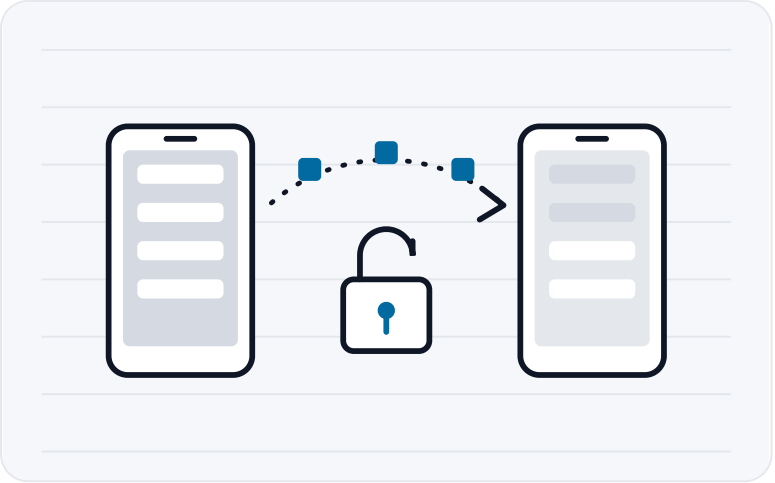
A-SIT Technology
E-Government Innovationszentrum

11. November 2024 Analyse · Mobile Sicherheit · 15 Min. Lesezeit

Sicherheitsanalyse von Daten-Migrations-Lösungen für Mobilgeräte

Florian Draschbacher



Autorinnen und Autoren	Florian Draschbacher
Stand	2024-11-11
Quelle	https://technology2.a-sit.at/veroeffentlichungen/sicherheitsanalyse-von-daten-migrations-loesungen-fuer-mobilgeraete/

Kernaussagen

- Bei Xiaomi Mi Mover wird der WLAN-Schlüssel (PSK) aus der SSID abgeleitet; die Funktion steckt als Security-by-Obscurity in einer nativen Bibliothek.
- Außer WPA2 nutzt Xiaomi Mi Mover kein weiteres Sicherheitsprotokoll, ein Offline-Angriff auf die Kommunikation wäre daher möglich.
- Ein passiver Angreifer in WLAN-Reichweite konnte per Exploit alle von Xiaomi Mi Mover übertragenen Daten mitlesen.
- Apple Move to iOS nutzt die SSID ebenfalls als PSK, schützt die TCP-Verbindung aber mit SRP und TLS; nur 4 der 6 Pin-Ziffern sind geheim.

> - Der Prototyp-Exploit und eine Zusammenfassung der Analyse wurden im Oktober 2024 an Xiaomi übermittelt.

Um den Umstieg auf ein neues Mobilgerät zu erleichtern, bieten viele Gerätehersteller Software-Lösungen an, mit denen bestehende Daten vom alten Gerät einfach übertragen werden können. Für den größtmöglichen Nutzerkomfort weisen diese Lösungen meist eine tiefe Integration ins Betriebssystem auf. Dennoch stehen keine aktuellen detaillierten Analysen über die Übertragungsmechanismen und Sicherheit von Daten-Migrations-Apps zur Verfügung.

Im Rahmen dieses Projekts wurden diese Analysen für die Tools zweier populärer Hersteller von Mobilgeräten erhoben. Dazu wurden im ersten Schritt die Protokollebenen der jeweiligen Übertragungsmechanismen eingehend analysiert. Auf Basis der Erkenntnisse wurden dann verschiedene Angriffsziele definiert und mögliche Angriffsvektoren detailliert evaluiert. Für gefundene Sicherheitsprobleme wurden Exploits geschrieben und den Herstellern übermittelt.

