Einführung in Wireless Security

Bedeutung von Wireless Security

In der heutigen Zeit sind drahtlose Netzwerke überall - von Smartphones über Laptops bis hin zu Smart-Home-Geräten. Wireless Security ist wichtig, um die Privatsphäre und Sicherheit von Informationen in diesen Netzwerken zu schützen. Wenn ein drahtloses Netzwerk nicht ausreichend gesichert ist, können Angreifer auf persönliche Daten zugreifen, den Datenverkehr manipulieren oder das Netzwerk sogar lahmlegen.

Herausforderungen der Sicherheit in drahtlosen Netzwerken

Drahtlose Netzwerke sind anfälliger für Angriffe als kabelgebundene Netzwerke, da die Kommunikation über Funkwellen stattfindet. Diese können von jedem innerhalb der Reichweite des Signals abgefangen oder gestört werden. Daher müssen wir spezielle Sicherheitsmaßnahmen ergreifen, um unsere drahtlosen Netzwerke zu schützen.

Grundlagen von Wireless-Technologien und Funkwellen

Wireless-Technologien ermöglichen die Kommunikation zwischen Geräten ohne physische Verbindungen, indem sie elektromagnetische Wellen, sogenannte Funkwellen, verwenden. Die am häufigsten verwendeten Wireless-Technologien sind Wi-Fi, Bluetooth, NFC und Zigbee.

Funkwellen sind elektromagnetische Wellen, die Informationen übertragen, indem sie die Frequenz, Amplitude oder Phase der Wellen modulieren. Sie breiten sich in alle Richtungen von der Antenne aus, die sie abstrahlt, und können von anderen Antennen empfangen werden. Die Reichweite von Funkwellen ist begrenzt und hängt von der Sendeleistung, der Empfangsempfindlichkeit und den Umgebungsbedingungen ab.

Bedrohungen und Angriffe auf drahtlose Netzwerke

a. Eavesdropping (Lauschangriffe)

Eavesdropping ist der Prozess, bei dem ein Angreifer den drahtlosen Datenverkehr abfängt und überwacht, um vertrauliche Informationen wie Passwörter oder persönliche Daten abzugreifen. Dies kann erreicht werden, indem man sich in Reichweite des drahtlosen Signals aufhält und spezielle Software oder Hardware verwendet, um den Datenverkehr abzuhören.

b. Man-in-the-Middle-Angriffe

Bei einem Man-in-the-Middle-Angriff fängt ein Angreifer Kommunikationen zwischen zwei Geräten ab, dies baut meist auf anderen Angriffen auf(siehe Rogue AP, Evil Twin). Der Angreifer kann die Kommunikation manipulieren, indem er Informationen ändert oder hinzufügt, bevor sie an das ursprüngliche Ziel weitergeleitet werden.

c. Rogue Access Points (bösartige Zugangspunkte)

Ein Rogue Access Point ist ein unbefugter drahtloser Zugangspunkt mit meist ähnlichem Namen wie bestehende APs, der in einem Netzwerk eingerichtet wurde, um unbemerkt Daten abzugreifen oder Angriffe auszuführen. Benutzer, die sich versehentlich mit dem Rogue Access Point verbinden, können Opfer von Datendiebstahl oder Man-in-the-Middle-Angriffen werden.

d. Denial-of-Service (DoS) Angriffe

Ein Denial-of-Service-Angriff tritt auf, wenn ein Angreifer absichtlich den Datenverkehr in einem drahtlosen Netzwerk überlastet oder stört, um es unbenutzbar zu machen. Dies kann durch Überflutung des Netzwerks mit gefälschtem Datenverkehr oder durch gezielte Störung der Funkkommunikation erreicht werden.

e. Spoofing und Fälschung von Netzwerkadressen

Spoofing bezieht sich auf das Vorgeben, ein anderes Gerät im Netzwerk zu sein, indem man dessen Identität, wie zum Beispiel die MAC- oder IP-Adresse, annimmt. Angreifer können Spoofing-Techniken verwenden, um sich als legitimes Gerät auszugeben und Zugang zu vertraulichen Informationen zu erlangen oder das Netzwerk zu manipulieren.

f. Wireless-Phishing und Evil Twin-Angriffe

Wireless-Phishing ist eine Form des Phishing-Angriffs, bei dem ein Angreifer ein gefälschtes drahtloses Netzwerk erstellt, das einem legitimen Netzwerk sehr ähnlich ist. Benutzer, die sich mit dem gefälschten Netzwerk verbinden, können ihre Anmeldedaten und persönlichen Informationen preisgeben. Ein Evil Twin ist ein spezieller Typ eines Rogue Access Points, der einem legitimen Zugangspunkt sehr ähnlich ist, um Benutzer dazu zu verleiten, sich damit zu verbinden.

