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.**
***Index Terms*—Diese, index, terms, existieren, noch, nicht**

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 in heutigen Zeiten 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 [13]. 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 4 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 [13].

Damit Nachrichten überhaupt über große Distanzen versendet und empfangen werden können, wird eine gewisse Infrastruktur für den Mobilfunk benötigt. 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 der Empfänger aus irgendeinem Grund nicht erreichbar ist und die Nachricht nicht zugestellt werden kann, wird sie im SMSC temporär gespeichert. Sobald der Empfänger wieder erreichbar ist, wird die Nachricht endgültig zugestellt und aus dem SMSC gelöscht [13]. 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.

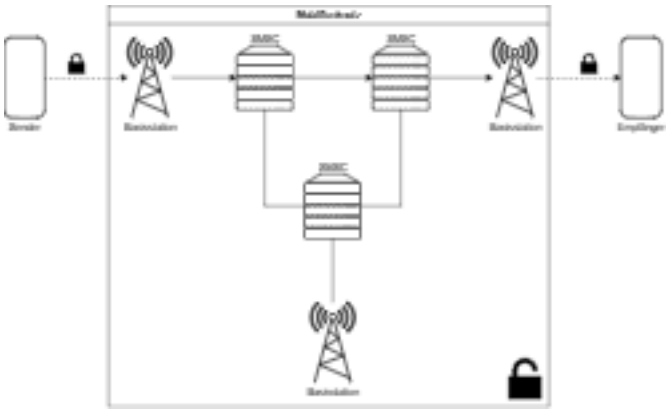

Fig. 1. Beispiel Mobilfunknetz

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 genutzt. 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

[2]

...

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 [5]. Früher war die Nutzung des Dienstes mit einem kostenpflichtigen Abo verbunden, ist allerdings mittlerweile vollständig kostenlos nutzbar [6].

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 [7]. 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 [8]. 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 [7]. 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 [7], [8].

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 [8].

III. Rich Communication Services

A. Definition

Seit dem Aufstieg von OTT sinkt die Nutzung von klassischen Kommunikationsarten wie SMS. Laut einer Statistik der Bundesnetzagentur ist die Nutzung von SMS im Jahr 2015 bereits um 41 % gesunken [1]. 2008 veröffentlichte die "Groupe Speciale Mobile Association" (GSMA) die erste Version des Universal Profiles, welche die Funktionen der Rich Communication Services (RCS) definiert [9]. Zu den Grundideen gehört unter anderem die Verknüpfung verschiedener Dienste, wie das Nachrichtenschreiben, die Kontakte-App und die Kontakte-App. Außerdem sollen die Funktionen nativ im Betriebssystem implementiert sein. Für die Implementierung sind die Entwickler des Betriebssystems bzw. der Gerätehersteller zuständig. Beispiel dafür ist die Android-Implementierung in Google Messages [10]. Seit 2024 ist RCS auch auf iOS-Geräten über iMessage verfügbar [11]. Alternativ gibt es die Möglichkeit, RCS-Funktionalität durch das Installieren einer dafür entwickelten App zu erhalten [3].

B. Funktionen

- Spam kann vermieden werden

[3]

Die Funktionen sind grundsätzlich in drei Kategorien eingeteilt: "Enriched Messaging", "Enriched Calling" und "Enriched Phonebook". Beim "Enriched Messaging" gibt es das klassische "1-to-1 Messaging", sprich den Nachrichtenaustausch zwischen zwei Personen, wie man es auch von SMS kennt, und die Möglichkeit, in Gruppenchats mit mehreren Personen gleichzeitig zu kommunizieren. Innerhalb der Chats ist es möglich, Dateien zu versenden. Dabei kann jeder Dateityp versendet werden. Bestimmte Dateiformate werden auf eine bestimmte Weise im Chat dargestellt, wie z.B. pdf-Dateien mit Dokumentenvorschau, direkt im Chat abspielbare Audio-Dateien und animierte GIFs. Bilder und Videos sind ebenfalls möglich. Nach dem Senden kann für gesendete Dateien der Sende-Status eingesehen werden. Dadurch kann geprüft werden, ob eine Datei korrekt versendet wurde oder ob der Transfer noch aussteht oder sogar fehlgeschlagen ist. Sprachnachrichten können direkt in der App aufgenommen und verschickt werden. Der aktuelle Standort des Senders kann ebenfalls geteilt werden, entweder als Snapshot oder Live-Standort. Bei jeder verschickten Nachricht kann der Sender sehen, ob die Nachricht angekommen ist und ob sie bereits vom Empfänger gelesen wurde. Außerdem sieht der Chatteilnehmer, wenn der jeweils Andere 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.

[3]

...

Die Idee beim "Enriched Phonebook" ist, dass Nutzer sich ihr eigenes Profil einrichten können. Dadurch kann jeder andere Nutzer das Profil sehen. (freiwillig, beide müssen Profil teilen)

[9]

...

