Rich Communication Services als Nachfolger der SMS

David Olbertz
Hochschule Bonn-Rhein-Sieg
Sankt-Augustin, Germany
davidolbertz@gmail.com

***Abstract*—Der Abstract wurde noch nicht verfasst.**

I. Einleitung

Heutzutage ist das Smartphone ein wichtiger Bestandteil des Alltags. Es ermöglicht unter anderem die Kommunikation über große Distanzen hinweg, egal ob im privaten oder beruflichen Umfeld.

Zur Kommunikation existiert neben der Telefonie der altbekannte Short Message Service (SMS), welcher es ermöglicht, einfache Kurznachrichten zu versenden. Allerdings wird diese Kommunikationsmethode mittlerweile immer weniger genutzt und wurde größtenteils durch Over-the-Top Instant Messenger, welche deutlich mehr Funktionalitäten bieten, wie z.B. Gruppenchats und das Teilen von Medien. Zusätzlich sind Nachrichten meist Ende-zu-Ende-Verschlüsselt und das Senden ist gebührenfrei [1]. Dieser Trend bewegte die GSM Association dazu, einen neuen moderneren Kommunikationsstandard zu entwickeln, welcher ähnliche Funktionen wie die Over-the-Top Instant Messenger bieten. Anders ist, dass es von Mobilfunkbetreibern anstatt von einem großen Unternehmen betrieben wird und dadurch auf fast allen Endgeräten verfügbar ist [2], [3].

Ziel dieser Seminararbeit ist, Rich Communication Services (RCS) als Nachfolger der SMS zu betrachten. Dazu werden zuerst die aktuell gängigen Technologien behandelt und anschließend auf RCS im Detail eingegangen. Neben der Definition und Funktionsweise werden auch weitere Aspekte, wie die Vor- und Nachteile der RCS, dargestellt. Dabei werden auch die Eigenschaften von RCS mit denen von SMS verglichen, wobei besonders die Sicherheit eine große Rolle spielt.

II. Entwicklung

A. Short Message Service

Der Short Message Service, kurz SMS, ist seit den späten 1990er Jahren im Einsatz [4]. Dafür wurde der Global System for Mobile Communications Standard etabliert, welcher von dem European Telecommunications Standards Institute entwickelt wurde [5]. SMS erlaubt es Nutzern mittels eines Mobiltelefons kurze Textnachrichten an andere Personen zu verschicken, unabhängig von der Distanz [4]. Die Nachrichten können standardmäßig in der 7-Bit-Kodierung eine Länge von 160 Zeichen haben. Das SMS Protokoll besteht aus vier Schichten, die alle Informationen zum Versenden, wie unter anderem den Empfänger und der Nachrichteninhalt selbst, enthalten. Zu den Schichten gehört der Application Layer, Transfer Layer, Relay Layer und Link Layer [5].

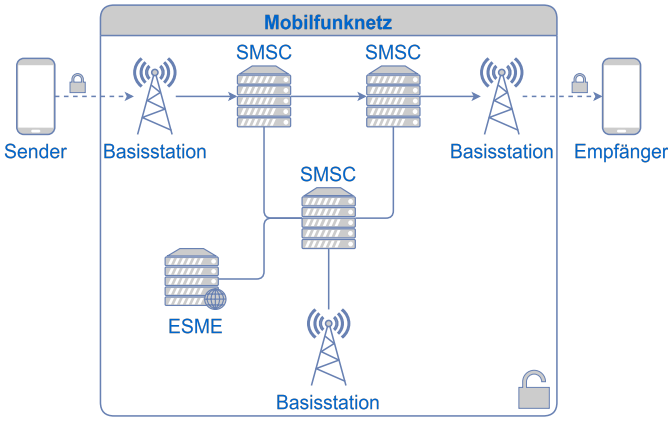

Fig. 1. Beispiel Mobilfunknetz [4]

Damit Nachrichten über große Distanzen versendet und empfangen werden können, wird eine entsprechende Infrastruktur für den Mobilfunk benötigt (siehe Fig. 1). Das Mobilfunknetz besteht aus Basisstationen, mit denen sich die Endgeräte drahtlos verbinden können, und aus Short Message Service Centers (SMSC), welche die versendeten Nachrichten an den korrekten Empfänger weiterleiten [4]. Falls die Zielperson aus irgendeinem Grund nicht erreichbar sein sollte und die Nachricht nicht zugestellt werden kann, wird sie temporär im SMSC zwischengespeichert. Sobald die Erreichbarkeit wiederhergestellt ist, wird die Nachricht zugestellt und anschließend aus dem SMSC gelöscht [5]. Während der Übermittlung der Nachricht ist der Bereich zwischen dem Endgerät und der Basisstation verschlüsselt, innerhalb des Mobilfunknetzes allerdings nicht mehr [4]. Es besteht also die Möglichkeit, dass der Mobilfunknetzbetreiber die Nachrichten auslesen kann.