1. Einleitung

Der Markt für Mobilgeräte wie Smartphones und Tablets ist sogar innerhalb des ohnehin schon schnelllebigen Sektors für Elektronikprodukte besonders häufigen Veränderungen ausgesetzt. In engen Intervallen versuchen die großen Hersteller, die Kunden mit immer neuen Produktvorstellungen vom eigenen Angebot zu überzeugen. Selbst wenn ein Nutzer vom Angebot eines Konkurrenzprodukt überzeugt war, so scheute er einen Wechsel allerdings häufig schon allein aufgrund des administrativen Aufwands, alle in das alte Gerät eingepflegten Daten (Apps, Konfigurationen, Internet-Accounts, Wifi-Zugangsdaten, Dokumente, Bilder, ...) auf das neue Gerät zu übertragen. Um dieses Hemmnis aus dem Weg zu schaffen, führten die meisten Hersteller von Mobilgeräten in den letzten Jahren eigene Daten-Migrationstools ein. Diese erlauben es meist, Daten entweder von einem anderen Gerät desselben Herstellers oder von einem Gerät eines anderen Herstellers auf das neue Gerät zu übertragen. In diesem Bericht wird insbesondere auf solche Datenübertragungsapp eingegangen, die die Migration auf ein Android-Gerät ermöglicht.

Obwohl dem Nutzer wohl kaum bewusst, muss hier die besondere Rolle dieser Datenübertragungs-Tools in der Sicherheitsarchitektur von Android hervorgehoben werden. Ein zentrales Element in der Sicherheitsarchitektur ist die App-Sandbox. Diese beschränkt nicht nur den Zugriff von Apps auf die Ressourcen des Betriebssystems, sondern stellt auch sicher, dass die Daten einer App für keine andere App zugreifbar sind. Apps speichern hier häufig etwa Zugangsdaten für Online-Accounts ab, sodass ein Zugriff auf diese Daten (etwa einer bösartigen App am selben Gerät) unter Umständen weitreichende Konsequenzen für den Nutzer hätte. Selbst Apps, die am Gerät vorinstalliert sind, erhalten hier keine Ausnahme. Einzig das Betriebssystem ist im regulären Betrieb in der Lage, auf die Daten der installierten Apps zugreifen. Das Betriebssystem verfügt auch alleinig über Zugriff auf Gerätekonfigurationen, wie etwa Wifi-Zugangsdaten.

In der Regel bestimmt der Hersteller des neuen Geräts darüber, welches Datenmigrationstool der Nutzer verwenden muss. Das Tool wird meist am neuen Gerät schon mit ausgeliefert und im Rahmen der Ersteinrichtung ausgeführt. Am alten Gerät wird das Tool meist über den Play Store nachgeladen. Während

das Tool zur einfacheren automatisierten Integration der empfangenen Daten am neuen Gerät meist vom Gerätehersteller (effektiv als Teil des Betriebssystems) mit besonderen Berechtigungen ausgestattet ist, läuft es am alten Gerät in der Regel als Drittanbieter-App ohne besondere Berechtigungen. Der Grund hierfür ist erneut in der Sicherheitsarchitektur von Android zu finden: Apps können nur dann mit besonderen Berechtigungen ausgestattet werden, wenn sie mit demselben Zertifikat signiert werden, wie auch das Betriebssystem selbst. In der Praxis bedeutet das meist, dass nur Apps vom Gerätehersteller über besondere Berechtigungen verfügen können.

Einen interessanten Spezialfall bildet die Migration zwischen zwei Geräten desselben Herstellers. Das Migrations-Tool läuft hier auf beiden Geräten mit besonderen Berechtigungen. Damit können nicht nur die empfangenen Daten am neuen Gerät automatisiert integriert werden, sondern auch am alten Gerät mehr Daten extrahiert werden. Das Migrations-Tool erhält hier etwa Zugriff auf die oben erwähnten App-Daten oder auf Wifi-Zugangsdaten. Effektiv verlassen hier Daten das Gerät, die üblicherweise vom Betriebssystem vor dem unerlaubten Zugriff geschützt werden.

Für diesen Bericht wurde eine Datenmigrationslösung im Hinblick auf die Migration zwischen zwei Geräten desselben Herstellers untersucht (die Erkenntnisse lassen auch Aussagen auf die Migration von einem Gerät eines anderen Herstellers zu), sowie eine App, die die Migration zwischen zwei Geräten verschiedener Plattformen (Android und iOS) erlaubt.