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 [12], oder Chats zum Empfangen von 2FA-Codes. Diese Unternehmenskontakte beinhalten in deren Profil zusätzlich Informationen zum Chatbot bzw. zum Unternehmen.

[3]

C. Technik

Damit möglichst alle Funktionen von RCS reibungslos funktionieren, müssen sich die Mobilfunk-Operatoren auf eine gängige Implementierung einigen. Um dies zu erreichen haben sich 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 [2].

Da aber trotz solchen Maßnahmen immer noch Implementierungsverschiedenheiten existieren können, existiert die "Capability Discovery"-Funktion. Sie dient dazu, den Clients zu zeigen, welche RCS-Funktionen verfügbar sind. Damit eine Funktion verfügbar ist, muss sie bei beiden Clients implementiert sein bzw. vom Mobilfunkanbieter unterstützt werden. Falls die Funktionen verfügbar sind, werden sie automatisch aktiviert. Falls dies nicht der Fall sein sollte, wird dem Nutzer angeboten, seine Nachricht alternativ als SMS zu verschicken [3]. Dabei entscheidet der "Unified Composer", ob die Nachricht als SMS oder MMS (bei Mediendateien) verschickt werden muss [9].

- über 4G / 5G / WiFi
- Authentifizierung mit One-Time-Password OTP und IMSI (International Mobile Subscriber Identity)
- IMSI ist eine private ID auf der SIM
- OTP zur Verifizierung wird unsichtbar als SMS verschickt und automatisch vom System geladen
- Keyserver für den Schlüsselaustausch der Ende-zu-Ende-Verschlüsselung
- Media Server für das Zwischenspeichern der verschickten Dateien

[15]

D. Sicherheit

Um sich bei RCS zu authentifizieren, gibt es je nach Plattform unterschiedliche Methoden. Auf mobilen Endgeräten wird meist die SIM-basierte Authentifizierung genutzt, sprich eine Anmeldung über die Telefonnummer. Auf anderen 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 [3].

...

Alle Nachrichten sind während der Übertragung durch gängige Protokolle, wie TLS und IPSec, verschlüsselt [3]. Falls beide Nutzer Google Messages verwenden, sind die Nachrichten zusätzlich Ende-zu-Ende-Verschlüsselt. Diese Funktion funktioniert allerdings auch nur in diesem Fall, da die GSMA keine offizielle Implementierung definiert hat. Dadurch ist dies nicht plattformübergreifend verfügbar [14].

IV. Vorteile von RCS gegenüber SMS

Wenn man einen Instant Messenger, wie z.B. WhatsApp, nutzen möchte, muss man den entsprechenden Client installieren. Dazu gehört zum einen das Herunterladen und Installieren der App auf dem Gerät, zum anderen dann noch das Einrichten der App. Dagegen muss für die Nutzung von RCS kaum etwas selbst getan werden, da es direkt im Betriebssystem integriert ist. Es muss nur die Nachrichten App (auf Android Google Messages) geöffnet werden und schon wird man beim Schreiben von Nachrichten automatisch bei RCS angemeldet und falls verfügbar auch genutzt.

- anstatt für jeden Instant Messenger eigenen Client zu installieren, der Leistung braucht, universeller integrierter Messenger
- es ist möglich, RCS über ein Mobilgerät oder auch PC zu nutzen

[2]

- man kann clients auf mehreren Geräten nutzen
- bei Dual-SIM ist RCS mit beiden Karten gleichzeitig möglich

[3]

- es fallen keine Zusatzkosten an
- ist bereits im Betriebssystem integriert, keine zusätzliche App nötig
- es besitzt viele moderne Funktionen, die auch in OTT Messengern vorhanden sind
- senden auch über WLAN möglich, wenn man z.B. keinen guten Empfang hat
- es gibt keine strikte Längenbegrenzung für Nachrichten
- Instant Messenger müssen von Jedem installiert werden, RCS nicht

[15]

V. Schwächen von RCS

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

...

Damit die Kommunikation auch über Ländergrenzen hinweg nahtlos funktionieren kann, müssen alle Mobilfunkanbieter

zusammenarbeiten. Funktionen von RCS können nur funktionieren, 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 [2].

...

Unabhängig davon, ob die Opfer 4G, 5G oder WiFi nutzen, können ihre Accounts kompromittiert und ausgenutzt werden [15].

...

Eine Möglichkeit, die Ende-zu-Ende-Verschlüsselung auszuhebeln, ist die sogenannte "Downgrade" Attacke. Bei dieser gibt der Angreifer vor, dies 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].