WLAN (IEEE 802.11X)

Unterschiede zwischen 2,4 GHz und 5 GHz Wi-Fi-Frequenzbändern

Wi-Fi-Netzwerke arbeiten auf zwei Hauptfrequenzbändern: 2,4 GHz und 5 GHz. Jedes Band hat seine eigenen Vor- und Nachteile, die sich auf die Leistung und Reichweite des drahtlosen Netzwerks auswirken.

2,4 GHz-Frequenzband

Das 2,4 GHz-Band war das erste Frequenzband, das für Wi-Fi-Netzwerke verwendet wurde und ist bis heute weit verbreitet.

Vorteile:

- **Bessere Reichweite:** Die 2,4 GHz-Frequenzwellen haben eine größere Reichweite und können leichter durch Wände und andere Hindernisse dringen. Dies macht sie ideal für den Einsatz in größeren Häusern oder Gebäuden, in denen eine gute Abdeckung erforderlich ist.
- **Kompatibilität:** Da das 2,4 GHz-Band länger in Gebrauch ist, sind die meisten Wi-Fi-fähigen Geräte damit kompatibel. Dies gewährleistet eine breite Geräteunterstützung in Ihrem drahtlosen Netzwerk.

Nachteile:

- **Störanfälligkeit:** Das 2,4 GHz-Band ist anfälliger für Interferenzen durch andere Geräte, die im gleichen Frequenzbereich arbeiten, wie zum Beispiel Mikrowellen, schnurlose Telefone und Bluetooth-Geräte. Dies kann zu einer schlechteren Verbindungsqualität und geringeren Datenübertragungsraten führen.
- **Geringere maximale Datenübertragungsraten:** Das 2,4 GHz-Band bietet im Allgemeinen niedrigere maximale Datenübertragungsraten im Vergleich zum 5 GHz-Band.

5 GHz-Frequenzband

Das 5 GHz-Band wurde später eingeführt, um die Nachteile des 2,4 GHz-Bandes zu überwinden und bietet einige Verbesserungen in Bezug auf Geschwindigkeit und Störfestigkeit.

Vorteile:

- **Höhere maximale Datenübertragungsraten:** Das 5 GHz-Band ermöglicht höhere Datenübertragungsraten im Vergleich zum 2,4 GHz-Band.

Dies führt zu schnelleren Downloads und besserer Leistung bei bandbreitenintensiven Anwendungen wie Video-Streaming oder Online-Gaming.

- **Weniger Störungen:** Das 5 GHz-Band ist weniger anfällig für Interferenzen durch andere Geräte, da es weniger überfüllt ist und mehr nicht überlappende Kanäle zur Verfügung stehen. Dies resultiert in einer stabileren und zuverlässigeren Verbindung.

Nachteile:

- **Kürzere Reichweite:** Die 5 GHz-Frequenzwellen haben eine kürzere Reichweite und können nicht so leicht durch Wände und andere Hindernisse dringen. Dies kann zu einer schlechteren Abdeckung in größeren Gebäuden führen.
- **Eingeschränkte Kompatibilität:** Nicht alle Wi-Fi-Geräte sind mit dem 5 GHz-Band kompatibel, insbesondere ältere Geräte. Dies kann die Geräteunterstützung in Ihrem drahtlosen Netzwerk einschränken.

Verschlüsselung und Authentifizierung

Wired Equivalent Privacy (WEP)

WEP war der erste Sicherheitsstandard für Wi-Fi-Netzwerke und sollte ein Sicherheitsniveau bieten, das dem kabelgebundener Netzwerke entspricht. WEP verwendet eine symmetrische Verschlüsselung, um den Datenverkehr zwischen Geräten und Zugangspunkten zu schützen. Allerdings wurde WEP aufgrund von Schwachstellen in der Verschlüsselung und Authentifizierung schnell als unsicher eingestuft und ist heute veraltet.