External Short Message Entities (ESME) sind ebenfalls Bestandteil des Netzes und werden meist von Unternehmen genutzt. Verwendungszweck dafür ist das Senden und Empfangen einer großen Menge an Nachrichten. Dies wird z.B. für das Versenden von One-Time-Passwords oder Notfallmeldungen eingesetzt. ESMEs fungieren also als Schnittstelle und erlauben so einen direkten Zugriff auf die SMSCs oder Verkaufen den Zugriff an Dritte weiter. Es existieren zum Beispiel Systeme, die einzelne Telefonnummern auf einer

Website öffentlich zugänglich machen, damit Nutzer ohne Angabe persönlicher Daten darüber Nachrichten empfangenen kann. Das wird teilweise noch weiter getrieben, sodass es Dienste gibt, bei denen man ganz einfach an Telefonnummern kommt, mit denen auch Nachrichten versendet werden können. Da hier wieder keine Angaben persönlicher Daten notwendig sind, werden solche Nummern oft für Betrugszwecke ausgenutzt. Nicht zuletzt sollte aus Sicht des Datenschutzes beachtet werden, dass die gesendeten und empfangenen Nachrichten eventuell für längere Zeit von ESMEs gespeichert werden [4].

...

SIM Swap Attack: Der Angreifer kann sich bei dem Mobilfunkanbieter melden und sich als das Opfer ausgeben. Er kann behaupten, seine SIM Karte verloren zu haben, um eine Ersatz-SIM zu erhalten. So kann er dann die SMS Nachrichten abfangen und zum Beispiel an One-Time-Passwörter gelangen, um sich in Accounts des Opfers einzuloggen [4].

B. Over-the-Top Instant Messenger

- jeder Nutzer muss Client installieren

[3]

...

Ein populäres Beispiel für einen OTT Messenger ist WhatsApp. WhatsApp wurde ursprünglich 2009 als eigenständiges Unternehmen gegründet und ist seit 2014 Teil von Meta Platforms Inc [6]. Früher war die Nutzung des Dienstes mit einem kostenpflichtigen Abo verbunden, ist allerdings mittlerweile vollständig kostenlos nutzbar [7].

Der WhatsApp Messenger bietet zahlreiche Funktionen an, die über einfache Textnachrichten hinaus gehen. Es ist möglich, verschiedene Arten von Medien zu versenden, wie unter anderem Fotos, Videos, Audio und Dokumente. Weitere Nachrichtentypen, wie Live-Standort und Kontaktdaten sind ebenfalls vorhanden. Auf Nachrichten kann mit Emojis reagiert werden. Für sensiblere Nachrichten gibt es die Möglichkeit, selbstlöschende Nachrichten zu aktivieren, welche nach einer voreingestellten Zeit oder nach einmaligem anschauen automatisch gelöscht werden [8]. Damit die Sicherheit und Privatsphäre der Nutzer gewährleistet sind, sind alle Nachrichten Ende-zu-Ende-Verschlüsselt und können nur auf den entsprechenden Endgeräten der Nutzer entschlüsselt werden. Der komplette Nachrichtenverkehr wird über die WhatsApp-Server abgewickelt [9]. Gruppenchats erlauben die Kommunikation mit mehreren Personen gleichzeitig. Die Telefonie-Funktion beinhaltet den Videoanruf, welcher Live-Videos von den teilnehmenden Personen übertragen. Während dem Anruf kann man weiterhin auf die Chats zurückgehen und wie gewohnt parallel nutzen [8]. Wer WhatsApp gerade nicht auf einem mobilen Endgerät nutzen möchte, kann auf WhatsApp Web oder WhatsApp Desktop ausweichen, um den Dienst auch auf anderen Plattformen wie Desktop-PCs zu nutzen. Die Verknüpfung des Accounts findet über das Scannen eines QR-Codes statt [8], [9].

Mit WhatsApp Business ist es möglich, dass Nutzer mit Unternehmen kommunizieren können. Dies kann für z.B. Support, aber auch automatisierte Chatbots genutzt werden. Allerdings muss bedacht werden, dass nicht alle Unternehmen direkt über WhatsApp Business kommunizieren, sondern mittels eines Dienstes Dritter über die WhatsApp API. Dadurch ist die Ende-zu-Ende-Verschlüsselung nicht mehr vollständig gewährleistet [9].