2. Hintergrund

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

2.1. Android

Android ist das populärste Betriebssystem für Mobilgeräte wie Smartphones und Tablets. Das System wird im Rahmen des Android Open Source Project (AOSP) von einigen Geräte-Herstellern unter Federführung von Google entwickelt. Aus technischer Sicht handelt es sich um ein Betriebssystem auf Basis eines Linux-Kernels. Die Userspace-Komponenten weichen jedoch wesentlich von denen jeder anderen Linux-Distribution ab. Sie wurden speziell für die Anforderungen von Mobilegeraten neu entwickelt.

2.2. Sicherheitsarchitektur

Die Sicherheitsarchitektur von Android im Dateisystem basiert auf einer strengen Trennung der Daten jeder einzelnen App. Jede Anwendung läuft in einer isolierten Umgebung („Sandbox“) und erhält ihr eigenes, privates Datenverzeichnis auf dem Dateisystem, das ausschließlich für sie zugänglich ist. Diese privaten Datenordner befinden sich im Verzeichnis /data/data/[App-Paketname]/ und werden automatisch beim Installieren der App erstellt. Nur die jeweilige App selbst hat standardmäßig die Berechtigung, auf ihren Ordner zuzugreifen.

In diesem privaten Ordner kann die App sensible Daten speichern, etwa Benutzereinstellungen, Datenbanken und Cache-Dateien. Die Linux-Berechtigungen und die eindeutige Benutzer-ID (UID), die jeder App zugewiesen wird, sorgen dafür, dass andere Apps und Prozesse standardmäßig nicht auf diesen Ordner zugreifen können. Dadurch wird verhindert, dass Daten unbefugt gelesen oder manipuliert werden.

Auf Android-Geräten gibt es eine Vielzahl von vorinstallierten Apps, die entweder vom Gerätehersteller, Netzbetreiber oder Google selbst stammen. Diese vorinstallierten Apps, oft als “System-Apps” bezeichnet, unterscheiden sich von regulären Benutzer-Apps durch besondere Berechtigungen und eine tiefere Integration in das Betriebssystem. Diese privilegierten Berechtigungen können ihnen Zugriff auf sensiblere Daten und Systemressourcen geben, beispielsweise auf Hardwaresteuerungen, Systemprotokolle, Netzwerkeinstellungen und Standortdaten. Die Berechtigungen für diese Apps werden direkt im Systemcode oder in den Android-Berechtigungslisten definiert und müssen bei der Installation nicht separat vom Benutzer genehmigt werden.

Neben vorinstallierten System-Apps haben auch später installierte Apps die Möglichkeit, privilegierte Berechtigungen zu erhalten, sofern sie mit dem Systemzertifikat des Herstellers signiert sind. Das Systemzertifikat ist ein kryptografisches Zertifikat, das nur vom Gerätehersteller erstellt und kontrolliert wird. Durch diese Signatur wird sichergestellt, dass die App vom Hersteller stammt und als vertrauenswürdig betrachtet wird. Wenn eine App, die nicht ursprünglich vorinstalliert war, mit dem Systemzertifikat signiert ist, kann sie auf spezielle Berechtigungen zugreifen, genau wie die vorinstallierten System-Apps.

Hersteller nutzen diese Möglichkeit häufig, um bestimmte Anwendungen oder Updates für bereits ausgelieferte Geräte bereitzustellen, die tief in die Systemfunktionalitäten integriert sein müssen. Da diese privilegierten Apps potenziell sensible Systemfunktionen beeinflussen können, muss das Betriebssystem sicherstellen, dass nur korrekt signierte und authentifizierte Apps diese Berechtigungen erhalten. Android prüft beim Installationsprozess, ob das Systemzertifikat vorhanden ist und verweigert gegebenenfalls die Installation, falls eine App fälschlicherweise auf Systemrechte zugreifen möchte.

Die Möglichkeit, privilegierte Apps später zu installieren, ist jedoch für den Endnutzer stark eingeschränkt und wird hauptsächlich von den Geräteherstellern und Netzbetreibern genutzt. Nutzer können normalerweise keine Apps selbst mit Systemrechten installieren, da das Zertifikat nicht öffentlich zugänglich ist und für die Sicherheit des Geräts ein wichtiger Kontrollmechanismus bleibt.