Wi-Fi Protected Access (WPA) und WPA2

WPA wurde als Ersatz für WEP entwickelt und bietet verbesserte Sicherheitsfunktionen, wie die Temporal Key Integrity Protocol (TKIP)-Verschlüsselung und die 802.1X-Authentifizierung. WPA2, der Nachfolger von WPA, führte die Advanced Encryption Standard (AES)-Verschlüsselung ein, die für eine höhere Sicherheit sorgt. WPA2 ist der am häufigsten verwendete Sicherheitsstandard für Wi-Fi-Netzwerke und wird für die meisten drahtlosen Netzwerke empfohlen.

Wi-Fi Protected Access 3 (WPA3)

WPA3 ist der neueste Wi-Fi-Sicherheitsstandard und bietet verbesserte Sicherheitsfunktionen im Vergleich zu WPA2. Dazu gehören eine stärkere Verschlüsselung, verbesserte Schutzmechanismen gegen Brute-Force-Angriffe und eine einfachere Konfiguration für IoT-Geräte. WPA3 wird zunehmend in neuen Geräten und Netzwerken eingesetzt, um ein höheres Sicherheitsniveau zu bieten.

802.1X-Authentifizierung und Extensible Authentication Protocol (EAP)

Die 802.1X-Authentifizierung ist ein Standard, der in WPA und WPA2 verwendet wird, um Benutzer und Geräte zu authentifizieren, bevor sie auf das Netzwerk zugreifen können. 802.1X verwendet das Extensible Authentication Protocol (EAP), um verschiedene Authentifizierungsmethoden wie Passwörter, digitale Zertifikate oder Smartcards zu unterstützen. Dies ermöglicht ein flexibles und sicheres Authentifizierungssystem für drahtlose Netzwerke.

Pre-shared Key (PSK) und Enterprise-Authentifizierung

Drahtlose Netzwerke können entweder eine Pre-shared Key (PSK)- oder eine Enterprise-Authentifizierung verwenden. Bei der PSK-Authentifizierung teilen sich alle Benutzer und Geräte im Netzwerk denselben Passwortschlüssel, der für den Zugriff auf das Netzwerk erforderlich ist. Diese Methode ist einfach einzurichten und für Heim- und kleine Unternehmensnetzwerke geeignet. Allerdings ist sie anfälliger für Angriffe, da ein einziger kompromittierter Schlüssel das gesamte Netzwerk gefährdet.

Enterprise-Authentifizierung, hingegen, verwendet individuelle Anmeldeinformationen für jeden Benutzer und erfordert in der Regel die Verwendung eines Remote Authentication Dial-In User Service (RADIUS)-Servers. Enterprise-Authentifizierung bietet mehr Sicherheit und Kontrolle, ist jedoch komplexer einzurichten und wird hauptsächlich in größeren Unternehmensnetzwerken eingesetzt.

Wi-Fi Protected Setup (WPS)

Wi-Fi Protected Setup (WPS) ist ein optionaler Standard, der entwickelt wurde, um die Einrichtung von Wi-Fi-Netzwerken für Benutzer zu vereinfachen. WPS ermöglicht es Benutzern, Geräte schnell und einfach mit dem Netzwerk zu verbinden, indem sie entweder eine PIN eingeben, einen physischen Knopf am Router drücken oder eine NFC-Verbindung (Near Field Communication) verwenden.

Obwohl WPS bequem ist, hat es auch bekannte Sicherheitsprobleme, insbesondere im Zusammenhang mit der PIN-basierten Methode. Da die PIN in der Regel nur acht Ziffern hat, kann sie durch Brute-Force-Angriffe relativ einfach geknackt werden. Um die Sicherheit zu erhöhen, empfiehlt es sich, WPS auf dem Router zu deaktivieren und alternative Methoden zur Verbindung von Geräten zu verwenden.

Konkrete Angriffe auf WLAN-Netzwerke

Es gibt verschiedene Angriffstechniken, die speziell darauf abzielen, die Sicherheit von WLAN-Netzwerken zu kompromittieren. Einige der bekanntesten Angriffe

sind der Deauthentication-Angriff, der Yes Man (Ja-Sager)-Angriff und der Karma-Angriff.

