A-SIT

Zentrum für sichere Informationstechnologie - Austria

Man-In-The-Middle-Angriffe auf Wi-Fi

Man-In-The-Middle-Angriffe auf Wi-Fi

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

Datum: 07.01.2026

Abstract/Zusammenfassung:
Drahtlose Netzwerkkommunikation mittels Wi-Fi ist heute ein selbstverständlicher Teil des Alltags. Besonders auf Mobilgeräten wie Smartphones wird die Technologie vielfältig genutzt, etwa nicht nur zur Anbindung des Geräts selbst an das Internet, sondern auch zur Weitergabe von Mobilfunkverbindungen an andere Geräte. Den meisten Anwendern sind trotz der selbstverständlichen Nutzung dieser Technologie allerdings die vielfältigen Sicherheits-Schwächen nicht bewusst, die der Fachwelt teils schon seit Jahrzehnten bekannt sind.

Im Rahmen dieses Projekts wurde anhand des konkreten Szenarios von Internetfreigabe mittels Wi-Fi-Tethering erforscht, inwieweit Netzwerk-Stacks aktueller Smartphones von bekannten Sicherheits-Schwächen von Wi-Fi betroffen sind, bzw. welche Angriffe dadurch ermöglicht werden. In diesem Bericht erläutern wir dazu 3 verschiedene Angriffe und ihre Implementierung, evaluieren sie im genannten Szenario und vergleichen ihre Charakteristiken. Abschließend diskutieren wir Möglichkeiten zur Erkennung und Unterbindung der Angriffe.

Inhalt

1. Einleitung

Die breite Verfügbarkeit von schnellem drahtlosem Internet über Wi-Fi bildet einen der Grundpfeiler der heutigen digitalen Welt. Zwar bieten moderne Mobilfunkverträge mittlerweile so hohe Datenvolumina, dass Smartphones permanent im Netz sein können, doch verfügen Endgeräte wie Laptops noch immer nur in Ausnahmefällen über Mobilfunkmodule. Soll etwa ein Laptop unterwegs mit dem Internet verbunden werden, so kommt in der Regel Wi-Fi zum Einsatz. Hotels, Restaurants, Cafés oder öffentliche Verkehrsmittel bieten hierzu immer häufiger kostenlose Wi-Fi-Hotspots an. Steht ein solcher nicht zur Verfügung, so greifen Nutzer üblicherweise auf Wi-Fi-Tethering zurück. Dabei wird die mobilfunkbasierte Internetverbindung des Smartphones via Wi-Fi an den Laptop weitergegeben. Auf technischer Ebene startet das Smartphone dazu einen Wi-Fi-Hotspot und überbrückt Daten zwischen dem Wi-Fi- und dem Mobilfunk-Netzwerkadapter.

Die drahtlose Übertragung von Netzwerkdaten mittels Wi-Fi ermöglicht hier Nutzungsszenarien, die mit traditionellen Kabelverbindungen nicht oder nur wesentlich unbequemer möglich wären. Zum Beispiel erlaubt Wi-Fi das freie Bewegen des Geräts innerhalb des Empfangsbereichs. Während diese gewonnene Bequemlichkeit der Technologie sofort augenscheinlich ist, verfügen drahtlose Netzwerkverbindungen auch über geänderte Anforderungen in Bezug auf die Übertragungssicherheit.

Das Internet und eine Vielzahl weiterer Netzwerkanwendungen nutzen die Protokolle der TCP/IP-Familie als technische Basis für die Kommunikation. Auch bei Wi-Fi-Verbindungen wird TCP/IP verwendet, um die übertragenen Daten zu verpacken und geordnet zwischen verschiedenen Geräten zu übertragen. TCP/IP wurde allerdings ursprünglich für kabelgebundene Anwendungen konzipiert. In dieser Konfiguration sind Gefahrenszenarien relativ übersichtlich. Informationen werden nur entlang der physischen Verbindungen ausgetauscht, sodass ein potentieller Angreifer zunächst physischen Zugang zu einer Netzwerkbuchse oder einem Kabel benötigt. Im Gegensatz dazu werden die Informationen bei Wi-Fi-Netzwerken (etwas vereinfacht) als Funkwellen in alle Richtungen übertragen. Um zu verhindern, dass jeder Unbeteiligte in Funk-Reichweite die Kommunikation mitlesen bzw. beeinflussen kann, müssen die Daten verschlüsselt werden. Ein weiterer entscheidender Unterschied ergibt sich aus den verwendeten Routing-Mechanismen. Bei kabelgebundenen Verbindungen werden üblicherweise moderne Netzwerk-Switches verwendet, um mehrere Netzwerkteilnehmer miteinander zu verbinden. Diese Switches enthalten Logik, um Netzwerkpakete nur an den im Paket vermerkten Empfänger weiterzuleiten. Ein unbeteiligtes ans Netzwerk angeschlossenes Gerät kann also keine Kommunikation mitlesen, die zwischen zwei anderen Teilnehmern ausgetauscht wird. In einem Wi-Fi-Netzwerk sind alle Teilnehmer über ein gemeinsames Medium (die Luft bzw. Funkwellen in der Luft) verbunden, sodass eine solche Filterung nicht möglich ist. Ein bösartiger Netzwerkteilnehmer kann also, falls keine zusätzliche Verschlüsselung verwendet wird, die Kommunikation aller anderen Teilnehmer abhören. Unabhängig von der Verschlüsselung ist die Manipulation der Kommunikation möglich. Konkret kann ein Angreifer im einfachsten Fall zum Beispiel Störsignale senden, die dazu führen, dass die Wi-Fi-Pakete nicht ankommen.

