren, selbst bei Geräten ohne Pass-Through Charging. Warum genau sich aktivitäten-induzierte Fluktuationen im Verbrauch über den Akku hinweg am Ladestrom messen lassen, haben wir nicht nachvollzogen, weil dazu die komplexe Ladeelektronik im Gerät hätte analysiert werden müssen. Es liegt jedenfalls die Vermutung nahe, dass bei Pass-Through Charging mit deutlich weniger Signalrauschen zu rechnen ist, da hier der gemessene Stromverbrauch ausschließlich auf die direkt in die Nutzeraktivität eingebundenen Komponenten (insbesondere CPU, Display und Kommunikationsmodule) zurückzuführen ist.

6. Zusammenfassung

In diesem Projekt wurden Seitenkanäle bzw. Side Channels, und hier insbesondere Power Side Channels, auf aktuellen Smartphones untersucht. Nach einem Überblick über bestehende Arbeiten in den Bereichen Software- und Hardware-Sidechannels wurde eine eigene Evaluierungsplattform geschaffen, auf deren Basis ein anschaulicher Seitenkanal gezeigt wurde, der es erlaubt, anhand des Stromverbrauchs beim Laden zu erkennen, wann das Smartphone zum Telefonieren genutzt wird. Nicht nur konnte dieser Seitenkanal visuell erfasst werden, sondern auch mithilfe eines Convolutional Neural Network automatisiert und evaluiert werden. Abschließend wurde in einem kurzen Ausblick die zukünftige Relevanz von Power Side Channels hervorgehoben. Aufgrund technischer Entwicklungen und immer besserer Maßnahmen gegen klassische USB-basierte Angriffe gewinnen Power Line Side Channels für Angreifer immer mehr an Attraktivität. Nicht zuletzt deshalb muss sich auch die Forschung vermehrt dieser Angriffe und möglicher Gegenmaßnahmen annehmen.

Referenzen

[1] P. C. Kocher, J. Jaffe und B. Jun, „Differential Power Analysis," in *CRYPTO*, 1999.

[2] R. Spreitzer, V. Moonsamy, T. Korak und S. Mangard, „Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices," *IEEE Communications Surveys & Tutorials,* Bd. 20, Nr. 1, 2017.

[3] S. Jana und V. Shmatikov, „Memento: Learning Secrets from Process Footprints," in *IEEE S&P*, 2012.

[4] X. Zhou, S. Demetriou, D. He, M. Naveed, X. Pan, X. Wang, C. A. Gunter und K. Nahrstedt, „Identity, location, disease and more: inferring your secrets from android public resources," in *ACM CCS*, 2013.

[5] Q. A. Chen, Z. Qian und Z. M. Mao, „Peeking into Your App without Actually Seeing It: UI State Inference and Novel Android Attacks," in *USENIX Security*, 2014.

[6] R. Spreitzer, F. Kirchengast, D. Gruss und S. Mangard, „ProcHarvester: Fully Automated Analysis of Procfs Side-Channel Leaks on Android," in *AsiaCCS*, 2018.

[7] Y. Michalevsky, D. Boneh und G. Nakibly, „Gyrophone: Recognizing Speech from Gyroscope Signals," in *USENIX Security*, 2014.

[8] Z. Ba, T. Zheng, X. Zhang, Z. Quin, B. Li, X. Liu und K. Ren, „Learning-based Practical Smartphone Eavesdropping with Built-in Accelerometer," in *NDSS*, 2020.

[9] M. Lipp, D. Gruss, R. Spreitzer, C. Maurice und S. Mangard, „ARMageddon: Cache Attacks on Mobile Devices," in *USENIX Security*, 2016.

[10] Y. Michalevsky, A. Schulman, G. A. Veerapandian und D. Boneh, „PowerSpy: Location Tracking Using Mobile Device Power Analysis," in *USENIX Security*, 2015.

[11] M. Oberhuber, M. Unterguggenberger, L. Maar, A. Kogler und S. Mangard, „Power-Related Side-Channel Attacks using the Android Sensor Framework," in *NDSS*, 2025.

[12] D. Genkin, L. Pachmanov, I. Pipman, E. Tromer und Y. Yarom, „ECDSA Key Extraction from Mobile Devices via Nonintrusive Physical Side Channels," in *ACM CCS*, 2016.

[13] Q. Yang, P. Gasti, G. Zhou, Farajidavar, Aydin und K. S. Balagani, „On Inferring Browsing Activity on Smartphones via USB Power Analysis Side-channel," *IEEE Transactions on Information Forensics and Security,* Bd. 12, Nr. 1, 2017.

[14] R. Matovu, A. Serwadda und A. V. G.-S. I. Bilbao, „Defensive Charging: Mitigating Power Side-Channel Attacks on Charging Smartphones," in *CODASPY*, 2020.

[15] P. Cronin, X. Gao, C. Yang und H. Wang, „Charger-Surfing: Exploiting a Power Line Side-Channel for Smartphone Information Leakage," in *USENIX Security*, 2021.

[16] P. Lifshits, R. Forte, Y. Hoshen, M. Halpern, M. Philipose, M. Tiwari und M. Silberstein, „Power to peep-all: Inference Attacks by Malicious Batteries on Mobile Devices," in *PoPETS*, 2018.

[17] Y. Wang und H. Y. Q. Guo, „GhostTalk: Interactive Attack on Smartphone Voice System Through Power Line," in *NDSS*, 2022.

[18] T. Ni, Y. Chen, W. Xu, L. Xue und Q. Zhao, „XPorter: A Study of the Multi-Port Charger Security on Privacy Leakage and Voice Injection," in *ACM MobiCom*, 2023.

[19] A. S. La Cour, K. K. Afridi und G. E. Suh, „Wireless Charging Power Side-Channel Attacks," in *ACM CCS*, 2021.

[20] T. Ni, J. Li, X. Zhang, C. Zuo, W. Wang, W. Xu, X. Luo und Q. Zhao, „Exploiting Contactless Side Channels in Wireless Charging Power Banks for User Privacy Inference via Few-shot Learning," in *ACM MobiCom*, 2023.