HOCHSCHULE
MITTWEIDA
University of Applied Sciences

MASTERARBEIT

Herr
Florian Meyer, B.Sc.

Caller ID Spoofing

Technik, Methoden und Gegenmaßnahmen

Mittweida, Mai 2023

Fakultät **Angewandte Computer- und Biowissenschaften**

MASTERARBEIT

Caller ID Spoofing

Technik, Methoden und Gegenmaßnahmen

Autor:
Florian Meyer

Studiengang:
Cybercrime/Cybersecurity

Seminargruppe:
CY19wC-M

Erstprüfer:
Prof. Dr. rer. nat. Dirk Labudde

Zweitprüfer:
Kriminaloberrat Stefan Ockenfeld, M.A.

Einreichung:
Mittweida, 05.05.2023

Verteidigung/Bewertung:
Mittweida, 2023

Faculty of **Applied Computer Sciences & Biosciences**

MASTER THESIS

Caller ID Spoofing

Technology, methods and countermeasures

Author:
Florian Meyer

Course of Study:
Cybercrime/Cybersecurity

Seminar Group:
CY19wC-M

First Examiner:
Prof. Dr. rer. nat. Dirk Labudde

Second Examiner:
Kriminaloberrat Stefan Ockenfeld, M.A.

Submission:
Mittweida, 05.05.2023

Defense/Evaluation:
Mittweida, 2023

Bibliografische Beschreibung:

Meyer, Florian:
Caller ID Spoofing, *Technik, Methoden und Gegenmaßnahmen*. – 2023. – 82 S.
Mittweida, Hochschule Mittweida – University of Applied Sciences, Fakultät Angewandte Computer- und Biowissenschaften, Masterarbeit, 2023.

Referat:

Die hier vorliegende Arbeit beschäftigt sich mit den methodischen Abläufen des Kriminalitätsphänomens **Caller ID Spoofing**, dessen technische Hintergründe, sowie der Detektion und den sich daraus ergebenden Maßnahmen der Abwehr seitens der Betroffenen. Dabei soll im theoretischen Teil sowohl auf das Phänomen des **Caller ID Spoofing** an sich und dessen Einordnung in den Deliktbereich Cybercrime als auch auf die technischen Hintergründe bei der Verschleierung der eigenen Telefon-Identität eingegangen werden. Des Weiteren wird der Faktor Mensch als Schwachstelle von IT-Systemen beleuchtet. Der methodische Teil der Arbeit legt den Fokus auf die Entwicklung effektiver Lösungen zur Erkennung und Abwehr von **Caller ID Spoofing**, sowohl aus technischer als auch aus soziologischer Sicht. Während für ersteres bereits eine Vielzahl von wissenschaftlichen Ansätzen existieren, soll sich bei zweiteren auf den Begriff der Security Awareness konzentriert werden.

Aus Gründen der besseren Lesbarkeit wird in dieser Arbeit auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Personenbezeichnungen gelten nichtsdestotrotz ausdrücklich gleichermaßen für alle Geschlechter.

Inhaltsverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

AES ..... Advanced Encryption Standard

APT ..... Advanced Persistent Threat

AT-T ..... American Telephone and Telegraph Company

CLIP ..... Calling Line Identification Presentation

CLIR ..... Calling Line Identification Restriction

DNS ..... Domain Name System

EDGE ..... Enhanced Data Rates for GSM Evolution

ENUM ..... Telephone Number URI Mapping

FCC ..... Federal Communications Commission

FVSt ..... Fernvermittlungsstellen

GPRS ..... General Packet Radio Service

GSM ..... Global System for Mobile Communications

HTTP ..... Hypertext Transfer Protocol

IETF ..... Internet Engineering Task Force

IMS ..... IP Multimedia Subsystem

IP ..... Internet Protocol

ISDN ..... Integrated Services Digital Network

LTE ..... Long Term Evolution

PSTN ..... Public Switched Telephone Network

RTCP ..... RTP Control Protocol

RTP ..... Real-Time Transport Protocol

SDP ..... Session Description Protocol

SIP ..... Session Initiation Protocol

SIPS ..... Session Initiation Protocol Secure

SMS ..... Short Message Service

SRTP ..... Secure Real-Time Transport Protocol

SS7 ..... Signaling System No. 7

StGB ..... Strafgesetzbuch

StPO ..... Strafprozessordnung

TCP . . . . . Transport Control Protocol

TKG . . . . . Telekommunikationsgesetz

TKÜ . . . . . Telekommunikationsüberwachung

TVSt . . . . . Teilnehmervermittlungsstellen

UDP . . . . . User Datagram Protocol

UMTS . . . . . Universal Mobile Telecommunications System

URI . . . . . Uniform Resource Identifier

VoIP . . . . . Voice Over Internet Protocol

VoLTE . . . . . Voice Over Long Term Evolution

1 Einleitung

"Of all the life skills available to us, communication is perhaps the most empowering."

"Von allen Lebenskompetenzen, die uns zur Verfügung stehen, ist Kommunikation wohl die mächtigste."

So beschrieb es Bret Morrison, ein amerikanischer Schauspieler des 20. Jahrhunderts [1]. Die Kommunikation ist das höchste Gut des Menschen und seit jeher kommunizieren wir über die Sprache. Sie ist die höchste Kommunikationsform, welche die Evolution hervorgebracht hat. Im Verlauf der Geschichte entstanden mit der Erfindung des Telefons und dem beginnenden Aufbau des Telefonnetzes zum Ende des 19. Jahrhunderts, sowohl in Europa als auch in den USA, neue Möglichkeiten der Kommunikation auf Grundlage der menschlichen Sprache [2]. Seither ist es möglich, sich über kabelgebundene und kabellose Netzwerke, über alle Distanzen hinweg, global und nahezu unbegrenzt zu unterhalten. Richtungsweisende Neuerungen und Entwicklungen legten im weiteren zeitlichen Verlauf den Grundstein für das heutige digitale Kommunikationsnetz, mit allen einhergehen Vor- und Nachteilen.

Im Jahr 2021 erreichte nach Aussagen des Bundeskriminalamtes die Anzahl an Straftaten aus dem Deliktfeld der Cyberkriminalität einen neuen Höchststand von 124.137 polizeilich erfasster Fälle. Im Vergleich zum Vorjahr handelt es sich dabei um einen Anstieg von über 12% [3, S. 6] und entspricht damit rund 2,5% aller erfassten Straftaten in diesem Jahr. [4] Das darin nicht eingeschlossene Dunkelfeld, die Anzahl an Straftaten, welche polizeilich nicht erfasst werden, dürfte auch nach Einschätzungen des Kriminologischen Forschungsinstitutes Niedersachsen, gerade im Deliktbereich *Phishing*, um einiges größer ausfallen. Dies liegt unter anderem auch an der Nicht-Anzeige von Sicherheitsvorfällen in Unternehmen aus verschiedenen Gründen,beispielsweise der Angst vor einem daraus resultierenden Image-Schaden. [5, S. 86] Während die Zahl der im digitalen Raum verübten Verbrechen signifikant immer weiter steigt, verbessert sich die Aufklärungsquote dieser nur minimal und liegt mit *„knapp unter 30% weiterhin deutlich unter dem PKS-Durchschnitt."* [3, S. 6] Das klassische *Phishing* gehört dabei auch weiterhin zu einem Hauptphänomen des Cybercrime. [3, S. 6]

Die Täter bedienen sich dafür im Hintergrund jedoch immer neuer Möglichkeiten, Angriffsvektoren und -methoden zur Durchführung ihrer Handlungen, darunter auch das immer verstärkt auftretende Phänomen des **Caller ID Spoofing**. Während bis vor einiger Zeit bei einem betrügerischen Telefonanruf noch die Rufnummer ausländischer Call-Center angezeigt wurde, werden Anrufen verbrecherischen Inhaltes heute oftmals zum Schein über vertrauenerweckende, deutsche Rufnummern getätigt. Das Hauptmotiv des Betrugs bleibt von dieser Handlung unberührt. [6]

Auch heute noch zählt die klassische Telefonie, neben Messenger-Diensten, e-Mails und Telefon- und Videokonferenzen zu dem am weiterhin häufigsten genutzten Medium zur Kommunikation zwischen Personen. Während die Anzahl der Festnetzanschlüsse in privaten Haushalten stark rückläufig ist, von 91,0% in 2016 auf 84,3% in 2021, nahm die Zahl der Mobiltelefone zu, bis zuletzt auf 97,6% pro Haushalt. Je 100 Haushalte wird die Anzahl von Mobiltelefonen auf 184,6 angegeben, darunter 158,5 Smartphones. [7]

1.1 Problemstellung

„Der Mensch ist immer noch das häufigste Angriffsziel für Cyber-Kriminelle. Ganz gleich ob beim Phishing, Chef-Betrug oder bei dubiosen Stellenangeboten als Finanzagent: Immer wieder gelingt es Betrügern, Bankkunden dazu zu verleiten, persönliche Daten preiszugeben oder gar Transaktionen vorzunehmen. [. . .]“ [8]

So definiert Andreas Krautscheid, Hauptgeschäftsführer des Bundesverbandes deutscher Banken, 2019 anlässlich des *Safer Internet Day* die gegenwärtige digitale Sicherheits-Lage. [8] Doch auch drei Jahre später, im Jahr 2022, gehört *Phishing*, und damit das Abgreifen höchstpersönlicher Daten unter Ausnutzung des Faktor Mensch, laut dem jährlichen Lagebericht Cybercrime des Bundeskriminalamtes zu einer der häufigsten Straftaten im digitalen Raum. [3, S. 13]

„Die verwendeten Narrative sind mannigfaltig und passen sich dem aktuellen politischen wie gesellschaftlichen Geschehen an.“ [3, S. 15]

Ähnlich beschreibt es der Lagebericht des Bundeskriminalamtes und gewährt damit gleichzeitig auch Einblick in die Probleme, vor welchen die Ermittlungsbehörden alltäglich stehen. Eine schnelle Reaktion auf neue kriminelle Phänomene und Modi Operandi sind unabdingbar bei der effektiven Bekämpfung und Aufklärung von Straftaten, gerade im digitalen Raum. Diese schnelle Reaktion erfordert ein umfassendes Wissen über digitale Tatmittel und deren Verwendung sowie umfassende technische als auch personelle Ressourcen, aber auch Vernetzung der Strafverfolgungsbehörden, sowie ein regelmäßiger Austausch untereinander und mit Akteuren aus Wirtschaft und Forschung.
Gerade in den vergangenen Jahren konnten Cyber-Kriminelle, durch die Corona-Lage und die zuletzt weltpolitischen Spannungen ausgelösten Ängste und Isolationen, das Vertrauen vieler Personen und Institutionen ausnutzen, um persönliche Daten gezielt mit Themen aus den Bereichen Impfstoffe oder finanzieller Absicherung abzuschöpfen. [9] Unabhängig davon bleibt das Motiv der Täter gleich: Vertrauliche Daten abzugreifen und für weitere kriminelle Zwecke zu missbrauchen, sei es der reine Verkauf auf Darknet-Marktplätzen oder als Ausgangs- bzw. Eintrittspunkt für weitere Straftaten zum Nachteil des Dateninhabers. [3, S. 13]

Caller ID Spoofing ist damit auch "nur" eine weitere Methode krimineller Akteure, durch Ausnutzung technischer Schwachstellen, die Effizienz ihrer Taten zu steigern und den daraus geschlagen Profit bei, im besten Fall, geringerem Aufwand zu erhöhen. Unter Vortäuschung einer glaubwürdigen Identität im Rahmen eines Telefonanrufes werden die Opfer manipuliert und zu für diese nachteilige Handlungen, wie die Herausgabe von Wertgegenständen oder Geld, verleitet. Die Aufklärung über das Phänomen, dessen Hintergründe und technische Grundlagen, sowohl unter den handelnden Ermittlungsbehörden als auch unter der Bevölkerung ist damit Teil der Eindämmungsstrategie, zu welcher auch diese Arbeit beitragen soll.

1.2 Zielsetzung

Ein weiterer Cybercrime-Lagebericht des Unternehmens Microsoft prognostiziert bereits jetzt einen vermehrten Anstieg an Phishing-Angriffen in den kommenden Jahren [10, S. 21]. Bereits im vergangenen Jahr 2022 konnten durch die hauseigenen Systeme 710 Millionen Phishing-Mails geblockt werden, die Dunkelziffer dürfte demnach um einiges höher liegen. Diese Zahlen lassen erkennen, dass bereits jetzt eine Intensivierung der Aufklärung des digitalen Raumes und der in diesem stattfindenden kriminellen Phänomene erfolgen muss, um eine effektive Strafverfolgung und die Durchsetzung des Rechts auch hier sicherzustellen. Zu einem Teil dieser Aufklärung, explizit über das aktuell vorherrschende Phänomen des **Caller ID Spoofing**, soll diese Arbeit beitragen.

Dazu soll

- ein formeller und juristischer Rahmenaufbau zur Betrachtung geschaffen,
- die technischen Hintergründe erläutert,
- das Vorgehen der Täter analysiert und
- geeignete Abwehrmaßnahmen definiert werden

Grundlegende Kenntnisse über die technischen Abläufe, welche sich die Kriminellen zur Tatbegehung zunutze machen, sind essentiell zu deren Verfolgung und Bekämpfung. Aus diesem Grund soll der Fokus dieser Arbeit auf den Erwerb eines technischen Grundverständnisses über das Phänomen **Caller ID Spoofing** gelegt werden. Schwerpunkt dabei soll der verwendete Standard des *Voice over IP* sowie das *Session Initiation Protocol* sein.

1.3 Vorgehensweise

Im Kapitel *Grundlagen und Definitionen* werden zunächst für den Sachverhalt relevante Begriffe definiert und in Kontext gesetzt. Weiterhin werden die Straftaten an sich und unter diesen auch das Phänomen **Caller ID Spoofing** aus juristischer Sicht betrachtet, sowie ein Einblick in die gegenwärtige Bedrohungslage aus Sicht der Ermittlungsbehörden gewährt.

Im Kapitel *Technische Hintergründe* soll die historisch-technische Entwicklung der Telefonie und deren aktueller Entwicklungsstand beleuchtet werden. Dabei wird hauptsächlich auf die mittlerweile weit verbreite Technik der *VoIP* unter Verwendung des *SIP*-Protokolls eingegangen. Außerdem sollen die konkreten technischen Hintergründe und Möglichkeiten des **Caller ID Spoofing** dargelegt und mögliche Vorgehen zu dessen Durchführung herausgestellt werden.

Im Kapitel *Methoden und Durchführung* sollen diese Vorgehen im Anschluss analysiert und an konkreten Anwendungsbeispielen präsentiert werden.

Im Kapitel *Abwehrmaßnahmen und Aufklärung* sollen anhand der vorgestellten Beispiele geeignete Gegenmaßnahmen, sowohl aus dem Bereich der *Security Awareness* als auch aus dem Gesichtspunkt des aktuellen Forschungsstandes vorgestellt werden.

Im Kapitel *Zusammenfassung und Diskussion* sollen die zuvor zusammengetragenen Sachverhalte noch einmal gemeinsam betrachtet werden, um daraus eine Diskussion zum Umgang mit den gewonnen Erkenntnissen zu entwickeln.

Im Kapitel *Fazit und Ausblick* soll ein abschließendes Fazit gezogen und ein möglicher Ausblick für weitere künftige Ansätze und Arbeiten in diesem Bereich gewährt werden.

2 Grundlagen und Definitionen

Zum besseren Verständnis der im Verlauf dieser Arbeit benutzten Begrifflichkeiten werden in diesem Kapitel zunächst einige im Zusammenhang stehende Grundlagen aus dem Bereich des *Cybercrime* betrachtet. Weiterhin wird der Begriff des **Caller ID Spoofing** definiert, als Deliktfeld eingeordnet und in einen juristischen Kontext gesetzt.

2.1 Cybercrime

Der Begriff *Cybercrime* ist eine Zusammensetzung aus den Worten *Cyber* ("Wortbildungselement mit der Bedeutung 'die von Computern erzeugte virtuelle Scheinwelt betreffend'") [11] und *Crime* (zu deutsch "Kriminalität").Trotz dessen, dass der Ausdruck *Cybercrime* für viele ein Begriff darstellt, fällt dessen genaue Definition deutlich schwieriger aus.

Grundlegend und in den meisten Fällen beschreiben die Begriffe *Cybercrime* oder *Cyberkriminalität "Straftaten, bei denen die Täter moderne Informationstechnik nutzen."* [12] Strafrechtlich ergeben sich dadurch allerdings keine neuen Tatbestände, es erfolgt lediglich eine Subsumtion bestehender Paragraphen auf die sich durch die Digitalisierung ergebenden Sachverhalte. [12]

Eine grundlegende Unterscheidung von Cybercrime wird in die Bereiche *im engeren Sinne* und *im weiteren Sinne* vollzogen. Während sich Delikte *im engeren Sinne* von Cybercrime gezielt gegen Informationstechnische Systeme, das Internet, oder digitaler Daten im Allgemeinen richten, umfassen Delikte *im weiteren Sinne* eben jene Straftaten, die unter Zuhilfenahme dieser Systeme begangen werden. [13]

2.2 Social Engineering

Nicht allein Computersysteme und -netzwerke weisen mitunter eklatante Schwächen und Lücken aufgrund struktureller Fehler in ihrer Programmierung auf und werden damit interessant für kriminelle Akteure, auch deren jeweiligen Nutzer bieten eine Vielzahl an Angriffsmöglichkeiten, welche im Deliktbereich Cybercrime genutzt werden können. Die darin beschriebenen Angriffsvektoren lassen sich im Bereich des *Social Engineering* verorten.

Social Engineering, aus den Begriffen *social* (zu deutsch "sozial") und *engineering* (zu deutsch "entwickeln, konstruieren") definiert im Kontext der Informationssicherheit den Faktor Mensch als Eintritts- und Angriffspunkt eines Computersystems- oder Netzwerkes. Die Benutzer dieser werden dabei gezielt unter Einsatz verschiedener Methoden dahingehend unbemerkt manipuliert, dass sie für den Täter bestimmte, förderliche Handlungen ausführen, wie zum Beispiel das Herausgeben vertraulicher Informationen wie Zugangsdaten oder Betriebsgeheimnisse oder das Durchführen von Finanzzahlungen zum Vorteil der Täter. Der dabei entstehende Schaden macht sich oftmals erst im Nachgang des Angriffes bemerkbar. [14, S. 29–31] [15]

Im Generellen bezeichnet *Social Engineering* einen psychologischen Angriff auf die Verhaltensweise eines Menschen und ist damit im historischen Kontext betrachtet ebenso alt wie die Menschheit selbst. Viele der beim *Social Engineering* genutzten Techniken beruhen auf evolutionären menschlichen Verhaltensweisen, die sich über eine Vielzahl an Studien nachweisen lassen. Selbst in Unkenntnis über diese Verhaltensweisen, lassen sich gezielte Manipulationen menschlichen Handelns auch im Alltag wiederfinden, beginnend bei wohl platzierter Werbung bis hin zu unbewusster Manipulation am Arbeitsplatz. [15]

Kriminelle Akteure machen sich diese Verhaltensweisen gezielt zunutze, um ihre Vorhaben umzusetzen. Besonders in Verbindung mit IT-Systemen ergeben sich neue Methoden und Ziele für *Social Engineering*-Angriffe. Diese bedrohen hauptsächlich das informatische Schutzziel der Vertraulichkeit. Die Herausgabe von vertraulichen Informationen basiert zumeist auf dem gezielten Einsatz von Authentizität, Nichtabstreitbarkeit und Zuverlässigkeit bereits erworbener oder frei zugänglicher Informationen, über welche die Täter eine Beziehung zu ihren Opfern aufbauen. Individuelle Angriffe auf Einzelpersonen oder Unternehmen mittels *Social Engineering* erfolgen nach keinem fest definierten Schema. Zwar existieren eine Vielzahl an Techniken und bewährte Tricks zum Erlangen vertraulicher Daten, nichtsdestotrotz muss jeder Angriff gezielt auf das Opfer zugeschnitten werden. Auch die Grundlage an individuellen Informationen, die im Vorfeld gesammelt werden, haben letztendlich Einfluss auf den Tatablauf. [16]

Im Vergleich dazu lassen sich *Phishing*-Angriffe, auch trotz ihres in der Regel zunächst für eine Vielzahl an Personen bestimmten Aufbaus, ebenfalls als *Social Engineering* verorten. Dabei wird meist auf wirtschaftlich bewährte Techniken und Ziele zurückgegriffen, welche sich auch an aktuellen gesellschaftlichen Aspekten und Themen orientieren, beispielsweise der Corona-Pandemie. Gerade Neuerungen und bislang unbekannte, neue Technologien und Angriffsarten erbringen den Tätern die meisten Erfolge. Ermittlungs- und IT-Behörden reagieren auf entstehende Phänomene mit entsprechenden Warnungen und Aufklärungsarbeit. [17, S. 4]

2.3 Phishing

Zur Ausführung einer Vielzahl von Straftaten bedarf es im Vorfeld weiterer Handlungen, oftmals kriminellen Hintergrundes, in Vorbereitung auf die eigentliche Haupttat. *Phishing* vom englischen Wort *fishing* (zu deutsch "fischen") abgeleitet, beschreibt das Abgreifen persönlicher und vertraulicher Daten von Einzelpersonen oder Wirtschaftsunternehmen im digitalen Raum mittels elektronischer Kommunikationswege und ist damit einer der *„Haupteintrittsvektoren für Schadsoftware und war [auch im Jahr 2021] ursächlich für den massenhaften Abgriff sensibler personenbezogener Daten, wie beispielsweise Bankdaten.“* [3, S. 13]

Diese abgeschöpften Daten, zumeist Zugangs- und Anmeldedaten, werden gesammelt und im Anschluss für weitere Straftaten im Deliktfeld *Cybercrime* verwendet oder im Darknet[1] zum Verkauf angeboten. *Phishing* führt bei den Betroffenen oftmals zu finanziellen Verlusten aufgrund der Kompromittierung von Nutzerkonten bei Banken oder Onlineshops. [3, S. 12] Die Täter bedienen sich dabei des Modus Operandi der Fälschung von Absenderdaten und greifen damit die Schutzziele der Integrität und Authentizität an. Unter Vorspiegelung vermeintlich seriös wirkender e-Mails sollen die Empfänger dazu gebracht werden, maliziöse Links zu öffnen, welche auf ebenfalls seriös wirkende, aber gefälschte Websites verweisen, auf welchen die Dateneingabe erfolgt. Teilweise enthalten die e-Mails auch Dateianhänge mit Schadsoftware, welche mit gezielten Formulierungen, zum Beispiel es handle sich dabei um ein wichtiges Dokument, zum Öffnen gebracht werden. Diese schaffen wiederum den Tätern Eintrittsmöglichkeiten zum Gerät des Opfers. *Phishing*-Mails werden breit gestreut und an eine hohe Anzahl an Personen versandt, welches jedoch für die Täter keinerlei Mehraufwand erzeugt. [19]

Die Anzahl allein von Websites mit *Phising*-Hintergrund stieg seit 2015 um mehr als 1200% auf zuletzt über 384.000 weltweit an [20]. *Phishing* ist damit für Kriminelle eine der finanziell lukrativsten Formen von *Cybercrime* und der Faktor Mensch das ideale Einfallstor.

2.3.1 Sonderformen Phishing

Die heutige digitalisierte Welt unterliegt einem ständigen Wandel durch neue technische Entwicklungen und Innovationen. Diese zwingen die Täter ebenfalls zu immer neuen (technischen) Vorgehensweisen im Umgang mit ihren Opfern. Daraus resultieren auch immer neue Varianten von *Phishing*-Angriffen, basierend auf technischen Neuerungen und gesellschaftlichen Entwicklungen.

[1] Verborgener, verschlüsselter und überwiegend anonymer Teil des Internet, welcher nur mittels Anonymisierungsnetzwerken erreichbar ist [18]

Spear-Phishing

Spear-Phishing beschreibt einen gezielten *Phishing*-Angriff auf eine Einzelperson oder ein Unternehmen, hier gegebenenfalls auch als Teil eines APT (siehe Kapitel 2.6.4). Beim *Spear-Phishing* werden gezielt öffentlich zugängliche oder bereits im Vorfeld abgegriffene Daten und Informationen in Nachrichten, vorwiegend E-Mails, eingesetzt, um die Betroffenen zu einer Herausgabe von vertraulichen Informationen zu bewegen. *Spear-Phishing* steht im Gegensatz zum herkömmlichen *Phishing*, bei welchem relativ ungesteuert versucht wird, über eine große Anzahl versandter *Phishing*-Mails Nutzerdaten abzugreifen. [21]

Vishing

Vishing beschreibt eine weitere Form von *Phishing*-Angriffen mit dem Ziel, vertrauliche Nutzerdaten abzugreifen. Im Vergleich zum herkömmlichen, textbasierten, *Phishing* wird beim *„Vishing“*, zusammengesetzt aus den Worten *„voice“* und *„fishing“*, der Kommunikationsweg der Telefonie genutzt. Die Täter kommunizieren somit zum Teil direkt mit den Opfern und bringen diese aktiv im mündlichen Gespräch dazu, sensible Daten preiszugeben. Dabei können sich *Vishing*-Angriffe von Aufbau und Ablauf stark unterscheiden. Ähnlich des Mail-*Phishing* werden beim *Vishing* teilweise *„Auto dialer“*[2] verwendet, um eine Vielzahl an Rufnummern anzurufen. Bei Annahme des Gespräches erfolgt zunächst die Antwort mittels vordefinierten Band-Ansage. Erst wenn das Opfer auf diese reagiert und beispielsweise einen geforderten Tastendruck tätigt, wird es mit einer realen Person verbunden. *Auto dialer* fungieren dabei als Filter, um misstrauische Personen direkt auszuschließen und die Erfolgsquote des Angriffes zu erhöhen beziehungsweise den Personalaufwand zu optimieren. [22]

Smishing

Eine weitere Form von *Phishing*, auch in Kombination mit *Vishing* genutzt, ist das *Smishing*. Zusammengesetzt aus den Worten *„SMS“* und *„phishing“* beschreibt es das Abgreifen vertraulicher Informationen über den Versand von SMS-Kurznachrichten. Ähnlich wie beim herkömmlichen *Phishing* werden hierbei vertrauenerweckende Nachrichten eines vermeintlich vertrauenswürdigen Absenders versandt, um das Aufrufen von enthaltenen Links zu fordern. Dies kann zum einen erneut auf gefälschte Websites zur Eingabe vertraulicher Informationen führen, zum anderen zum Download maliziöser App-Software aufrufen. Auch beim *Smishing* werden bereits im Vorfeld gesammelte Daten genutzt. Teilweise fordern die Nachrichten auch einen Anruf zu einer definierten Rufnummer, welcher dann in einem *Vishing*-Angriff resultiert. [23]

[2] Programm, welches automatisiert vordefinierte Telefonnummern anruft

2.4 Spoofing

Spoofing, aus dem Englischen für *"Manipulation"* oder *"Verschleierung"* [24], beschreibt in der Informations- und Kommunikationstechnik das Vorgehen, bei welchem ein System oder die dahinterstehende Person durch Verschleierung dessen Identität, beispielsweise über die *Internet Protocol (IP)*-Adresse, als eine andere ausgegeben wird. Gründe hierfür können zum Beispiel das absichtliche Vortäuschen einer falschen, jedoch für das Opfer vertrauenswürdigeren, aber auch einer komplett anonymen Identität sein. Der Hintergrund von Spoofing ist fast ausschließlich negativen Charakters, da dabei zumeist Betrugsabsichten, wie beispielsweise Phishing als Motiv, zugrunde liegen. Spoofing zielt damit auf das erweiterte Schutzziel der Authentizität ab. Es existieren unterschiedliche Arten von *Spoofing*, danach differenziert, welche Art von Absender-Daten verfälscht werden. [25, 26]

2.4.1 Sonderformen Spoofing

Auch *Spoofing* unterliegt einem stetigen technischen und gesellschaftlichen Wandel. Dabei unterliegen digitale Daten einer permanenten Gefahr der absichtlichen Manipulation zu Schadzwecken, welche sich exemplarisch an den folgenden Beispielen verdeutlichen lässt.