2.3. WLAN und WPA2

Die untersuchten Datenmigrations-Tools verwenden für die Datenübertragung WLAN. Diese Technologie, auch bekannt als Wi-Fi, basiert auf dem IEEE-802.11-Standard und ermöglicht drahtlose Netzwerkverbindungen über Funkwellen. Der Standard definiert verschiedene Versionen und Erweiterungen, die unterschiedliche Geschwindigkeiten, Reichweiten und Frequenzbänder bieten. Die gängigsten Frequenzbereiche sind das 2,4-GHz- und das 5-GHz-Band. Die 802.11-Standards umfassen mehrere Varianten, darunter 802.11a, 802.11b, 802.11g, 802.11n, und 802.11ac, die zunehmend höhere Datenübertragungsraten und verbesserte Netzwerkeffizienz ermöglichen. WLAN wird weltweit in privaten Haushalten, Büros und öffentlichen Bereichen verwendet, um Geräte wie Computer, Smartphones, Tablets und Smart-Home-Technologie zu vernetzen. Die Kommunikation findet in der Regel zwischen einem Access Point und einem Client statt. Es sind im alltäglichen Gebrauch Reichweiten bis 45 Meter (2,4-GHz-Band) bzw. 15 Meter (5-GHz-Band) möglich. Abhängig von der Umgebung und verwendeten Endgeräten können diese Werte aber noch deutlich übertroffen werden.

Um zu verhindern, dass die Kommunikation von Angreifern in dieser Reichweite abgehört werden kann, werden Wi-Fi-Netzwerke in der Regel mit einem Sicherheitsprotokoll abgesichert. Aufgrund der breiten Nutzung bei den untersuchten Datenmigrationstools wird hier auf WPA2 näher eingegangen, das als

Nachfolger von WPA und WEP (Wired Equivalent Privacy) entwickelt wurde. Es basiert auf dem AES (Advanced Encryption Standard)-Verschlüsselungsalgorithmus. WPA2 schützt sowohl die Authentifizierung als auch die Datenübertragung und stellt sicher, dass nur autorisierte Geräte auf das Netzwerk zugreifen können. WPA2 wurde 2004 eingeführt und ist bis heute ein weit verbreiteter Standard, der für die meisten modernen WLAN-Netzwerke empfohlen wird. In vielen Fällen verwenden Netzwerke die WPA2-PSK (Pre-Shared Key)-Variante. Diese basiert auf einem geteilten, vorab festgelegten Schlüssel mit einer Mindestlänge von 8 Zeichen. Möchte ein Client eine Verbindung mit dem Access Point aufnehmen, so bekundet er dieses Anliegen dem Access Point, der mit einem zufälligen Wert (Anonce) antwortet. Der Client erzeugt nun ebenfalls einen zufälligen Wert (Snonce), den er an den Access Point sendet. Auf Basis des PSK, des Netzwerknamens (SSID; der vom Access Point in regelmäßigen Abständen unverschlüsselt ausgesendet wird) und der beiden Nonces berechnen beide Kommunikationspartner dann einen Pairwise Transient Key (PTK), der zur Verschlüsselung der weiteren Kommunikation verwendet wird. In der Regel kommt AES als Chiffre zum Einsatz.

Hier muss auf mehrere entscheidende Schwächen von WPA2 eingegangen werden, die es den geprüften Datenmigrations-Tools erschweren, eine sichere Kommunikation zu implementieren:

- Wenn ein passiver Angreifer in Reichweite des Access Points und eines bestimmten Clients den PSK (Passwort des Netzwerks) kennt, kann er deren gesamte Kommunikation entschlüsseln.
- WPA2 ermöglicht Offline-Attacken. Dabei kann ein Angreifer die verschlüsselte Kommunikation aufzeichnen und später knacken.

Um diese Design-Schwächen auszugleichen, müssen Kommunikationspartner zusätzliche Sicherheitsprotokolle auf einer höheren Protokollebene verwenden. Wird das Wi-Fi-Netz für den Internetzugang verwendet, so erfüllt diese Funktion in der Regel die TLS-Verschlüsselung der HTTPS-Verbindungen. Zwar steht mit WPA3 auch schon ein verbessertes Sicherheitsprotokoll für Wi-Fi zur Verfügung, das die Schwächen von WPA2 beseitigt, allerdings wird dieses noch nicht breit eingesetzt.