III. Rich Communication Services

A. Definition

Seit dem Aufstieg von OTT sinkt die Nutzung von klassischen Kommunikationsarten wie SMS [1]. Die Bundesnetzagentur veröffentlichte dazu zuletzt im Juli 2024 eine Statistik über die Anzahl der versendeten SMS über mehrere Jahre. Laut dieser ist die Nutzung von SMS im Jahr 2012 bei 59,8 Milliarden versendeten SMS gewesen. Im Jahr 2023 lag die Zahl allerdings nur noch bei 5,3 Milliarden. Das entspricht einem Abstieg von circa 91 % [10]. 2008 veröffentlichte die "Groupe Speciale Mobile Association" (GSMA) die erste Version des Universal Profiles, welche die Standards der Rich Communication Services (RCS) spezifiziert und deren Umsetzung definiert [11]. Die Grundidee dabei ist die Unterstützung mehrerer moderner Funktionen, wie man sie auch aus OTT-Messengern kennt. Außerdem sollen diese nativ im Betriebssystem implementiert werden. Für die Implementierung sind die Entwickler des Betriebssystems bzw. der Gerätehersteller zuständig. Beispiel dafür ist die Android-Implementierung in Google Messages [12]. Seit 2024 ist RCS auch auf Apple-Geräten mit iOS 18 oder höher über iMessage verfügbar [13]. Alternativ gibt es die Möglichkeit, RCS-Funktionalität durch das Installieren einer dafür entwickelten App zu erhalten [2].

B. Funktionen

Die Funktionen von RCS sind grundsätzlich in drei Kategorien eingeteilt: "Enriched Messaging", "Enriched Calling" und "Enriched Phonebook" [2], [11].

Beim "Enriched Messaging" gibt es das klassische "1-to-1 Messaging", sprich den Nachrichtenaustausch zwischen zwei Personen, wie man es auch von SMS kennt. Dazu kommt die Möglichkeit, in Gruppenchats mit mehreren Personen gleichzeitig miteinander zu kommunizieren. Innerhalb der Chats ist es möglich, Dateien zu versenden. Dabei kann jeder Dateityp verschickt werden. Bestimmte Dateiformate werden im Chat besonders dargestellt, wie z.B. der Standort mit Kartenvorschau, direkt im Chat abspielbare Audio-Dateien und animierte GIFs. Bilder und Videos werden ebenfalls gesondert abgebildet. Nach dem Senden von Dateien kann deren Übermittlungsstatus eingesehen werden. Dadurch kann geprüft werden, ob eine Datei korrekt versendet wurde oder ob der Transfer noch aussteht oder sogar fehlgeschlagen ist. Für eine persönlichere Kommunikation können Nutzer, anstatt Textnachrichten zu schreiben, auch Sprachnachrichten direkt in der App aufnehmen und verschicken. Ebenso ist es möglich, den aktuellen Standort mit anderen zu teilen. Bei jeder verschickten Nachricht kann der Absender sehen, ob diese angekommen ist und bereits vom Empfänger gelesen

wurde. Außerdem sieht der Chatteilnehmer in Echtzeit, wenn der Gesprächspartner gerade eine Nachricht am Eintippen ist.

Mit ”Enriched Calling” kann man während einem Anruf unter anderem einen Dateitransfer durchführen. Dies ermöglicht Videoanrufe, bei denen die Teilnehmer live die Aufnahme ihrer Kamera teilen können [2].

Die Idee beim ”Enriched Phonebook” war, dass Nutzer sich ihr eigenes Profil einrichten können, welches er mit Informationen über sich selbst füllen kann. Dazu würden zum Beispiel Name, Profilbild oder auch eine kurze Statusmeldung gehören. Das Profil wäre für seine Kontakte sichtbar. Allerdings ist das Enriched Phonebook aktuell nicht Teil des Universal Profiles der GSMA [2], [11].

RCS bietet auch kommerzielle Funktionen, die an Unternehmen gerichtet sind. Anstatt nur mit Personen zu interagieren, existiert die Möglichkeit, mit Diensten zu kommunizieren. Dazu gehören Chatbots, wie z.B. die Integrierung von Gemini in Google Messages [14], Chats zum Empfangen von 2FA-Codes oder auch Support. Diese Unternehmenskontakte beinhalten in deren Profil zusätzlich Informationen zum Chatbot bzw. zum Unternehmen [2].

C. Technik

Der Rich Communication Service funktioniert sowohl im 4G und 5G Mobilfunknetz, als auch über WiFi [15].

Damit möglichst alle Funktionen von RCS reibungslos genutzt werden können, müssen sich die Mobilfunk-Operatoren auf eine gängige Implementierung einigen. Um dies zu erreichen haben 2011 mehrere große Unternehmen, darunter die Deutsche Telekom, Telefonica und Vodafone angekündigt, einen Zusammenschluss zu bilden und eine gemeinsame RCS-Implementierung, auch RCS-e (Rich Communication Services enhanced) genannt, zu definieren [3].