a. Mitlesen von unverschlüsselten Traffic

Das Mitlesen von unverschlüsseltem WiFi-Verkehr, auch als "Sniffing" bekannt, ist ein Prozess, bei dem ein Angreifer Datenpakete, die über ein drahtloses Netzwerk gesendet oder empfangen werden, abfängt und analysiert. Wenn das WiFi-Netzwerk nicht durch eine Verschlüsselungstechnologie wie WPA2 oder WPA3 gesichert ist, werden die Datenpakete in Klartext übertragen. Dies ermöglicht es einem Angreifer, der die richtige Software und Hardware (wie einen WiFi-Adapter im Promiscuous-Modus) verwendet, vertrauliche Informationen wie Benutzernamen, Passwörter, Kreditkartendaten oder andere persönliche Informationen zu sehen, wenn sie über das Netzwerk gesendet werden. Dies unterstreicht die Wichtigkeit der Verwendung von Verschlüsselung, um die Privatsphäre und Sicherheit von Daten in WiFi-Netzwerken zu gewährleisten.

b. Deauthentication-Angriff (Deauth)

Ein Deauthentication-Angriff ist eine Art von Denial-of-Service (DoS)-Angriff, bei dem der Angreifer gefälschte Deauthentifizierungspakete an ein WLAN-Gerät oder einen Zugangspunkt sendet. Diese Pakete täuschen vor, von einem legitimen Gerät oder Zugangspunkt zu stammen, und veranlassen das Ziel, die Verbindung zum Netzwerk zu trennen. Durch wiederholtes Senden dieser Pakete kann ein Angreifer die Verbindung eines Geräts zum Netzwerk effektiv stören und es daran hindern, wieder eine Verbindung herzustellen.

Einschub: WLAN-Beaconing

WLAN-Beaconing ist ein Kommunikationsprozess in einem drahtlosen Netzwerk, bei dem ein Endgeräte regelmäßig "Beacon"-Pakete über ihm bekannte Netzwerke aussenden. Diese Beacon-Pakete enthalten wichtige Informationen über das Netzwerk, wie zum Beispiel die Netzwerk-SSID (Service Set Identifier), die Verschlüsselungs- und Authentifizierungsmethoden, die unterstützt werden, sowie die Kanalnummer, auf der der Zugangspunkt sendet.

Beacon-Pakete werden typischerweise alle 100 ms gesendet und dienen dazu, die Existenz des Netzwerks für Wi-Fi-Geräte in Reichweite bekannt zu machen. Wenn ein Gerät nach verfügbaren WLAN-Netzwerken sucht, empfängt es die Beacon-Pakete von den verschiedenen Zugangspunkten in seiner Nähe und zeigt sie in der Liste der verfügbaren Netzwerke an.

Es ist erwähnenswert, dass WLAN-Beaconing auch einige Sicherheitsbedenken mit sich bringt. Da Beacon-Pakete unverschlüsselt gesendet werden und die Netzwerk-SSID sowie andere Informationen enthalten, können Angreifer diese Pakete abfangen und verwenden, um Informationen über das Netzwerk zu sammeln. Dies kann als Ausgangspunkt für weitere Angriffe auf das WLAN-Netzwerk

dienen, wie zum Beispiel den oben erwähnten Karma-Angriff. Aus diesem Grund ist es wichtig, sichere Authentifizierungs- und Verschlüsselungsmethoden zu verwenden, um den Schutz Ihres drahtlosen Netzwerks zu gewährleisten.

c. Ja-Sager-Angriff (Auch oft Karma genannt)

Ein Yes Man- oder Ja-Sager-Angriff ist eine Variante des Rogue Access Point-Angriffs. Bei diesem Angriff stellt der Angreifer einen unbefugten Zugangspunkt auf, der automatisch alle Verbindungsanfragen von Wi-Fi-Geräten in Reichweite akzeptiert, unabhängig von der SSID oder den Sicherheitseinstellungen. Diese Taktik kann dazu führen, dass ahnungslose Benutzer automatisch mit dem bösartigen Zugangspunkt verbunden werden, wenn sie nach einem bekannten Netzwerk suchen oder wenn die Verbindung zu ihrem bevorzugten Netzwerk verloren geht. Sobald ein Benutzer mit dem bösartigen Zugangspunkt verbunden ist, kann der Angreifer den Datenverkehr abfangen oder Man-in-the-Middle-Angriffe durchführen.