Typosquatting

Die simpelste Form eines *Spoofing*-Angriffes beschreibt das *Typosquatting*. Bei diesem werden Personen durch selbst hervorgerufene Tippfehler beim Aufrufen einer Website auf eine manipulierte Seite geleitet. Diese kann dann der ursprünglich anvisierten Seite im exakt gleich Aussehen nachempfunden sein, um beispielsweise Login-Daten abzugreifen. Diese werden von den Opfern freiwillig in dem Glauben eingegeben, sich auf der echten Website zu befinden. Teilweise wird die Person auch nur auf eine weitere, dritte Seite ohne Bezug zum Original weitergeleitet, welche lediglich mit Werbung gefüllt ist. [27]

GNSS-Spoofing

Eine weitere, aber deutlich komplexere Art des Spoofings ist das *Global Navigation Satellite System (GNSS) Spoofing*. Hierbei werden gezielt die Signale von Navigationssatelliten und Positionssystemen durch entsprechende Sender so überlagert, dass Endgeräte zur Positionsbestimmung falsche Positionsangaben errechnen und dadurch ihren Standort falsch bestimmen. Fahrzeuge, Flugzeuge und auch Schiffen können damit absichtlich auf Irrwege geführt und deren Sicherheit somit gefährdet werden. [28, S. 76] Gezielt eingesetzt wird *GNSS-Spoofing* überwiegend von politischen Akteuren in Russland, Syrien und auf der Krim. Einem Bericht der Non-Governmental Organization (NGO) C4ADS zufolge wurden nach eigenen Recherchen in diesen Gebieten fast über 10.000 Störungen durch *GNSS-Spoofing* seit Februar 2016 registriert. Allein insgesamt 1311 zivile Schiffe seien davon betroffen gewesen. [29, S. 20] Motive dahinter sind sowohl der Schutz militärischer und politischer Einrichtungen, der von wichtigen Personen gegen Drohnen-Angriffe, aber auch der Einsatz in Kriegsgebieten zur Unterstützung der Luftabwehr. [29, S. 26 ff.]

2.5 Caller ID Spoofing: Definition

Caller ID Spoofing ist die Bezeichnung für das Verschleiern der eigenen Telefonidentität bei einem Telefonanruf gegenüber dem Angerufenen. Konkret wird dabei auf dem Endgerät des Empfänger eine andere, vom Anrufer frei wählbare, Identität dargestellt. Zumeist erfolgt diese Darstellung über die Telefonnummer, allerdings ist auch die Anzeige eines frei wählbaren Namens möglich, sofern dies von der genutzten Peripherie unterstützt wird. [30]

Das Phänomen **Caller ID Spoofing** lässt sich dabei aus rein technischer Sicht nicht ausschließlich als klares Kriminalitätsphänomen verorten, da auch andere Anwendungen der Technik möglich sind. Diese werden im Folgenden beschrieben.

2.6 Einordnung Caller ID Spoofing

Das Phänomen **Caller ID Spoofing** umfasst mehrere technische und methodische Vorgänge bei der Verschleierung jener eigenen Identität, die durch das Übermitteln der zu dieser zugeordneten Telefonnummer abgebildet wird. Diese Möglichkeit besteht sowohl bei Sprach-Anrufen als auch bei der Übermittlung einer SMS-basierten Textnachricht. Die Einordnung von **Caller ID Spoofing** als kriminelle Handlung ist rechtlich zwar klar abgegrenzt, lässt sich jedoch auch aus anderen, legalen Blickwinkeln betrachten. Nach Definition handelt es sich bei **Caller ID Spoofing** um eine Begleiterscheinung bei der Durchführung des bereits beschriebenen *Vishing*. In der Anwendung lassen sich jedoch grundlegend zwei unterschiedliche, wenn auch mitunter harmonierende Hauptmotive erkennen. **Caller ID Spoofing** kann im kriminellen Kontext sowohl gezielt als Modus Operandi zur Umsetzung weiterer Straftaten als auch zur reinen Verschleierung, demnach als Begleitphänomen betrachtet werden. Eine weitere Abgrenzung lässt sich beispielsweise aber auch ziehen, indem das Vorgehen der Täter als gezielt und ungezielt betrachtet wird. [30]

2.6.1 Caller-ID Spoofing als Haupttat

Caller ID Spoofing im Hauptkontext einer Straftat wird verwendet, um dem Opfer gezielt eine falsche Absender-Identität vorzutäuschen, mit dem Hintergrund, dieses dadurch zu für den Täter förderlichen Handlungen zu bewegen. Dies ist hauptsächlich bei Betrugsdelikten der Fall, bei welchen die Opfer durch Vortäuschen einer falschen Identität beispielsweise zur Herausgabe von Geld oder Informationen überzeugt werden sollen. Die jeweilige, für die Tatgeschichte passende Telefonidentität soll dabei unterstützen und dem Opfer eine höhere Glaubwürdigkeit des Anrufers gegenüber einem Anruf mit einer komplett fremden Rufnummer vermitteln. Die Telefonnummer oder der Anzeigename als übermittelte Identität beim **Caller ID Spoofing** im Hauptkontext einer Straftat ist damit nicht frei wählbar und wird gezielt auf das Opfer angepasst. [30] [31]

Die Techniken des **Caller ID Spoofing** lassen sich ebenfalls als Maßnahme des *Social Engineering* betrachten, sofern die verwendete Rufnummer eben nicht wahllos und zur reinen Identitätsverschleierung genutzt wird. Mit einer gezielten Wahl der Rufnummer kann dem Opfer eine Identität simuliert werden, welche eine erhöhte Vertrauensbasis für das Gespräch bilden kann. Auch dem Täter bekannte Rufnummersperren ankommender Anrufe können so umgangen werden. [31]

Wie in vielen anderen Kriminalitätsfeldern, unterliegt auch das **Caller ID Spoofing** und dessen nachgelagerten Vorgehensweisen und Straftaten einem ständigen Wandel. Dies erfolgt durch die kriminellen Akteure in Reaktion auf aktuelle gesellschaftliche Gegebenheiten mit Motiv der Gewinnmaximierung unter möglichst minimalem Aufwand. [31]

Anrufe im Namen von Polizeibehörden

Ein schon länger, weit verbreiteter Modus Operandi unter Zuhilfenahme von **Caller ID Spoofing** ist das Durchführen manipulierter Anrufe unter Vorgabe, dass diese von nationalen oder internationalen Ermittlungsbehörden wie Interpol, Europol oder dem FBI (Bundespolizeibehörde der USA) getätigt werden. Die dazu verwendeten Rufnummern lassen sich dabei mitunter tatsächlich Dienststellen der genannten Behörden zuordnen. [31]

Dafür wird zunächst ein automatisierter, von *Auto-Dialern* durchgeführter Anruf, wahllos an Rufnummern initiiert. Erst mit Annahme des Gespräches durch eine geforderte Reaktion des Angerufenen wird dieser an eine reale Person vermittelt. Diese wiederum versucht dann, das Opfer sowohl durch Vortäuschen einer erfundenen Geschichte als auch den durch die Hoheitsstellung der Behörde ausgeübten zusätzlichen Druck, zu einer Geldzahlung in digitalen Währungen, oder aber auch zu einer Bargeldübergabe oder die Herausgabe von Wertgegenständen zu bewegen. [30] [31]

Mit der zuletzt erfolgten Sperrung der Polizeirufnummer *110* als Absenderufnummer (siehe Kapitel 2.8) wurde diese Vorgehensweise teilweise unterbunden, jedoch erfolgen nach wie vor Anrufe unter abgewandelten Rufnummern und demselben Modus Operandi. [31]

Neighbor-Spoofing

Als *Neighbor-Spoofing* wird eine spezielle Form des **Caller ID Spoofing** bezeichnet, bei welchem dem Angerufenen eine ihm ähnliche, beziehungsweise aus demselben Nummernblock stammende Rufnummer präsentiert wird. Diese dem Angerufenen gegenüber suggerierte „Nähe“ erhöht die Chancen der Rufannahme durch das Opfer. Die den Opfern präsentierte Täuschung wird diesem Modus Operandi entsprechend angepasst. [32]

2.6.2 Caller-ID Spoofing als Maßnahme der Verschleierung

Als Begleitphänomen ist **Caller ID Spoofing** bei der Durchführung einer weiteren kriminellen Haupthandlung zu betrachten, wenn diese, wie bei Phishing-Angriffen, lediglich dem Zweck der Anonymisierung und Verschleierung der eigenen Identität dient, wodurch die nachträgliche Tataufklärung deutlich erschwert werden soll. Dabei ist die verwendete Identität, die Telefonnummer, frei gewählt, da hier keine gezielte Absenderidentität notwendig ist. Genutzt wird die Maßnahme der Anonymisierung hauptsächlich bei Werbeanrufen, auch von ausländischer Call-Centern ausgehend, bei welchen eine deutsche Telefonnummer zur Steigerung der Seriosität verwendet wird. [33]

Aufgrund der Ungebundenheit bei der Wahl der verwendeten Rufnummer kann es unter Umständen dazu kommen, dass vergebene, von realen unbeteiligten Dritten verwendete Rufnummern, als Absendernummer ohne deren Wissen verwendet werden. Dieses Vorgehen erzeugt somit immer zwei Opfer von **Caller ID Spoofing**. Zum einen die Person, welche mittels einer gefälschten Rufnummer angerufen wird, zum anderen die Person, welche im eigentlichen Besitz der benutzten Rufnummer ist und gegebenenfalls unerwartete Rückrufe vermeintlich angerufener Personen erhält. [30]

Schockanrufe

Sogenannte *„Schockanrufe“* sind unter Cyberkriminellen eine weit verbreitete Methode aus der Reihe des Trickbetrugs zur schnellen Erlangung hoher Geldbeträge bei minimalem Aufwand und Risiko. Bei dieser Masche wird sich den Opfern, zumeist im höheren Lebensalter, gegenüber zunächst als nahestehende Person eines Familienmitgliedes, als behandelnder Arzt eines solchen oder aber als Polizist oder Autoritätsperson ausgegeben. Dabei suchen die Täter gezielt in Telefonbüchern nach Nachnamen, welche auf ein hohes Lebensalter der Person hinweisen. Mit Methoden des *Social Engineering* wird Vertrauen zu den Opfern aufgebaut, parallel dazu aber auch Druck und Stress ausgeübt. [34] Ähnliches Vorgehen lässt sich beim sogenannten *"Enkeltrick"* beobachten. [35]

Inhaltlich präsentieren die Täter Geschichten, nach welcher das nahestehende Familienmitglied in einen Unfall, eine Straftat oder ähnliches verwickelt gewesen sei und nun schnell eine größere Summe Bargeld benötige, um beispielsweise Krankenhaus-, Anwalts-, oder Versicherungskosten decken zu können. Andernfalls würden schlimme Konsequenzen drohen. Das Motiv der Täter ist, die Opfer durch den dadurch ausgelösten „Schock“ zu unüberlegtem Handeln zu bewegen. Lässt sich das potenzielle Opfer auf die Geschichte ein, wird zeitnah eine Geldübergabe arrangiert, bei welcher sich die Täter ebenfalls als nahestehende Person oder auch als Polizist ausgeben. [36]

Mitunter werden bei *Schockanrufen* auch gefälschte Telefonnummern, wie zum Beispiel die Notrufnummer der Polizei *110* verwendet, um gegenüber den Opfern von Beginn an eine Autoritätsstellung zu suggerieren. Parallel dazu dienen die gefälschten Nummern gleichwohl der Anonymisierung der Täter. [34]

Aktuelle Recherchen zeigen, mit welchen Tricks und technischen Methoden die Täter agieren und von wo aus sie operieren. Professionelle "Schockanrufer" arbeiten dabei immer öfter mit Techniken vergleichbar eines Call-Centers und den Strukturen herkömmlicher, legaler Unternehmen. Es existiert eine Firmenhierarchie und die Mitarbeiter werden anteilig nach Provision bezahlt. Der Standort dieser auf Betrug ausgelegten Telefonzentralen lassen sich, aufgrund technischer und rechtlicher Motive, zumeist im Ausland verorten. Nichtsdestotrotz werden von hier aus auch durch deutschsprachige Täter, Betrugsdelikte in Deutschland durchgeführt. [36] Weiter wird darauf im Kapitel 3 eingegangen.

Tech-Support-Betrug

Eine weiteres, gegenwärtig häufig auftretendes Phänomen sind Anrufe falscher Support-Mitarbeiter, beispielsweise der Firma *Microsoft*. Diese versuchen durch ihre Opfer, unter dem Vorwand, technische Probleme an der verwendeten Peripherie lösen zu wollen, einen virtuellen Zugang zu deren Computer-Systemen zu erlangen. Bei Erfolg wird im Anschluss zumeist versucht, Geldleistungen für die vermeintlich erfolgte Reparatur zu erpressen. Weiterhin ist es den Tätern allerdings auch möglich, Schadsoftware auf dem betroffenen Gerät zu installieren oder vertrauliche Informationen abzugreifen. [37]

2.6.3 Cybercrime as a Service

Die beschrieben Phänomene lassen Einblick in die Strukturen und Vorgehen der Täter gewähren und eröffnen damit gleichzeitig Möglichkeiten eines eigenen, gewerbsmäßigen Geschäftsfeldes. Das Bereitstellen solcher Dienstleistungsangebote zur Begehung von kriminellen Straftaten im digitalen Raum werden als *Cybercrime as a Service* beschrieben.

Mit voranschreitender Digitalisierung haben auch kriminelle Akteure die sich daraus neu ergebenden Möglichkeiten der Monetarisierung krimineller Dienstleistungen entdeckt und bieten diese frei verkäuflich auf entsprechenden Plattformen an. Mittlerweile können auf diesen digitalen Marktplätzen sämtliche Arten krimineller Handlungen gegen Bezahlung erworben werden. Diese Professionalisierung eröffnet Personenkreisen mit kriminellen Absichten die Möglichkeit, Straftaten im digitalen Raum zur Gewinnsteigerung zu begehen, welche andernfalls nicht über derartige Fähigkeiten oder Ressourcen verfügen. Dazu zählt beispielsweise das Entwickeln und Bereitstellen von Viren, Trojaner und Ransomware[3], das Anbieten von DDos-Attacken[4] oder der Verkauf gestohlener Daten wie Kreditkartennummern oder Passwörter. [13]

In Bezug auf **Caller ID Spoofing** lassen sich Anwendungsfelder von Cybercrime as a Service, beispielsweise in der Bereitstellung von entsprechender Hard- und Software zur Durchführung gefälschter Telefonanrufe, durchaus erahnen, auf welche eine Vielzahl an Tätern, wie beispielsweise in den oben beschrieben Call-Centern, zugreifen können. [34]

2.6.4 APT

Advanced Persistent Threat (APT) ist die Bezeichnung eines gezielten digitalen Großangriffes auf ein bestimmtes System oder Systeme eines bestimmten Ziels. Ausgeführt werden *APT* von gut ausgebildeten und technisch ausgestatteten Angreifern, oftmals von staatlicher Seite unterstützt. Ziel dabei ist die Informationsgewinnung über einen langen Zeitraum, sowie Manipulation des betroffenen Systems. Diese können wirtschaftlicher, aber auch wissenschaftlicher oder staatlicher Natur sein. Der eigentlichen Angriffsphase eines *APT* geht oftmals eine ebenso aufwendige Phase zur Informationsgewinnung über das Ziel voraus. **Caller ID Spoofing** kann im Rahmen dessen zur gezielten Informationsbeschaffung über Methoden des *Social Engineering* eingesetzt werden, indem Mitarbeiter gezielt Insiderwissen entlockt wird. [38]

[3] Schadsoftware zur Verschlüsselung von Dateien, welche nur gegen Bezahlung freigegeben werden
[4] Gezielte Attacke auf Systeme durch Überlastung des Datenverkehrs

2.6.5 Caller-ID Spoofing im positiven Kontext

Neben den zahlreichen Anwendungsfeldern von **Caller ID Spoofing** seitens krimineller Akteure existieren auch Nutzergruppen, welche aus nicht-kriminellen Motiven ihre Rufnummer verschleiern. Dazu zählen unter anderem Journalisten, Aktivisten, Detekteien und Anwaltskanzleien, die so zum Beispiel ihre eigene Rufnummer zu Recherchezwecken und verdeckten Ermittlungen verändern, um an benötigte Informationen zu gelangen. Neben diesen existieren noch weitere Einrichtungen, welche sich der Verschleierung der eigenen Identität bei der Abwicklung von Telefonanrufen bedienen. Dazu zählen zum Beispiel Frauenhäuser, Einrichtungen für Schutzbefohlene und weitere Institutionen, welche einer potenziell erhöhten Bedrohung von außen ausgesetzt sind. Auch gibt es rein pragmatische Ansätze für **Caller ID Spoofing**. Ärzte oder Anwälte könnten zum Beispiel Telefonate mit privaten Geräten, außerhalb ihrer Arbeitszeit oder aus dem Home-Office führen, und die Rufnummer ihres Arbeitsplatzanschlusses als Absende-Rufnummer verwenden. Noch simpler ist der Anwendungsfall bei Call-Centern, in denen zwar jedes verwendete Endgerät und damit auch jeder Mitarbeiter faktisch unter einer ihm zugeordneten Rufnummer telefoniert, in der Praxis jedoch eben nicht diese Durchwahl, sondern die übergeordnete Haupt-Nummer der Hotline als Initiator der Verbindung angibt. Nichtsdestotrotz unterliegen die genannten Personen und Institutionen auch unter verständlichen und begründbaren Motiven für **Caller ID Spoofing** nach deutschem Recht dem Telekommunikationsgesetz, welches keinerlei Sonder- und Ausschlussregelungen enthält. Die generelle Übermittlung einer falschen oder nicht zugeordneten Telefonnummer ist nach diesem strafbar. Dieser Sachverhalt wird in anderen Ländern allerdings anders eingeschätzt. Nach amerikanischer Rechtsprechung ist beispielsweise das Motiv des Spoofings ausschlaggebend für dessen legale Nutzung. Weiterhin sind in diesem auch generelle Sonder- und Ausnahmereglungen für Strafverfolgungsbehörden festgesetzt, siehe Kapitel 2.8. [39, 833 ff.]

2.7 Gegenwärtige Lage

Zur Erlangung einer ungefähren Einschätzung der tatsächlichen Gefährdungslage durch **Caller ID Spoofing** wurden mehrere Polizeidienststellen verschiedener Bundesländer (Niedersachsen und Sachsen) schriftlich zu ihren Erfahrungen im Umgang mit dem Thema befragt. Inhaltlich umfasste die Befragung die folgenden Bereiche:

- Allgemeine Erfahrungen mit dem Einsatz gefälschter Telefonnummern zur Begehung von Straftaten
- Statistiken und Kennzahlen der erfassten Fälle und Einordnung in Deliktbereiche
- (Technische) Maßnahmen der Aufklärung/Anruferermittlung
- Überbehördliche Zusammenarbeit mit anderen Dienststellen, Telekommunikationsanbietern oder der Bundesnetzagentur

Die gesammelten Informationen stammen dabei aus den Abteilungen für Cybercrime der Kriminalpolizeiinspektion Göttingen sowie den jeweiligen Landeskriminalämtern Niedersachsen und Sachsen.

Rückschlüsse auf das generelle Vorkommen und die Häufigkeit auftretender Straftaten unter Verwendung von **Caller ID Spoofing** lassen sich aus den übereinstimmenden Aussagen aller befragter Dienststellen treffen. Demnach bearbeiten alle befragten Abteilungen gegenwärtig Verfahren, welche in Bezug mit gefälschten Rufnummern stehen, hauptsächlich in den Bereichen Vermögensbetrug und Phishing. Allein die Zentrale Kriminalpolizeiinspektion Göttingen bearbeitet gegenwärtig ein Großverfahren im Deliktbereich des Anlagenbetrug, welches circa 300 gefälschte Rufnummern beinhaltet. Dazu kommen weitere Verfahren unter Verwendung von SIM-Karten, welche unter falscher Identität registriert wurden, sowie von den Tätern gemietete Rufnummernkontingente zur Begehung diverser Betrugsstraftaten. Eine statistische Auswertung aller erfasster Fälle erfolgte bislang jedoch nicht.

Auf die polizeilichen Möglichkeiten im Rahmen der Aufklärung von Straftaten unter Verwendung von **Caller ID Spoofing** wird im Kapitel 5.3.1 eingegangen.

2.8 Rechtliche Einordnung Caller-ID Spoofing

Der (legitime) Einsatz von **Caller ID Spoofing** unterliegt den rechtlichen Rahmenbedingungen des Landes, in welchem der Anruf durchgeführt wird. Im folgenden sollen die teils unterschiedlichen Rahmenbedingungen und die dafür verantwortlichen Akteuren betrachtet werden.

2.8.1 Rechtslage in Deutschland

Anruf

Einen Anruf beschreibt nach § 3 (1) Telekommunikationsgesetz (TKG) *"eine über einen öffentlich zugänglichen interpersonellen Telekommunikationsdienst aufgebaute Verbindung, die eine zweiseitige oder mehrseitige Sprachkommunikation ermöglicht"*. [40] Das Gesetz umfasst damit sowohl die herkömmliche drahtgebundene Telefonie, sowie *IP*-Telefonie und Mobilfunk als auch Videotelefonie.

Bundesnetzagentur

Die Bundesnetzagentur mit Sitz in Bonn ist eine selbständige obere Bundesbehörde im Geschäftsbereich des Bundesministeriums für Wirtschaft und Klimaschutz, mit einigen Aufgabenbereichen in der Fachaufsicht des Bundesministeriums für Digitales und Verkehr. Als Nachfolgebehörde des Bundesministeriums für Post und Telekommunikation und dem Bundesamt für Post und Telekommunikation obliegt ihr als zentrale Infrastrukturbehörde die Regulierung von Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen in der Bundesrepublik Deutschland. Gleichzeitig wahrt sie den Verbraucherschutz, die Interessen der Bundesbürger gegenüber den Anbietern der genannten Medien. Im Bereich der Telekommunikation reguliert die Bundesnetzagentur den *"chancengleichen und funktionsfähigen Wettbewerb"* [41] der Anbieter und sichert die flächendeckende Grundversorgung von Telekommunikationsdiensten. Als Aufsichtsbehörde verwaltet sie zudem die Frequenzen und Rufnummern im Bundesgebiet und bekämpft aktiv deren Missbrauch und Störungen. Grundlage für die Arbeit der Bundesnetzagentur bildet das Telekommunikationsgesetz. [41]

Telekommunikationsgesetz

Die rechtliche Grundlage für die Abwicklung der telefonischen Telekommunikation innerhalb Deutschlands bildet das TKG der Bundesrepublik. Als Bundesgesetz reguliert und fördert dieses *"technologieneutral"* den *"Wettbewerb im Bereich der Telekommunikation und [den] leistungsfähige[n] Telekommunikationsinfrastrukturen"*. [42]

Weiterhin soll darüber eine angemessene und flächendeckende Dienstleistung im Bereich der Telekommunikation sichergestellt werden. Dem Gesetz *"unterliegen alle Unternehmen oder Personen, die im Geltungsbereich dieses Gesetzes Telekommunikationsnetze oder Telekommunikationsanlagen betreiben oder Telekommunikationsdienste erbringen sowie die weiteren, nach diesem Gesetz Berechtigten und Verpflichteten."* [42]

Die ursprüngliche Version des Gesetzes wurde im Juli 1996 beschlossen, die aktuelle Fassung entspricht dem Stand vom 01.12.2021. Relevant für den Tatbestand des **Caller ID Spoofing** ist maßgeblich § 120 TKG. Dieser definiert, wie und unter welchen Voraussetzungen und Rahmenbedingungen Telekommunikationsanbieter die Rufnummer eines Anrufers dessen Angerufenen zu übermitteln haben. [43, S. 1]

Grundsätzlich dürfen Endnutzer nach § 120 (2) TKG nur Rufnummern *"aufsetzen und in das öffentliche Telekommunikationsnetz übermitteln, wenn sie ein Nutzungsrecht an der entsprechenden Rufnummer haben und es sich um eine Rufnummer des deutschen Nummernraums handelt."* [44] *"Rufnummern für Auskunftsdienste, Massenverkehrsdienste oder Premium-Dienste, Nummern für Kurzwahldienste sowie die Notrufnummern 110 und 112 dürfen nicht als Rufnummer des Anrufers übermittelt werden."* [44]

Abgewichen hiervon darf lediglich nach § 120 (2) TKG nur *¨im Falle einer Rufumleitung"*, wenn *"als zusätzliche Rufnummer die übermittelte und angezeigte Rufnummer des Anrufers aufgesetzt"* [wird]. [44] Ausgenommen davon sind nach § 120 (2) TKG jedoch auch explizit *"Rufnummern für Auskunftsdienste, Massenverkehrsdienste oder Premium-Dienste, Nummern für Kurzwahldienste sowie die Notrufnummern 110 und 112"*. [44]

Mit der zuletzt erfolgten Novellierung des Telekommunikationsgesetzes müssen seit 01.12.2022 *"sämtliche an der Verbindung beteiligte Anbieter öffentlich zugänglicher Telekommunikationsdienst"* sicherstellen, *"dass Rufnummern für Auskunftsdienste, Massenverkehrsdienste oder Premium-Dienste, Nummern für Kurzwahldienste sowie die Notrufnummern 110 und 112 nicht als Rufnummer des Anrufers übermittelt und angezeigt werden."* [44].

Gleichzeitig müssen selbige Anbieter *"sicherstellen, dass als Rufnummer des Anrufers nur dann eine national signifikante Rufnummer des deutschen Nummernraums angezeigt wird, wenn die Verbindung aus dem öffentlichen deutschen Telefonnetz übergeben wird."* [44]

Im Falle der Anzeige einer *"national signifikante Rufnummer des deutschen Nummernraums"* [44], welche jedoch aus einem ausländischen Telefonnetz übergeben wird, *"haben die Anbieter sicherzustellen, dass netzintern der Eintrittsweg der Verbindung in das deutsche Netz eindeutig gekennzeichnet wird; die Rufnummernanzeige ist zu unterdrücken."* [44]

Dies soll zum einen sogenannte Ping-Anrufe unterbinden, bei welchem mittels eines für die Annahme des Gespräches viel zu kurzen Anrufes ein gezielter Rückruf auf eine teure Rufnummer provoziert wird. [45] Zum anderen soll das Blockieren der Absende-Rufnummer *110* und *112* das Phänomen der Schockanrufe beziehungsweise Anrufe mit erpresserischer Absicht unterbunden werden.