Trotz solcher Maßnahmen können weiterhin Implementierungsunterschiede auftreten, weshalb die ”Capability Discovery”-Funktion entwickelt wurde. Sie dient dazu, den Clients zu zeigen, welche RCS-Funktionen verfügbar sind. Damit eine Funktion genutzt werden kann, muss sie sowohl bei beiden Clients implementiert als auch vom Mobilfunkanbieter unterstützt werden. Verfügbare Funktionen werden automatisch aktiviert. Falls RCS nicht unterstützt sein sollte, wird dem Nutzer angeboten, seine Nachricht alternativ als SMS zu verschicken [2]. Dabei entscheidet der ”Unified Composer”, ob die Nachricht als SMS oder, im Fall von Mediendateien, als MMS versendet wird [11].

Der Kommunikationsablauf über RCS beginnt mit der Anmeldung beim Dienst. Dafür werden die benötigten Informationen der Nutzer zum Bestätigen der Identitäten mit dem Profil-Server geteilt. Nutzer A möchte eine Nachricht an Nutzer B verschicken. Sein Gerät sendet eine Verbindungsanfrage an den Nachrichten-Server. Dieser leitet die Anfrage über das Netzwerk-zu-Netzwerk Interface (NNI) weiter an das Netzwerk von Nutzer B. Wenn dieser Prozess erfolgreich abgelaufen ist, besteht eine Chat-Sitzung zwischen den Geräten beider Chatteilnehmer [15]. Fig. 2 zeigt die im Kommunikationsprozess involvierten Netzwerkelemente.

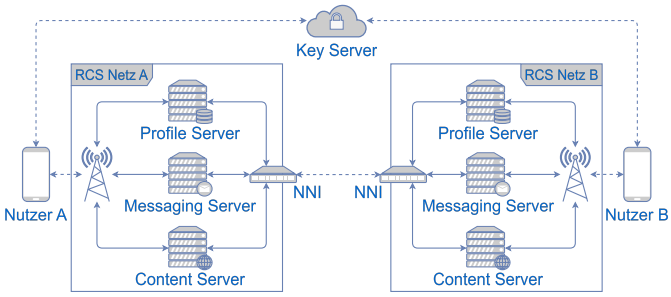

Fig. 2. Beispiel RCS-Netz [15]

Beim Verschicken von Dateien werden diese gesondert über den Content Server geleitet. Dort werden sie bei Bedarf temporär zwischengespeichert. Dies passiert zum Beispiel dann, wenn der Empfänger gerade nicht verfügbar ist und die Datei nicht sofort zugestellt und heruntergeladen werden kann [15].

D. Sicherheit

Um sich bei dem Dienst zu authentifizieren, werden je nach Plattform unterschiedliche Methoden angewendet.

Auf mobilen Endgeräten wird meist die SIM-basierte Authentifizierung genutzt [2]. Dafür wird die International Mobile Subscriber Identity (IMSI) und ein One-Time-Passwort (OTP) eingesetzt. Die IMSI ist eine einzigartige, private Identifikationsnummer, welche auf der SIM Karte gespeichert ist. Das OTP wird als eine unsichtbare SMS an die Telefonnummer der SIM geschickt und automatisch vom System gelesen. Zur Authentifizierung werden dann sowohl IMSI als auch das OTP an den Profile Server gesendet [15].

Auf Geräten ohne SIM Karte werden andere Möglichkeiten für die Anmeldung genutzt, wie z.B. der Login mit Nutzername und Passwort oder die Verknüpfung mit dem mobilen Endgerät über das Einscannen eines QR-Codes [2].

Alle Nachrichten sind während der Übertragung durch gängige Protokolle, wie TLS und IPSec, verschlüsselt [2]. Falls beide Nutzer Google Messages verwenden, sind die Nachrichten zusätzlich Ende-zu-Ende-Verschlüsselt [16]. Dazu wird ein separater Key Server für den Schlüsselaustausch genutzt (siehe Fig. 2) [15]. Diese Funktion ist allerdings nur in diesem Fall verfügbar, da die GSMA keine offizielle Implementierung definiert hat. Dadurch ist dies nicht unbedingt plattformübergreifend nutzbar [16].

IV. Vorteile von RCS

Rich Communication Services bietet zahlreiche Vorteile, die es von herkömmlichen SMS-Diensten abheben. In einigen Aspekten übertrifft es sogar OTT-Messenger.

Um einen Instant Messenger wie z.B. WhatsApp zu nutzen, muss zuerst der entsprechende Client in Form einer App heruntergeladen und auf dem Gerät installiert werden. Zusätzlich ist eine Einrichtung erforderlich, bevor der Messenger einsatzbereit ist [3], [15].