Angesichts der Vielzahl an Möglichkeiten für Angriffe auf Wi-Fi im Vergleich zu kabelgebundenen Netzwerkverbindungen und der weiten Verbreitung von Wi-Fi insbesondere in Mobilgeräten, stellt sich die Frage der Umsetzbarkeit bzw. Praxisrelevanz von Angriffen auf Wi-Fi. Im Rahmen dieses Projektes wurde daher das mobile Betriebssystem Android auf die Anfälligkeit auf 3 verschiedene Angriffe getestet. Ein besonderer Fokus wurde hier auf solche Angriffe gelegt, die dem Angreifer nicht nur das Auslesen, sondern auch die Manipulation der entschlüsselten Kommunikation ermöglichen. Zwar wurden hierfür keine grundsätzlich neuen Angriffe gefunden, jedoch wurden bestehende Ansätze für den Netzwerk-Stack von Android adaptiert bzw. optimiert. Das Ziel dieses Berichts ist es, auf Basis der Praxisrelevanz der verschiedenen Angriffe das Bewusstsein für Datensicherheit in Wi-Fi-Netzwerken zu schärfen. In diesem Sinne wird abschließend ein kurzer Überblick über Maßnahmen zur Erkennung und Unterbindung

von Angriffen geboten. Dabei werden sowohl Techniken diskutiert, die in die bestehenden Protokoll-Stacks integriert werden können, als auch allgemeine Empfehlungen an Endanwender.

2. Hintergrund

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

2.1. TCP/IP

Das Internet und zahlreiche lokale Netzwerkanwendungen basieren auf der TCP/IP-Protokollfamilie als technische Grundlage für die Kommunikation. TCP/IP definiert dabei ein Schichtenmodell mit klaren Verantwortlichkeiten: die Link-Schicht (physisches Medium und MAC-Adressierung), die Internet-Schicht (IP-Adressierung und Routing), die Transport-Schicht (z. B. TCP, UDP) sowie die Anwendungsschicht (HTTP, DNS u. a.). Diese Aufteilung ermöglicht, dass unterschiedliche Übertragungsmedien wie Kupferkabel, Glasfaser oder Funk dieselben darüber liegenden Protokolle nutzen können.

Auf der Link-Schicht identifizieren Media Access Control (MAC)-Adressen Netzwerkinterfaces eindeutig innerhalb eines lokalen Übertragungsbereichs (meist ein Local Area Network bzw. LAN). MAC-Adressen sind hardwarebezogen und werden von Netzwerkgeräten beim Versand von Netzwerkpaketen (sogenannten Netzwerk-Frames) genutzt, um Ziel und Quelle innerhalb eines LANs anzugeben. Auf der Internet-Schicht übernehmen IP-Adressen (IPv4 oder IPv6) die logische Identifikation von Hosts und sind notwendig, damit Router Pakete zwischen unterschiedlichen Netzwerken weiterleiten können. Die Adressierung in beiden Schichten ist komplementär: MAC steuert die lokale Zustellung, IP das bereichsübergreifende Routing.

Die darüberliegende Transport-Schicht unterscheidet zwischen verbindungsorientierten Diensten (Transport Control Protocol bzw. TCP) und verbindungslosen Diensten (User Data Protocol bzw. UDP). TCP stellt Zuverlässigkeit durch Verbindungsaufbau, Sequenzierung, Wiederholung verlorener Pakete und Flusskontrolle sicher - Eigenschaften, die für viele Anwendungen wichtig sind. UDP bleibt leichtgewichtig und eignet sich für zeitkritische Anwendungen, ist jedoch ohne zusätzliche Maßnahmen nicht zuverlässig.