Zudem müssen nach § 120 (4) TKG *"sämtliche an der Verbindung beteiligte Anbieter öffentlich zugänglicher Telekommunikationsdienste“* [sicherstellen], *"dass als Rufnummer des Anrufers nur dann eine national signifikante Rufnummer des deutschen Nummernraums angezeigt wird, wenn die Verbindung aus dem öffentlichen deutschen Telefonnetz übergeben wird."* [44]

Sollte dies nicht der Fall sein und mittels Caller ID Spoofing eine *"Rufnummer des deutschen Nummernraums"* aus einem ausländischen Telefonnetz übergeben werden, muss der Netzanbieter sicherstellen, *"dass netzintern der Eintrittsweg der Verbindung in das deutsche Netz eindeutig gekennzeichnet wird."* Die Anzeige der Rufnummer ist zu unterdrücken. Alle Absätze beziehen sich nach § 120 (5) TKG gleichwohl auf die*"Übertragung von Textnachrichten über das öffentliche Telekommunikationsnetz."* [44]

Verstöße

Zur Verfolgung von Verstößen gegen des § 120 TKG stehen der Bundesnetzagentur verschiedene rechtliche und technische Möglichkeiten zur Verfügung. Diese werden im § 123 TKG beschrieben. [46]

Grundsätzlich kann die Bundesnetzagentur nach § 123 (1) TKG *"im Rahmen der Nummernverwaltung Anordnungen und andere geeignete Maßnahmen treffen, um die Einhaltung gesetzlicher Vorschriften, aufgrund dieses Gesetzes ergangener Verpflichtungen und der von ihr erteilten Bedingungen über die Zuteilung von Nummern sicherzustellen."* [46]

Dazu kann sie nach § 123 (2) TKG *"die Betreiber von öffentlichen Telekommunikationsnetzen und die Anbieter öffentlich zugänglicher Telekommunikationsdienste verpflichten, Auskünfte zu personenbezogenen Daten wie Name und ladungsfähige Anschrift von Nummerninhabern und Nummernnutzern zu erteilen"[...].* [46]

Dies ist insbesondere dann von Relevanz, wenn nach § 123 (2) TKG *"der Bundesnetzagentur eine Beschwerde vorliegt, die Bundesnetzagentur aus anderen Gründen eine Verletzung von Pflichten annimmt oder die Bundesnetzagentur von sich aus Ermittlungen durchführt."* [46]

Explizit bei der Verfolgung von Verstößen gegen § 120 TKG kann die Bundesnetzagentur nach § 123 (3) TKG *"Auskunft über die Rufnummer, von der ein Anruf ausging, sowie über für die Verfolgung erforderliche personenbezogene Daten wie Name und ladungsfähige Anschrift des Nummerninhabers und des Nummernnutzers"* [46] von den Telekommunikationsanbietern verlangen. Ferner kann sie *im Falle der gesicherten Kenntnis von der rechtswidrigen Nutzung einer Rufnummer gegenüber dem Netzbetreiber, in dessen Netz die Nummer geschaltet ist, die Abschaltung der Rufnummer anordnen."* [46]

Zur *"Durchsetzung der Anordnungen"* können nach § 123 (8) TKG Zwangsgelder von 1.000 bis 1.000.000 Euro verhängt werden. [46]

2.8.2 Rechtslage in den Vereinigten Staaten von Amerika

Die amerikanische Regelung bezüglich **Caller ID Spoofing** ist im *"Truth in Caller ID Act"* aus dem Jahr 2009 festgesetzt.

Truth in Caller ID Act of 2009

Diese 2009 von der *Federal Communications Commission (FCC)* angeregte Gesetzesänderung wurde 2010 vom Senat verabschiedet und als gültige Rechtsprechung definiert. Sie verbietet die wissentliche Übertragung einer (*"misleading or inaccurate caller identification information"*) mit der Absicht eines Betrugs, eines Diebstahls oder einer Sachbeschädigung (*"defraud, cause harm, or wrongfully obtain anything of value"*). Dies gilt sowohl für (*"telecommunications service"*) als auch für (*"IP-enabled voice service"*). Parallel dazu regelt die Gesetzgebung auch Ausnahmen von dieser für Strafverfolgungsbehörden *("authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States")*). [47]

3 Technische Hintergründe

3.1 Vorbetrachtung

Kommunikation liegt in der Natur des Menschen. *"Man kann nicht nicht kommunizieren"* beschreibt es Paul Watzlawick in seinem Buch *Menschliche Kommunikation* [48, S. 53].

Der Begriff Kommunikation selbst entstammt dem Lateinischen Wort für *"Mitteilung"*. Sie ist *"ein Prozess der Übermittlung und die Wahrnehmung von Zeichen aller Art, [. . .] ein Prozess der Übertragung von Nachrichten zwischen einem Sender und einem Empfänger"*. [49, S. 2, 12]

Angefangen mit Höhlenmalereien, über Trommeln, Feuer- und Rauchzeichen, schafften es bereits Menschen in den Anfängen der Zivilisationen, auch über entfernte Strecken hinweg zu kommunizieren. Parallel dazu lernten sie, sich über Gesten und Laute zu verständigen, welche in einer Jahrtausend langen Entwicklungsphase in den heutigen globalen Hochsprachen mündete. Die direkte sprachliche Kommunikation zwischen Menschen blieb für eine lange Zeit das Hauptkommunikationsmedium. Mit Beginn der Industrialisierung und Erfindung der Telefonie schaffte sich die Menschheit eine Möglichkeit, diese Kommunikation über die Sprache mit dem Austausch über entfernte Wegstrecken zu verbinden. [49, S. 2]

3.2 Historie der Telefonie

Mit Entdeckung der Signalübertragung mittels elektrischer Leiter begann vor rund 150 Jahren die Entwicklungsgeschichte der Telefontechnik.

3.2.1 Drahtgebundene Telefonie

Als ausschlaggebender Meilenstein und Vorläufer der Telefontechnik wird die Erfindung der elektrischen Telegraphie, die Übertragung von Zeichen über drahtgebundene Telegraphen, zu Beginn des 19. Jahrhunderts betrachtet. Bereits im Jahr 1849 erfolgte die Freigabe des zuvor rein für den staatlichen Betrieb ausgelegten Telegraphennetzes für die Zivilbevölkerung und ebnete so den Weg zur modernen Telefonie. Später, im Jahr 1860, entwickelte der Lehrer Johann Philipp Reis (1834-1874) eine erste Apparatur zur erfolgreichen Übertragung von Sprache und Musik über 100 Meter, welche er ein Jahr später der Öffentlichkeit präsentierte. Aufgrund mangelnder Aufmerksamkeit, Kontakte zur Industrie und die allgemeine Überzeugung der Überlegenheit der Telegraphie gelang Reis mit seiner Erfindung kein Durchbruch. [2, S. 54–59] [50, S. 2]

Dies gelang erst dem Taubstummenlehrer schottischer Abstammung Alexander Graham Bell (1847-1922), welcher an die Praktikabilität der Telefonie glaubte und am 14. Februar 1876 das amerikanische Grundpatent auf die Erfindung des Telefons anmeldete. [2, S. 60] Rund zwei Stunden später desselben Tages beantragte auch Elisha Gray (1835-1901) das Patent auf seine Version des Telefonapparates, welchen er parallel zur Bell'schen Erfindung entwickelt hatte.

Trotz dessen, dass das Gray'sche Gerät im Vergleich zu Bell's tatsächlich funktionierte, erhielt letzterer am 07. März 1876 das Patent auf die Erfindung des Telefons. Das wiederum mündete 1877 in der Gründung der Bell Telephone Association, welche mit dem Aufbau des amerikanischen Telefonnetzes betraut wurde. Nach der Umbenennung 1885 in American Telephone and Telegraph Company (AT-T) gilt diese auch heute noch als die größte Telefongesellschaft der Welt. [50, S. 3]

Bei der Streitfrage, wer nun als Erfinder des Telefons gilt, dürfte, ungeachtet von Bell und Gray, nach neusten Erkenntnissen jedoch am wahrscheinlichsten der US-Italiener Antonio Santi Giuseppe Meucci (1808-1889) in Frage kommen. Dieser hatte schon im Jahr 1871 eine entsprechende Patentanmeldung beantragt, welche allerdings aufgrund säumiger Gebühren im Jahre 1874 auslief. Mit Meucci's Tod 1889 endete auch ein noch zwei Jahre zuvor begonnener Versuch der Behörden, Bell das erteilte Patent nachträglich abzuerkennen, ohne jedoch die Frage nach der Ersterfindung abschließend geklärt zu haben. Dies geschah erst mit offiziellem Beschluss vom 11. Juni 2002, welcher Meucci die Erfindung des Telefons zusprach. [50, S. 3]

Als *"Geburtstag des Fernsprechers in Deutschland"* [2, S. 63] gilt der 26.10.1877, als der deutsche Generalpostmeister Heinrich von Stephan sich nach einem erfolgreichen Test der Bell'schen Telefone im Berliner Haupttelegraphenamt für die Verbreitung der Telefonie in Deutschland einsetzte. Die Bezeichnung "Fernsprecher" lässt sich ebenfalls auf von Stephan zurückführen. [2, S. 63–64]

Bereits Ende 1877 begann die deutsche Firma Siemens mit dem Verkauf deutscher Telefone auf der Grundlage von Bell. *"Am 14. Dezember 1877 erhielt Werner v. Siemens das 'Deutsche Reichspatent' 2399 für 'Telephone und Rufapparate mit magnetischer Gleichgewichtlage der schwingenden Teile'"*. [2, S. 64]

Im Jahr 1881 besaßen bereits 458 Personen einen Anschluss in das Telefonnetz mit einer Länge von inzwischen 5460 Kilometern [2, S. 39]. Schon das Telegraphennetz basierte auf Verteilungsämtern, welche die händische Vermittlung der einzelnen Teilnehmer übernahm. Dieses System war ebenfalls Ausgangspunkt beim Aufbau des Telefonnetzes [2, S. 66].

Abbildung 3.1: Telefonistinnen bei der Arbeit im händischen Vermittlungsamt [51, S. 26]

Rund 10 Jahre später, im Jahr 1900, wurden die ersten öffentlichen Münzfernsprecher eingeführt. Durch die Erfindung und den darauffolgenden Siegeszug des Hebdrehwählers mit Drehscheibe zur automatisierten Anrufvermittlung wurde im selben Jahr in Berlin das erste Amt für die automatisierte Vermittlung von Anrufen eröffnet. Grund dafür war auch die Kompensation der bis dahin massiv gestiegene Anzahl an Telefonanschlüssen. Trotz der offensichtlichen Vorteile wurde, auch aufgrund der infrastrukturellen Schäden durch den zweiten Weltkrieg, die letzte händische Ortsvermittlungsstelle erst 1966 geschlossen. Parallel dazu existierten in Deutschland bereits 6000 Ortsvermittlungsstellen, welche mit dem System des Edelmetall-Motor-Drehwählers arbeiteten. [2, S. 68–71]

In den 1960er Jahren begann mit der fortschreitenden Erkundung des Weltraumes auch das Zeitalter der Satellitentelefonie, durch welche der interkontinentale Telefonverkehr zwischen Europa und dem amerikanischen Kontinent verbessert wurde. Bis in die 1980er Jahre hinein erfolgte die stetige Verbesserung der verwendeten Verbindungskabel, Anschluss- und Vermittlungsapparate sowie der Telefoniegeräte. [2, S. 73–74]

Der Beginn des digitalen Zeitalters zwischen 1980 und 1990 führte auch in der Telefontechnik zu maßgeblichen Änderungen und Neuerungen. Dies betraf hauptsächlich den Übergang von der herkömmlichen analogen Sprachübermittlung, hin zur heute als Standard zählenden Paketdatenvermittlung. Dafür wurde im ersten Schritt zunächst die Kommunikation zwischen den einzelnen Vermittlungsstellen digitalisiert, während die Übertragung der Sprachdaten zwischen Teilnehmer und Vermittlungsstelle noch analog erfolgte. Mit Einführung dieser computergesteuerten Vermittlungsstellen wurde nach und nach ebenfalls die Teilnehmerschaltung über ein Sternnetz zu einem Maschennetz überführt. Bei diesem sind die auch heute noch anzutreffenden Zentralvermittlungsstellen durch Querverbindungen ebenfalls miteinander verbunden. [2, S. 141–143]

Durch die Einführung von *Integrated Services Digital Network (ISDN)* erfolgte in der weiteren Entwicklung die Umwandlung ins Digitale in den Endgeräten der Nutzer und die Übertragung der Sprache damit rein digital. Ende der 1950er Jahre nahm parallel dazu die mittlerweile immer leistungsfähiger gewordene drahtlose Kommunikation in Form des *A-Netzes* den Betrieb auf. [2, S. 150][52]

3.2.2 Mobilfunknetz

Bereits sei dem 19. Jahrhundert wurde neben der Entwicklung drahtgebundener Kommunikation an der drahtlosen Übermittlung von Sprache geforscht. Sowohl eine Steigerung der Reichweite wie auch an eine Verbesserung der Praktikabilität sollten dadurch erreicht werden. Über die Entwicklung einzelner Prototypen zur Übertragung von Zeichen über wenige Meter, der drahtlosen Telegraphie, der Erfindung des Rundfunks, bis hin zur Errichtung des ersten öffentlichen Mobilfunknetzes in Deutschland durch die Deutsche Bundespost vergingen ebenfalls Jahrzehnte.

A-Netz

Trotz der unförmigen und teuren Mobilgeräte der ersten Generation, hielten ab 1951 über das *A-Netz* mehr als 20 Jahre lang immerhin bereits 10.000 Teilnehmer Kontakt miteinander, hauptsächlich über Autotelefone. Die Vermittlung erfolgte manuell im Handbetrieb. Trotz dessen signalisiert das *A-Netz* sowohl den Beginn des heutigen Mobilfunknetzes als auch die Anfänge moderner Smartphones. [2, S. 143][52]

B-Netz

Auch das darauffolgende *B-Netz* besaß lediglich eine Reichweite von rund 30 Kilometern und wurde ebenfalls über Autotelefone genutzt, von welchen allerdings der Standort dem Anrufer in etwa bekannt sein musste. Auch die Anzahl der gleichzeitig möglichen Gespräche war aufgrund der wenigen Sprachkanäle äußerst begrenzt. Dennoch wurde mit dem *B-Netz* auch im Mobilfunkbereich die automatische Vermittlung der Gespräche eingeführt. [2, S. 143][52]

C-Netz

Im Jahr 1986 löste das *C-Netz* seinen Vorgänger ab. Durch den zellularen Aufbau des Netzes und einer einheitlichen Vorwahl war ein Wissen über den Aufenthaltsort des Angerufenen nicht länger von Relevanz. Durch die Einführung eines Telekartensystems bestand außerdem erstmals die Möglichkeit der Identifikation und eindeutige Erreichbarkeit der einzelnen Nutzer. Durch Fortschreiten der Technologie entwickeln sich auch die Telefongeräte immer weiter. Geräte des *C-Netz*es waren erstmals tragbar, wenn auch noch von enormer Größe. [2, S. 144][52]

D-Netz

Mit dem Start des *D-Netz*es unter Verwendung des digitalen *Global System for Mobile Communications (GSM)* Standards 1992 endet die Ära der analogen Funknetze in Deutschland. Trotz dessen zählt *GSM*, ebenso wie seine Vorgänger, nach wie vor zu den leitungsvermittelnden Kommunikationsnetzen. Bei diesen wird die Verbindung, identisch zum herkömmlichen Festnetz, über eine direkte Leitung zwischen Anrufer und Angerufenem aufgebaut. Parallel dazu rückten mit Voranschreiten der Digitalisierung auch weitere Formen der Kommunikation wie E-Mail, soziale Netzwerke etc. immer mehr in den Vordergrund. Diese basieren jedoch im Gegensatz zur leitungsorientierten Telefonie auf *GSM*-Basis mit paketdatenbasiertem Datenaustausch. Somit etablierten sich gleichzeitig zwei Netze in Koexistenz. Aufgrund der Ineffizienz dieser Methode, entschieden sich die Netzbetreiber schon bald, auch die Übermittlung der Sprachdaten, nach Umwandlung in Datenpakete, innerhalb des Kernnetzes, über unter Verwendung des Internet Protokolls, zu übertragen. Aufgeteilt auf zwei Betreiber besitzt das *D1* und *D2* Netz jeweils 124 Kanäle, aufgeteilt auf wiederum acht jeweilige Sprachkanäle, auf welche die Anrufe im Zeilenschlitzverfahren verteilt werden. 1994 wird über das *D-Netz* ebenfalls die erste Short Message Service (SMS) versandt. [2, S. 145] [53]

Long Term Evolution (LTE)

Über die Entwicklung und Einführung der Nachfolgegenerationen des digitalen Mobilfunks *Enhanced Data Rates for GSM Evolution (EDGE)* und *Universal Mobile Telecommunications System (UMTS)*, folgte 2010 mit *LTE* der Start der 4. Generation Mobilfunk in Deutschland. [54]

Bereits bei der 1. Generation im *C-Netz* erfolgte mit *General Packet Radio Service (GPRS)* die Entwicklung eines Dienstes zur Paketdatenvermittlung als Erweiterung zum sprachübertragungsorientierten *GSM*-Standard. Damit erfolgte die Ausrichtung auf eine verbesserte Datenübertragung aufgrund der immer mehr in den Fokus gerückten Internetdiensten auf Mobilgeräten. Im Gegensatz zum leitungsvermittelnden *GSM* konnten nun Datenpakete übertragen werden, ohne dafür einen exklusiven Kanal zwischen zwei Teilnehmern zu belegen und damit einen effizienteren Netzdurchsatz ermöglichen. Bis hin zu *LTE* wurde diese Effizienz mit Fortschreiten der technologischen Entwicklung immer weiter gesteigert.

Eine der entscheidendsten Neuerungen von *LTE* gegenüber dessen Vorgängern ist die Konzentration auf ein rein paketvermittelndes Kernnetz, über welches alle Dienste auf *IP*-Basis abgewickelt werden. Parallel dazu wurde ebenfalls die Kommunikation zwischen den Vermittlungs- und Basisstellen und den einzelnen Netzwerkkomponenten des Mobilfunknetzes auf *IP* aufgebaut. Lediglich die Sprachübertragung der Telefonie basierte bei *LTE* bis 2014 aufgrund von Inkompatibilität nach wie vor auf dem *GSM*-Netz. Die Umstellung erfolgte erst mit der Weiterentwicklung und stückweisen Einführung des eigenen *VoLTE* Dienstes. [53, S. 272]

Voice over LTE (VoLTE)

Mit *VoLTE* erfolgte erstmals seit Einführung des mobilen, drahtlosen Funknetzes eine Trennung und Aufteilung der Sprach- und Datendienste auf zwei unterschiedliche Kanäle. Hierbei erfolgt weiterhin erstmals die Übertragung der Sprachdaten mittels *IP Multimedia Subsystem (IMS)*, welches wiederum auf dem *SIP*-Protokoll basiert. [53, S. 295]

3.3 Aufbau Festnetz

Das Telefonnetz, wie wir es heute kennen, hat mit dem vor 150 Jahren nicht mehr viel gemein. Lediglich die Grundidee, die menschliche Sprache von einem zum anderen Ort zu übertragen, ist gleich geblieben. Mit der zuletzt flächendeckenden Umstellung auf *VoIP* erlebte das *"Intelligente Netz"* erneut einen großen Entwicklungssprung. [53, S. 4]

3.3.1 Analoger Aufbau Telefonnetz

Bereits vor Einführung von *VoIP* und *ISDN* bildete das hiesige, analoge Telefonnetz ein komplexes physisches Gebilde aus verschiedenen Stellen, Knotenpunkten und verbindenden Leitungen. Die Knotenpunkte wurden durch die *Ortsvermittlungsstellen* bzw. *Teilnehmervermittlungsstellen (TVSt)* als Teil eines weitaus größeren hierarchischen Netzwerkes gebildet. Mehrere *TVSt* wurden in nächster Ebene durch wiederum eine Vielzahl an *Fernvermittlungsstellen (FVSt)* verbunden. Beide Instanzen bildeten in ihrer Gesamtheit das öffentliche Telefonnetz *Public Switched Telephone Network (PSTN)*. Die Verbindung zweier Teilnehmer erfolgte direkt. Das Gespräch musste über bestimmte Zeichentöne, die beim Wählen der Telefonnummer und beim Anheben und Auflegen des Hörers ebenfalls über den Sprachkanal übertragen wurden, initiiert und beendet werden. Dieser Prozess bildet die Signalisierung, welche in veränderter Form auch im heutigen *VoIP*-Netz nach wie vor den Beginn eines Telefongespräches darstellt. [50, S. 4]

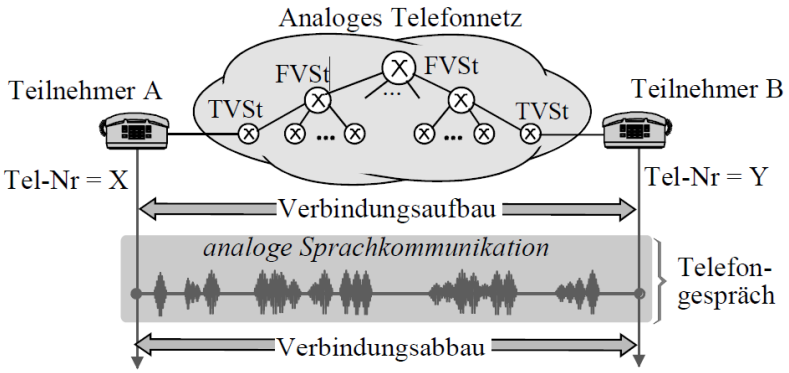

Abbildung 3.2: Rufaufbau im analogen Telefonnetz über Teilnehmer- und Fernvermittlungsstellen [50, S. 4]

Zum Austausch zweiter Teilnehmer, wurde nach Aufnahme der gesprochenen Wörter durch das Mikrofon im verwendeten Telefonapparat die Sprache als analoges Signal über den physischen Sprachkanal, ausgelegt auf eine Bandbreite von 4 kHz, übertragen. Die Vermittlung des Signals erfolgte durch die *TVSt* und *FVSt*. [50, S. 4]

3.3.2 Digitaler Aufbau Telefonnetz

Der Beginn des Aufbaus eines digitalen Netzes erfolgte mit der Digitalisierung der Verbindung zwischen den *TVSt* und *FVSt*. Dieser Schritt markiert damit ebenfalls den ersten großen Entwicklungsschritt in Richtung der heutigen digitalen Sprachkommunikation. In diesem, trotz bloßer Teildigitalisierung, bereits als digital bezeichneten Netzes wurden erstmals die Signalisierungsdaten als Bitstrom mit einer Bitrate von 64 kbit/s über das *Signaling System No. 7 (SS7)*-Protokoll zwischen den *TVSt* und *FVSt* übermittelt. Parallel dazu erfolgte die Digitalisierung der Abläufe in den Vermittlungsstellen selbst. *SS7* signalisiert damit gleichzeitig den ersten Einsatz eines digitalen Netzwerkprotokolls in der Telefonie. [50, S. 5]

3.3.3 Heutiger Stand Telefon- und Datennetz

Mit Umstellung auf *IP*-Technologie sowohl für den Sprach- als auch den Datenaustausch erfolgt eine ständige Weiterentwicklung und Verbesserung der verwendeten Technologien und Infrastrukturen. So wurden die Begriffe *Teilnehmer- und Fernvermittlungsstelle* von der Bezeichnung *Betriebsstelle* abgelöst. In diesen weiterhin flächendeckend verteilten Knotenpunkten laufen die mittlerweile größtenteils verwendeten Glasfaser- aber auch die nach wie vor genutzten Kupferleitungen der Multifunktionsanschlüsse des abzudeckenden Gebietes ein. Diese werden innerhalb der Betriebsstelle mittels eines *Digital Subscriber Line Access Multiplexer (DSLAM)* und *Multi Service Access Node (MSAN)* miteinander auf *IP*-Basis vernetzt, um den (Sprach-) Datenaustausch zwischen allen verwendeten Technologien zu ermöglichen. Alle Signale werden im Anschluss daran von den Betriebsstellen über das *Broadband Network Gateway (BNG)* an die nationalen Knotenpunkte *INXS* in München oder *DE-CIX* in Frankfurt am Main weitergeleitet und an ihre jeweilige Zieladresse verteilt. [55]

3.3.4 Rufaufbau im digitalen Netz

Beim Verbindungsaufbau beziehungsweise der Signalisierung eines Telefongespräches im digitalen Netz erfolgt dessen Vermittlung zwischen den *TVSt* und *FVSt* ebenfalls über das *SS7*-Protokoll. Dieser Ablauf ist in Abbildung 3.2 dargestellt. Nach dem Wählen der Rufnummer durch den Anrufer (Teilnehmer A) sendet zunächst die *TVSt* zu Beginn eine *Initial Address Message (IAM)* an die *TVSt* des Empfängers (Teilnehmer B), welche im Falle dessen Verfügbarkeit wiederum mit einer *Address Complete Message (ACM)* antwortet. Gleichzeitig beginnt das Gerät des Empfängers mit der Anrufsignalisierung. Im Falle einer Beantwortung des Anrufes erfolgt eine *Answer Message (ANS)* und das Gespräch kommt zustande. [50, 58 ff.]

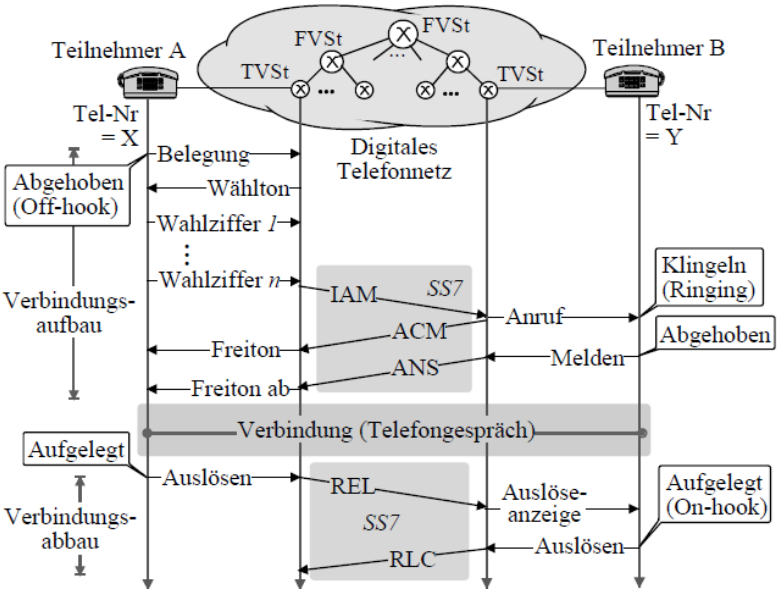

Abbildung 3.3: Detaillierter Ablauf des Rufauf und -abbau im digitalen Telefonnetz [50, S. 59]

Der Verbindungsabbau, ebenfalls von Teilnehmer A initiiert, erfolgt über eine *Release (REL)* Nachricht, auf die eine *Release Complete (RLC)* Nachricht von Teilnehmer B folgt. Trotz der Bezeichnung *digitales Netz* erfolgte sowohl die Kommunikation der jeweiligen Endgeräten mit ihren *TVSt* als auch die Sprachübertragung nach wie vor über einen anlogen Sprachkanal. [50, 58 ff.]