3. Sicherheitsanalysen

In diesem Abschnitt beschreiben wir die Sicherheitsanalysen, die im Rahmen dieses Projekts durchgeführt wurden.

3.1. Untersuchte Datenmigrations-Tools

Im Rahmen dieses Projekts wurden die Datenmigrationstools zweier populärer Hersteller von mobilen Endgeräten untersucht:

- Xiaomi Mi Mover 4.2.8
- Apple Move to iOS 3.5.5

Beide Anwendungen wurden laut Google Play auf über 100 Millionen Geräten installiert. Auch die grundsätzliche Funktionsweise der beiden Apps ähnelt sich: Das neue Gerät startet einen Wi-Fi-Hostpot, agiert also als Access Point. Das alte Gerät verbindet sich mit diesem Access Point. Danach werden über TCP die Daten vom alten an das neue Gerät übertragen.

3.2. Methodik

Die Anwendungen wurden zunächst einmal ausgeführt, um die Funktionsweise zu analysieren:

- Welche WPA-Version wird verwendet?
- Wie wird die Verbindung aufgebaut?

Anschließend wurde jede App statisch untersucht, um Informationen zu möglichen Schwachstellen zu erlangen:

- Wie wird der WPA2 Pre-Shared-Key errechnet?
- Wird ein zusätzliches Sicherheitsprotokoll verwendet, um die Schwachstellen von WPA2 auszugleichen?

Zur statischen Analyse kamen die Tools JADX (für Dalvik Bytecode) und Ghidra (für native Shared Objects) zum Einsatz.

Wenn durch die statische Analyse der Verdacht auf Schwachstellen aufkam, intensivierten wir unsere Untersuchungen mittels dynamischer Analyse. Hier wurde unter anderem die Wi-Fi-Kommunikation aufgezeichnet und mit dem (in der Benutzeroberfläche angezeigten) PSK entschlüsselt. Dazu verwendeten wir Kali-Linux auf einem Raspberry Pi 5. Zum Mitlesen der Wi-Fi-Frames muss ein Wi-Fi-Adapter verwendet werden, der den sogenannten Monitor-Modus unterstützt. Wir verwendeten hier einen Adapter mit dem mt7610u-Chipsatz von Mediatek.

4. Ergebnisse

4.1. Apple Move to iOS

Das Tool dient der Migration von Daten von einem Android-Gerät zu einem iOS-Gerät. Da die App Android-seitig über keine besonderen Berechtigungen verfügt, können nur Daten übertragen werden, die über öffentliche Schnittstellen zugänglich sind. Insbesondere sind hier Bilder, Videos und Dokumente zu erwähnen, die dennoch höchst persönliche Inhalte haben können.

Zum Verbindungsaufbau setzt die App voraus, dass der Nutzer einen am (neuen) iOS-Gerät angezeigten 6-stelligen Pin abliest und am (alten) Android-Gerät in die Move to iOS-App einträgt. Der am iOS-Gerät gestartete Wi-Fi-Hotspot verwendet WPA2.

Bei der statischen Analyse der App zeigt sich, dass die SSID des Access Points auch als dessen PSK verwendet wird. Da die SSID regelmäßig unverschlüsselt an alle Geräte in der Umgebung ausgesendet wird, kann dadurch jedes beliebige Gerät in Reichweite eine Wi-Fi-Verbindung mit dem iOS-Gerät herstellen. Kenntnis des oben beschriebenen Pins ist dazu nicht nötig. Die SSID des Access Points ergibt sich aus einem konstanten String und den ersten 5 Zeichen der hexadezimalen Darstellung des SHA1-Hashes der ersten 2 Ziffern des Pins. Aufgrund des sehr begrenzten Suchraumes, können also anhand der SSID die ersten 2 Ziffern des Pins mittels Brute-Forcing errechnet werden. Effektiv sind damit also nur die restlichen 4 Ziffern des Pins tatsächlich geheim. Es gibt damit lediglich 10^4 mögliche Pins.