2.2. ARP

Wie oben beschrieben, verfügen Netzwerkteilnehmer in TCP/IP-Netzwerken in der Regel über 2 verschiedene Adressen: Eine MAC-Adresse und eine IP-Adresse. Dabei dient die MAC-Adresse (zumindest theoretisch) zur eindeutigen Identifikation eines Netzwerkinterfaces. Sie wird in der Regel vom Hersteller in der Fabrik weitgehend zufällig zugewiesen. In der höherliegenden Transportschicht wird zur Adressierung von Paketen die IP-Adresse verwendet. Um Pakete der Transportschicht (Adressierung mit IP-Adresse) mittels Frames auf Link-Schicht (MAC-Adressen) zustellen zu können, müssen die Netzwerkteilnehmer wissen, unter welcher MAC-Adresse der Teilnehmer mit der gewünschten IP-Adresse verfügbar ist. Hierfür wird das Address Resolution Protocol (ARP) [1] verwendet. Möchte ein Netzwerkteilnehmer ein Datenpaket an einen anderen Teilnehmer mit einer bestimmten IP-Adresse verschicken, so sendet er mittels Broadcast eine ARP-Anfrage an alle anderen Teilnehmer im Netzwerk. Die Anfrage enthält die IP-Adresse, deren Besitzer gefunden werden soll, sowie die MAC-Adresse und IP-Adresse der nachfragenden Partei. Jeder Teilnehmer, der die Nachfrage empfängt, vergleicht die enthaltene IP-Adresse mit der eigenen. Liegt eine Übereinstimmung vor, so antwortet der Teilnehmer direkt an den Fragesteller. Dieser kann nun mit der Zustellung der IP-Kommunikation beginnen.

Netzwerkanwendungen werden meist im Hinblick auf Performance-Eigenschaften wie Datendurchsatz und Latenz optimiert. Hier ist es natürlich hinderlich, wenn für jede neue Verbindung auf IP-Ebene zunächst die MAC-Adresse abgefragt werden muss. Aus diesem Grund speichern sich Netzwerkteilnehmer diese Zuordnung in einem Cache namens ARP-Tabelle. So müssen nur dann ARP-Abfragen abgewickelt werden, wenn für den gewünschten Teilnehmer (Ziel-Host) kein Eintrag in der Tabelle besteht. Um zusätzlich sicherzustellen, dass ARP-Anfragen möglichst selten geschickt werden müssen, senden Teilnehmer üblicherweise bei Änderung ihrer IP-Adresse proaktiv sogenannte gratuitous (sinngemäß unangefordert) ARP-Nachrichten. Hier handelt es sich um ARP-Antworten, die ohne entsprechende Nachfrage an alle Netzwerkteilnehmer im LAN ausgesendet werden. Diese werden dann in der ARP-Tabelle berücksichtigt.

2.3. DHCP

Als weiterer wichtiger Bestandteil des TCP/IP-Netzwerkstacks muss hier noch DHCP, das Dynamic Host Configuration Protocol [2], beschrieben werden. Dieses wird benötigt, um die Teilnehmer in einem Netzwerk dynamisch mit IP-Adressen auszustatten. Hat sich ein Netzwerkteilnehmer auf Link-Level mit einem Netzwerk verbunden, so sendet er eine DHCP-Discover-Nachricht als Link-Layer-Broadcast an alle anderen Teilnehmer. Befindet sich unter diesen ein DHCP-Server, so antwortet er üblicherweise mit einem DHCP Offer, in dem er die Nutzung einer konkreten IP-Adresse für eine bestimmte Dauer anbietet. Möchte der neue Teilnehmer (DHCP-Client) dieses Angebot annehmen, so antwortet er mit einem DHCP Request, der abschließend noch vom DHCP-Server mit einem DHCP Acknowledgement bestätigt wird. Um die Dauer dieser Interaktion zu verkürzen, steht bei entsprechender Unterstützung von Server und Client ein beschleunigter Prozess namens Rapid Commit zur Verfügung. Hier reagiert der DHCP-Server anstatt des DHCP Offers schon in der ersten Antwort mit einem DHCP Acknowledgement. Er stellt damit in einer einzigen Nachricht schon eine sofort nutzbare IP-Lease zur Verfügung, die vom Client nicht mehr separat angefragt werden muss.