3.3.5 SS7

Mit der Überführung der Telefonie in das digitalen Netz, dem *ISDN* und *GSM*, bedurfte es, neben der Übermittlung der eigentlichen Sprachdaten, ebenfalls eines Austauschs von zusätzlichen Verbindungsinformationen zwischen den Vermittlungsstellen. *SS7* stellt dabei eine Sammlung einzelner Protokolle bereit, welche schichtweise aufeinander aufbauen und Gespräche über die einzelnen Schnittstellen und Komponenten des verwendeten Kommunikationsnetzes zwischen zwei Teilnehmern über entsprechende Signalisierungskanäle vermitteln. [50, S. 68] Ursprünglich für drahtgebundene Festnetzkommunikation entwickelt, existieren ab dem Mobilfunkstandard *GSM* zusätzliche Protokolle zur Abwicklung von Gesprächen innerhalb des Mobilfunknetzes. In diesem erfolgt der Austausch der Signalisierungsinformationen ebenfalls über einen eigenen Signalisierungskanal. [53, S. 7]

3.3.6 ISDN

Zu Beginn der 90er Jahre erfolgte schließlich mit der Einführung von *ISDN* der Aufbau eines volldigitalen Telefonnetzes zum Sprach- und Datenaustausch. In diesem erfolgt, im Gegensatz zum bisherigen *digitalen Netz*, nun auch die Signalisierung zwischen Endgerät und *TVSt* digital über einen zusätzlichen 16 kbit/s Signalisierungskanal *(D-Kanal)* mit entsprechendem Protokoll *(D-Kanal-Protokoll)*. Die Übermittlung der (Sprach-) Daten erfolgte ebenfalls erstmalig im *ISDN* über einen digitalen, bitstrombasierten Sprachkanal mit einer Bitrate von 64 kbit/s. Die Verbindung muss dabei nichtsdestotrotz aufgrund des leitungsvermittelnden Aufbaus auch im *ISDN* nach wie vor über die einzelnen Netzknoten zwischen den Teilnehmern direkt aufgebaut werden. Die Signalisierung zwischen den Vermittlungsstellen erfolgt weiterhin über das *SS7*-Protokoll.

Als universelles Netz erlaubte *ISDN* weiterhin die Einbindung weiterer Netzwerkgeräte wie Fax oder Modems, zum universellen Sprach-, Daten- und Bildaustausch. Zur Anbindung von analogen Endgeräten erfolgt eine Analog/Digital-Umwandlung in den *TVSt*. [50, S. 57–62]

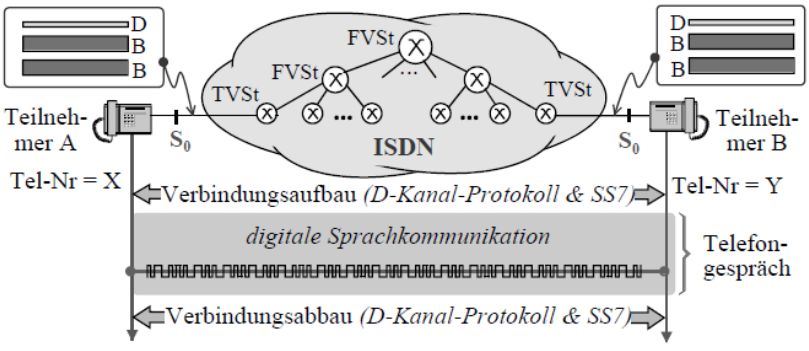

Abbildung 3.4: Rufaufbau im ISDN-Netz über Teilnehmer- und Fernvermittlungsstellen unter Verwendung des D-Kanal- und des SS7-Protokolls [50, S. 5]

3.4 Dienstbezogene Leistungsmerkmale

Die Umstellung des Telefonnetzes auf *ISDN* erlaubt es erstmals, neben der herkömmlichen Sprachübertragung, weitere Zusatzdienste anzubieten. [50, S. 4]

Diese werden als *Dienstbezogene* beziehungsweise *Sessionbezogene Leistungsmerkmale* oder kurz *Leistungsmerkmale* zusammengefasst und dienen der Verbesserung und Aufwertung der herkömmlichen Telefonie durch zusätzliche Funktionen. [50, S. 332]

Als dienstbezogene oder vermittlungstechnische Leistungsmerkmale werden Dienstleistungen bezeichnet, welche beiden Teilnehmern eines Telefongespräches, im öffentlichen Netz, netzseitig durch den Netzbetreiber zur Verfügung gestellt werden. Sie sind in der *ITU-T Rekommandation I.250* durch die *International Telecommunication Union (ITU)* definiert und dienen in erster Linie unterstützend bei der Durchführung von Telefonaten. Trotz dessen, dass sich die *ITU-T Recommendation I.250* ursprünglich auf die Anwendung im *ISDN* bezieht, wird sie bedingt auch auf das *VoIP*-Netz angewandt. [56] [57, 358 f.]

Darunter fällt beispielsweise das "Halten" und die Annahme einer weiteren Session (*Call Hold*), die Weiterleitung und Übernahme von Gesprächen (*Call Pickup*) und die Anrufweiterleitung (*Call Forwarding*). [50, 332 ff.]

Caller ID

Die *Caller ID* ist ein fester Bestandteil der Telefoninfrastruktur und existenziell bei der Abwicklung jeglicher Telefongespräche, unabhängig von der verwendeten Technologie und des Übertragungsmediums. Sie entspricht im Allgemeinen der Telefonnummer von Teilnehmern in einem Telefonnetz, wird aber durch entsprechend verwendete Protokolle angepasst, transferiert oder in ein anderes Format übersetzt. [58, S. 3]

Je nach Konfiguration wird die Caller ID des Anrufers dem Angerufenen angezeigt oder unterdrückt. Definiert wurde die *Caller ID* zuerst 1993 als Calling Line Identification Presentation (CLIP) in der *Telecommunication Standardization Sector (ITU-T) Recommendation Q.731.3 for the Signaling System No. 7 (SS7)*. [58, S. 3]

CLIP

Das vermittlungstechnische Leistungsmerkmal der *CLIP* beschreibt unter *ISDN* die Übermittlung der Rufnummer des Anrufers gegenüber dem Angerufenen. In der praktischen Anwendung wird dabei die Rufnummer des Anrufenden auf dem Display des Angerufenen abgebildet. Diese beschränkt sich auf ankommende Anrufe und kann damit nur von der angerufenen Seite deaktiviert oder aktiviert werden, sofern die Übertragung nicht bereits durch die anrufende Seite blockiert wurde (*Calling Line Identification Restriction (CLIR)*). Dies entspricht dem Anruf mit unterdrückter Rufnummer. [56, S. 4]

CLIR

Das vermittlungstechnische Leistungsmerkmal der *CLIR* beschreibt das Unterdrücken der eigenen Rufnummer auf Anruferseite gegenüber dem Angerufenen unter *ISDN*. Der Dienst beschreibt damit die klassische Rufnummerunterdrückung. Bei aktivierten *CLIP* erhält der Netzbetreiber dennoch die Rufnummer, diese wird im weiteren Verlauf allerdings nicht an den gerufenen Teilnehmer übermittelt. Im Gegensatz zu Einsatzleitstellen von Polizei, Feuerwehr und Rettungsdienst haben Privatpersonen keinerlei Möglichkeit der Umgehung von *CLIR*. Entsprechend genannte Stellen haben durch das Leistungsmerkmal *CLIPRO* die Möglichkeit, eine Rufnummerübermittlung zu erzwingen und die Rufnummer entsprechend angezeigt zu bekommen. [59, S. 3]

Calling Line Identification Presentation -no screening- (CLIP -no screening-)

Das vermittlungstechnische Leistungsmerkmal der *CLIP -no screening* beschreibt die Übermittlung einer selbst gewählten Nummer im öffentlichen Telefonnetz gegenüber dem Angerufenen und kann auf der anrufenden Seite aktiviert beziehungsweise definiert werden. Bei diesem Dienst wird, zusätzlich zur eigentlichen, netzseitig vergebenen Rufnummer (Network Provided Number) eine weitere, kundenspezifische Nummer (User Provided Number) dem Angerufenen übertragen. [60]

Dieses Leistungsmerkmal wird beispielsweise von Großunternehmen oder Call-Centern, in Kombination mit dem Leistungsmerkmal CLIR verwendet, um, statt der direkten Durchwahl-Rufnummer des Anrufenden, eine entsprechende Service-Nummer oder die Rufnummer der Telefonzentrale zu übermitteln. [61]

Rechtlich unterliegt der Dienst *CLIP -no screening-* in Deutschland dem § 120 TKG und stellt unter dessen Einhaltung eine legale Form des **Call ID Spoofing** im *ISDN* dar, bei welchem allerdings sowohl die netzseitige als auch die kundenspezifische Rufnummer des Anrufenden an den Netzbetreiber und den angerufenen Teilnehmer übertragen wird. Je nachdem, welche weiteren Dienste auf beiden Seiten aktiv sind, werden eine der beiden oder beide Nummern dem Angerufenen angezeigt.

3.5 VoIP

Das mittlerweile als Standard zählende System zur Abwicklung von Telefongesprächen wird als *VoIP* bezeichnet.

Im Gegensatz zu allen bisherigen Systemen, werden bei *VoIP* sowohl die Sprach- als auch die Signalisierungsdaten nicht mehr als Bitstrom, sondern als Datenpakete über das *IP*-Protokoll übertragen. Mit VoIP entfällt gleichzeitig die Verwendung des *D-Kanal*-Protokolls als auch die des *SS7*-Protokolls. Statt des herkömmlichen Verbindungsaufbaus einer festen Verbindung von Endgerät zu Endgerät erfolgt bei *VoIP* eine Reservierung von Ports, über welche die *"Session"*, der Austausch der Datenpakete, durchgeführt wird. Eine Session lässt sich dabei vereinfacht als Nachbildung der ehemals physikalischen Telefonverbindung zur Übertragung von Sprachpakten beschreiben. [50, S. 10]

Ebenso wie bereits bei *ISDN* erfolgt bei *VoIP* die Trennung der Signalisierung des Anrufes und dem Kanal zur eigentlichen (Sprach)-Datenübertragung. Diese Übertragung der Datenpakete in Echtzeit erfolgt dabei zumeist über das *Real-Time Transport Protocol (RTP)* beziehungsweise *Secure Real-Time Transport Protocol (SRTP)*-Protokoll. Ein Abgleich der Sprachqualität und weiterer Parameter zur Regulierung des Anrufes erfolgt parallel über das *RTP Control Protocol (RTCP)*-Protokoll. Zum Aufbau einer *VoIP*-Session, der Signalisierung des Anrufes, wird zumeist entweder auf das am weitesten verbreitete *SIP*-Protokoll oder die *H.323*-Protokollsammlung zurückgegriffen. [62, 245 ff.]

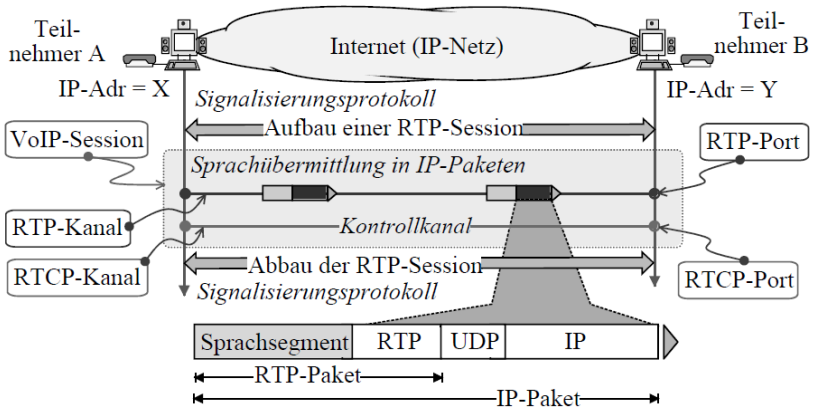

Abbildung 3.5: Rufaufbau im *VoIP* über ein Signalisierungsprotokoll und dem Datenaustausch über *RTP* beziehungsweise *RTCP* [50, S. 9]

Die Erweiterung des *ISDN*-Netzes durch das *IP*-Netz setzte zunächst weitere Bestandteile voraus, darunter *VoIP*-Gateways, welche von den Telekommunikationsanbietern eingesetzt werden, um eine Verbindung zwischen den *IP*-adressierten *VoIP*-Telefone und den herkömmlichen *ISDN*-Nummerntelefonen zu ermöglichen.

3.5.1 VoIP-Gateways

Eine der relevantesten Komponenten in modernen Telekommunikationsinfrastrukturen sind *Gateways* beziehungsweise konkret als *VoIP-Gateways* oder *Media-Gateways* bezeichnet. Diese dienen der gegenseitigen Übersetzung zwischen der modernen IP-basierten VoIP-Kommunikation und der nach wie vor verwendeten *ISDN* auf Rufnummernbasis. Rein technisch erfolgt in diesen die Umsetzung zwischen den *IP*-Paketen der *VoIP*-Technik und des unter *ISDN* zur Sprachdatenübermittlung verwendeten kontinuierlichen 64kbit/s Bitstrom. [50, S. 12] Dafür werden die Protokolle *Media Gateway Control Protocol (MGCP)* und *Media Gateway Control (Megaco)* eingesetzt. [50, S. 104]

Gateways sind zur Abwicklung beziehungsweise Übertragung sämtlicher Daten über ein (glasfaserbasiertes) *IP*-Netz fester Bestandteil der Betriebsstellen der Telekommunikationsanbieter. [50, S. 13]

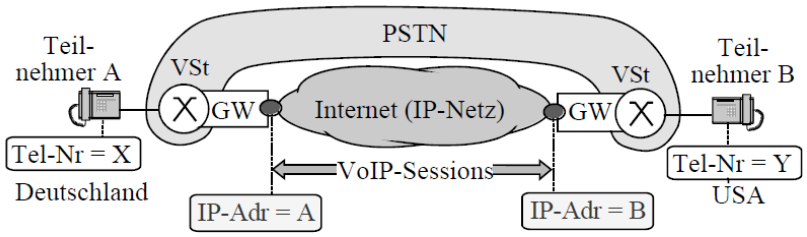

Abbildung 3.6: Einsatz von Gateways unter Verwendung von VoIP am Beispiel eines Telefongespräches zwischen Deutschland und den USA [50, S. 14]

3.5.2 Session

Gespräche über *VoIP* folgen dem Aufbau einer dafür einzeln einzurichtenden *VoIP*-Session. Jede Session verfügt dabei über mindestens einen logischen *Media Channel (MC)* zur Übertragung der (Sprach-) Daten über das *RTP*-Protokoll und einen *Media Control Channel (MCC)* auf Basis des *RTCP*-Protokolls. [50, S. 166]

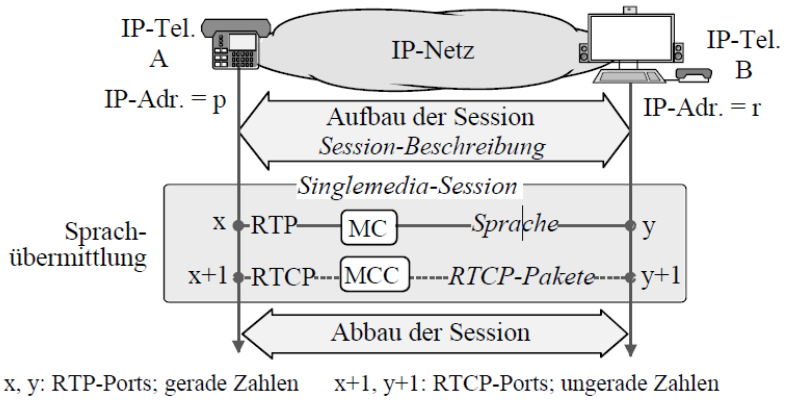

Abbildung 3.7: Aufbau VoIP-Session [50, S. 165]

Bei *VoIP*-Gesprächen auf *SIP*-Basis erfolgt der Session-Aufbau über das Session Description Protocol (SDP). Unter Verwendung von *H.323* kommt das untergeordnete *H.245*-Protokoll zur Anwendung. [50, S. 166]

SDP

Das Session Description Protokoll *SDP* ist nach dem Grundprotokoll *SIP* das wichtigste bei der Signalisierung und dem Verbindungsaufbau über *VoIP*. Es regelt die genauen Spezifikationen der aufzubauenden Session und wird vom Initiator der Verbindung nach seinen technischen Voraussetzungen vorgeschlagen. [50, 313 f.]

3.5.3 Quality of Service

Mit voranschreitender Entwicklung der Telefonietechnik stiegen gleichzeitig die an diese gestellten Anforderungen. Merkmale dieser sind beispielsweise Benutzbarkeit und Wirtschaftlichkeit der verwendeten Infrastruktur und Peripherie. Aber auch rein technische Qualitätsmerkmale gerieten immer mehr in den Fokus und sind mit der Einführung von *VoIP* fester Bestandteil bei Entwicklung und Aufbau des neuen digitalen Netzes. Zusammengefasst werden diese Anforderungen unter dem Begriff Quality of Service (QoS) und betreffen überwiegend die Sprachqualität von Anrufen über *VoIP*. Maßgeblich beeinflusst wird diese durch die schwankenden Übermittlungszeiten und den Verlust der übertragenen *IP*-Pakete. Um einen gleichmäßigen Sprachfluss zu wahren, wird ebenfalls Wert auf die Zeit gelegt, welche vom Aussenden des akustischen Sprachsignals von Endgerät A bis zum ebenfalls akustischen Wahrnehmens am Endgerät B vergeht. Begegnen lassen sich diese Probleme mit dem Einsatz von Paket-Filtern, der Zwischenpufferung von Paketen und der Priorisierung von Sprachpaketen innerhalb des *IP*-Netzes. [50, 116 ff.]

3.5.4 (Sprach)-Datenübertragung in VoIP

Zur Abwicklung moderner Sprachkommunikation über *VoIP* bedarf es international geltender Festlegungen und Standards zum geregelten Datenaustausch innerhalb eines *IP*-Netzes. Diese Standards werden in Protokollen definiert, die Art und Weise der Sprach- und Signaldatenübertragung vorgeben. Dazu kommen weitere Protokolle zur Einbindung des *ISDN*-Netzes. [50, S. 102]

Zu den bekanntesten Signalisierungsprotokollen zählen *SIP* und *H.323*. Während jedoch *H.323* eine Sammlung von Unterprotokollen zur Signalisierung und dem (Sprach)-Datenaustausch darstellt, definiert *SIP* lediglich die Signalisierung zwischen den Teilnehmern. Beide Protokolle sind dabei unabhängig der verwendeten Transportprotokolle (*User Datagram Protocol (UDP)* und des *Transport Control Protocol (TCP)*), benutzen jedoch beide das wiederum auf diesen aufbauende *RTP* und *RTCP*. [62, S. 245]

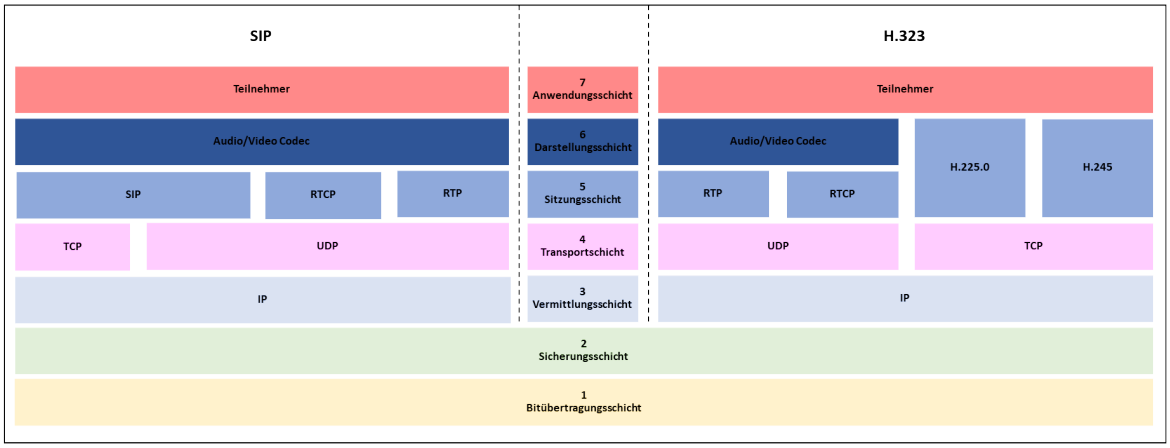

Abbildung 3.8: Vergleich der Schichten des OSI-Referenzmodells des *SIP*- und *H.323*-Protokolls [62, S. 246] [63]

UDP

Das verbindungslose *UDP* ist ein viel genutztes Transportprotokoll in der *TCP*/*IP*-Protokollfamilie, hauptsächlich bei der Übertragung von *Domain Name System (DNS)*-Anfragen und Echtzeitanwendungen, welche mit dem entsprechenden Paketverlust des Protokolls umgehen können. Bedingt wird dieser durch das Fehlen von Schutzmechanismen im Aufbau des Protokolls, wie beispielsweise die Möglichkeit zur Empfangsbestätigung eines *UDP*-Datenpaketes oder der Nummerierung selbiger. Im Vergleich zum *TCP*-Protokoll, umfasst der Header von *UDP* dafür lediglich eine Größe von 8 Byte und ist aufgrund dessen im Vergleich verbindungsschonender als der *TCP*-Header mit einer Größe von 20 Byte. [62, S. 195–196]

RTP

Das *Real-Time Transport Protokoll (RTP)* ist ein von der Internet Engineering Task Force (IETF) entwickeltes, paketbasiertes Daten-Transport-Protokoll zur kontinuierlichen Übertragung von, zumeist Multimedia-Daten, in Echtzeit. Bei VoIP-Telefonie ist *RTP* für die Übertragung der Audio- und Videoströme nach der Signalisierung und dem Aufbau des Gesprächs über *VoIP* verantwortlich. *RTP* baut auf dem verbindungslosen Transportprotokoll *UDP* auf und hat sich als Standard bei der *IP*-Telefonie etabliert. [62, S. 196] [50, S. 164]

Im Vergleich zu *UDP* verfügt *RTP* über Möglichkeiten zur Feststellung von Paketverlusten. Die Qualität und Quantität der übertragenen Daten wird mittels des parallel laufenden *RTCP* sichergestellt. Bei Bedarf kann allerdings auch auf das verbindungsorientierte *TCP*-Protokoll zurückgegriffen werden, welches bereits über eigene Qualitätssicherungsmechanismen verfügt. In diesem Fall entfällt die Verwendung des *RTCP*-Protokolls. [50, 164 ff.]

RTCP

Um die Qualität der übermittelten Sprachdaten mittels RTP zu überwachen, wird parallel zu diesem das *RTCP*-Protokoll angewandt. Dieses dient der Sicherstellung der *Quality of Service (QoS)* in *VoIP*. [50, S. 164]

SRTP

Das *SRTP*-Protokoll ist eine Erweiterung des *RTP* mit zusätzlichen Sicherheitskomponenten zur Erhöhung der Datensicherheit gegen Angriffe. Diese umfassen unter anderem die Verschlüsselung der übertragenen Pakete mittels des Advanced Encryption Standard (AES)-Algorithmus[5] zum Schutz gegenüber Abhören. [50, S. 199]

TCP

Bei *TCP* handelt es sich um ein verbindungsorientiertes Protokoll mit den dazugehörigen Schutzmechanismen. *TCP*-Pakete lassen sich aufgrund ihrer Nummerierung unabhängig voneinander versenden und können am Ziel korrekt zusammengesetzt werden. Ebenfalls in *TCP* implementiert ist eine Fehlerbehandlung und eine Flusssteuerung zur Übermittlung des besten Übertragungsweges der Datenpakete. [62, S. 189–190]

[5] Standardisiertes, symmetrisches Verschlüsselungsfahren zur Verschlüsselung von Dokumenten und Kommunikationsverbindungen mit einer Block- und Schlüssellänge bis zu 256 Bit [64]

3.5.5 Rufnummernvergabe

Trotz der mittlerweile flächendeckend erfolgten Umstellung auf *VoIP* erfolgt nach wie vor die Adressierung der Teilnehmer über eine numerische Rufnummer. Im Hintergrund erfolgt die Vermittlung jedoch nicht mehr über leitungsgebundenen Ortsvermittlungsstellen sondern auf digitalisiertem Weg. [55]

Um die Erreichbarkeit aller Teilnehmer des Telefonnetzes, unabhängig der verwendeten Technologie, sicherzustellen, bedarf es einer geordneten Vergabe der zu verwendenden Rufnummern eines jeden Netzzuganges zur Zuweisung in das digitale *VoIP*-Netz. Verantwortlich für diese Zuordnung beziehungsweise Verteilung an die Telekommunikationsanbieter nach einem festgelegten Rufnummernplan ist die Bundesnetzagentur [65].

Unterteilt sind diese in insgesamt 5200 Ortsnetze, welche jeweils mit eindeutigen Ortsnetzkennzahlen (Vorwahl) adressiert werden. Diese lassen Rückschlüsse auf die geografische Position des Anschlusses ziehen und werden auch unter Verwendung von *VoIP* entsprechend verteilt. [66]

Deutsche *VoIP*-Telekommunikationsanbieter müssen demnach die Lokalität eines Nutzers überprüfen und damit dessen Standort sicherstellen, um eine geeignete Ortsrufnummer zuweisen zu können. Dies trifft auch auf international agierende Anbieter mit Sitz im Ausland zu, welche dafür zunächst Nutzungs- und Vergaberechte deutscher Rufnummernblöcke bei der Bundesnetzagentur erwerben müssen. [66]

3.5.6 Adressierung unter VoIP: ENUM

Die Erweiterung der Telefonie um das digitale Angebot der *VoIP* stellte die Betreiber und Anbieter telefonbasierter Telekommunikationsdienstleistungen vor neue Herausforderungen. Während bei *ISDN* der Verbindungsaufbau über das D-Kanal-Protokoll und die anschließende Sprachübertragung über einen digitalen Sprachkanal erfolgte, werden seit *VoIP* paketbasierte Übertragungsmechanismen angewandt. Sowohl bei der Signalisierung, als auch der darauf folgenden Sprachübermittlung. Dieser Umstand bedeutet auch eine (Teil-) Umstellung der bislang erfolgten Adressierung der Teilnehmer des neuen *IP*-Netzes, bei gleichzeitigem Weiterbetrieb des alten *ISDN*-Netzes. Während bis unter der Verwendung von *ISDN* die Telefonnummer als Identifikationsmerkmal durch den zuständigen Betreiber fest an einen Anschluss gebunden war, und an diesen entsprechend vermitteln konnte, ergeben sich durch die Digitalisierung zwangsweise neue Möglichkeiten, Teilnehmer innerhalb des Netzes zu adressieren. [50, 6 ff.]