Es gibt allerdings auch eine komplexere Methode, welche es ermöglicht, den Schlüssel für die Verschlüsselung über den Key Server auszutauschen. Dadurch wird der Chat des Opfers weiterhin als sicherer und verschlüsselt angezeigt. Der Angreifer kann so komplett unbemerkt sich für den anderen Teilnehmer ausgeben [15].

...

Mittels File Sharing Spam kann man das Gerät des Opfers überladen, indem konstant große Dateien verschickt werden. Der Empfänger-Client wird automatisch versuchen, alle Dateien parallel herunterzuladen [15].

- kompromittierte Accounts können ausgenutzt werden, egal ob über 4G / 5G / WiFi
  - dann bringt selbst Ende-zu-Ende-Verschlüsselung nicht viel
- oft wird nicht komplette IMSI genutzt, sondern nur ein Teil davon, welcher aber oft zum Mobilfunkanbieter gehört und dadurch leicht über die Telefonnummer geholt werden kann
- OTP SMS kann über eine dritte App abgefangen werden
- Anmeldung bei RCS über gespoofte Telefonnummer und IMSI
- Hack funktioniert unabhängig vom Handymodell

[15]

...

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.

VI. Fazit

...

References

[1] N. Wellmann, "Are OTT messaging and mobile telecommunication an interrelated market? An empirical analysis", Telecommun. Policy, Bd. 43, Nr. 9, Oktober 2019, doi: 10.1016/j.telpol.2019.101831.

[2] M. Lin und J. Arenzana Arias, "Rich Communication Suite: The challenge and opportunity for MNOs", in 2011 15th International Conference on Intelligence in Next Generation Networks, Okt. 2011, S. 187–190. doi: 10.1109/ICIN.2011.6081071.

[3] GSMA. "RCS Universal Profile Service Definition Document". Zugegriffen: 06.11.2024. [Online]. Verfügbar unter: https://www.gsma.com/solutions-and-impact/technologies/networks/wp-content/uploads/2019/10/RCC.71-v2.4.pdf

[4] B. Reaves, N. Scaife, D. Tian, L. Blue, P. Traynor, und 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), Mai 2016, S. 339–356. doi: 10.1109/SP.2016.28.

[5] "Danke für 10 Jahre", WhatsApp.com. Zugegriffen: 4. Dezember 2024. [Online]. Verfügbar unter: https://blog.whatsapp.com/thank-you-for-10-years

[6] "WhatsApp kostenlos und nützlicher machen", WhatsApp.com. Zugegriffen: 4. Dezember 2024. [Online]. Verfügbar unter: https://blog.whatsapp.com/making-whats-app-free-and-more-useful

[7] "WhatsApp-Hilfebereich". Zugegriffen: 4. Dezember 2024. [Online]. Verfügbar unter: https://faq.whatsapp.com/

[8] WhatsApp. "WhatsApp Encryption Overview Technical White Paper". Zugegriffen: 4. Dezember 2024. [Online]. Verfügbar unter: https://faq.whatsapp.com/820124435853543#nachrichtenaustausch-mit-unternehmen

[9] K. Henry, Q. Liu, und S. Pasquereau, "Rich Communication Suite", in 2009 13th International Conference on Intelligence in Next Generation Networks, Okt. 2009, S. 1–6. doi: 10.1109/ICIN.2009.5357089.

[10] ""RCS-Chats" in Google Messages aktivieren - Google Messages". Zugegriffen: 16. Dezember 2024. [Online]. Verfügbar unter: https://support.google.com/messages/answer/7189714?sjid=17429263824577998783-EU&hl=de

[11] "Was ist der Unterschied zwischen iMessage, RCS und SMS/MMS? - Apple Support (DE)", Apple Support. Zugegriffen: 16. Dezember 2024. [Online]. Verfügbar unter: https://support.apple.com/de-de/104972

[12] "Gemini in Google Messages verwenden - Google Messages". Zugegriffen: 16. Dezember 2024. [Online]. Verfügbar unter: https://support.google.com/messages/answer/14599070?hl=de

[13] J. Brown, B. Shipman, und R. Vetter, "SMS: The Short Message Service", Computer, Bd. 40, Nr. 12, S. 106–110, Dez. 2007, doi: 10.1109/MC.2007.440.

[14] "So schützen wir die Vertraulichkeit von RCS-Chats - Google Messages". Zugegriffen: 23. Dezember 2024. [Online]. Verfügbar unter: https://support.google.com/messages/answer/9592174?sjid=2530033474497695451-EU&hl=de#zippy=%2Chow-we-protect-your-data%2Csosch%C3%BCtzen-wir-ihre-daten

[15] J. Zhao, Q. Li, Z. Yuan, Z. Zhang, und S. Lu, "5G Messaging: System Insecurity and Defenses", in 2022 IEEE Conference on Communications and Network Security (CNS), Okt. 2022, S. 37–45. doi: 10.1109/CNS56114.2022.9947238.