DHCP wird meist nicht nur zur zentralen und dynamischen Verwaltung von IP-Adressen verwendet, sondern auch, um neuen Netzwerkteilnehmern die IP-Adressen von wichtigen Anlaufstellen im Netzwerk mitzuteilen. So enthalten die vom DHCP-Server ausgeschickten Antworten die IP-Adressen des DNS-Servers, der zur Übersetzung von Domänennamen zu IP-Adressen kontaktiert werden kann, und des Standard-Gateways. Dieser dient als Brücke zu anderen Netzwerken, und in der Regel auch zum Internet. Vereinfacht gesagt werden alle Pakete, die an IP-Adressen gesendet werden sollen, die nicht im lokalen Netzwerk existieren, dem Standard-Gateway zur Weitervermittlung übergeben. Dieser verfügt in der Regel über Routing-Tabellen, mithilfe derer er entscheiden kann, wohin er das Paket weiterleitet. Dieser Mechanismus ist essentiell für die Möglichkeit, IP-Pakete zwischen verschiedenen Netzwerken auf Link-Ebene zu übertragen.

2.4. Wi-Fi und WPA/WPA2/WPA3

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. In der Praxis kommen hier heutzutage üblicherweise WPA2 und WPA3 zum Einsatz. WPA2 wurde als Nachfolger von WPA und WEP (Wired Equivalent Privacy) entwickelt, die mittlerweile als unsicher eingestuft werden. 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. 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. Obwohl WPA2-PSK besonders bei privaten Anwendern große Popularität genießt, enthält der Standard entscheidende Schwächen. Nicht nur teilen alle Netzwerkteilnehmer denselben Pre-Shared-Key (umgangssprachlich meist Wi-Fi-Passwort genannt), zusätzlich lässt sich bei WPA2-PSK bei Kenntnis des PSKs und des Client-Handshakes der PTK ableiten. Der Client-Handshake kann von einem Angreifer in Wi-Fi-Reichweite trivial mitaufgezeichnet werden. In vielen Szenarien (etwa öffentliche Hotspots in Cafes, Hotels, etc.) ist auch der PSK einer großen Anzahl an Personen bekannt. Das Szenario einer Aufzeichnung aller übertragenen Daten (die nicht auf höheren Netzwerkschichten zusätzlich verschlüsselt sind) ist also durchaus realistisch. Im Unterschied zu WPA2 kann beim neueren WPA3-Standard der Pairwise Transient Key auch dann nicht nachvollzogen werden, wenn der Angreifer über Kenntnis des PSK und eine Aufzeichnung des Client-Handshakes verfügt. WPA3 ist also WPA2 in allen Anwendungsfällen vorzuziehen. Zwar verfügen viele Wi-Fi-Hotspots schon über die Möglichkeit für WPA3-Verbindungen, allerdings werden sie oft im Transition Mode betrieben, um auch die Kompatibilität mit älteren Geräten sicherzustellen. Der Client hat dabei die Wahl, ob WPA2 oder WPA3 verwendet wird. Entscheidet er sich für WPA2, so bestehen immer noch die oben beschriebenen Einschränkungen in Bezug auf die Verbindungssicherheit.

3. Konkretes Evaluierungssetup

Im Rahmen dieses Projektes wurde die Umsetzbarkeit und Effektivität verschiedener Man-In-The-Middle-Angriffe auf Wi-Fi-Verbindungen von mobilen Endgeräten evaluiert. Bei einem Man-In-The-Middle-Angriff (oder auch Machine-In-The-Middle-Angriff) befindet sich der Angreifer in einer Position zwischen zwei Geräten (im Weiteren Gerät A und B), die miteinander kommunizieren. Zwar wirkt es für die beiden Geräte, als ob sie direkt miteinander kommunizieren würden, tatsächlich aber gehen alle gesendeten Pakete zunächst an den Angreifer, der sie dann an das jeweils andere Gerät weiterleitet. Selbst wenn die Pakete verschlüsselt sind und der Angreifer keine Kenntnisse zum Schlüssel hat, hat er also die Möglichkeit, die Kommunikation zu beeinflussen, indem er etwa selektiv Pakete unterschlägt, also nicht an das andere Gerät weiterleitet. Verfügt der Angreifer über Kenntnisse des Schlüssels (etwa weil WPA2 verwendet wird und der Angreifer den PSK kennt und damit aus einem aufgezeichneten Handshake den PTK ableiten kann) oder werden Daten unverschlüsselt übertragen (zum Beispiel weil in einem Wi-Fi-Netzwerk gar keine Verschlüsselung verwendet wird), so kann er die Daten mitlesen oder vor dem Weiterleiten auch verändern.

Um einen solchen Angriff in einem realen Umfeld umsetzen zu können, muss sich der Angreifer innerhalb der Reichweite von Wi-Fi befinden. Bei Netzwerken im 2.4GHz-Spektrum bedeutet das eine ungefähre maximale Distanz vom Hotspot von 30 Metern bzw. 20 Meter für Netzwerke im 5Ghz-Spektrum.