Prinzipiell erfolgt die Adressierung in *IP*-basierten Netzwerken über *IP*-Adressen auf Basis der einheitlichen Standards *IPv4* und *IPv6*[6]. Somit besitzt jedes an ein *IP*-Netz angeschlossenes Endgerät eine ihm fest zugeordnete *IP*-Adresse, an welche die für ihn bestimmten Datenpakete adressiert werden. Dies trifft damit auch für die mit ihrer *IP*-Adresse im digitalen Netz registrierten *VoIP*-Telefone zu. Aus diesen Gründen, zur Übersetzung der etablierten Telefonnummern auf die nun verwendeten *IP*-Adressen, aber auch zur Inkompatibilität zwischen altem und neuem Netz, wurde ein entsprechender Dienst benötigt, der diese Aufgaben übernimmt. [50, S. 7]

[6] Vierter bzw. sechste Version des Internet-Protokolls zur Adressierung von Geräten in lokalen und globalen Netzwerken

Telephone Number URI Mapping (ENUM) ist ein von der *IETF* standardisierter Dienst zur Übersetzung herkömmlicher Telefonnummern auf dienstspezifische Adressen, wie unter anderem auch die *SIP-Uniform Resource Identifier (URI)*. [50, S. 109]

ENUM versteht sich dabei als Erweiterung von *DNS* im `arpa`-Adressbereich[7]. Dieser *ENUM-DNS* teilt sich dabei in verschiedene, aufeinander aufbauende und auf unterschiedlichen Ebenen agierende Level-Domains. Während die *ENUM*-Top-Level-Domain (Tier 0) `e164.arpa` der RIPE NCC[8] auf europäischer Ebene agiert, verwalten nationale Organisationen, wie beispielsweise die *DENIC eG* in Deutschland, als *ENUM*-Second-Level-Domains (Tier 1) die Nummern auf nationaler Ebene. [50, S. 109]

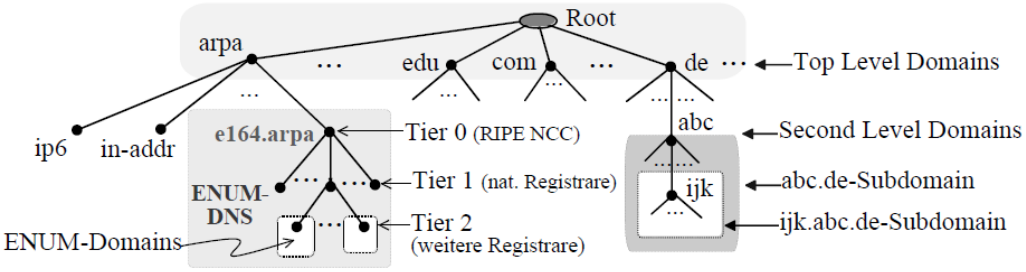

Abbildung 3.9: Schematische Darstellung der Rufnummerermittlung unter Verwendung von ENUM [50, S. 109]

Zur Übersetzung einer Telefonnummer auf eine Internetadresse erfolgt dabei eine Zuweisung dieser auf den Namen einer *ENUM*-Domain. Diese wiederum beinhaltet mehrere *Resource Records (RRs)* vom Typ *NAPTR (Naming Authority Pointer)*, welche dann die jeweiligen dienstspezifische Adressen, wie beispielsweise unter anderem auch die *SIP-URI* enthalten. Jeder *ENUM*-Eintrag beziehungsweise der *ENUM*-Domainname bildet sich dabei aus der umgekehrten Telefonnummer, mit Punkten als Trennzeichen sowie der Endung `e164.arpa`. Aus der Telefonnummer `+49987654321` wird somit: `1.2.3.4.5.6.7.8.9.4.e164.arpa`.

[7] Address and Routing Parameter Area (arpa): Übergeordnete Domain des *DNS* zur Umsetzung technischer Belange des Internets [67]

[8] Réseaux IP Européens Network Coordination Centre (RIPE NCC): Non-Profit-Organisation zuständig für die Verwaltung und Vergabe von *IP*-Adressen im europäischen Raum [68]

3.6 H.323

Neben dem weltweit am verbreitetsten Standard *SIP* ist *H.323* ein von der Internationalen Fernmeldeunion *ITU-T* ebenfalls empfohlener Standard zur Übertragung von Audio- und Videosignalen, unter anderem zur Abwicklung von Telefongesprächen. Während *SIP* Hauptanwendung in der *VoIP*-Telefonie findet, wird das 1996, eigentlich ausschließlich für Videotelefonie entwickelte *H.323*, eher beim älteren *ISDN*-Standard verwendet, in der Übergangsphase dennoch auch noch bei *VoIP*. [69]

3.6.1 Aufbau H.323

H.323 bezeichnet eine Sammlung (Framework) mehrerer Protokolle, darunter *H.225.0* zum Aufbau, *Q.931* zur Signalisierung und *H.245* zur Abwicklung der Telefongespräche. Ähnlich wie *SIP* ist *H.323* lediglich für den Verbindungsaufbau zwischen den Teilnehmern eines Gespräches verantwortlich, die eigentliche Datenübertragung erfolgt über *RTP* oder *RTCP*. Zur Übertragung der Sprachdaten wird dabei ausschließlich, im Gegensatz zu *SIP*, auf das *TCP*-Transportprotokoll gesetzt. Die beiden Protokolle *H.225.0* und *H.245* werden als Signalisierungsprotokolle unter der Bezeichnung *H.323*-SIG zusammengefasst. [50, 224 ff.]

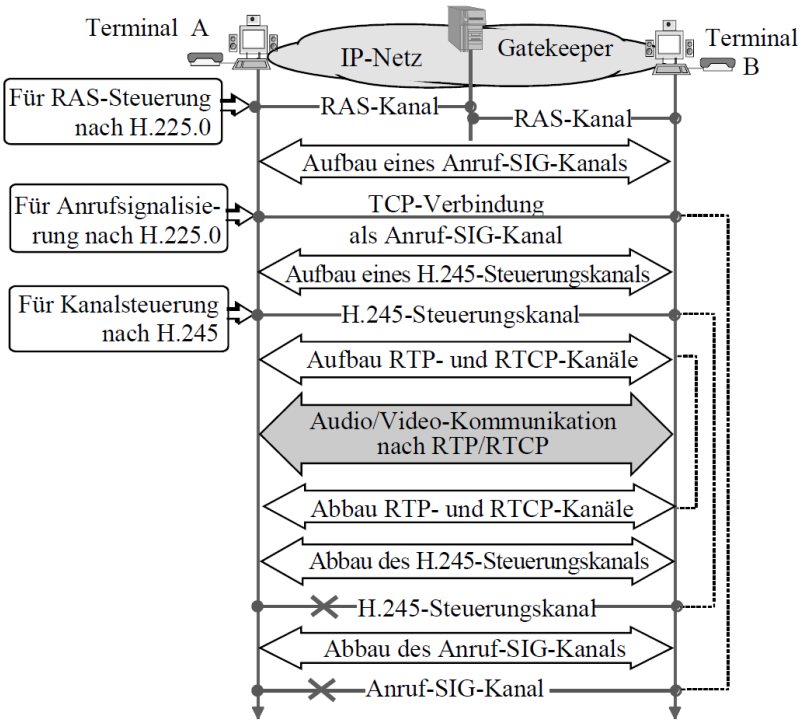

Abbildung 3.10: Schematische Darstellung des Rufauf- und Abbau unter Verwendung von *H.323* als Signalisierungsprotokoll [50, S. 229]

Gatekeeper

Zur Überwachung der *Quality of Service* unter Verwendung von *H.323* werden *Gatekeeper* eingesetzt, welche ein ihnen jeweils zugeordnetes Subnetz (*Zone*) von Terminals (Endgeräte) überwachen. Diese können per Telefonnummer, Mailadresse oder speziellen *H.323*-URLs adressiert werden. Die Konvertierung dieser in *IP*-Adressen und die Verwaltung der Leitungsauslastung ist ebenfalls Aufgabe des *Gatekeeper*. Untereinander vernetzt sind die *Gatekeeper* über *RAS-Kanäle* (Registration) im *IP*-Netz. Zur Übermittlung von Gesprächen in externe oder öffentliche Netze abseits von *H.323* bedarf es weiterhin eines Gateways, welches in der Lage ist, verschiedene Netzwerkprotokolle miteinander zu verbinden. [50, S. 224]

3.6.2 Signalisierung in H.323

Während *SIP* als reines Signalisierungsprotokoll alle benötigten Techniken in sich vereint, bezeichnet *H.323* eine Protokollsammlung mehrerer Standards, welche einzeln zur Abwicklung von *VoIP* eingesetzt werden. [50, S. 224]

H.225.0

H.225.0 bildet gemeinsam mit H.245 als Protokoll zur Anruf-Signalisierung (Anruf-SIG-Protokoll) das Signalisierungsprotokoll *H.323*-Signalisierung (*H.323*-SIG). Vergleichen lässt sich dabei *H225.0* mit dem im *ISDN* verwendeten *D-Kanal-Protokoll* unter Verwendung von *TCP*. [50, S. 242–243]

H.245

Bei einem *VoIP*-Anruf unter Verwendung von *H.323* erfolgt dessen Signalisierung zunächst über das *H.225.0*-Protokoll. Über das anschließend verwendete *H.245*-Protokoll werden dann die logischen Übermittlungskanäle unter Verwendung von *RTP* und *RTCP* aufgebaut.

3.7 SIP

Das *Session Initiation Protocol (SIP)* ist ein 1996 von der *IETF* entwickeltes und definiertes Protokoll *„für den Auf- und Abbau sowie die Steuerung von Kommunikationsverbindungen zwischen zwei oder mehr Teilnehmern“* [70]. Am häufigsten wird es bei der Abwicklung von *VoIP* zur Durchführung von Sprach- und Videotelefonie für den Auf- und Abbau der Telefonverbindung zwischen den Geräten genutzt. Es ist, neben *H.323*, das für *VoIP* am häufigsten genutzte Protokoll. Eingesetzt wird *SIP* zumeist auf *IP*-basierten Telefonanlagen, welche mittlerweile die klassischen, leitungsorientierten *Private Branch Exchange (PBX)*[9] vermehrt verdrängen. [50, 273 ff.]

Als Signalisierungsprotokoll übernimmt es *"die Einleitung, Aufrechterhaltung, Änderung und Beendigung von Echtzeit-Kommunikationssitzungen zwischen IP-Geräten"* auf Paketdatenbasis. [72] Daneben erlaubt das *SIP* weiterhin das Einbetten erweiterter Funktionen, wie die Übertragung von Anruferdaten. *SIP* wird sowohl von *IPv4* als auch *IPv6* unterstützt. Es regelt dabei jedoch lediglich den Ablauf der Gesprächsverbindung, nicht aber die eigentliche Sprachübertragung. Hierfür wird ebenfalls das *RTP* oder auch verschlüsselt als *SRTP* Protokoll verwendet. [72]

Trotz der zeitlichen längeren Entwicklung von *H.323* konnte sich *SIP* aufgrund der Flexibilität, der einfacheren Implementierbarkeit, des generell simpleren und schnelleren Aufbaus einer Session und aufgrund der unkomplizierten Auflösung von *SIP*- in *IP*-Adressen gegenüber *H.323* durchsetzen. [72]

Aufgrund der genannten Gründe fokussiert sich diese Arbeit hauptsächlich auf das *SIP*-Protokoll.

3.7.1 Komponenten des SIP

Zur Abwicklung von Telefongesprächen über das *SIP*-Protokoll bedarf es sowohl entsprechend geeigneter Endgeräte als auch proprietärer Hard- und Software zum Absenden und Empfangen von Gesprächsdaten in beziehungsweise aus dem öffentlichen *IP*-Netz. [57, S. 133]

User Agent

Alle Endgeräte innerhalb eines Netzes, welche an einer *SIP*-Kommunikation teilnehmen, unabhängig davon, ob es sich dabei um physische Geräte oder softwarebasierte Anwendungen (*Soft-Phones*)[10] handelt, werden als *User Agent (UA)* bezeichnet. Diese können sowohl als Server (*UAS - User Agent Server*), wenn darüber ein Anruf empfangen wird, als auch als Client (*UAC - User Agent Client*), wenn darüber ein Anruf initiiert wird, bezeichnet werden. Adressiert werden die *User Agents* über die *SIP-URI*. [57, S. 133]

[9] Technische Bezeichnung Telefonanlage zur Einbindung mehrerer Endgeräte in das öffentliche Telefonnetz. Auch Nebenstellenanlage (NstAnl) oder Teilnehmervermittlungsanlage (TVA) [71]

[10] Telefoniesoftware, welche alle Funktionen eines Telefongerätes auf einem beliebigen Computer abbildet [73]

SIP Uniform Ressource Identifier (SIP-URI)

Der *SIP Uniform Ressource Identifier (SIP-URI)* fungiert bei der Abwicklung eines Verbindungsaufbaus über das *SIP*-Protokoll als Identifizierung der Nutzer und ist vergleichbar mit einer konventionellen Telefonnummer. Umgangssprachlich wird die *SIP-URI* auch als einfache *SIP*-Adresse bezeichnet. [57, S. 134]

Der Aufbau der *SIP-URI* zur Abwicklung von VoIP folgt dem Syntax

```
sip:[User][:Passwort]@[Host][:Port-Nummer][:Parameter][:Header]
```

und entspricht damit dem Konzept der Adressierung in *IP*-Netzen. [50, 278 f.]

Unterschieden werden die Adressen in temporäre und ständige *SIP-URI*.

Die temporäre *SIP-URI* wird bei der Aktivierung eines User Agents innerhalb einer Netzwerkes automatisch, jedoch umgebungsabhängig erzeugt. Sie folgt ebenfalls dem Syntax

```
sip:[User]@[Host]
```

wobei der *User* frei wählbar ist, der *Host* allerdings immer der *IP*-Adresse des *User Agents* entspricht. [57, 134 f.]

Ständige *SIP-URI* dienen der verbesserten Adressierung von Teilnehmern und werden vom jeweilig genutzten Telekommunikationsanbieter vergeben. Die Registrierung dieser ständigen *SIP-URI* erfolgt über den *SIP-Registrar*. Auch die ständige *SIP-URI* folgt dem Syntax

```
sip:[User]@[Host]
```

wobei jedoch der *User* ein beim Telekommunikationsanbieter registrierter Nutzername und der *Host* die Domain des Anbieters darstellt. [57, 135 f.]

Ständige *SIP-URI* sind nutzerbezogen, einmalig und verfügen über keine Angabe eines Domain-Namens. Dies hat den Vorteil der einfachen Migration von Nutzern innerhalb der Domain-Grenzen. [50, 278 f.]

Im Heimnetzbereich entspricht der *User* dabei zumeist der vom Anbieter für diesen Anschluss vergebenen Rufnummer. Dies hat den Vorteil der Einbindung von *VoIP* in die Strukturen der Telekommunikationsanbieter und der Nutzung eines vorkonfigurierten Internet-Routers, bereitgestellt durch selbigen, welcher ohne weiteres Zutun des Nutzers mittels Plug-and-Play einfach installiert und genutzt werden kann. [74]

SIP-Server

Aufgrund des Aufbaus von *SIP* wird in diesem der Begriff *SIP-Server* für verschiedene Funktionsbausteine innerhalb des Protokolls verwendet, vereint aber hauptsächlich in sich die Komponenten des *SIP-Proxy*, des *Location-Servers*, des *SIP-Registrar* und des *Redirect-Servers*. Sie dienen hauptsächlich der Adressierung der Teilnehmer über die ständige *SIP-URI* und stehen dafür sowohl mit den User Agents als auch untereinander in Kontakt. [57, S. 192]

Die beschriebenen Komponenten werden allerdings nicht als eigenständige Hardware-Komponenten, sondern als Softwarelösung auf einem klassischen Server realisiert. Dieser wird dann als *VoIP*-Telefonanlage betrachtet. Ein klassischer zentraler, hardwarebasierte *SIP*-Server als Mittelpunkt einer Kommunikationsverbindung zwischen mehreren Endgeräten, wie beispielsweise auch eine herkömmliche Telekommunikations-Anlage, existiert im *SIP* nicht. Vielmehr werden in der Regel alle Module als softwarebasierte Lösung auf gesonderten Rechnern untergebracht, mit welchen die lokalen Clients kommunizieren. Parallel dazu wird bei jedem *VoIP*-Gespräch über *SIP* nach Request-/Response-Prinzip ein Gerät (Initiator der Verbindung) als *SIP*-Server und das Gegenüber als *SIP*-Client (Empfänger) bezeichnet. [50, 273 ff.]

SIP-Registrar

Zur Adressierung der Teilnehmer über die ständige *SIP-URI* erfolgt über den *SIP-Registrar* eine Registrierung der temporären *SIP-URI* mit der vom Telekommunikationsanbieter fest zugeordneten *SIP-URI* innerhalb einer Domain. [57, 193 f.]

Location-Server

Der *Location-Server* beschreibt innerhalb des *SIP*-Netzwerkes eine Datenbank dar, in welcher die vom *SIP-Registrar* zugeordneten temporären und ständigen *SIP-URI* abgelegt werden. Diese Informationen stehen wiederum dem *SIP-Proxy* innerhalb einer Domain bei der Vermittlung von *SIP*-Gesprächen zur Verfügung. [57, 194 f.]

Redirect-Server

Der *Redirect-Server* übernimmt innerhalb der *SIP*-Architektur Informationsanfragen bezüglich der *User Agents*, wie beispielsweise Rufumleitungen. [57, S. 201]

SIP-Proxy

Im Mittelpunkt *SIP*-basierter Telefonsysteme stehen der *SIP-Proxy*. Er übernimmt das Routing der *SIP*-Botschaften auf Basis der vom *SIP-Registrar* und *Location-Server* zur Verfügung gestellten Informationen. Dafür kommuniziert dieser direkt mit den angebundenen *User Agents*. [57, 195 f.]

Damit dient er gleichzeitig zur Erreichbarkeit jener Endgeräte aus Netzwerken über die eigene Domain heraus. Dafür besitzt der *SIP*-Proxy ebenfalls eine *IP*-Adresse zur Erreichbarkeit über das globale Internet. Bei solch einem Kommunikationsaufbau über das Netz des eigenen Anbieters hinaus, kommunizieren die *SIP-Proxy*-Server beider Netzanbieter zur Übermittlung der *IP*-Adressen miteinander. [53, S. 296]

Alle benötigten *SIP*-Adressen werden über *DNS*-Server aufgelöst. Zusätzliche Informationen dazu können über den *Naming Authority Pointer-Resource Record (NAPTR)* und den *Service-Resource Record (SRV)* bezogen werden. [50, 280 ff.]

3.7.2 Kommunikationsablauf SIP-Komponenten

Mit Einschalten des Endgerätes registriert sich dieses zunächst mit einer temporärer *SIP-URI* beim *SIP-Registrar* als authentifizierende Stelle aller Teilnehmer innerhalb einer Domain. Der *SIP-Registrar* verknüpft die temporär vom *User Agent* verwendete *SIP-URI* mit der vom Telekommunikationsanbieter fest zugeordneten *SIP-URI*. Dies erfolgt über eine `Register`-Botschaft an den *SIP-Registrar*. [57, 193 f.] Die Ermittlung der Adresse des *SIP-Registrar* erfolgt dabei über eine *DNS*-Abfrage. [53, S. 296]

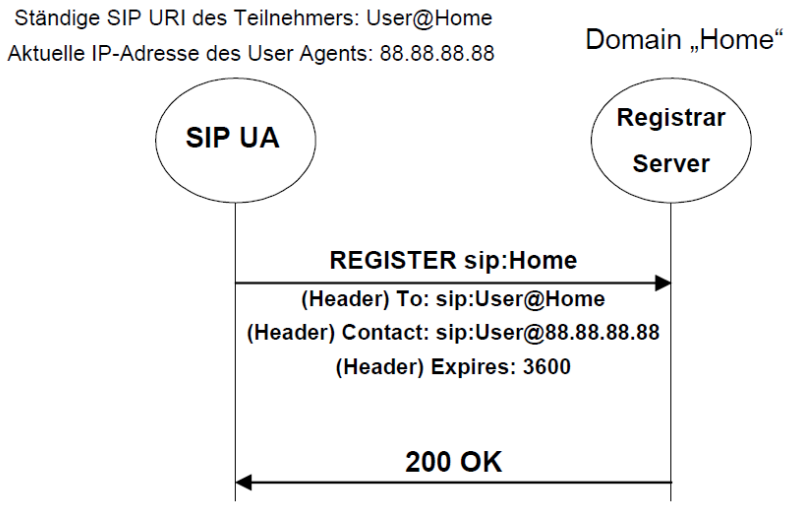

Abbildung 3.11: Registrierung der ständigen *SIP-URI* des User Agents beim *SIP-Registrar* [57, S. 194]

Nach erfolgreichem Schlüsselaustausch und Registrierung des Gerätes speichert der *SIP-Registrar* dieses unter der verwendeten *IP*-Adresse und des dazugehörigen *UDP*-Port zur Vermittlung ankommender Verbindungen in der Teilnehmerdatenbank, dem *Location-Server*, ab. Der *SIP-Proxy* kann auf Grundlage dessen die Vermittlung zwischen ankommenden *SIP*-Botschaften und den jeweiligen Endgeräten (*User Agents*) übernehmen. [53, S. 296]

Kommunikationsablauf der SIP-Komponenten nach Trapezoid-Modell

Aufgrund des Aufbaus der Kommunikation der *SIP*-Komponenten

- User Agent (UAC)
- Proxy Server (UAS)
- Location-Server (LS)
- *DNS*-Server (DNS)

untereinander werden diese auch als *Trapezoid-Modell* dargestellt:

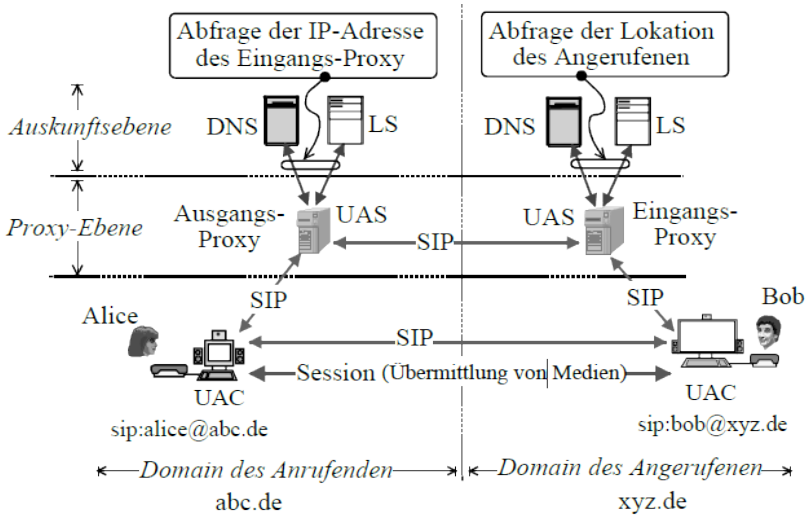

Abbildung 3.12: Kommunikation der *SIP*-Komponenten untereinander abgebildet als Trapezoid-Modell [50, S. 282]

3.7.3 Botschaften im *SIP*: Request- und Response-Typen

Bei der Anrufinitiierung über *SIP* übermitteln die teilnehmenden Clients mehrere textbasierte Botschaften unterschiedlichen Informationsgehaltes. Diese unterscheiden sich in Anfragen seitens des initiierenden Clients, sogenannten Request-Botschaften und den darauf von der Gegenstelle antwortenden Response-Botschaften, welche sich wiederum am *Hypertext Transfer Protocol (HTTP)-Standard*[11] orientieren. Während Request-Botschaften einen hohen Informationsgehalt aufweisen, beinhalten die *Response*-Botschaften zumeist nur eine auf einen Status-Code beschränkte Reaktion auf diese. [50, S. 303] Jede *SIP*-Botschaft besteht aus einer Startzeile, einem *Message Header* und einem *Message Body*, wobei dieser optional und botschaftsabhängig ist. [50, S. 307]

INVITE-Request

Der *INVITE-Request* ist als zuerst ausgeführte Nachricht bei der Anrufinitiierung im *SIP*-Protokoll der für den Verbindungsaufbau entscheidende Teil. Mit ihm werden alle für die nachfolgenden Schritte und den im weiteren Verlauf stattfindenden Verbindungsaufbau relevanten Informationen übermittelt, darunter die *SIP*-Adressen der Teilnehmer und die zu verwendenden Codecs zur Sicherstellung der Kompatibilität der Clients. [50, S. 303]

ACK-Request

Der *ACK-Request* ist eine Standard-Botschaft bei der informationstechnischen Datenübertragung und dient der Bestätigung (Acknowledgement) einer zuvor erhaltenen Botschaft. Im *SIP* dient der *ACK-Request* der Bestätigung des erfolgreichen Nachrichteneinganges und signalisiert gleichzeitig das Ende des Sessionaufbaus. [50, S. 303]

BYE-Request

Mit der Übersendung des *BYE-Request* signalisiert ein Teilnehmer die Initiierung des Abbaus der bestehenden *SIP*-Session. [50, S. 303]

Provisional-Responses

Provisional-Response-Botschaften antworten unter anderem auf *INVITE-Request* und signalisieren dem Sender die Weiterverarbeitung dieser. Botschaften dieser Art handeln alle im Zahlenraum 1xx. *Provisional-Response*-Botschaften zählen *100 Trying* und *180 Ringing*. [50, S. 306]

Success-Responses

Bei *Success-Response*-Botschaften handelt es sich um Nachrichten im Zahlenraum 2xx. Sie signalisieren dem Absender die erfolgreiche Übertragung eines Request. Zu ihnen gehören unter anderem *200 OK*. [50, S. 306]

[11] Kommunikationsprotokoll nach Client-Server-Prinzip, auf welchem das Internet basiert, hauptsächlich um Webseiten von den dazugehörigen Servern anzufordern und anzuzeigen [62, S. 225]

3.7.4 Aufbau SIP-Botschaften am Beispiel INVITE-Request

Jede Botschaft im *SIP* folgt demselben text- und zeilenbasierten Aufbau.