Im Gegensatz dazu muss für die Verwendung von RCS nicht viel vom Nutzer selbst getan werden, da es direkt im Betriebssystem integriert ist. Sofern unterstützt, wird RCS

automatisch im Hintergrund konfiguriert. Der Nutzer kann die Standart-Nachrichten-App des Betriebssystems öffnen und sofort den Dienst in Anspruch nehmen (solange der Gesprächspartner ebenfalls RCS unterstützt) [3], [15].

Während das Versenden einer SMS meist eine kleine Gebühr kostet (0,09 €, Telekom MagentaMobil Prepaid [17]), fallen bei RCS keine Zusatzkosten an (0,00 €, Telekom MagentaMobil Prepaid [18]).

Des Weiteren ist es möglich, RCS nicht nur auf einem Mobilgerät zu verwenden, wie es bei SMS der Fall ist. Aufgrund der Multi-Plattform-Funktionalität kann der Dienst auch über mehrere Geräte mit unterschiedlichen Plattformen genutzt werden, welche unter Umständen keine SIM Karte besitzen und nur über WiFi kommunizieren. So ist die Nutzung beispielsweise auch auf Laptops oder Tablets gewährleistet [2], [3].

Darüber hinaus verfügt RCS über viele moderne Funktionen, die man aus OTT-Messengern kennt, wie zum Beispiel das Versenden von Dateien oder dem Standort [2], [8].

Ein weiterer Vorteil ist die Möglichkeit, Nachrichten nicht nur über das mobile Netz (4G / 5G) zu verschicken, sondern auch über WiFi [15]. Dadurch kann an einem Ort, der zwar keinen Empfang hat, aber einen WiFi-Hotspot anbietet, weiterhin der Dienst genutzt werden. Außerdem existiert für Nachrichten keine strikte Längenbegrenzung wie bei SMS, wodurch längere Texte problemlos verschickt werden können.

V. Schwächen von RCS

A. Zusammenarbeit aller Parteien

Trotz aller Vorteile und modernen Funktionen gibt es auch einige Schwächen, die bei RCS berücksichtigt werden sollten.

Da RCS im Gegensatz zu SMS über das Internet läuft, können keine Nachrichten im Hintergrund empfangen werden, wenn man an seinem Gerät Internet komplett ausgeschaltet hat.

Damit die Kommunikation auch über Ländergrenzen hinweg nahtlos funktionieren kann, müssen alle Mobilfunkanbieter zusammenarbeiten. Funktionen von RCS sind nur verfügbar, wenn sie bei allen Kontaktteilnehmern unterstützt werden. Dafür braucht es idealerweise eine standardisierte Implementierung von RCS. Ebenfalls müssen die Hersteller von Mobilgeräten zusammenarbeiten, diese Implementierung umzusetzen und die Verbreitung von RCS voranzutreiben [3].

B. Sicherheitsprobleme

Dadurch, dass die Authentifizierung bei RCS SIM-basiert stattfindet, kann die klassische ”SIM Swap”-Attacke auch hier weiterhin ausgenutzt werden [4].

Obwohl zur Authentifizierung bei RCS eine Kombination aus der privaten International Mobile Subscriber Identity (IMSI) und einem One-Time-Password (OTT) genutzt wird, ist diese Methode nicht vollständig vor Angriffen geschützt. Angreifer können sich mittels einer Spoofing Attacke als einen anderen Nutzer ausgeben und deren RCS Account kompromittieren, unabhängig davon, ob die Opfer sich in einem 4G-, 5G- oder WiFi-Netz befinden. Handymodell und Betriebssystem des Geräts sind ebenfalls für die Attacke irrelevant. Das Hauptproblem bei dieser Authentifizierungsmethode ist, dass viele Mobilfunkanbieter nicht die komplette IMSI zum Authentifizieren nutzen, sondern nur einen kleinen Teil. Dieser Teil ist allerdings oft spezifisch zum Mobilfunkanbieter und kann über die Telefonnummer des Opfers leicht ermittelt werden. Zusätzlich können OTTs über eine mit Schadcode versetzten App abgefangen werden. Das OTT wird beim Authentifizieren bei RCS als unsichtbare SMS dem Opfer zugeschickt. Die App kann diese abgreifen und dem Angreifer übermitteln, ohne dass das Opfer was davon mitbekommt. Nachdem sowohl IMSI als auch OTT ermittelt wurden, kann sich der Angreifer per Spoofing als das Opfer ausgeben und sich bei RCS anmelden [15].

An sich stellt die Ende-zu-Ende-Verschlüsselung kein Hindernis bei der Initiierung einer Chat-Sitzung dar, aber es existiert auch eine Möglichkeit, diese auszuschalten. Diese Methode ist unter der Bezeichnung der ”Downgrade” Attacke bekannt. Bei dieser gibt der Angreifer vor, die Ende-zu-Ende-Verschlüsselung nicht zu unterstützen. Wenn eine RCS-Funktion nicht bei beiden Geräten verfügbar ist, ist sie nicht nutzbar. Aus diesem Grund wird dann automatisch die Ende-zu-Ende-Verschlüsselung deaktiviert und der Angreifer kann die unverschlüsselten Nachrichten abfangen [15].