Zusätzlich muss der Angreifer über passende Hardware verfügen, konkret ein Wi-Fi-Interface, das im Monitor-Mode betrieben werden kann. Günstige Varianten können schon für etwa 20€ erworben werden.

Für dieses Projekt wurde folgendes konkretes Szenario evaluiert. Es wurde ein Smartphone verwendet, um einen Wi-Fi-Hotspot mittels Tethering (also der Möglichkeit zur drahtlosen Freigabe der mobilen Internetverbindung an andere Geräte via Wi-Fi) zu starten. Dieses Gerät fungiert auch als Gerät A, auch wenn im Allgemeinen die Funktion von Hotspot und Gerät A nicht zwangsläufig im gleichen Gerät vereint sein müssen. Anschließend wurde ein zweites Smartphone als Wi-Fi-Client verwendet, der sich mit dem Wi-Fi-Hotspot verbindet. Dabei handelt es sich um das im Weiteren Gerät B bezeichnete Opfer des Angriffs.

Das Ziel des Angreifers war es in allen Fällen, die Netzwerkkommunikation zwischen den Geräten A und B so umzuleiten, dass er eine Man-In-The-Middle-Position erlangt. Dazu wurden Angriffstechniken auf unterschiedlichen Ebenen des Netzwerk-Stacks evaluiert. Es muss festgehalten werden, dass moderne Android-Geräte in der Regel ihre MAC-Adresse für jede neue Netzwerkverbindung zufällig generieren. Der Angreifer kennt daher im Vorfeld weder die MAC-Adresse noch die IP-Adresse von Gerät B.

Alle Angriffe wurden auf einem Raspberry Pi 5 umgesetzt, auf dem Kali Linux ausgeführt wurde. Die Angriffe wurden jeweils in Python auf Basis der Bibliothek Scapy [3] implementiert. Da für manche Angriffe ein Wi-Fi-Interface benötigt wurde, das in den Monitor-Mode versetzt werden kann, wurde über USB ein externes Interface auf Basis des Chipsatzes MT7921 der Marke Mediatek angeschlossen. Im Monitor-Mode kann dieses auch Wi-Fi-Frames mitlesen, die an andere Netzwerkteilnehmer adressiert wurden. Die Effektivität mancher Angriffe kann durch die Verwendung mehrerer Netzwerk-Interfaces erhöht werden. Hier verwendeten wir 2 der beschriebenen externen Interfaces.

4. ARP Spoofing

Beim ARP-Spoofing versucht der Angreifer, den ARP-Cache des Opfers (Gerät B) so zu modifizieren, dass die Auflösung einer bestimmten IP-Adresse (zB. die von Gerät A) in der MAC-Adresse des Angreifers statt des tatsächlichen Ziel-Geräts resultiert. Dazu sendet der Angreifer gratuitous ARP-Nachrichten, um anderen Netzwerkteilnehmern weißzumachen, er sei der legitime Besitzer der IP-Adresse eines anderen Netzwerkteilnehmers. Da der Angriff oberhalb des Link-Layers stattfindet, muss der Angreifer entweder ein offenes Wi-Fi-Netzwerk vorfinden oder über Kenntnis des PSK verfügen.

Bei der Implementierung dieses Angriffs muss der Angreifer zunächst eine Verbindung zum Wi-Fi-Hotspot herstellen. Weiters wurde davon ausgegangen, dass der Angreifer diese Verbindung noch vor dem Opfer herstellt. Er muss dann möglichst früh erkennen, dass sich Gerät B mit dem Netzwerk verbindet. Je früher er dies erkennt, desto kürzer ist die Zeit, in der der ARP-Cache von Gerät B die korrekte MAC-Adresse für Gerät A enthält. In dieser Zeit verfügt der Angreifer über keine MITM-Position. Für unsere Implementierung beobachten wir daher die DHCP-Broadcasts im Netzwerk. Sobald Gerät B auf Link-Level die Verbindung aufgebaut hat, beantragt es mittels DHCP Discover eine IP-Adresse. Ab diesem Zeitpunkt hat der Angreifer alle nötigen Informationen, um das eigentliche ARP-Spoofing zu starten. Er schickt nun in möglichst rascher Abfolge gratuitous ARP-Nachrichten, die als Quell-MAC-Adresse die tatsächliche MAC-Adresse des Angreifers, aber als IP-Adresse jene von Gerät A enthalten. Hat das Opfer die Nachricht empfangen und seine ARP-Tabelle entsprechend adaptiert, so schickt es IP-Pakete, die eigentlich an Gerät A gehen sollten, an den Angreifer. Der Angreifer kann nun entscheiden, ob er die Pakete an Gerät A weiterleitet bzw. ob er sie vorher noch modifiziert.