Die *Request-Line* beinhaltet dabei Angaben über den Typ der Botschaft (INVITE, BYE, ACK etc.) und signalisiert den Beginn einer Botschaft. Auf diese folgt die *Request-URI* mit der *SIP*-Adresse des Ziels der Botschaft und der *SIP*-Version. Beispiel für eine *Request-Line* eines *INVITE-Request* ist `INVITE sip:bob@xyz.de SIP/2.0`. Auf die *Request-Line* folgt der *Message Header*, welcher sich auch mehreren *Header Fields* zusammensetzt, beispielsweise Via, Route, Call-ID, From, To, etc. Diese enthalten wiederum einzelne *field-value*, die Inhaltsinformationen. Der *Message Header* eines *INVITE-Request* folgt dem Aufbau: [50, 307 f. f.]

```
Via: SIP/2.0/UDP pc3.abc.de;branch=z8hD4bK556asdhds
Max-Forwards: 20
To: Bob <sip:bob@xyz.de>
From: Alice <sip:alice@abc.de>
Call-ID: a74b4c76e55710@pc3.abc.de
CSeq: 284164 INVITE
Contact: <sip:alice@pc3.abc.de>
```

An den *Message Header* ist der *Message Body* angehangen, welcher die eigentlichen Nutzdaten der Nachricht darstellt. In diesem werden nach dem *SDP*-Protokoll unter anderem die Session betreffenden Informationen zur Aushandlung der Kompatibilität übermittelt. Diese beinhalten den Initiator der Session, die Identifikation, die verwendeten Ports sowie die Media-Typen. [50, 308 f.]

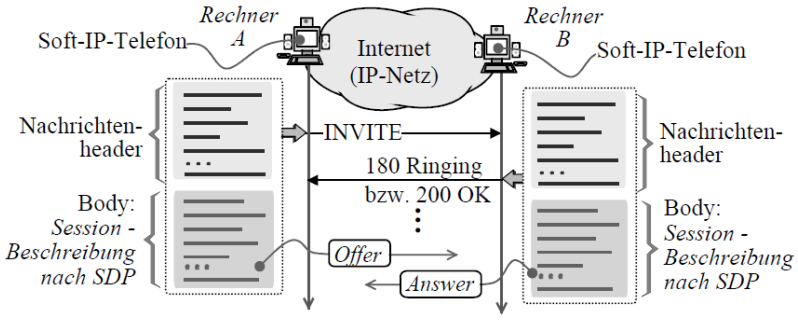

Abbildung 3.13: Schematisch Darstellung des Rufaufbau unter Verwendung von *SIP* [50, S. 314]

3.7.5 Header Fields

Header Fields sind Bestandteil des *Message Header* eines jeden *SIP*-Request und beinhalten relevante Informationen zum Verbindungsaufbau, die *field-values*. Pflicht-*Header Fields* sind dabei `Via`, `Max-Forwards`, `From`, `To`, `Call-ID` und `CSeq`.

- `Via` gibt Auskunft über die Versionsnummer des *SIP*, das verwendete Transportprotokoll und den Absender inklusive der Transaktions-ID. Sobald ein *SIP-INVITE-Request* über mehrere *Proxy-Server* übermittelt wird, enthält dieser weitere `Via`-Felder, in der Anzahl der *Proxy-Server*. Über diese ist es möglich, den Sendeverlauf der Nachricht zurückzuverfolgen. Alle `Via`-Felder werden ebenfalls in der darauf antwortenden *SIP-Response*-Nachricht übernommen. Dieser Vorgang wird als *SIP-Response-Routing* bezeichnet. Das `Via`-Feld folgt dem Aufbau
  `Via: SIP/2.0/UDP pc3.abc.de` [50, S. 309]

- `Max-Forwards` gibt die Anzahl der maximal zu verwendenden Proxy-Server bei der Übermittlung eines *SIP-INVITE-Request* an:
  `Max-Forwards: 20` [50, 311 f.]

- `To` gibt die Zieladresse der Anfrage, in der Regel des Angerufenen, an. Es folgt der Struktur
  `To: [display-name] <SIP URI>` [50, S. 312]

- `Call-ID` stellt eine zufällig gewählte Zeichenkette dar, welche zur Identifikation des Anrufes genutzt wird. Sie kann einzeln, aber auch in Verbindung mit dem vollständigen Hostnamen des anrufinitiierenden Endgerätes eingesetzt werden:
  `Call-ID: a1b2c3d4e5@abteilung.unternehmen.de` [50, S. 310]

- `CSeq` (Command Sequence) ist die Sequenznummer eines *Request* und dient der Nummerierung dieser des jeweiligen Typs/Endgerätes. Die von der Gegenstelle darauf antwortenden *Response*-Nachrichten enthalten jeweils die Sequenznummer des *Request*, auf welche sie sich beziehen. Aufgrund dessen, dass jeder *INVITE-Request* einen neuen Verbindungsaufbau signalisiert, kann die Sequenznummer auch als fortlaufende Transaktionsnummer betrachtet werden:
  `CSeq: 1234 INVITE` [50, 310 f.]

- `From` beinhaltet Informationen über den Absender eines *SIP-INVITE-Request* und damit über den Initiator einer *VoIP*-Verbindung, entsprechend der Registrierung beim benutzten Telekommunikationsbieter. Es folgt dem vorgegeben Aufbau
  `From: [display-name] <SIP URI>[; tag=random string]`
  wobei `display-name` und `tag=random string` optional sind. Mit der Angabe `Anonymous` kann außerdem die Übergabe der Identität des Anrufers an den Angerufenen unterbunden werden. [50, S. 311]

- `Contact` enthält die Zieladresse, an welche die Antwort auf die übermittelte *SIP*-Botschaft gesendet werden soll. [50, S. 310]
- `P-Preferred-Identity` ist ein optionales Feld, über welches der User-Agent den Wunsch nach einer von der Registrierung abweichenden, zunächst frei wählbaren Identität in Form eines Klartextnamens und einer Rufnummer beziehungsweise einer *SIP-URI* an den *SIP*-Proxy übermitteln kann. Diese wird vom *SIP*-Proxy im Feld `P-Asserted-Identity` übernommen. [75]

- `P-Asserted-Identity` beeinhaltet nach Verifizierung der Nutzeridentität und der rechtmäßigen Nutzung der zu übermittelnden Identität die Angaben des `P-Preferred-Identity`-Feldes. `P-Asserted-Identity` wird laut IETF-Richtlinie lediglich von sich untereinander vertrauenden *SIP*-Komponenten unterstützt und entsprechend weitergegeben. [75] Des Weiteren wird das Feld genutzt, um bei der Übergabe eine *SIP*-Gespräches in das *ISDN*-Netz, die Rufnummer des Nutzers an das *Gateway* zu übergeben. [50, S. 311]

  ```
  From: Bob <sip:nutzer@abc.de>;tag=hsmw12
  P-Asserted-Identity:<+49987654321>
  ```

3.7.6 Gesprächsaufbau und -abwicklung über SIP

Im Folgenden ist der Ablauf eines Standard-Rufaufbaus über das *SIP*-Protokoll schematisch dargestellt.

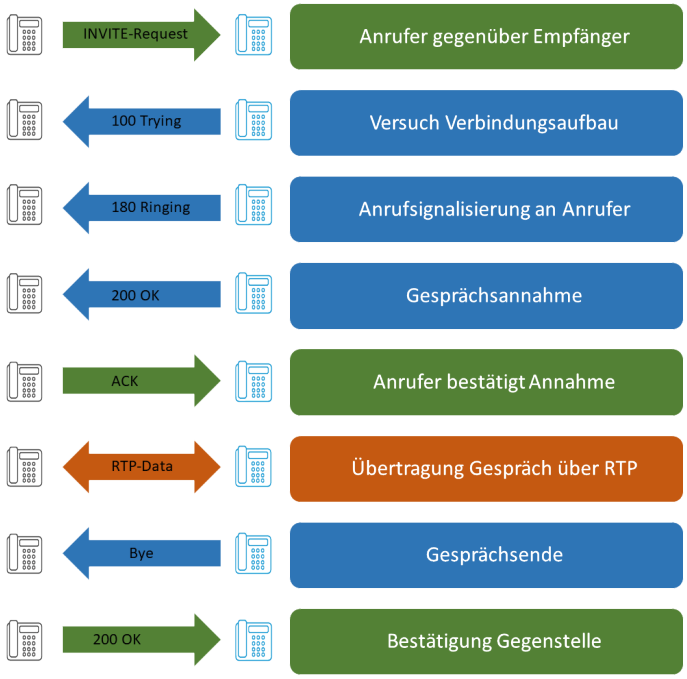

Abbildung 3.14: Grafische Darstellung der übertragenen Botschaften beim Rufaufbau unter Verwendung von *SIP* [76]

Anhand der Darstellung in Verbindung mit den *SIP*-Komponenten lässt sich der Ablauf in folgender Grafik erkennen

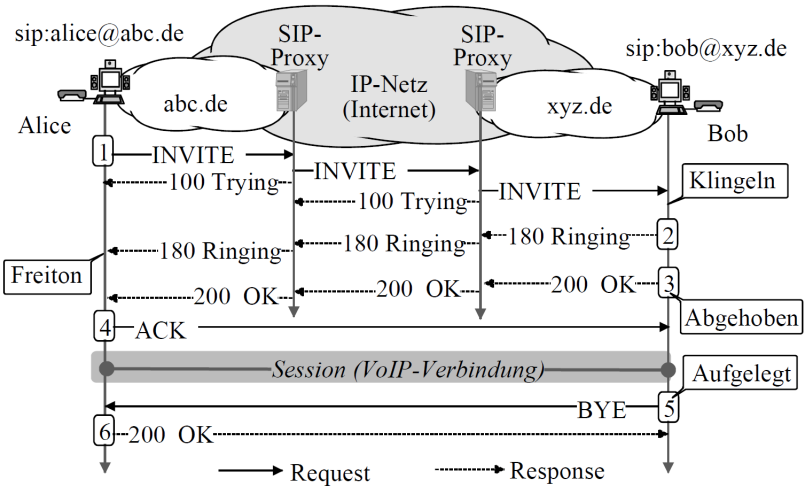

Abbildung 3.15: Schematische Darstellung der übertragenen Botschaften beim Rufauf- und Abbau unter Verwendung von *SIP* [50, S. 288]

Die Teilnehmer in diesem Beispiel sind *Alice* (Anrufer) mit der *SIP-URI* `sip:alice@abc.de` und *Bob* (Empfänger) mit der *SIP-URI* `sip:bob@xyz.de`. [50, 288 ff.]

Zu Beginn einer Session erfolgt zunächst das Übersenden des *SIP-INVITE-Request* von Anrufer (*Alice*) mit der *SIP*-Adresse von *Bob* an den *SIP-Proxy* der Domain `abc.de`. Dieser ersucht aufgrund dessen die *IP*-Adresse des *SIP-Proxy-Server* der Domain `xyz.de` beim zugeordneten *DNS-Server*. [50, 288 ff.]

Nach Auskunft wird der *SIP-INVITE-Request* vom *SIP-Proxy-Server* der Domain `abc.de` an den *SIP-Proxy-Server* der Domain `xyz.de` übermittelt. Dieser wiederum quittiert dieses mit dem *Response* `100 Trying` an das Endgerät von *Alice* und ermittelt parallel über den *Location-Server* den Standort und über den *DNS-Server* die *IP*-Adresse von *Bob*. Nach erfolgreicher Ermittlung wird diesem der *SIP-INVITE-Request* zugestellt. [50, 288 ff.]

Insofern dass beide Endgeräte, von *Alice* und *Bob*, kompatibel sind, beginnt letzteres zu klingeln und quittiert dieses *Alice* mit dem *SIP-Response* `180 Ringing`. *Alice* erfährt dadurch von *Bobs* Verfügbarkeit und der Kompatibilität mit dessen Peripherie. Durch *Bobs* Gesprächsannahme sendet er gleichzeitig den *SIP-Response* `200 OK` an *Alice*, welche dies wiederum mit dem *SIP-Request* `ACK` bestätigt. Der Aufbau der *VoIP*-Verbindung ist damit abgeschlossen, der weitere Datenaustausch erfolgt über das *RTP*-Protokoll. [50, 288 ff.]

Zum Beenden des Gespräches übersendet einer der beiden Teilnehmer ein `BYE`-*Request*, in diesem Fall *Bob* an *Alice*. Dies signalisiert den Verbindungsabbau, welcher von beiden Seiten mit einem `200 OK`-*Response* bestätigt wird. [50, 288 ff.]

3.7.7 Anonymisierung in SIP

Die Themen Privatsphäre und Datenschutz spielen in der heutigen digitalisierten Welt eine immer größere Rolle und wurden auch bei der Konzeption von *SIP* betrachtet. In diesem erfolgt die Offenlegung beziehungsweise Darstellung der Identität hauptsächlich über die *SIP-URI*, welche gleichzeitig zur Adressierung der Nachrichten benötigt wird, und gegebenenfalls einen Anzeigenamen. Dazu kommen weitere Informationen wie zum Beispiel die genutzten Zwischenpunkte der Botschaft (*Via*). Auf dem Übertragungsweg der *SIP*-Nachrichten zwischen Sender und Empfänger kann es an jeder Schnittstelle beziehungsweise Weiterleitung über einen Punkt der digitalen Infrastruktur (beispielsweise *SIP*-Proxy, *SIP*-Registrar, Systemkomponenten der Telekommunikationsanbieter) zu einer Veränderung der insbesondere hier zu betrachtenden *SIP-INVITE*, kommen. Unberührt davon sind zwar strukturell wichtige Felder wie *To* und *From*, doch auch diese können durch bestimmte Leistungsmerkmale für den Empfänger unkenntlich gemacht werden. [77]

A Privacy Mechanism for the Session Initiation Protocol (SIP)

Dieses Leistungsmerkmal von *SIP* wird in der RFC 3323 der IETF beschrieben. Ziel dieser ist es, den Nutzern unter Verwendung von *SIP* Anonymisierungsmöglichkeiten zu bieten und gleichzeitig die korrekte Adressierung der Botschaften sicherzustellen. Neben dem offensichtlichen, für kriminelle Zwecke zu missbrauchendem Hintergrund dieser Technologie existieren auch weitere, verständlichere Motive zur Verdeckung der eigenen Identität bei der Durchführung eines Telefonanrufes. Diese wurden bereits im Kapitel Caller-ID Spoofing im positiven Kontext betrachtet. [77, 1 ff.]

Die Anonymisierung nach RFC 3323 basiert dabei auf drei unterschiedlichen Stufen der Privatsphäre nutzerseitiger und serverseitiger Methoden zur Identitätsverschleierung. Gleichwohl ist jeder Empfänger anonym gesendeter Botschaften gleichzeitig dazu berechtigt, diese abzulehnen. Dies ist ebenfalls Teil der nutzerseitigen Konfiguration des Caller-Agent. [77, S. 5]

Serverseitig kann diese entweder durch den *SIP*-Anbieter durch entsprechende Implementierung in den *SIP-Server* oder extern zur Verfügung gestellt werden. Der Benutzer selbst kann durch Einstellungen in seinem User Agent ebenfalls Teile seiner Identität anonymisieren. [57, S. 397] [77, 6 f.]

Nutzerseitig kann eine Anonymisierung beispielsweise bereits über die Verwendung einer nicht-Nutzerbezogenen *SIP-URI* erfolgen. Während eine falsche oder anonymisierte Angabe der *SIP-URI* im Header-Feld `Contact` nicht möglich ist, kann im `From`-Feld eine Anonymisierung erfolgen. Dies setzt allerdings die zwingende Angabe eines `tag`-Parameters, die Nutzung des `Via`-Headers und weitere Angaben im SDP-Protokoll voraus, über welche die *Response*-Botschaft dem *Request* zugeordnet werden kann. [77, 9 f.]

```
From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=123456789
```

entspricht demnach einer zulässigen Angabe innerhalb einer *SIP*-Kommunikation. Dazu kommen weitere Möglichkeiten der Identitätsverschleierung über eine Verschlüsselung der Botschaften, das Verwenden vordefinierter Routing-Verläufe, sowie der generelle Einsatz von *Session Initiation Protocol Secure (SIPS)*[12]. [77, 9 f.]

3.8 Aufbau Mobilfunknetz

Parallel zu dem heimnetzgebundenen Telekommunikationszugang über *VoIP* erfolgte auch die Umstellung des mobilen Übertragungsweges von (Sprach-) Daten bis hin zur heutigen, volldigitalen Übertragung über mehrere Schritte.

3.8.1 Vorbetrachtung

Ebenso wie das klassische Festnetz wurde das *GSM*-Mobilfunknetz ursprünglich als leitungsvermittelndes Netz konzipiert und entsprechend aufgebaut. Mit der Weiterentwicklung des Internets und der steigenden Anzahl *IP*-basierter Dienste, Dienstleistungen und der entsprechenden mobilen Endgeräte erkannten auch Anbieter den Bedarf zur Anbindung dieser in das mobile Telekommunikationsnetz und begannen mit dem Aufbau jenes, eigens für internetbasierten Dienste. Dies führte gleichzeitig jedoch zu einem Doppelbetrieb zweier getrennter Netze und Übertragungswegen, für die leitungsorientierte Sprachübertragung und die paketgebundene Datenübertragung, was gleichwohl eine Kostenverdopplung bedeutete. Kompensiert wurde dies erst mit dem Einsatz von *Media Gateways*, durch welche die Übertragung der Sprachdaten zwischen den Vermittlungsstellen fortan ebenfalls *IP*-basiert erfolgte. Dieser Standard wurde auch mit Einführung von *UMTS* beibehalten. [53, 1 f.]

[12] Verwendung des *SIP*-Protokoll unter Anwendung des Transport Layer Security Protokolls (TLS) [77, S. 13]

3.8.2 VoLTE

Auf dem Weg zum volldigitalen, *IP*-basierten Netz erfolgte mit steigendem Bedarf an Bandbreite und Geschwindigkeit bei der Übertragung von Daten die Einführung des dritten Standards der Mobilfunkübertragung: *LTE*. Mit diesem entschied man sich für eine Bündelung aller zu übertragenden (Sprach-) Daten in einem paketvermittelnden Kernnetz, inklusive der Verbindungen zwischen den einzelnen Netzwerkkomponenten. [53, 205 f.]

Der in *LTE* für die Sprachdatenübertragung zuständige Dienst wird als *VoLTE* bezeichnet und zählt auch in den späteren Entwicklungsstufen des Mobilfunknetzes wie 5G als Standard bei der Übertragung digitaler Sprachdaten. *VoLTE* basiert dabei auf dem *3GPP IP Multimedia Subsystem (IMS)*, welches wiederum auf *SIP* beruht. [53, 295 f.]

3.8.3 SIP in VoLTE

Zur Anwendung des *SIP*-Protokolls in Mobilfunknetzen wurde dieses um das *3GPP*-Protokoll erweitert. In dieser Erweiterung wird dies als *IMS* bezeichnet. Abweichend vom klassischen *SIP* sind hierbei jedoch die verwendeten Bezeichnungen. So werden die Funktionen des *SIP-Registrar* und des *SIP-Proxy* bei *VoLTE* vereint und von der Serving Call Session Control Function (S-CSCF) übernommen. Dieser kommuniziert direkt mit dem Home Subscriber Server (HSS), welcher wiederum das *LTE*-adäquat des Home Location Register (HLR) [13] darstellt. Dieser ist fester Bestandteil der Mobilfunkkommunikation und wird von den Mobilfunkbetreibern bereitgestellt.

[13] Teilnehmerdatenbank mit Informationen über Dienste des Mobilfunknetzwerkes

3.9 Caller ID Spoofing im SIP

Wie jedes digitale System unterliegt *VoIP* im Allgemeinen als auch explizit *SIP* verschiedenster Sicherheitsbedrohungen krimineller Akteure. Darunter zählt nicht nur das hier beschriebene Vorgehen des **Caller ID Spoofing** unter Ausnutzung von *VoIP*-Techniken, sondern auch direkte Bedrohungsszenarien der klassischen Informationstechnik. Diese richten sich abermals gegen die folgenden Schutzziele und den dazugehörigen Bedrohungsszenarien:

Vertraulichkeit

- Abhören von Telefonaten

Integrität

- Manipulation der Signalisierung
- Manipulation von Gesprächen

Authentizität

- Identitätsfälschung
- Vortäuschen falscher Authentizität

Verfügbarkeit

- *Denial of Service (DoS)*[14]
- *Spam over IP Telephony (SPIT)*[15]

Caller ID Spoofing bedroht das Schutzziel der Authentizität durch Vortäuschen einer falschen Identität. Während jedoch gegen eine Vielzahl anderer Bedrohungen (*DoS-Angriffe*, *Call Hijacking*[16], Abhören von Gesprächen) bereits Sicherungsmaßnahmen bestehen, lässt sich das Vortäuschen einer falschen Identität deutlich ungehinderter durchführen. Die Hintergründe dafür sollen im Folgenden erläutert werden.

[14] Angriff auf Netzwerkkomponenten, bei denen durch Überlastung die Verfügbarkeit gestört wird [50, S. 455]
[15] Unerwünschte Werbeanrufe unter Verwendung von *VoIP* [50, S. 467]
[16] Unberechtigte Weiterleitung eines Anrufes durch Manipulation des *SIP-Proxy* [50, S. 457]

3.9.1 Zusammenfassung und Problemstellung

Nach Betrachtung der vorangegangenen Aussagen lassen sich in Bezug auf **Caller ID Spoofing** erste Rückschlüsse ziehen.

Zunächst sei anzumerken, dass der Begriff **Caller ID Spoofing** inflationär unabhängig der verwendeten Technologie verwendetet werden kann. Während die *Caller ID* lediglich bis unter *ISDN* Anwendung fand (3.4), ist die Verwendung des Begriffes unter Anwendung von *VoIP* rein technisch nicht mehr korrekt. Stattdessen wird in Bezug darauf von **SIP-URI-Spoofing** oder generell von **Identity-Spoofing** gesprochen. Bei diesem wird weiterhin eine Unterscheidung in **SIP-Request-Spoofing**, bei der Verschleierung der Identität in der *SIP-INVITE-Request* und **SIP-Response-Spoofing** bei der Manipulation des *SIP-Response*. [50, S. 468]

Bei dem in dieser Arbeit betrachteten Vorgehen zur Identitätsmanipulation handelt es sich demnach rein technisch um ein **SIP-Request-Spoofing**, genauer noch um ein **INVITE-Spoofing** beziehungsweise **Session-Spoofing**, da die Veränderung der Absenderufnummer im *INVITE-Header* erfolgt. [50, S. 468]

Aufgrund der in der Literatur und dem allgemeinen Sprachgebrauch verwendeten Bezeichnung **Caller ID Spoofing** wird diese auch in der vorliegen Arbeit in Bezug auf *VoIP* und *SIP* angewandt.

Während bis unter Verwendung von *ISDN* der Netzzugang und die durch diesen genutzten Dienste (beispielsweise Internet und Telefonie) eine Einheit desselben Anbieters darstellten, besteht nun mit dem Aufbau der neuen Telekommunikationsnetze erstmalig die Möglichkeit der Trennung beider Instanzen. Netzzugang und Netzdienste müssen unter Verwendung von *IP* nicht mehr zwangsläufig vom selben Anbieter bereitgestellt werden. Damit entfallen jedoch gleichzeitig auch eine Vielzahl an Kontrollmechanismen und Regulierungsfunktionen.

So wurde durch das gleichzeitige Bereitstellen des Telefondienstes und des Netzzuganges durch einen Anbieter, die Identität des Nutzers über dessen Rufnummer, im Bereich der öffentlichen Telefonie, zuletzt über *ISDN*, sichergestellt. Die Zuordnung dieser erfolgte netzseitig zu einem Anschluss. Während also im leitungsgebundenen Festnetz jeder Heimanschluss und damit zumeist jeder Teilnehmer über lediglich eine feste Rufnummer verfügte, erfolgte mit *VoIP* eine Umstellung dieses starren Systems und die Einbindung der Telefonie in das globale Internet. Durch diese Trennung können Teilnehmer in das anwachsende Next-Generation-Network standortunabhängig, Sprachdaten in Form von Datenpaketen einleiten und beliebig verteilen, lediglich die Adressierung des Empfängers Absenders müssen dabei korrekt sein. Dazu bedarf es lediglich einer Registrierung bei einem entsprechenden *SIP*-Anbieter, welcher einen virtuellen *SIP-Server* beziehungsweise *SIP-Proxy* zur Verfügung stellt. Diese kann durch den Nutzern frei konfiguriert und bei Bedarf angepasst werden. Die Telekommunikationsanbieter übernehmen in diesem Fall lediglich den Transport der Datenpakete und stellen Gateways zur Überleitung in andere Netze und die Verbindung zu weiteren notwendigen Diensten (beispielsweise *DNS*-Server zur Signalisierung) zur Verfügung.

Gleichzeitig wird gerade im Heimnetz-Bereich auf den integrierten Telefondienst der Telekommunikationsanbieter zurückgegriffen, welcher auch über *SIP* abgewickelt wird. Folgend daraus betreiben diese ebenfalls *SIP-Server* und integrieren diese in die bestehenden Infrastrukturen. Eine Tatsache, die den meisten Nutzern von Heimtelefonie unbekannt ist. Dies lässt sich unter anderem auch auf die Bereitstellung vorkonfigurierter *DSL-Router* zurückführen, in welchen moderne Geräte eine Vielzahl an Funktionen enthalten. [78]

Die beschriebene Unwissenheit trifft ebenfalls auf die Verwendung von *VoLTE* zu, welche zwar in modernen Smartphones unter Verwendung eines entsprechenden Vertrages Anwendung findet, jedoch ohne weiteres Zutun und oft auch ohne Kenntnis der Nutzer. Telefonie im Kontext von *VoIP* ist demnach lediglich ein Dienstangebot unter vielen, welches optional, anbieterunabhängig, gewissermaßen standortunabhängig und zumeist ohne Kenntnis darüber genutzt wird oder werden kann.

Allein diese Unkenntnis über die technischen Hintergründe der genutzten Technologien kann als einer der Ausgangspunkte für das generelle Wirken von Cyberkriminellen angesehen werden.

Neben den eigenen *VoIP*-Angeboten der großen Internet- und Telefonanbietern (beispielsweise Telekom, Vodafone und O2) im Privat- und Geschäftskundenbereich existiert eine hohe Anzahl unabhängiger *VoIP*-Anbietern, die ihre Dienstleistungen global über das Internet anbieten, auch unter Verwendung deutscher Rufnummern.

Kunden können bei diesen dezentrale *VoIP*-Lösungen auf *SIP*-Basis buchen und benötigen zur Durchführung der Telefonie einzig einen Internetzugang. Die Überleitung in das (deutsche) Telefonnetz erfolgt dann durch die hiesigen Telekommunikationsanbieter. Während jedoch unter deutschen Anbietern der Identitätsprüfung sorgfältig nachgegangen wird, erfolgt diese bei internationalen Anbietern eher sporadisch, trotz dessen, dass diese ebenfalls von der Bundesnetzagentur zugeteilte deutsche Rufnummern zur Benutzung anbieten. Den Tätern von **Caller ID Spoofing** steht es also frei, bei einem der unzähligen *SIP*-Anbieter eine deutsche Rufnummer zu buchen, ohne ihren tatsächlichen Standort nachweisen zu müssen.

Gleichzeit kann selbst unter Verwendung eines deutschen Anbieters unter Zuhilfenahme gefälschter Nachweisdokumente ein *VoIP*-Anschluss genutzt werden. In jedem Fall kann die genutzte Verbindung unter Zuhilfenahme eines VPN-Dienstes[17] zusätzlich anonymisiert werden.

All diese Umstände werden von kriminellen Akteuren ausgenutzt und für gesetzeswidrige Handlungen missbraucht.