Eine weitere, komplexere Methode ermöglicht es, den Schlüssel für die Verschlüsselung über den Key Server auszutauschen. Dadurch wird der Chat des Opfers weiterhin als sicher und verschlüsselt angezeigt. Der Angreifer kann sich so komplett unbemerkt für den anderen Teilnehmer ausgeben [15].

Die modernen Chat-Funktionen können ebenfalls von Angreifern genutzt werden. Wenn sich der Angreifer als Chatteilnehmer ausgibt, kann er die andere Person dazu überreden, ihren Standort zu teilen, um z.B. den Wohnort des Opfers herauszufinden. Beim File Sharing Spam wird das Versenden von Dateien dafür ausgenutzt, konstant große Dateien zu verschicken. Der Empfänger-Client wird automatisch versuchen, alle parallel herunterzuladen, wodurch das Gerät eventuell überladen wird [15].

...

Yang et. al. [19] haben 2024 mittels eines selbst entwickelten Tools Sicherheitstests durchgeführt und weitere Probleme aufgedeckt. Bei den Tests kam heraus, dass mehrere Mobilfunkanbieter Server nutzen, welche öffentlich zugänglich sind und die Integrität und Vertraulichkeit von gesendeten Daten nicht gewährleisten.

Durch nicht verschlüsselte Nachrichten während dem Transfer und somit der Verletzung der Vertraulichkeit können Nachrichten leicht mitgelesen werden. Theoretisch ist es möglich, dass der Angreifer das Signal während der Übermittlung aus der Luft abzufangen und aufzunehmen.

Dieses Problem kann durch die Nutzung eines Virtual Private Networks (VPN) gelöst werden. Bei aktiviertem VPN wird die Nachrichtenübermittlung über den gesicherten VPN-Server geleitet und ist so theoretisch vor dem öffentlich zugänglichen Mobilfunk geschützt. Allerdings sollte bedacht

werden, dass viele Nutzer kostenlose VPN Dienste nutzen, welche oft nicht so sicher sind, wie sie beworben werden. Ein Großteil der kostenlosen Anbieter überwacht heimlich den Internetverkehr über deren Server und kann so durch die fehlende Vertraulichkeit mitlesen.

Zusätzlich wurde festgestellt, dass die TLS-Validierung auf der Client-Seite nicht immer ordnungsgemäß durchgeführt wird. Häufig wird nur geprüft, ob das Zertifikat von einer legitimen Certificate Authority ausgestellt wurde und nicht, ob zum Beispiel der angegebene Hostname mit dem offiziellen RCS-Server übereinstimmt. So kann der Angreifer über seinen eigenen Server einen RCS-Server imitieren, welcher über eine separate TLS-Verbindung und Domain läuft. Auf diese Weise kann ein Man-In-The-Middle-Angriff ausgeführt werden.

Dadurch, dass bei manchen Mobilfunkanbietern die Integrität nicht geprüft wird, können Daten beim Senden manipuliert werden. Es kam heraus, dass die Software von einigen Smartphone-Herstellern Fehler aufweisen, welche zu Abstürzen des Dienstes führen können. Zum Beispiel hat Samsung eine Restriktion in die hauseigene Nachrichten-App eingebaut, wodurch Vorschaubilder nur eine bestimmte maximale Dateigröße besitzen dürfen. Das ist normalerweise auch kein Problem, da beim Versenden das Bild zuerst komprimiert wird und so beim Empfänger in der vorgesehenen Dateigröße ankommt. Wenn allerdings die URL zum Vorschaubild innerhalb der Metadaten zu einem Bild geändert werden, welches größer als erlaubt ist, kommt das Bild nicht beim Empfänger an, sondern lässt stattdessen den Dienst auf deren Gerät abstürzen. Bei Xiaomi findet sich ein ähnliches Problem, welches den gleichen Effekt hat. Wenn ein Standort empfangen wird, der eine korrupte Standort-URL enthält und nicht dem gültigen Format entspricht, stürzt der Dienst ebenfalls ab.

Dieses Problem kann für eine Denial-of-Service-Attacke gegen einen Nutzer ausgenutzt werden. Dabei werden in regelmäßigen Abständen zu große Dateien beziehungsweise korrupte Standortdaten an das Gerät geschickt, wodurch der Dienst permanent abstürzt. Somit ist das Gerät von der Kommunikation über RCS abgeschnitten.