Um festzustellen, ob der Angriff funktioniert, wurde auf Gerät A ein HTTP-Server gestartet, auf den von Gerät B zugegriffen wurde. Der Angreifer wurde als simpler Proxy implementiert, der die empfangenen

Anfragen protokolliert, aber unverändert an das eigentliche Zielgerät weiterleitet.

In unserer Evaluierung funktionierte dieser Angriff bei verschiedenen Android-Geräten von Samsung und Google mit Android 14, 15 und 16 zuverlässig. Es ist allerdings festzuhalten, dass für einen kurzen Augenblick direkt nach dem Herstellen der Wi-Fi-Verbindung von Gerät B dessen ARP-Tabelle die korrekte MAC-Adresse von Gerät A für dessen IP-Adresse enthält. Baut Gerät B genau in diesem Moment eine Verbindung zu Gerät A auf, so ist diese nicht vom MITM-Angriff betroffen.

5. DHCP Spoofing

DHCP Spoofing setzt auch oberhalb des Link-Layers an, dort aber etwas früher als ARP Spoofing. Der Angriff besteht im Wesentlichen aus zwei Schritten. Im ersten Schritt beansprucht der Angreifer alle zur Verfügung stehenden DHCP-Leases für sich. Im zweiten Schritt übernimmt er die Rolle des DHCP-Servers im Netzwerk und antwortet selbst auf DHCP-Anfragen. Das eigentliche Ziel des Angriffs ist nun nicht die Kontrolle über die Zuweisungen von IP-Adressen, sondern über die Informationen zum DNS-Server und Standard-Gateway, die ebenfalls in den DHCP-Antworten enthalten sind. Positioniert sich der Angreifer als Standard-Gateway, gehen beispielsweise alle Pakete, die an externe Netzwerke (zB. das Internet) weitergeleitet werden müssen, an ihn.

Um die DHCP-Leases des Servers aufzubrauchen muss der Angreifer so viele DHCP-Requests an den Server schicken, wie Leases zur Verfügung stehen. Die genaue Anzahl hängt von der Größe des Subnetzes ab. Die Android-Tethering-Implementierung verwendet ein Subnetz von maximal 255 Clients, sodass die Anzahl an benötigten DHCP-Requests überschaubar bleibt. In der Implementierung sind hier dennoch einige Besonderheiten zu berücksichtigen, auf die hier nicht näher eingegangen werden soll, um keine Hilfestellung für reale Angriffe zu liefern. Unsere Implementierung ist in der Lage, im getesteten Szenario alle Leases innerhalb von weniger als einer Sekunde aufzubrauchen.

Für alle weiteren Bitten um eine IP-Adresse antwortet der DHCP-Server nun mit einem NAK (Non-Acknowledgement), er teilt also mit, dass er leider nicht dienlich sein kann. Die DHCP-Client-Implementierung von Android (die das Verhalten des Linux-Programms dhcpcd nachempfindet) ignoriert diese NAK-Antworten im Wesentlichen und wartet weiterhin auf eine positive DHCP-Antwort inklusive DHCP-Lease. Diese Eigenheit der Implementierung kann sich der Angreifer hier zunutze machen: Da der Client zu Beginn der Interaktion keinerlei Information über den DHCP-Server hat, sendet er die DHCP-Discover-Nachricht als Broadcast an alle Teilnehmer im Netzwerk. Auch der Angreifer empfängt sie also, und kann anhand der enthaltenen Informationen (insb. Transaktions-Identifier) eine Antwort verfassen. In diese kann er beliebige Hosts als DNS-Server und Standard-Gateway eintragen. Bestimmt er sich selbst, so verfügt er nun über eine MITM-Position für alle Verbindungen in externe Netzwerke.

Um festzustellen, ob der Angriff funktioniert, nahmen wir hier der Einfachheit halber ein etwas verändertes Szenario an: Wir gingen davon aus, dass eine Anwendung auf Gerät B über die Android-API den Standard-Gateway abfragt und eine HTTP-Verbindung zu diesem aufbaut. Weiters gingen wir davon aus, dass der Standard-Gateway wie im schon oben beschriebenen Szenario mit Gerät A übereinstimmt.

Dieser Angriff funktionierte auf den erwähnten Android-Geräten von Samsung und Google mit Android 14, 15, und 16 einwandfrei.