[17] Virtual Private Network: Virtuelles Netzwerk zur Verschlüsselung und Anonymisierung im Internet

3.9.2 Asserted-Identities in SIP

Die Identität der Teilnehmer im Telefonnetz, unabhängig der verwendeten Peripherie, des Standards und der Art des Netzes wird seit jeher über eine numerische Rufnummer abgebildet, über welche sich die Teilnehmer nach wie vor gegenseitig adressieren. Über sie erfolgt auch heute noch, in Verbindung mit Angaben von *IP*-Komponenten (Server, *IP*-Adressen) und unter Verwendung von *DNS-Servern* die Registrierung der Teilnehmer in einem Netz.

Die *Asserted-Identities* sollen es jedoch nun den Nutzern unter Verwendung von *SIP* ermöglichen, eine weitere, ihnen zugeschriebene Identität in Form einer Rufnummer oder eines Namens, bei der Durchführung eines Telefonanrufes übermitteln zu können. Die *P-Asserted-Identity* dabei jedoch eigentlich der Bereitstellung einer entsprechende Rufnummer zur Übertragung eines *VoIP*-Gespräches in das *ISDN*-Netz über ein *VoIP-Gateway*. [50, S. 311]

P-Preferred-Identity

Die *P-Preferred-Identity* ist Teil der *Asserted-Identities* und folgt dem Syntax

```
P-Preferred-Identity: [display-name] <sip: SIP URI>
```

Sie dient der Übertragung der anzuzeigenden Identität von User Agent zum verwendeten *SIP-Proxy*. Der *SIP-Proxy* entscheidet dann, ob er die *P-Preferred-Identity* als *P-Asserted-Identity* weiter überträgt oder diese aus der Nachricht löscht. Weiterhin kann der *SIP-Proxy* dementsprechend durch den Nutzer konfiguriert werden, in Verbindung mit der übermittelten *SIP-URI*, an diese eine frei wählbare numerische Rufnummer anzuhängen. [79, S. 4]

P-Asserted-Identity

Die *P-Asserted-Identity* wird vom *SIP-Proxy* nach Verifizierung des *User Agents* aus der *P-Preferred-Identity* übernommen und bei entsprechender Konfiguration mit einer definierten Rufnummer erweitert. Die *P-Preferred-Identity* folgt dabei dem Syntax:

```
P-Asserted-Identity: [display-name] <sip:fluffy@cisco.com>
P-Asserted-Identity: [phnone-number]
```

In der Spezifikation heißt es weiterhin, *"The P-Asserted-Identity header field is used among trusted SIP entities (typically intermediaries) to carry the identity of the user sending a SIP message as it was verified by authentication."* (*"Das P-Asserted-Identity-Header-Feld wird zwischen vertrauenswürdigen SIP-Entitäten (in der Regel Vermittler) verwendet, um die Identität des sendenden Benutzers zu übermitteln, sobald diese durch Authentifizierung verifiziert wurde."*) [79, S. 8]

Mit *P-Asserted-Identity* besteht also die Möglichkeit, der regulierten, zusätzlichen Übermittlung einer frei wählbaren Rufnummer und Anzeigenamens von einem *SIP-Proxy* zum nächsten.

Nach der in der Spezifikation beschriebenen Definition dürfen also lediglich *SIP entities (typically intermediaries)* (beispielsweise *SIP-Proxy* die *P-Asserted-Identity* nur weitergeben beziehungsweise überhaupt akzeptieren, wenn diese durch vorherige Authentifizierung der wahren Identität des Nutzers sichergestellt wurde. Im deutschen Netz entspricht dies auch dem § 120 (2) TKG, nachdem Nutzer einer Rufnummer diese nur dann *"aufsetzen und in das öffentliche Telekommunikationsnetz übermitteln [dürfen], wenn sie ein Nutzungsrecht an der entsprechenden Rufnummer haben und es sich um eine Rufnummer des deutschen Nummernraums handelt."* [44].

Dazu kommt weiterhin, dass bei Verwendung der *P-Asserted-Identity* allein der *SIP-Proxy* entscheidet, welche der vom User Agent übergebenen Identität er weiter übermittelt. [79, S. 6]

Inwiefern ein *SIP-Proxy* den Zustand *"trusted"* (vertrauenswürdig) erreichen kann, wird nicht ausgeführt. Aufgrund dessen ist davon auszugehen, dass jeder Betreiber eines *SIP-Proxy* über dessen Konfiguration selbst entscheiden kann, welchen weiteren *Proxy-Servern* er vertraut.

3.9.3 From-Header

Eine weitere Möglichkeit zur Manipulierung der Rufnummer ist die Anpassung des *From-Headers* innerhalb der genutzten Telekommunikationsinfrastrukturen und vor Weiterleitung an den *SIP-Proxy*. Hierbei kann sich die in diesem Feld optionale Angabe des `[display-name]` zunutze gemacht werden. Aufgrund dessen, dass diese Angabe jedoch optional ist und somit keiner weiteren Prüfung unterliegt, kann in diesem jeder frei wählbare alphanumerische Anzeigename übertragen werden. Dementsprechend ist auch eine numerische Zahl in der Darstellungsform einer Rufnummer möglich. Die ebenfalls in diesem Feld übermittelte *SIP-URI* bleibt davon unberührt. [80, S. 3]

Der Nachteil dieser Variante des **Caller ID Spoofing** ist die Unsicherheit über den Fortbestand des `[display-name]` bei der Übertragung durch die Telekommunikationsinfrastrukturen. In Hinblick auf die Überleitung in andere Netze (Mobil und *ISDN*) besteht hier die Möglichkeit der Entfernung dieser Information und die Nutzung der *Asserted-Identities*.

Die Manipulation innerhalb der eigenen Strukturen vor Übertragung an den *SIP-Proxy* ist dahingegen jedoch als klarer Vorteil zu werten, da letzterer nicht noch einmal entsprechend konfiguriert werden muss.

3.9.4 Caller ID Spoofing *VoLTE*

Ebenso wie im herkömmlichen *SIP* unterliegt die *VoLTE* Version *IMS* aufgrund des Bezuges zu *SIP* denselben Sicherheitsschwächen in Bezug auf die Telefonidentität und *Caller ID Spoofing*.

Diesen werden jedoch im Nachrichtenverlauf bzw. dem INVITE-Request durch diverse Netzwerkkomponenten- und Funktionen begegnet. So werden Botschaften durch Komponenten des Netzwerks selbst angepasst und dadurch entsprechend verifiziert, bevor sie durch das Netzwerk weitergeleitet werden.

Das bereits angesprochene und für *Caller ID Spoofing* bzw. die Rufnummernidentität relevante Header-Feld *P-Asserted-Identitiy* wird so beispielsweise vom *P-CSCF*[18] aktiv vom Netzwerk selbst nach der tatsächlichen Rufnummer des in diesem registrierten Endgerätes in die *INVITE*-Botschaft eingefügt. Da alle weiteren Schnittstellen, auch in das *VoIP*-Netz mit der *P-Asserted-Identitiy* arbeiten, ist hier ein verlässlicher Schutz gegenüber *Caller ID Spoofing* aus dem Mobilfunknetz heraus gewährleistet. [53, S. 318]

Daneben werden auch weitere Informationen, wie zum Beispiel Herstellerinformationen, Modellname und die *IMEI*[19] vom System automatisch aus der Botschaft entfernt und erzeugen faktisch somit einen neuen *INVITE*-Request. [53, S. 318]

[18] Proxy Call Session Control Function: Schnittstelle zwischen *IMS* und Endgerät welches auch als *SIP-Proxy* agiert
[19] International Mobile Equipment Identity: Seriennummer bei Mobilfunkgeräten

4 Methoden und Durchführung

Im folgenden Kapitel wird ein möglicher Versuchsaufbau zur Durchführung eines Telefonanrufes unter Nutzung von **Caller ID Spoofing** beschrieben. Anhand dessen soll nachvollzogen werden, mit welchen Methoden Täter vorgehen können, um die Absenderidentität zu verschleiern.

4.1 Grundaufbau

Zur praktischen Demonstration eines **Caller ID Spoofing** Angriffes wird auf die im Folgenden beschriebene Hard- und Software zurückgegriffen.

Betriebssystem

Zunächst erfolgt die Installation der Linux-Distribution *Ubuntu Server* innerhalb einer virtuellen Maschine mittels der Software *Oracle VM VirtualBox* des Anbieters *Oracle*. [81] [82]

In dieser wird im Anschluss die genutzte, virtuelle Telefonanlage installiert.

4.1.1 Virtuelle Telefonanlage

Zur kostengünstigen Abwicklung und Durchführung von Telefonverkehr bietet sich der Einsatz einer Telefon-Software im Vergleich zu einer klassischen Telefonanlage an. Diese besitzt gegenüber einer Hardware-Lösung vor allem den Vorteil eines kostenneutralen Betriebs auf einem handelsüblichen Rechner mit Internetanschluss, welcher sich ohne große Vorkenntnisse einzurichten lässt.

Asterisk

Eines der bekanntesten dieser Programme ist die freie Software *Asterisk*, ein unter GNU GPL laufendes Software-Framework auf Linux-Basis, welches Funktionen einer Telefonanlage wie beispielsweise Sprachdienste, Anrufbeantworter und Telefonkonferenzen digital simuliert und umsetzt. Mit *Asterisk* können Telefonverbindungen über alle gängigen Anschlussarten wie *ISDN* und *VoIP* über eine bestehende Internetverbindung als auch die Anbindung in das analoge Telefonnetz über entsprechende Adapter aufgebaut werden. Zur Umsetzung von *VoIP* werden alle gängigen Protokolle wie *H.323* und *SIP* unterstützt. *Asterisk* kann kostenlos aus dem Internet heruntergeladen und genutzt werden. Parallel dazu finden sich darüber hinaus auch zahlreiche Anleitungen zur Einrichtung des Dienstes und konkreter auch zur Umsetzung von **Caller ID Spoofing**. [83] [84]

Bria Solo Free (X-Lite)

Bei *Bria Solo* handelt es sich um ein *Softphone* der Anbieters *CounterPath*, welches das Telefonieren über *VoIP* auf Desktop-Rechnern und Mobilgeräten ermöglicht. Für den Verbindungsaufbau unterstützt die Software eine Vielzahl an Service Providern und Telefonsysteme, unter anderem *Asterisk*. Es baut damit auf eine bereits bestehende VoIP-Infrastruktur und dient dem Anwender als digitales Abbild eines realen Telefons. [85]

4.1.2 Internettelefonie-Anbieter

Um Telefongespräche über das IP-Netz durchführen zu können, bedarf es der Einbindung des genutzten Endgerätes in dieses. Dafür stehen den Nutzern unterschiedliche Möglichkeiten zur Verfügung. Mobilfunkgeräte verbinden sich dahingehend automatisch mit dem Mobilfunknetz und übermitteln die Sprachdaten über *VoLTE* oder *GSM* ohne Zutun des Nutzers. Auch bei Festnetzanschlüssen erfolgt der digitale Verbindungsaufbau von Telefongesprächen nach Anschluss eines Endgerätes an den verwendeten Internetrouter nach der mittlerweile flächendeckenden Umstellung auf VoIP automatisiert. Parallel dazu existieren, neben den herkömmlichen Internet- und Telefonanbietern weitere, online-basierte Angebote verschiedener Anbieter, welche entsprechende *SIP-Server* betreiben. Weltweit existiert ein Vielzahl solcher Internet-Telefonie-Anbieter, auf welche Online zugegriffen werden kann und zumeist im gewerblichen Bereich zum Einsatz kommen, im Privaten ist dies aber ebenso möglich. In diesem Fall übernimmt der lokale Telekommunikationsanbieter lediglich den Datentransport, ohne Verbindung zu dem eigenen *SIP-Server*.

Sipgate

Sipgate ist ein 2004 gegründeter, deutscher Internettelefonie-Anbieter mit Sitz in Düsseldorf. Sipgate selbst bezeichnet sich als *"der erste deutsche VoIP-Anbieter"* [86]. Eine Registrierung bei *Sipgate* zur Buchung eines kostenlosen Probemonats ist ohne Probleme möglich. Lediglich eine Geschäftsanschrift wird verlangt, welche zunächst allerdings ohne eine Validierung frei gewählt werden kann. Erst im Anschluss nach der Registrierung verlangt *Sipgate* eine entsprechende Verifizierung des Unternehmensstandortes. Erst sobald dieser erfolgt ist, besteht die Möglichkeit zur Nutzung der bereitgestellten Telefonfunktionen. Zur Verifizierung lässt *Sipgate* die folgenden Dokumente zu [87]:

- GmbH, AG, KG, EK, UG: Handelsregisterauszug
- Ltd./ausländische Firmen mit deutschem Firmensitz: Nachweis vom Finanzamt aus dem die Gründung der Ltd. hervorgeht oder Handelsregisterauszug
- Partnerschaften (Kanzleien, Architekturbüros): Partnerschaftsregister
- GbR: Gesellschaftervertrag oder Innungsnachweis, Nachweis der Handwerkskammer
- Vereine: Vereinsregister
- Einzelunternehmen: Personalausweis und Gewerbeschein
- Freiberufler:innen: Personalausweis und Nachweis vom Finanzamt / Antwortschreiben ihres Finanzamtes aus dem sich die Anmeldung und die Zuweisung der USt-Nr.ergeben
- Arztpraxen: Eintrag bei der Ärztekammer oder Bescheinigung Kassenärztliche Vereinigung.
- Anwaltskanzleien: Eintrag bei der Rechtsanwaltskammer
- Land- und forstwirtschaftliche Betriebe: Eintrag bei der Landwirtschaftskammer

Die Möglichkeit der Nutzung von *Sipagte* ist demnach nur unter Angabe echter Daten und Unterlagen oder unter Verwendung gefälschter oder gestohlener Daten möglich. Während Ersteres eine erhöhte Gefährdung für die Täter in Bezug auf eine Strafermittlung darstellt, besteht in Zweiterem bereits ein Rechtsbruch und bedarf des Weiteren einer erweiterten Vorbereitung der eigentlichen Haupthandlung, zum Beispiel durch Erwerb entsprechender Unterlagen im Dark Net. Dies betrifft allerdings alle deutschen *VoIP*- beziehungsweise *SIP*-Anbieter, welche nach § 172 TKG Daten für Auskunftsersuchen der Sicherheitsbehörden die Identität des Nutzers der Rufnummer sowohl erfassen, als auch auf Verlangen der Bundesnetzagentur und Sicherheitsbehörden an dieser herauszugeben müssen. [88]

Somit ist die Nutzung ausländischer *VoIP*- beziehungsweise *SIP*-Anbieter zur Durchführung von **Caller ID Spoofing** deutlich wahrscheinlicher, für die Täter sicherer und unkomplizierter.

Nutzung Internettelefonie-Anbieter

Im Rechercheverlauf zu dieser Arbeit wurde festgestellt, dass mittlerweile und entgegen vieler im Internet verfügbaren Anleitungen zur Durchführung von *Caller ID Spoofing* nahezu alle Anbieter von *SIP-Diensten* eine Validierung der Identität über eine e-Mail-Adresse und eine Rufnummer erfordern.

Temporäre e-Mail-Adressen

Zur Verschleierung der Identität bei der Registrierung für einen *SIP-Dienst* stehen den Tätern verschiedene Möglichkeiten zur Verfügung. Dazu zählt auch die Nutzungen von Diensten, die eine temporäre e-Mail-Adresse zur Verfügung stellen. Diese kann genutzt werden, um Validierungs-Codes der Anbieter zu erhalten [89].

Während des Rechercheverlaufs wurde festgestellt, dass eine Vielzahl von Anbietern temporärer e-Mail-Adressen von den *SIP-Dienstleistern* für eine Validierung nicht akzeptiert wird.

Temporäre Mobilfunkrufnummer

Eine weitere Möglichkeit zur Verschleierung bei der Registrierung ist die Nutzung einer temporären Mobilfunkrufnummer zum Empfang von Validierungs-Code per SMS analog zum e-Mail-Verfahren. Während bei der Nutzung einer temporären e-Mail-Adressen die Lokalität dieser keine Rolle spielt, besteht bei der Nutzung einer temporären Rufnummer die Möglichkeit zur Auswahl der Länderkennung. [90]

Während des Rechercheverlaufs wurde festgestellt, dass ebenfalls die Mehrheit der Anbieter von temporären Mobilfunkrufnummern bei den *SIP-Anbietern* gesperrt sind. Dazu kommt weiterhin, dass einige Anbieter im weiteren Registrierungsprozess eine zur Länderkennung der Rufnummer äquivalente Rechnungsadresse verlangen, welche auf Konformität geprüft wird.

4.1.3 Durchführung

Zur Durchführung eines Anrufes mittels einer gefälschten Rufnummer wurde unter Verwendung nach den oben beschriebenen Methoden versucht, eine entsprechende Hard- und Softwareumgebung aus den Komponenten

- *SIP*-Anbieter
- Virtuelle Telefonanlage
- Softphone

aufzubauen. Während die Einrichtung der virtuellen Telefonanlage unter Verwendung von *Asterisk* und die Verbindung dieser mit dem Softphone Bria Solo Free (X-Lite) ohne Probleme erfolgte, bestand eine Problematik bei der Auswahl eines geeigneten *SIP*-Anbieters, welcher die folgenden Kriterien erfüllen sollte:

- Sprachlich verständlich (Deutsch oder Englisch)
- Registrierung mittels temporärer e-Mail-Adresse möglich
- Registrierung mittels temporärer Mobilfunkrufnummer möglich
- Keine Validierung einer Geschäftsdresse
- Kostenfreie Probenutzung möglich
- Keine monatlichen Grundgebühren
- Keine reine Kreditkarten-Zahlung

Im Rechercheverlauf konnte kein *SIP*-Dienstleister alle der genannten Kriterien erfüllen. Eine Durchführung eines Anrufes unter **Caller ID Spoofing** im Rahmen dieser Arbeit war demnach nicht möglich. Neben den beschriebenen wurden mehrere weitere Anbieter auf die genannten Kriterien und die benötigten Komponenten untersucht. Jedoch konnte keiner von diesen erfolgreich in den Versuchsaufbau integriert werden. Nichtsdestotrotz konnte im Verlauf des Versuchsaufbaus weiteres Wissen in Bezug zu dem Thema generiert werden.

So zeigen zum einen die beschriebenen Sicherungsmaßnahmen der *SIP-Telekommunikationsanbieter* gegenüber einer anonymen Registrierung bei diesen ein Bewusstsein für die bestehende Problematik.

Zum anderen zeigen die vorgefundenen Hürden eben jene auf, vor denen auch die kriminellen Akteure stehe. Dies lässt den Schluss zu, dass neben der eigentlichen Durchführung von **Caller ID Spoofing** mit einer hohen Wahrscheinlichkeit im Vorfeld weitere Straftaten begangen wurden, die technischen Voraussetzungen zu schaffen. Darunter fallen alle Maßnahmen zur Verschleierung der Identität bei der Registrierung, welche durch Ermittlungsbehörden genutzt werden könnten. Dazu zählen neben der legalen Nutzung von temporären Mail-Adressen und Rufnummern beispielsweise die Nutzung gefälschter Zahlungsinformationen, das Fälschen von Urkunden oder die Manipulation fremder Telekommunikationseinrichtungen.

Aufgrund dessen, dass die Mehrzahl an deutsch- und englischsprachigen *SIP*-Anbieter die beschriebenen Sicherungsmaßnahmen verwendet, unterstricht dies nochmal einen Sitz der Täter im Ausland unter Nutzung lokaler Telekommunikationsanbieter.

4.2 Dienste

Zur Durchführung von **Caller ID Spoofing** ohne grundlegende Vorkenntnisse im *VoIP*-Bereich finden sich sowohl im Internet selbst als auch in den AppStores unter Android und Apple-Mobilgeräten zahlreiche Websites und Applikationen, welche eben jenen Dienst gegen Bezahlung anbieten.

SpoofCard

SpoofCard ist ein 2005 gegründetes, US-amerikanisches Telekommunikations-Unternehmen, welches über deren Website und Mobile-Applikation die Möglichkeit bietet, seine Rufnummer beliebig zu Manipulieren, um sich nach eigener Aussage *"gegenüber Identitätsdiebstahl, Telefonwerbung und weiteren Situationen, bei denen Fremde von der eigenen Telefonnummer profitieren"* (*"It's the best way to protect yourself against identity theft, telemarketers, and other situations that all stem from your number being exposed"*)zu schützen. [91]

Eine Registrierung bei *SpoofCard* außerhalb der Vereinigten Staaten von Amerika, Kanada oder Mexiko ist allerdings nicht möglich, da eine Registrierung und anschließenden Nutzervalidierung mit einer Rufnummer dieser Länder erfolgen muss. Auch der Download aus dem AppStore ist blockiert.

Nach der im Kapitel 2.8 betrachteten Rechtsprechung für die USA ist SpoofCard ein legitimer Dienst, welcher unter Einhaltung *Truth in Caller ID Act of 2009* dort legal genutzt werden kann. Darauf wird auch in den *Terms of Service* hingewiesen [92]. In diesen wird auch auf die Zusammenarbeit mit Ermittlungsbehörden eingegangen, welche seitens *SpoofCard* uneingeschränkt unterstützt wird. In Zusammenhang mit der im Vorfeld zu erfolgenden Registrierung mittels einer echten Rufnummer ist eine Ermittlung der Täter seitens der Ermittlungsbehörden möglich.

Einem Funktionstest, auch in Hinsicht darauf, ob und wie deutsche Rufnummern mit dem Dienst erreicht werden können, konnte aufgrund der zuvor genannten Bedingungen nicht durchgeführt werden.

Weitere Dienste

Neben *SpoofCard* existieren unzählige weitere Online-Dienste und Mobile-Applikationen, welche **Caller ID Spoofing** ermöglichen sollen. All diese sind über die gebräuchlichen Suchmaschinen im Internet auffindbar. Eine Nutzung dieser Dienste ist allerdings nur unter vorherige Registrierung und gegen eine Entgeltzahlung, meist in der Form von *"Coins"* möglich. Auffällig dabei ist, dass die Coins auf einer überwiegenden Anzahl der recherchierten Webseiten nur mit Krypto-Währungen erworben werden können.

4.3 Virtuelle Rufnummer

Eine weitere Möglichkeit zur Verschleierung der eigenen Identität, welche allerdings kein **Caller ID Spoofing** darstellt, ist die Nutzung einer virtuellen Rufnummer in Form einer Mobile-Applikation. Diese stellt die legale Nutzung einer zweiten Rufnummer dar, welche innerhalb der Applikation verschiedener Anbieter käuflich erworben und genutzt werden kann. Die Nutzung der Rufnummer erfolgt "virtuell" in der jeweiligen Applikation, ohne Zusammenhang mit der geräteseitigen SIM-Karte und dem darüber genutzten Telekommunikationsanbieter [93].

Klar zu trennen ist die Nutzung einer virtuellen Rufnummer von der Technik einer *embedded SIM* (*eSIM*). Bei dieser handelt es sich um die virtuelle, softwarebasierte Umsetzung des *subscriber identity module* (SIM-Karte) auf einem eigens dafür in dem Mobilgerät verbauten Chip. Diese wird mit Abschließen eines Mobilfunkvertrages von dem entsprechenden Anbieter programmiert und in dessen Netz freigeschaltet [94].

5 Abwehrmaßnahmen und Aufklärung

Die effektive Erkennung und die daraus sich ableitende Abwehr von Anrufen mittels gefälschter Rufnummern ist Ziel verschiedener Institutionen, Behörden und Interessenverbänden Betroffener. In diesem Kapitel sollen die direkten Gegenmaßnahmen zu **Caller ID Spoofing** betrachtet und mögliche Ermittlungsansätze beleuchtet werden.

5.1 Abwehrmaßnahmen

Die Abwehr gespoofter Anrufe beruht zunächst in jedem Fall auf der Erkennung eines solchen. Für diese existieren grundlegend zwei Ansätze: Die Menschliche und die technische Erkennung.

Die Erkennung auf Basis menschlich rational getroffener Einschätzungen lassen sich unter den Stichworten der *Security Awareness* und *Human-as-a-Security-Sensor* zusammenfassen. Die technische Erkennung und Abwehr ist ein gegenwärtig breit gefächertes Forschungsfeld mit verschiedenen Ansätzen auf den unterschiedlichen Schichten des *OSI*-Referenzmodells und auf den Ebenen innerhalb der Kommunikationsnetze.

5.1.1 Technische Abwehrmaßnahmen

Technische Abwehrmaßnahmen gefälschter Rufnummern setzen an verschieden Punkten entlang des Übertragungsweges eines Telefonanrufes an. Trotz dessen, dass **Caller ID Spoofing** im Aufbau einen rein technischen Ursprung hat, bereits seit vielen Jahren bekannt ist und in diesen auch stark zugenommen hat, existieren bislang von offizieller Seite nahezu keine massentauglichen Ansätze zur effektiven Abwehr von Anrufen unter falscher Rufnummer.

Seitens der Bundesnetzagentur als für die Telekommunikation in Deutschland verantwortliche und überwachende Stelle heißt es wörtlich: *"Bei Anrufen mit manipulierten Absenderinformationen verfügt die Bundesnetzagentur über keinerlei technische Verhinderungsmöglichkeiten.* [95]

Vielmehr stehen *"technische Einwirkungsmöglichkeiten [...] vielmehr allein den Betreibern der telekommunikationsrechtlichen Einrichtungen, also den Netzbetreibern und Telekommunikationsanbietern, zur Verfügung.* Doch nach eigener Aussage liegen *auch von dort [...] höchst unterschiedliche Aussagen dazu vor, ob und in welchen konkreten Konstellationen eine derartige technische Verhinderungsmöglichkeit derzeit vorhanden ist."* [95]

Erklären lassen sich diese Aussagen mit dem technischen Aufbau von *VoIP* und dessen vermehrten Einsatzes bei der Telekommunikationsabwicklung. Während im analogen Netz die Signalisierung auf Grundlage einer Tonfolge erfolgte und die Sprachdaten über einen physischen Kanal übertragen wurde, werden unter *VoIP* alle zu übertragenden Informationen in Datenpakten verpackt und über das *IP*-Netz übertragen. Die Bundesnetzagentur selbst verfügt über keinerlei Zugriff auf diese Netze, die sich im Besitz der Telekommunikationsanbieter, zu weiten Teilen, der Deutschen Telekom, befinden. [96]

Innerhalb der Strukturen erfolgte bis zur Gesetzesanpassung (siehe 2.8) im Dezember 2021 scheinbar ebenfalls keinerlei Plausibilitätsprüfung bei der Übermittlung von Datenpaketen mit *VoIP-Bezug*. Dazu kommt außerdem, dass jede Schnittstelle theoretisch in der Lage ist, das Datenpaket durch zusätzliche Informationen zu erweitern oder auch solche aus diesen zu entfernen, siehe VoLTE. In jedem Fall würde eine Plausibilitätsprüfung jedes Datenpaketes, welches in *VoIP*-Bezug steht, innerhalb der Infrastruktur einen erhöhten technischen Aufwand bedeuten. Mit der gesetzlich geregelten Blockierung der Absenderufnummern *110* und 112 sowie deutsche Rufnummern als Absender aus ausländischen Netzen seitens der Telekommunikationsanbieter wurde eine solche Prüfung jedoch umgesetzt. Wie sich diese allerdings gestaltet, an welchen Punkten der Telekommunikationsinfrastruktur diese ansetzt und mit welchen Parametern diese agiert bleibt jedoch unklar.