Mobilfunknetze

Mobilfunknetze ermöglichen die drahtlose Kommunikation über große Entfernungen und sind eine der wichtigsten Technologien für mobile Geräte wie Smartphones und Tablets. Im Gegensatz zu Wi-Fi, das auf kurze Reichweiten und lokale Netzwerke ausgelegt ist, bieten Mobilfunknetze eine breitere Abdeckung und ermöglichen die Kommunikation zwischen Geräten, die kilometerweit voneinander entfernt sind.

a. Grundlegende Funktion und Komponenten von Mobilfunknetzen

Ein Mobilfunknetz besteht aus mehreren Komponenten, die zusammenarbeiten, um eine kontinuierliche Verbindung und Datenübertragung zwischen mobilen Geräten und dem Netzwerk zu ermöglichen:

1. **Mobiltelefone (Endgeräte):** Die mobilen Geräte, die mit dem Mobilfunknetz verbunden sind, um Sprachanrufe, SMS und mobile Datenverbindungen zu ermöglichen.
2. **Basisstationen (BTS) oder Funkzellen:** Basisstationen sind Funkmasten oder Antennen, die in einem geografischen Gebiet (einer Zelle) installiert sind und mit den mobilen Geräten kommunizieren. Sie übertragen und empfangen Funksignale und leiten sie an das Kernnetz weiter.
3. **Mobilfunknetz (Kernnetz):** Das Kernnetz ist das zentrale Kommunikationssystem, das die verschiedenen Basisstationen miteinander verbindet und die Anrufvermittlung, SMS-Dienste und den Internetzugang steuert.

b. Mobilfunkstandards und Sicherheitsmerkmale/Probleme

Es gibt verschiedene Mobilfunkstandards, die im Laufe der Jahre entwickelt wurden, um höhere Geschwindigkeiten, verbesserte Leistung und erweiterte Funktionen zu bieten. Im Folgenden finden Sie eine Übersicht über die verschiedenen Standards und ihre Sicherheitsmerkmale/Probleme:

1G (erste Generation)

1G war der erste Mobilfunkstandard, der in den 1980er Jahren eingeführt wurde. Er basierte auf analoger Technologie und bot nur grundlegende Sprachkommunikation. Die Sicherheitsmaßnahmen waren minimal und leicht angreifbar, da die Kommunikation unverschlüsselt war und leicht abgehört werden konnte.

2G (zweite Generation)

2G wurde in den 1990er Jahren eingeführt und war der erste digitale Mobilfunkstandard. Er führte Verschlüsselung und verbesserte Authentifizierung ein, um die Sicherheit der Kommunikation zu erhöhen. Der bekannteste 2G-Standard ist das Global System for Mobile Communications (GSM).

Einschub: "Export grade encryption" bezieht sich auf eine Zeit, in der die US-Regierung die Stärke der Verschlüsselungsalgorithmen einschränkte, die für den Export außerhalb der USA zugelassen waren. Diese schwächeren Verschlüsselungsstandards sollten den US-Geheimdiensten das Abhören und Entschlüsseln von Kommunikationen erleichtern. Export grade encryption war in den 1990er Jahren weit verbreitet, insbesondere während der Einführung von 2G-Mobilfunknetzen.

Der 2G-Standard, insbesondere das Global System for Mobile Communications (GSM), verwendete schwächere Verschlüsselungsalgorithmen, die als A5/2 bekannt sind. Diese waren weniger sicher als die stärkeren A5/1-Algorithmen, die in den USA und Europa eingesetzt wurden. A5/2 wurde aufgrund von Exportbeschränkungen in Ländern außerhalb der USA und der Europäischen Union verwendet. Die Schwäche der A5/2-Verschlüsselung führte dazu, dass 2G-Netzwerke anfällig für Angriffe waren, bei denen Kommunikationen abgehört und entschlüsselt werden konnten.

Trotz der Verbesserungen gegenüber 1G ist die Sicherheit von 2G immer noch anfällig für Angriffe. Beispielsweise verwendet GSM eine Verschlüsselung namens A5/1, die als unsicher gilt und durch verschiedene Angriffe geknackt werden kann, wie z. B. den Rainbow-Table-Angriff.

3G (dritte Generation)

3G wurde Anfang der 2000er Jahre eingeführt und bot höhere Datenübertragungsraten sowie bessere Sprachqualität im Vergleich zu 2G. 3G führte auch verbesserte Verschlüsselung und Authentifizierung ein, um die Sicherheit zu

erhöhen. Die bekanntesten 3G-Standards sind UMTS (Universal Mobile Telecommunications System) und CDMAhere Datenübertragungsraten sowie bessere Sprachqualität im Vergleich zu 2G. 3G führte auch verbesserte Verschlüsselung und Authentifizierung ein, um die Sicherheit zu erhöhen. Die bekanntesten 3G-Standards sind UMTS (Universal Mobile Telecommunications System) und CDMA2000.