6. Multi-Channel Man-In-The-Middle Angriff

Im Gegensatz zu den vorher beschriebenen Angriffen operiert dieser Angriff auf dem Link-Layer, also auf den Wi-Fi-Frames. Die generelle Wirkungsweise wurde von Mathy Vanhoef et al. erstmals präsentiert [4]. Sie basiert auf einer Lücke in der Wi-Fi-Spezifikation: Es ist als unauthentifizierter Angreifer möglich, an Netzwerkteilnehmer eine Aufforderung zum Wechsel der Kommunikationsfrequenz zu senden. Dazu muss der Angreifer den PSK des Netzwerks nicht kennen. Der Hotspot selbst bekommt von dieser Aufforderung nichts mit. Vollzieht ein Client den Wechsel, agiert der Angreifer nun als Proxy zwischen der legitimen Frequenz des Hotspots und der davon unterschiedlichen anderen Frequenz, auf die er die Wi-Fi-Clients umgeleitet hat. Er hat damit effektiv eine MITM-Position eingenommen.

Dieser Angriff wurde wie auch die anderen Angriffe auf Smartphones von Samsung und Google mit den Android-Versionen 14 bis 16 evaluiert. Auch wenn der Angriff prinzipiell funktioniert, muss erwähnt werden, dass es im von uns getesteten Setup immer wieder zu Problemen kam. In manchen Fällen konnten die Clients nicht davon überzeugt werden, die Kommunikationsfrequenz zu wechseln und kommunizierten daher weiterhin direkt mit dem Hotspot. Vanhoef et al. empfehlen für den Angriff ein etwas abweichendes Setup mit Wi-Fi-Interfaces auf Basis der Chipsets Atheros AR9001 oder AR9002 [5]. Die Probleme mit der Verlässlichkeit des Angriffs könnten mit diesem Unterschied zusammenhängen.

7. Vergleich der Angriffe

Alle implementierten Angriffe unterscheiden sich etwas hinsichtlich Verlässlichkeit und möglichen Einsatzzwecken. Hier soll daher kurz ein Vergleich geschaffen werden.

Die Kriterien die hier zur Unterscheidung herangezogen werden sind:

- **Funktions-Ebene (im Netzwerkstack) des Angriffs**
  Hiervon hängt ab, ob der Angreifer vor dem Angriff eine Netzwerkverbindung aufbauen muss. Dazu muss er entweder den PSK kennen oder ein unverschlüsseltes Netzwerk vorfinden.
- **Scope**
  Welche Verbindungen können angegriffen werden?
- **Verlässlichkeit**
  Wie zuverlässig funktioniert der Angriff, bzw. welche Quellen für Unzuverlässigkeit gibt es?

Der Vergleich zwischen den evaluierten Angriffen stellt sich wie in *Tabelle 1* gezeigt dar.

Angriff	Funktions-Ebene	Scope	Verlässlichkeit
ARP Spoofing	Internet-Schicht (ARP)	Lokale Verbindungen	Sehr hoch nach kurzer Einrichtung
DHCP Spoofing	Internet-Schicht (DHCP)	Verbindungen in externe Netze	Sehr hoch
Multi-Channel MITM	Link-Schicht (802.11)	Alle Verbindungen	Abhängig von Setup

Tabelle 1 *Vergleich der evaluierten Angriffe*

8. Gegenmaßnahmen

Als Ergebnis unserer Evaluierung müssen wir feststellen, dass alle getesteten Angriffe nach wie vor effektiv ausgenützt werden können. Im Folgenden präsentieren wir einerseits Möglichkeiten zur automatischen Erkennung und Unterbindung solcher Angriffe, als auch andererseits vorbeugende Maßnahmen, die einen Angriff auf konkrete Nutzer verhindern können.

8.1. Automatische Erkennung bzw. Unterbindung der Angriffe

Dass die getesteten Angriffe trotz Bekanntheit nie behoben wurden, hat damit zu tun, dass häufig nicht so einfach zwischen bösartigem und gutartigem Verhalten unterschieden werden kann. Im Folgenden diskutieren wir trotzdem Möglichkeiten, wie Angriffe jeweils auf Protokoll-Ebene erkannt bzw. unterbunden werden können.

- ARP-Spoofing
  In der Forschung wurden hier in der Vergangenheit verschiedene Heuristiken präsentiert, die ARP-Spoofing-Angriffe entweder mittels passiver Beobachtung der Netzwerkkommunikation [6] oder mittels aktivem Probings [7] zu erkennen versuchen. Wurde ein Netzwerkteilnehmer als bösartig identifiziert, so kann er aus der ARP-Tabelle entfernt und jede weitere Kommunikation ignoriert werden.