Die Entropie des Pins spielt für die Sicherheit der weiteren TCP-Verbindung allerdings keine Rolle, da die App das Secure Remote Password-Protokoll verwenden. Dabei wird der Pin so in einen asymmetrischen Schlüsselaustausch eingeflochten, dass nicht nur ein passives Mitlesen verunmöglicht wird, sondern auch ein Man-In-The-Middle-Angriff ohne Kenntnis des Pins verhindert werden kann. Entscheidend ist hier, dass Brute-Forcing des Pins unterbunden wird, indem ein Verbindungsaufbau mit einem falschen Pin sofort dazu führt, dass ein neuer Pin generiert und verwendet wird. Wir konnten in der statischen Analyse feststellen, dass genau das in allen möglichen Fehlerfällen geschieht. Der mittels SRP ausverhandelte Schlüssel wird dann dazu genutzt, verschlüsselt TLS-Zertifikate auszutauschen. Diese werden dann für eine TLS-Verbindung genutzt, über die die eigentlichen Daten übertragen werden.

4.2. Xiaomi Mi Mover

Xiaomi Mi Mover dient der schnellen Einrichtung eines neuen Xiaomi-Geräts mit Daten eines vorher genutzten Android-Geräts. Im Allgemeinen überträgt die App App-Installationsdateien (APK), nicht aber die durch den Betrieb der Apps abgelegten App-Daten. Außerdem können insbesondere Bilder, Videos und Dokumente übertragen werden. Handelt es sich auch beim alten Gerät um ein Xiaomi-Gerät, können weit mehr Informationen übernommen werden. Unterstützt werden dann etwa die App-Daten, System-Einstellungen und die eingespeicherten Zugangsdaten zu Wi-Fi-Netzwerken.

Bei der Analyse der Funktionalität zeigt sich, dass der Verbindungsaufbau weitestgehend automatisch vonstatten geht. Der Nutzer muss lediglich in der Benutzeroberfläche am alten Gerät das neue Gerät (das den Access Point startet) auswählen. Diese Funktionsweise legt die Vermutung nahe, dass irgendeine Art von Kommunikation im Nahbereich (NFC, Bluetooth) verwendet wird, um im ersten Schritt den PSK des Wi-Fi-Netzes an das alte Gerät so zu übergeben, dass physische Nähe und damit Beobachtbarkeit des kommunizierenden Geräts gegeben sind.

Die statische Analyse der App zeigt, dass zwar solche Funktionalität in der App vorhanden ist, allerdings nicht genutzt wird. Stattdessen wird der PSK von der zufälligen SSID des Access Points abgeleitet. Das bedeutet, dass bei Kenntnis der genauen Ableitungs-Funktion jeder Angreifer in Wi-Fi-Reichweite des Access Points den PSK selbst ableiten und die Kommunikation aller in Reichweite befindlichen Clients entschlüsseln kann. Um Angreifern die Kenntnis der Ableitungs-Funktion zu erschweren, wurde sie in einer nativen Bibliothek implementiert. Es handelt sich hier also um einen Fall von Security-by-Obscurity.

Die weitere Analyse der App zeigt außerdem, dass abgesehen von WPA2 kein weiteres Sicherheitsprotokoll verwendet wird. Das bedeutet, dass selbst bei Nutzung eines zufälligen Wi-Fi-Passwortes ein Offline-Angriff auf die Kommunikation möglich wäre.

Als zusätzliche „Sicherheitsmaßnahme“ darf sich im vom Xiaomi Mi Mover erstellten Access Point nur ein einzelner Client befinden. Versucht sich ein weiterer Client zu verbinden, wird der Handshake selbst bei korrektem PSK zurückgewiesen. Mit dieser Vorkehrung soll wohl verhindert werden, dass ein Angreifer sich während einer laufenden Verbindung einschleicht und Daten in die Kommunikation injiziert. Hier wird allerdings übersehen, dass es mittels Multi-Channel Man-In-The-Middle-Angriff auch möglich ist, Wi-Fi-Frames in die Verbindung so zu injizieren, dass es für den Access Point aussieht, als käme alle Kommunikation von einem einzelnen (dem legitimen) Client.