Es gibt noch weitere Attacken, welche ebenfalls das Manipulieren der Metadaten ausnutzen, um Schaden anzurichten. Bei der ”Zero Click Remote Information Leakage”-Attacke schickt der Angreifer eine Datei mit einer manipulierten Download-URL an das Opfer. Auf dem Gerät des Opfers wird diese Datei automatisch heruntergeladen. Da die URL nicht auf die ursprüngliche Datei, sondern auf einen Server des Angreifers führt, kann der Angreifer die Verbindung abfangen und Informationen über das Opfer erlangen, wie zum Beispiel seine IP-Adresse, das Handymodell und weitere Details.

Ein weiterer Angriff ist das erzwungene Herunterladen von großen Dateien. Es wird wieder eine Datei mit manipulierter URL geschickt, welche auf eine sehr große Datei zeigt. Dadurch, dass diese beim Empfänger automatisch im Hintergrund heruntergeladen wird, füllt sich unbemerkt der Handyspeicher und viel mobiles Datenvolumen wird verbraucht.

Schließlich gibt es noch die Möglichkeit, eine ”Reflection Amplification DDOS”-Attacke gegen einen RCS-Server durchzuführen. Dabei wird wieder eine Datei mit manipulierter Download-URL, welche auf eine sehr große Datei zeigt, präpariert. Diese wird dann an mehrere Geräte geschickt, die sich im gleichen Netz befinden und somit auf den gleichen Content Server zugreifen. Die Geräte versuchen dann gleichzeitig von selben Server herunterzuladen, wodurch die Netzwerkbandbreite vollständig ausgenutzt und der reguläre Datenverkehr enorm beeinträchtigt wird [19].

VI. Fazit

Rich Communication Services (RCS) ist eine moderne Alternative zum klassischen Short Message Service (SMS) und bietet zahlreiche Funktionen, wie man sie auch aus den häufig genutzten Over-The-Top (OTT) Instant Messengern kennt. Neben dem Schreiben von Textnachrichten ist es auch möglich, Mediendateien zu versenden, Gruppenchats zu starten oder sogar, falls verfügbar, mittels Ende-zu-Ende-Verschlüsselung die Kommunikation noch besser zu schützen. Somit entspricht RCS den Anforderungen der heutigen digitalen Kommunikation.

Ein wichtiger Vorteil von RCS ist, dass es nativ im Betriebssystem integriert ist. Es muss also nicht eine separate App installiert werden, um den Dienst nutzen zu können. Außerdem wird RCS nicht von einem einzelnen Unternehmen betrieben, sondern wird von den Mobilfunkanbietern in ihren Netzen bereitgestellt.

Allerdings sind Trotz des moderneren Ansatzes mehrere Schwächen zu finden. Der Umstand, dass es von verschiedenen Mobilfunkanbietern betrieben wird, kann bereits zu Problemen führen. Damit alle Funktionen von RCS reibungslos funktionieren, muss die Implementierung überall einheitlich sein. Das bedeutet, dass alle Mobilfunkanbieter weltweit einen gemeinsamen Standard nutzen. Gleiches gilt für die Gerätebeziehungsweise Betriebssystemhersteller für die Bereitstellung des RCS-Clients. Sicherheitsprobleme, wie Spoofing oder das Manipulieren der Metadaten stellen ebenfalls schwerwiegende Probleme dar.

Zusammenfassend lässt sich sagen, dass Rich Communication Services das Potenzial hat, als Nachfolger der SMS zu ersetzen. Es müssen allerdings noch Verbesserungen durchgeführt werden, damit RCS sicher als Ersatz genutzt werden kann. Dazu gehören zum einen, die Sicherheitsprobleme zu beseitigen und zum anderen, durch eine standardisierte Implementierung und Zusammenarbeit der Mobilfunkanbieter und Hersteller die Technologie zu fördern und weiterzuverbreiten.

References

[1] N. Wellmann, “Are OTT messaging and mobile telecommunication an interrelated market? An empirical analysis,” *Telecommun. Policy*, vol. 43, no. 9, 2019, Accessed: Nov. 10, 2024. [Online]. Available: https://doi.org/10.1016/j.telpol.2019.101831

[2] GSMA, “RCS Universal Profile Service Definition Document v2.4,” Accessed: Nov. 6, 2024. [Online]. Available: https://www.gsma.com/solutions-and-impact/technologies/networks/wp-content/uploads/2019/10/RCC.71-v2.4.pdf

[3] M. Lin and J. Arenzana Arias, "Rich Communication Suite: The challenge and opportunity for MNOs," in *2011 15th International Conference on Intelligence in Next Generation Networks*, Oct. 2011, pp. 187–190, Accessed: Nov. 21, 2024. [Online]. Available: https://doi.org/10.1109/ICIN.2011.6081071