Trotz der Sicherheitsverbesserungen in 3G sind immer noch einige Schwachstellen und Angriffe möglich, insbesondere aufgrund von Schwächen in der Implementierung oder in älteren Protokollen, die noch in den Netzwerken verwendet werden.

4G (vierte Generation)

4G wurde Ende der 2000er Jahre eingeführt und bietet im Vergleich zu 3G deutlich höhere Datenübertragungsraten und bessere Netzwerkeffizienz. Der bekannteste 4G-Standard ist LTE (Long-Term Evolution). 4G hat die Sicherheit weiter verbessert, indem es stärkere Verschlüsselung und bessere Authentifizierungsmethoden eingeführt hat.

Dennoch gibt es auch in 4G einige Sicherheitsprobleme, wie z. B. Angriffe auf die Datenschutz- und Anonymitätsmechanismen, die es Angreifern ermöglichen könnten, den Standort von Benutzern zu verfolgen oder ihre Kommunikation abzufangen.

5G (fünfte Generation)

5G ist der neueste Mobilfunkstandard, der in den 2020er Jahren eingeführt wurde. Er bietet im Vergleich zu 4G noch höhere Datenübertragungsraten, geringere Latenz und verbesserte Konnektivität. 5G setzt auf die Sicherheitsverbesserungen der vorherigen Generationen auf und führt zusätzliche Sicherheitsmechanismen ein, wie z. B. verbesserte Verschlüsselung und stärkere Benutzerauthentifizierung.

Angriffe auf Mobilfunknetze

Mobilfunknetze, genau wie andere Kommunikationsnetze, sind anfällig für verschiedene Angriffe, die sowohl die Privatsphäre der Benutzer als auch die Integrität der Netzwerkinfrastruktur beeinträchtigen können. Im Folgenden sind einige der bekanntesten Angriffe auf Mobilfunknetze beschrieben:

a. IMSI-Catcher (International Mobile Subscriber Identity-Catcher)

Ein IMSI-Catcher ist ein Gerät, das verwendet wird, um Mobiltelefone in seiner Nähe zu identifizieren und abzuhören, indem es vorgibt, eine legitime Basisstation (Funkzelle) zu sein. Das Gerät fängt die IMSI-Nummern ab, die die eindeutige

Identität jedes Mobiltelefons im Netzwerk darstellen. Angreifer können IMSI-Catcher verwenden, um den Standort von Mobiltelefonen zu verfolgen, Gespräche abzuhören oder SMS-Nachrichten zu lesen.

b. SS7-Angriffe (Signalling System No. 7)

SS7 ist ein Kommunikationsprotokoll, das in Telekommunikationsnetzen verwendet wird, um Sprach- und SMS-Dienste zu ermöglichen. Sicherheitslücken im SS7-Protokoll können Angreifern ermöglichen, Anrufe und SMS-Nachrichten abzufangen, den Standort von Mobiltelefonen zu verfolgen und sogar Gespräche abzuhören. Diese Angriffe sind oft schwer zu erkennen und können ohne physischen Zugriff auf das Zielgerät durchgeführt werden.

c. Downgrade-Angriffe

Downgrade-Angriffe treten auf, wenn ein Angreifer die Kommunikation zwischen einem Mobiltelefon und einer Basisstation manipuliert, um die Verbindung auf einen älteren, unsicheren Standard herabzustufen. Zum Beispiel könnte ein Angreifer einen 4G-LTE-Handybenutzer zwingen, eine Verbindung über das weniger sichere 2G- oder 3G-Netzwerk herzustellen. Sobald die Verbindung herabgestuft wurde, kann der Angreifer die Schwächen des älteren Standards ausnutzen, um Kommunikationen abzufangen oder den Standort des Benutzers zu verfolgen.

d. SIM-Swap-Angriffe

Ein SIM-Swap-Angriff tritt auf, wenn ein Angreifer die Kontrolle über die Telefonnummer eines Opfers übernimmt, indem er den Mobilfunkanbieter dazu bringt, die Telefonnummer auf eine andere SIM-Karte zu übertragen, die sich im Besitz des Angreifers befindet. Diese Angriffe werden oft durch Social Engineering oder Insider-Betrug ermöglicht. Sobald der Angreifer die Kontrolle über die Telefonnummer hat, kann er Anrufe und SMS-Nachrichten empfangen, die an das Opfer gerichtet sind, und so möglicherweise Zugang zu persönlichen Daten oder Konten des Opfers erhalten.