Sobald ein Client sich erfolgreich mit dem Access Point am neuen Gerät verbunden hat, konfiguriert Mi Mover diesen neu, sodass das 5GHz-Band genutzt wird. Dies soll wohl eine höhere Datenrate ermöglichen. Anschließend wählt der Nutzer am alten Gerät die zu übertragenden Daten aus und bestätigt den Transport. Dieser wird dann über ein proprietäres Protokoll abgewickelt, das auf Protobuf basiert. Daten werden zu TAR-Archiven zusammengefasst und in dieser Form übertragen. Vor jeder Übertragung werden Metadaten übermittelt, die zum Beispiel Applikations-Pakete so markieren, dass sie am Zielgerät nach erfolgreicher Übertragung samt ihrer App-Daten installiert werden. Zur Datenübertragung werden mehrere parallele Verbindungen aufgebaut.

5. Angriff auf Xiaomi Mi Mover

Auf Basis der Erkenntnisse der Sicherheitsanalyse von Xiaomi Mi Mover wurde ein Angriff (Exploit) implementiert, der es einem passiven Angreifer in Wi-Fi-Reichweite erlaubt, alle übertragenen Daten mitzulesen. Der Angreifer folgt dazu diesen Schritten:

1. Der Angreifer scannt die SSID Beacons in allen Wi-Fi-Channels im 5GHz-Band (der für die eigentliche Datenübertragung genutzt wird), bis er eine Netzwerk findet, das anhand des ersten Teils der SSID als Xiaomi Mi Mover identifiziert werden kann.

2. Der Angreifer nutzt etwa Wireshark, um die Kommunikation im identifizierten Netzwerk aufzuzeichnen, bis durch eine Dissoziation sichtbar wird, dass die Übertragung beendet wurde.

3. Der Angreifer benutzt eine leicht modifizierte Version der statischen Bibliothek (natives Shared Object) aus der Xiaomi Mi Mover-App, um aus der SSID den PSK zu errechnen. Als Teil der Modifikation wird der Signatur-Check entfernt, der sicherstellen soll, dass die Bibliothek nur in der unveränderten Mi Mover-App verwendet werden kann. Für unseren Exploit nutzen wir die Java-Bibliothek unidbg [1], um die Bibliothek zu emulieren, also unabhängig vom Android-Betriebssystem und vom ARM-Instruktionssatz auf einem beliebigen Computer ausführen zu können.

4. Der Angreifer nutzt etwa Wireshark [2], um die aufgezeichnete Kommunikation mittels des generierten PSK und der aufgezeichneten Nonces aus dem Handshake zu entschlüsseln.

5. Der Angreifer extrahiert die parallelen TCP-Streams aus der entschlüsselten Kommunikation, setzt die Pakete dabei in die richtige Reihenfolge und entfernt doppelt übertragene Pakete. Auch hierfür kann Wireshark genutzt werden.

6. Der Angreifer interpretiert die extrahierte Kommunikation auf Basis der Protobuf-Definitionen des proprietären Übertragungsprotokolls. Für unseren Exploit konnten wir diese Definitionen mittels einer Kombination aus manueller Arbeit und protodump [3] extrahieren. Ein eigens geschriebenes Tool trennt dann die Daten-Metadaten und Inhalte voneinander.

Ein Prototyp dieses Exploits wurde implementiert und mitsamt einer Zusammenfassung unserer Sicherheitsanalyse im Oktober 2024 an Xiaomi übermittelt.

6. Zusammenfassung

In diesem Projekt wurden zwei Daten-Migrationstools von populären Herstellern mobiler Geräte auf ihre Sicherheit hin untersucht. Hierzu wurden die Anwendungen zunächst augenscheinlich anhand ihrer Funktionalität beurteilt, sowie dann statischen und dynamischen Analysen ausgesetzt. Dabei zeigten sich bei Xiaomi Mi Mover erhebliche Sicherheitsprobleme, die zum unerkannten Diebstahl aller übertragenen Daten führen können.

Referenzen

[1] Banny, „unidbg: Emulate Android native libraries," 2024. [Online].

[2] W. Foundation, „WireShark: The world's most popular network protocol analyzer," 2024. [Online]. Available: https://www.wireshark.org.

[3] A. Tetelman, „protodump: A utility to dump all Protobuf file descriptors from a given binary as *.proto files," 2024. [Online]. Available: https://github.com/arkadiyt/protodump.