[4] B. Reaves, N. Scaife, D. Tian, L. Blue, P. Traynor, and K. R. B. Butler, "Sending Out an SMS: Characterizing the Security of the SMS Ecosystem with Public Gateways," in *2016 IEEE Symposium on Security and Privacy (SP)*, May 2016, pp. 339–356, Accessed: Nov. 06, 2024. [Online]. Available: https://doi.org/10.1109/SP.2016.28

[5] J. Brown, B. Shipman, and R. Vetter, "SMS: The Short Message Service," *Computer*, vol. 40, no. 12, pp. 106–110, Dec. 2007, Accessed: Nov. 6, 2024. [Online]. Available: https://doi.org/10.1109/MC.2007.440

[6] WhatsApp, "Danke für 10 Jahre," Accessed: Dec. 4, 2024. [Online]. Available: https://blog.whatsapp.com/thank-you-for-10-years

[7] ——, "WhatsApp kostenlos und nützlicher machen," Accessed: Dec. 4, 2024. [Online]. Available: https://blog.whatsapp.com/making-whats-app-free-and-more-useful

[8] ——, "WhatsApp-Hilfebereich," Accessed: Dec. 4, 2024. [Online]. Available: https://faq.whatsapp.com/

[9] ——, "WhatsApp Encryption Overview," Accessed: Dec. 4, 2024. [Online]. Available: https://scontent.xx.fbcdn.net/v/t39.8562-6/455962147_1148247109601582_1673264986279156121_n.pdf?_nc_cat=101&ccb=1-7&_nc_sid=e280be&_nc_ohc=EeDO1ShMWBwQ7kNvgFH0HX5&_nc_zt=14&_nc_ht=scontent.xx&_nc_gid=Ah3I6FJFlIToW6syXPpijVw&oh=00_AYBVIh7S5p_ntGMO7bH4fIydhGW-e2q4Ty1SUAqJE0DvVQ&oe=67562719

[10] Bundesnetzagentur, "Bundesnetzagentur - Digitales und Telekommunikation - Versendete SMS," Accessed: Jan. 5, 2025. [Online]. Available: https://www.bundesnetzagentur.de/DE/Fachthemen/Datenportal/1_Digitales_Telekommunikation/_svg_TK/TK_Mobilfunk/Versendete_SMS/Versendete_SMS.html

[11] K. Henry, Q. Liu, and S. Pasquereau, "Rich Communication Suite," in *2009 13th International Conference on Intelligence in Next Generation Networks*, Oct. 2009, pp. 1–6, Accessed: Nov. 8, 2024. [Online]. Available: https://doi.org/10.1109/ICIN.2009.5357089

[12] Google, ""RCS-Chats" in Google Messages aktivieren - Google Messages," Accessed: Dec. 16, 2024. [Online]. Available: https://support.google.com/messages/answer/7189714?sjid=17429263824577998783-EU&hl=de

[13] Apple, "Was ist der Unterschied zwischen iMessage, RCS und SMS/MMS? - Apple Support (DE)," Accessed: Dec. 16, 2024. [Online]. Available: https://support.apple.com/de-de/104972

[14] Google, "Gemini in Google Messages verwenden - Google Messages," Accessed: Dec. 16, 2024. [Online]. Available: https://support.google.com/messages/answer/14599070?hl=de

[15] J. Zhao, Q. Li, Z. Yuan, Z. Zhang, and S. Lu, "5G Messaging: System Insecurity and Defenses," in *2022 IEEE Conference on Communications and Network Security (CNS)*, Oct. 2022, pp. 37–45, Accessed: Dec. 29, 2024. [Online]. Available: https://doi.org/10.1109/CNS56114.2022.9947238

[16] Google, "So schützen wir die Vertraulichkeit von RCS-Chats - Google Messages," Accessed: Dec. 23, 2024. [Online]. Available: https://support.google.com/messages/answer/9592174?sjid=2530033474497695451-EU&hl=de

[17] Telekom, "Preisliste MagentaMobil Prepaid," Accessed: Dec. 29, 2024. [Online]. Available: https://www.telekom.de/dlp/agb/pdf/52943.pdf?

[18] ——, "Preisliste Zubuchoptionen Prepaid," Accessed: Dec. 29, 2024. [Online]. Available: https://www.telekom.de/dlp/agb/pdf/53209.pdf

[19] Y. Yang, Y. Zhang, T. Wan, C. Wang, H. Duan, J. Chen, and Y. Li, "Uncovering Security Vulnerabilities in Real-world Implementation and Deployment of 5G Messaging Services," in *Proceedings of the 17th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, ser. WiSec '24. New York, NY, USA: Association for Computing Machinery, 2024, pp. 265–276, Accessed: Jan. 7, 2025. [Online]. Available: https://doi.org/10.1145/3643833.3656131