- DHCP-Spoofing
  Die einfachste Lösung wäre hier, wenn Clients nach Erhalt eines NAK keine Antworten von anderen DHCP-Servern mehr akzeptieren. Vor allem im Privatanwender-Bereich befindet sich der legitime DHCP-Server meist auf jenem Host, der als Wi-Fi-Hotspot agiert. Da in Wi-Fi-Netzwerken die Kommunikation zwischen Netzwerkteilnehmern immer über den Wi-Fi-Hotspot erfolgen muss, empfängt also der legitime DHCP-Server Anfragen als Erster und kann auch als Erster antworten. Enthält jede Anfrage eine eindeutige zufällige Transaktions-ID, so besteht keine Möglichkeit, wie ein anderer Netzwerkteilnehmer vor dem legitimen DHCP-Server antworten kann.

- Multi-Channel-MITM
  Dieser Angriff funktioniert nur, solange Management-Frames für den Kanalwechsel unverschlüsselt akzeptiert werden. Eine naive Lösung wäre also, hier Verschlüsselung vorauszusetzen. Im Prinzip wird dies in WPA3 auch umgesetzt, wo Management Frame Protection verpflichtend genutzt werden muss. Allerdings sind Beacon-Frames von dieser Regelung ausgenommen, sodass Channel Switch Announcements noch immer gefälscht werden können [8].

8.2. Vorbeugende Maßnahmen für Endanwender

Endanwender sollten Vorsicht walten lassen, wann immer sie sich in Netzwerken befinden, zu denen eine große Zahl anderer (unbekannter) Nutzer Zugang hat. Besonders in solchen Netzwerken ist es wichtig, darauf zu achten, dass Verbindungen auf Anwendungsebene verschlüsselt sind. Wird das Netzwerk zum Webbrowsen verwendet, zeigt der Browser in der Regel an, falls eine Seite keine TLS-Verschlüsselung verwendet. Im Standardfall (bei Verwendung von HTTP über TLS, also HTTPS) besteht dann keine Gefahr, dass übertragene Daten ausgespäht oder modifiziert werden können. Dennoch kann ein Angreifer anhand der kontaktierten IP-Adressen aber zumindest grob nachvollziehen, mit welchen Websites kommuniziert wird. Dieses Risiko kann weiter reduziert werden, indem Nutzer nur über ein vertrauenswürdiges VPN auf das Internet zugreifen.

9. Zusammenfassung

Drahtlose Netzwerkverbindungen via Wi-Fi sind für die meisten Nutzer alltägliche Begleiter. Trotz dieser zentralen Rolle der Technologie in der modernen vernetzten Welt sind schon seit Jahren Schwachstellen in den involvierten Protokollen bekannt, die in Angriffen ausgenutzt werden können. In diesem Projekt haben wir untersucht, inwieweit diese Angriffe gegen moderne Mobilgeräte im konkreten Szenario des Wi-Fi-Tethering verwendet werden können. Wir mussten feststellen, dass mobile Geräte nach wie vor von ARP-Spoofing, DHCP-Spoofing und Multi-Channel-Man-In-The-Middle-Angriffen betroffen sind. Neben einem Vergleich dieser Angriffe auf Basis unserer Implementierungen diskutierten wir in diesem Bericht auch Möglichkeiten, um diese Angriffe zu unterbinden bzw. einem Angriff vorzubeugen.

Referenzen

[1] Network Working Group, „RFC 826," 11 1982. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc826.

[2] Network Working Group, „RFC 1531," 1993. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc1531.

[3] The Scapy community, „Scapy: the Python-based interactive packet manipulation program & library," 2024. [Online]. Available: https://github.com/secdev/scapy.

[4] M. a. P. F. Vanhoef, „Advanced Wi-Fi attacks using commodity hardware," in *Proceedings of the 30th Annual Computer Security Applications Conference (ACSAC '14)*, 2014.

[5] M. Vanhoef, „Multi-Channel Machine-in-the-Middle," 2022. [Online]. Available: https://github.com/vanhoefm/mc-mitm?tab=readme-ov-file#3-launching-the-attack.

[6] A. I. A. E. B. Mohammed M. Alani, „ARP-PROBE: An ARP spoofing detector for Internet of Things networks using explainable deep learning," *Internet of Things,* Bd. 23, 2023.

[7] V. N. S. Ramachandran, „Detecting ARP Spoofing: An Active Technique," in *Information Systems Security. ICISS 2005*, 2005.

[8] M. Vanhoef, „Attacking WPA3: New Vulnerabilities & Exploit Framework," 2022. [Online]. Available: https://conference.hitb.org/hitbsecconf2022sin/materials/D1T1%20-%20Attacking%20WPA3%20-%20New%20Vulnerabilities%20and%20Exploit%20Framework%20-%20Mathy%20Vanhoef.pdf.