Anfragen diesbezüglich an die drei größten Anbieter von Telekommunikationsdiensten in Deutschland Telekom, Vodafone, O2 und 1&1 zum Thema **Caller ID Spoofing** im allgemeinen und zu eigenen möglichen Abwehrmaßnahmen blieben unbeantwortet oder wurden als nicht beantwortbar zurückgemeldet. Zurückzuführen lässt sich das am ehesten auf Geheimhaltungsgründe über den eigenen Netzaufbau und die verwendete Infrastruktur, aber auch auf die Brisanz des gesamten Themas an sich unter den vorangegangenen Gesichtspunkten. Parallel dazu blieben allerdings auch mehrere Anfragen bei der Bundesnetzagentur zum selbigen Thema unbeantwortet. Die Gründe hierfür sind unklar.

Die Bundesnetzagentur verfügt als regulierende Stelle zwar über Hoheitsaufgaben in Bezug auf die Verwaltung des Netzes, jedoch nur sehr bedingt über Eingriffsfähigkeiten in dieses. Die einzige Möglichkeit zur Feststellung der wahren Identität obliegt einzig und allein den Anbietern des *VoIP*- beziehungsweise *SIP*-Dienstes, welche die entsprechenden Datenpakete entgegennehmen und weiterleiten.

STIR/SHAKEN

Secure Telephony Identity Revisited) (STIR) und *Secure handling of asserted information using tokens (SHAKEN)* sind zwei von amerikanischen Telekommunikationsanbietern entwickelte Standards zur Abwehr gefälschter Anrufe unter Verwendung von *VoIP*. Verpflichtend eingesetzt werden müssen diese bislang von allen Anbietern mit mehr als 100.000 Kunden in den Vereinigten Staaten von Amerika und Kanada.

STIR dient dabei nach RFC 8224 (Authenticated Identity Management in the Session Initiation Protocol (SIP)) der IETF zur Übertragung eines Identitätszertifikates nach asymmetrischen Verschlüsselungsverfahren über *SIP*, mit welchem der erstvermittelnde Netzbetreiber die Echtheit der übertragenen Rufnummer garantiert. Alle weiteren an der Kommunikation beteiligten Anbieter können diese mit dem Public-Key besagten Netzbetreibers dem Angerufenen gegenüber bestätigen. Dabei erfolgt eine Einteilung des Anrufes in die unterschiedliche Nachweisebenen:

- A - vollständige Bestätigung des Anrufers unter Verwendung der korrekten Rufnummer
- B - Bedingte Bestätigung des Anrufers durch Bestätigung des Netzbetreibers und
- C - Bestätigung durch das verwendeten Gateways.

Alle unterstützenden Telekommunikationsanbieter betreiben somit einen eigenen Authentifizierungsdienst innerhalb ihrer Infrastrukturen, in welcher der im *SIP-Header* übermittelte *Identity token* überprüft wird. [97] [98]

SHAKEN ist die parallele Umsetzung von *STIR* für noch bestehende analoge Netze auf *SS7*-Basis.

Mit *STIR/SHAKEN* wurde somit eine vollumfängliche und verpflichtende Lösung geschaffen, auf nationaler Ebene illegitimem **Caller ID Spoofing** zu begegnen.

5.1.2 Wissenschaftliche Ansätze

Aufgrund der bislang in weiten Teilen ausgebliebenen Schutzmechanismen von Anbieterseiten, existiert eine Vielzahl an wissenschaftlichen Ansätzen zur Erkennung und Abwehr von Anrufen mittels gefälschter Rufnummer. Diese setzten sowohl anwenderseitig auf den verwendeten Geräten als auch netzseitig an den Komponenten innerhalb der Netzinfrastruktur der Telekommunikationsanbieter an.

CEIVE

Ein Ansatz, welcher von Haotian Deng, Weicheng Wang und Chunyi Peng in ihrer Arbeit *CEIVE: Combating Caller ID Spoofing on 4G Mobile Phones Via Callee-Only Inference and Verification* [99] vorgestellt wird, ist die Anwendung eines Programms zur Abfrage des aktuellen Zustands der Rufnummer des anrufenden Teilnehmers. Dabei wird bei einem Anruf automatisch ein Rückruf zur übermittelten Nummer des Anrufers initiiert. Diese befindet sich, falls die Rufnummer echt und nicht gespoofed sein sollte, in jedem Fall im Zustand "Anruf" und kann demnach den gegenläufigen Anruf nicht entgegennehmen. Dies wird dem System mit bestimmten Response Signalen mitgeteilt. Sollte die durch den Anrufer verwendete Rufnummer jedoch gefälscht sein, ist eine Annehmen des Rückrufes an die echte Nummer möglich und die Nummer des laufenden Anrufes mit hoher Wahrscheinlichkeit gespoofed. *CEIVE* erweist sich sowohl unter Einsatz von *VoLTE* bzw. SIP als auch unter Verwendung von Circuit-Switched Fallback (CSFB), falls kein *VoLTE* unterstützt wird. Vorteil dieser Methode ist die reine Anwendung auf Seiten des Angerufenen bzw. dessen Gerätes ohne Veränderungen auf den Geräten potenzieller Anrufer. Nachteil der Methode ist die gegenwärtige Beschränkung auf modifizierte Endgeräte zum Beispiel zur Freischaltung der Funktion parallel zwei Anrufe führen zu können.

CallerDec

Einen ähnlichen Ansatz wie *CEIVE* wurde in der Arbeit *End-to-End Detection of Caller ID Spoofing Attacks* [100] entwickelt. Das dabei verwendete System *CallerDec* verwendet ebenfalls die Verifikation des Anrufers zur Abwehr von Anrufen mittels **Caller ID Spoofing**. Die Entwickler setzen dabei auf zwei unterschiedliche Varianten, eine SMS-basierte Version und eine timing-basierte Version ihres Programms.

Während die timing-basierte Version ebenfalls auf einem Verifikations-Rückrufs basiert, wird bei der SMS-basierten Version von *CallerDec* vor Initiierung des Anrufes ein Austausch von Challenge-Response-Botschaften über SMS durchgeführt. Durch diesen wird die Identität des Nutzers beziehungsweise des Gerätes sicher gestellt. [100]

Trusted Caller ID

Im Vergleich zu CEIVE und CallerDec stellen die Autoren in ihrem Artikel *A Mechanism to Authenticate Caller ID* [101] einen konträren Ansatz zur Abwehr vor gefälschten Anrufen vor. Sie schlagen dafür eine von den kommunizierenden Parteien unabhängige, dritte Instanz als Kontrollmedium zur Authentifizierung der Anrufe vor.

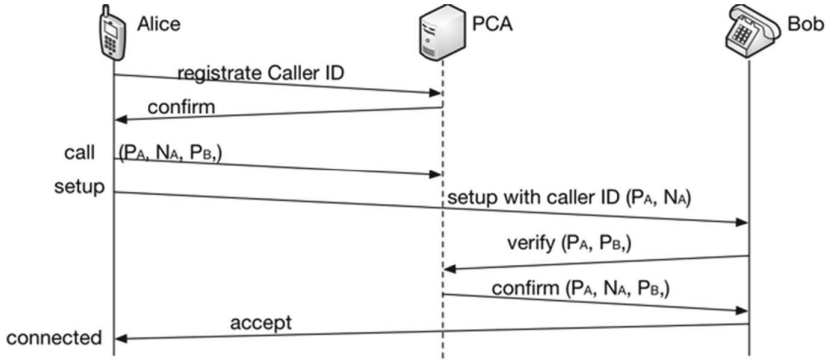

Abbildung 5.1: Schematische Darstellung des Ablaufs unter Einsatz von Trusted Caller ID [101, S. 750]

Zur Umsetzung dieser Abwehrmaßnahme ist eine vorherige Registrierung der Rufnummer bei einer *"Phone Call Authority"* notwendig. Hier kann sowohl die Registrierung der Rufnummer (P) als auch, mit entsprechenden Nachweisen, die des Namens (N) erfolgen. Im Rahmen eines Anrufes erfolgt dann zunächst eine Anfrage an diese authentisierende Stelle, bevor der eigentlich Anruf aufgebaut wird. Nach Bestätigung dieser folgt der herkömmliche Rufaufbau über die bekannten Kanäle und Protokolle. Bevor der Anruf vom Angerufenen angenommen wird, erfolgt dann ebenfalls automatisch eine Abfrage an die authentisierende Stelle. Erst wenn diese die Echtheit der Anruferdidentität bestätigt, erfolgt die Annahme und der Datenaustausch. Der Vorteil dieser Methode ist die nicht benötigte Installation diverser Software oder Applikationen, wie es bei *CEIVE* oder *CallerDec* der Fall ist. Dahingegen benötigt *Trusted Caller ID* die Einrichtung einer entsprechenden zertifizierenden Stelle zur Authentifizierung der Anrufe, welche in jedem Fall unabhängig jeglicher Manipulation sein sollte.

Neben den hier vorgestellten Abwehrmechanismen von **Caller ID Spoofing** existieren noch eine Vielzahl weiterer wissenschaftlicher Ansätze auf verschiedenen Anwendungsebenen. Diese reichen von simplen Verfahren wie dem Nutzen von Black- und White-Listening, um nur eine bestimmte Auswahl an Rufnummern zuzulassen [102], bis hin zu Turing Tests, bei denen geprüft werden soll, ob es sich bei dem Anrufer um einen realen Menschen oder ein Computersystem handelt [103]. Auch das Abgleichen des *DNS*-Eintrages des vermittelnden *SIP-Proxy* mit der angegeben Rufnummer [104] wird als weitere Variante vorgeschlagen.

Abschließend lässt sich festhalten, dass es im Allgemeinen zunächst eine große Anzahl praktikabler Ansätze auf unterschiedlichen Leveln der Umsetzbarkeit in Form wissenschaftlicher Arbeiten existieren. Die Gründe für eine bislang ausgebliebene Implementierung einer oder mehrerer dieser Methoden sind jedoch in gleichen Maßen unterschiedlich und differenziert zu betrachten. Zunächst wäre bei einer Umsetzung darauf zu achten, eine einheitliche Lösung, zumindest auf nationaler Ebene, für alle Systeme, Netze und Netzanbieter zu finden. Da Letztere final die entsprechende Umsetzung durchführen müssten, ist der Kostenfaktor ein nicht zu vernachlässigendes Argument. Dazu kommt, dass nach Möglichkeit alle Maßnahmen im laufenden Betrieb auf die bestehende Infrastruktur aufgesetzt beziehungsweise integriert werden müssen.

Die erfolgte Gesetzesanpassung im vergangenen Jahr (siehe Kapitel 2.8) hat gezeigt, dass bei den Telekommunikationsanbietern die Möglichkeit besteht, bestimmte Absenderufnummern (Notrufnummern *110* und *112*) und Nummern ausländischer Herkunft zu blockieren, wenn sie der Rechtsstaat dazu auffordert. In der Umsetzung sind die Maßnahmen auch deutlich einfacherer zu implementieren, als bei Zertifizierungsstellen, welche eine zusätzliche Datenlast erzeugen und zusätzlich den Datenstrom verlangsamen.

5.2 Menschliche Abwehrmaßnahmen

Neben technischen Ansätzen der Erkennung, ob ein Anrufer eine gefälschte Rufnummer verwendet, sind es vor allem Maßnahmen menschlichen Handelns, welche am effektivsten gegen Cyber-Kriminalität und insbesondere auch Anrufen mit kriminellem Hintergrund entgegenwirken.

5.2.1 Information Security Awareness

Alle Formen von Phishing, über jegliche Kommunikationswege hinweg, zielen auf den Faktor Mensch als Eintrittsvektor ab. Zu den davon betroffenen Systeme zählen einzelne Geräte, Nutzerkonten und ganze Serveranlagen. Dabei bedienen sich die Täter sozialpsychologischer Methoden zum Vertrauensaufbau und unbewusster Manipulation, um bestimmte Handlungen bei den Opfern anzuregen. Die effektivsten Methoden sind die der Autorität, Einschüchterung und Aufbau einer vermeintlichen Vertrauensbeziehung. Zusammengefasst werden diese Vorgehen unter dem Begriff Social Engineering [105]

Unter dem Begriff der *Information Security Awareness* oder kurz *Security Awareness* werden Methoden und Maßnahmen menschlichen Verhaltens zusammengefasst, die sich gegen diese Vorgehensweisen richten. *Security Awareness* umfasst dabei die Unterrichtung der Anwender informationstechnischer Systeme mit dem Ziel, *"sich beruflich wie privat so zu verhalten, dass sie weder wissentlich noch unwissentlich der Sicherheit der Informationen und Informationssysteme ihres Unternehmens schaden"*. Darunter fällt beispielsweise die Verwendung geeigneter Passwörter aber auch die Trennung privater und dienstlicher Informationssysteme. [105, S. 3]

Zwar bezieht sich *Security Awareness* nach formaler Definition zumeist auf die Informationssicherheit in Unternehmen, jedoch lassen sich daraus auch Ableitungen in den privaten Bereich und darin auch auf **Caller ID Spoofing** ziehen. So ist die Grundannahme der *Security Awareness* zur Abwehr digitaler Sicherheitsgefahren zunächst die Erkennung einer solchen. [105, S. 10]

Generelles Wissen über das Vorkommen von *Phishing*-Angriffen unter Verwendung gefälschter Rufnummern ist somit der erste große Schritt bei der Verhinderung von Schäden durch diesen Modus Operandi. In Erweiterung dazu kommen danach Kenntnisse darüber, auf welche Art an Informationen es die Täter abgesehen haben und welches Vorgehen diese nutzen um an welche Ziele zu gelangen. Dies trifft auch insbesondere auf die beschriebenen *Schockanrufe* oder Anrufe vermeintlich seriöser Absender zu. Aus dem Grundwissen über die Existenz dieser Vorgehensweisen resultiert dann ein gefahrenkonformes Verhalten gegenüber der Bedrohungslage, sowohl im Vorfeld als auch bei der akuten Bedrohung im Laufe eines Telefongespräches. Konkretes Verhalten im Vorfeld eines jeden Telefonanrufes spiegelt sich beispielsweise in einem generellen Misstrauen gegenüber unbekannten Rufnummern wieder. Diese stellen zwar nicht originär eine Gefahr dar, sollten beim Angerufenen jedoch zu einem entsprechenden Verhalten bei der Rufannahme führen. Gleichzeitig muss aber auch das Bewusstsein vorhanden sein, dass auch bekannte, vermeintlich seriöse Rufnummern unter **Caller ID Spoofing** eine Bedrohung darstellen können. Dies stellt den zweiten Baustein *Security Awareness* dar. [105, S. 10]

Die Umsetzung dieses Wissens in einem konkreten Verhalten ist der dritte Baustein innerhalb der *Security Awareness*. [105, S. 10]

In Umsetzung eines generellen Misstrauens wird so zunächst auf die Preisgabe vertraulicher Informationen während des Gespräches verzichtet. Gleichzeitig kann durch gezielte Fragen an den Anrufer der Versuch unternommen werden, dessen Identität zweifelsfrei zu verifizieren. Dies kann auch über das Beenden des Gespräches und einen gezielten Rückruf an die ursprüngliche Absenderufnummer oder, in Bezug auf *Schockanrufe*, mit einem Rückruf an das im Gespräch dargestellte Opfer erfolgen.

Dieses Verhalten ist effektiv sowohl gegenüber Anrufern mit unbekannter Rufnummern, als auch von Anrufen vermeintlich glaubwürdigen Absendern. Im Falle einer Unsicherheit gegenüber der Identität des Anrufers sollte jedoch immer auf die Preisgabe vertraulicher Informationen verzichtet werden.

Im Nachgang einer bestätigt abgewehrten Bedrohung ist außerdem eine Information an die zuständigen Ermittlungsbehörden ebenfalls unabdingbar. Zwar ist dies nicht direkt Teil einer aktiven Abwehr der Bedrohung, kann im Nachgang jedoch entscheidendes Wissen zur Verhinderung weiterer Taten beitragen.

Unter Maßgabe der aufgeführten technisches Abwehrmaßnahmen von **Caller ID Spoofing** sind die beschriebenen menschlichen Maßnahmen nach wie vor die effektivere Variante gegenüber diese Bedrohung. Während technische Umsetzungen einer längeren Vorlauf- und Planungszeit bedürfen, kann durch gezieltes Verhalten ad hoc auf neue Bedrohungslagen reagiert werden. Dieses Verhalten bedarf jedoch einer entsprechenden Informationsgrundlage und daraus resultierenden Handlungsleitfäden, bereitgestellt von den verantwortlichen Stellen.

Dies führt zwangsläufig wiederum zu einer Vorgabe an Behörden, Interessenverbände, Wissenschaft, Medien und Politik im Umgang mit digitalen Bedrohungslagen. Gezielte Informationen an die Gesellschaft müssen innerhalb dieser Strukturen permanent geniert und ausgegeben werden, um einen stets aktuellen Schutz gegenüber diesen Gefahren aufrecht zu erhalten.

5.3 Aufklärung

Die Aufklärung von Straftaten, welche unter Zuhilfenahme gefälschter Telefonnummern erfolgen, obliegt den Strafverfolgungsbehörden gemäß § 100g Strafprozessordnung (StPO). Dieser Paragraph regelt die Befugnisse für eine Verkehrsdatenabfrage bei bestimmten Straftaten nach Strafgesetzbuch (StGB).

Die Bundesnetzagentur als Bundesbehörde und für die Abwicklung sämtlicher Telekommunikation verantwortliche Stelle besitzt nach eigener Aussage dahingehend *"keine generelle Befugnis, den Ursprung von Anrufen aufzuklären."* [95]

Mit Wirkung der neuen Gesetzeslage zum 01.12.2022 sind die Netzanbieter verpflichtet sicherzustellen, dass zum einen nicht die Rufnummern *110* und *112* als Absenderufnummern verwendet werden, zum anderen *"dass bei Anrufen, die aus ausländischen Netzen übergeben werden, keine deutschen Rufnummern als Absenderinformation angezeigt werden. Die Nummernanzeige ist in solchen Fällen zu unterdrücken."* Dies bietet Kriminellen nichtsdestotrotz nach wie vor eine Vielzahl an Angriffsvektoren im Rahmen des **Caller ID Spoofing**, zum Beispiel dem prinzipiellen Unterdrücken der Rufnummer oder der Übermittlung einer deutschen Rufnummer. [106]

5.3.1 Polizeilich

Die polizeiliche Aufklärungsarbeit bei Straftaten unter Verwendung gefälschter Rufnummern ist Hauptbestandteil bei der Bekämpfung dieses Kriminalitätsphänomens. Im Rahmen der Recherche zu den aktuell bestehenden polizeilichen Möglichkeiten zur Aufklärung von der genannten Fälle wurde die zentrale Polizeiinspektion Göttingen zu deren Erfahrung im Umgang mit **Caller ID Spoofing** befragt.

Die Möglichkeiten zur Verschleierung der Identität zur Durchführung krimineller Handlungen ist nach Aussage der zentralen Polizeiinspektion Göttingen *"allgegenwärtig in fast allen Deliktsfeldern, wo Telefonie genutzt wird (z.B. Betrug, Betäubungsmittelhandel, Äußerungsdelikte, Tausch von Kinderpornographie, politisch motivierte Kriminalität)"* [107]. Dabei wird zumeist allerdings auch auf sogenannte *"Anonsims"* zurückgegriffen. Technisches **Caller ID Spoofing**, wie in dieser Arbeit beschrieben, trete vermehrt dort auf, *"wo Täter telefonisch Kontakt mit Geschädigten aufnehmen"* [107]. Dies ist zumeist bei der Durchführung der bereits beschriebenen Modi Operandi wie Schockanrufe oder falscher Support-Mitarbeiter gegebenen. Zusammengefasst werden diese Delikte als *"Call-Center-Straftaten"*. [107]

Nach Aussagen der zentralen Polizeiinspektion Göttingen stehen die Ermittler bei der Aufklärung von gefälschten Rufnummern vor einer Vielzahl von Problemen. Zunächst werden nicht alle durchgeführten Betrugsdelikte tatsächlich mit den beschriebenen Maßnahmen des **Caller ID Spoofing** durchgeführt. Neben diesem existieren noch weitere Möglichkeiten zur Verschleierung der eigenen Absenderidentität, wie zum Beispiel die Registrierung von SIM-Karten auf gefälschten Personalien. Somit muss zunächst geprüft werden, welches technische oder methodische Vorgehen die Täter nutzen, um ihre Identität zu kaschieren. Desweiteren *"laufen die üblichen Ermittlungsmaßnahmen zur Feststellung des Anschlussnutzers ins Leere"* [107].

Dies betrifft vor allem die Möglichkeiten der Telekommunikationsüberwachung (TKÜ), sowohl der Anschlüsse der Opfer als auch der verwendeten Rufnummer. Während bei Ersterem die Gespräche durch die *TKÜ* so dargestellt werden, *"als kämen sie legitim von den gespooften Rufnummern"* [107], verhindern rechtliche Festlegungen die Überwachung der rechtmäßigen Nutzer der verwendeten Rufnummern. Dies könnte demnach nur nach Zustimmung des Rufnummerninhabers erfolgen, dessen Gespräche allerdings im Rahmen einer solchen TKÜ ebenfalls überwacht werden würden. Als Ermittlungsansatz wird seitens des Landeskriminalamtes Niedersachsen vorgeschlagen, eine Auslandskopfüberwachung[20] zu den gefälschten Rufnummern zu installieren. [107]

Es lässt sich demnach festhalten, dass die polizeilichen Möglichkeiten in Bezug auf die Ermittlung der Absenderidentität bei **Caller ID Spoofing** stark eingeschränkt sind. Die betrifft vor allem kleinere Dienststellen, während Inspektionen mit eigenen Fachbereichen für Cybercrime bis hin zu Landes- und Bundesbehörden wie den Landeskriminalämtern und dem Bundeskriminalamt mehr Möglichkeiten zur Verfügung stehen. Nichtsdestotrotz greifen auch bei diesen herkömmliche Ermittlungsmaßnahmen wie die *TKÜ* aufgrund des technischen Ablaufes von **Caller ID Spoofing** unter Verwendung von *VoIP* und *SIP* nicht. Dies beschreibt auch der Abschlussbericht eines vom Bundeskriminalamt durchgeführten Forschungsprojektes, nach welchem *"eine Nachverfolgung des Routing nicht erfolgreich durchgeführt werden konnte"*. [107]

[20] inländische Telekommunikationsüberwachung nach Telekommunikations-Überwachungsverordnung (TKÜV), die Verbindungen von unbekannten Anschlüssen im Inland zu einem bestimmten Anschluss im Ausland" überwacht [108, S. 2]

6 Zusammenfassung und Diskussion

Authentizität bedeutet laut Definition *"den Tatsachen entsprechend und daher glaubwürdig"* [109]. Diese lässt sich, bei der Durchführung eines Telefonats und in Bezug auf **Caller ID Spoofing**, auf die Echtheit beziehungsweise Glaubwürdigkeit der Teilnehmeridentitäten übertragen. Mit der *P-Asserted-Identity* im *SIP*-Protokoll wurde unter anderem jedoch eine Möglichkeit geschaffen, im Gegensatz zur herkömmlichen leitungsgebundenen Telefonie, die Adressierung des Anrufers von seiner verwendeten Identität zu trennen. Dies mag aus den genannten Gründen Vorteile haben, dessen missbräuchliche Nutzung begünstigt allerdings die Durchführung von **Caller ID Spoofing**.

Durch das global gespannte Internet gestützt, ist es für Täter vergleichsweise simpel, aus dem Ausland Telekommunikationsdaten über einen unabhängigen *SIP*-Anbieter in das deutsche Netz zu übermitteln, ohne dass hier eine Identitätsüberprüfung der übermittelnden Person bei der Übertragung der Datenpakete durchgeführt wird oder überhaupt werden kann. Diese obliegt einzig und allein dem *"erstvermittelnden"* Dienst beziehungsweise Server, welcher sich in Betrachtung der für **Caller ID Spoofing** bereits in Erscheinung getretenen Fällen zumeist im Ausland befinden dürfte. Alle nachgeordneten Server, Dienste und Anbieter auf deutscher Seite, insbesondere die *SIP-Server* und *SIP-Gateways* müssen sich entweder auf die Korrektheit der ihnen übermittelten Informationen verlassen oder aber die Verbindung unterbrechen. Im Zuge dessen, einen maximal unterbrechungsfreien, globalen Netzzugang anbieten zu wollen, dürfte die letzte Option in den meisten Fällen bis zuletzt hinfällig gewesen sein. Dies betraf, bis zur Gesetzesänderung im Dezember 2021, auch die *VoIP*-Daten, welche mit einer angeblich deutschen Rufnummer aus dem Ausland übergeben wurden.

Dieses Vorgehen erschwert gleichzeitig den Ermittlungsansatz von Behörden und Justiz, welche im Ausland pauschal über keinerlei Befugnisse verfügen. Dazu kommen die unterschiedlichen Rechtslagen außerhalb von EU-Staaten und die generelle Unklarheit über den Standort des verwendeten Dienstes und die dort vorherrschende Gesetzeslage.

Unterstützt wird diese ausbleibende Regulierung auch durch die Tatsache, dass ein rechtlicher Verstoß gegen das *TKG* schwer nachzuweisen ist. Bis zur Anpassung des § 120 TKG zum 01.12.2022 erfolgte keine Haftung seitens der deutschen Telekommunikationsanbieter bei Verstoß gegen diesen. Die Verantwortung lag und liegt auch weiterhin noch beim Endnutzer, gegen welchen auch bei einem Verstoß ermittelt werden kann. Erst seitdem (*"[...] sämtliche an der Verbindung beteiligte Anbieter öffentlich zugänglicher Telekommunikationsdienste [...] "*) [44] sicherstellen müssen, dass bei einer Übergabe aus dem Ausland keine deutsche Rufnummer verwendet wird. Auch die Unterbindung der Absendernummer *110* und *112* wird hier erstmalig umgesetzt.

Die Möglichkeit einer Verifizierung der übermittelten Datenpakete seitens der deutschen Telekommunikationsanbieter, ob diese von einem ausländischen Absender unter Verwendung einer deutschen Identität in Form der darin übermittelten Rufnummer stammen ist demnach möglich. Diese Tatsache bedeutet jedoch auch, dass eine Plausibilitätsprüfung in der Zuordnung *IP-Adresse* - übermittelter Rufnummer stattfindet, keinesfalls aber eine wahre Identitätsprüfung. Dies trifft ebenfalls auf die Blockierung der Absenderufnummer *110* und *112* zu.

Mehrere Anfragen, sowohl bei den großen deutschen Telekommunikationsanbietern Telekom, Vodafone, 1&1 und O2 als auch bei der Bundesnetzagentur zu den angesprochenen Punkten und zum Themenkomplex **Caller ID Spoofing** im Allgemeinen blieben jedoch entweder gänzlich unbeantwortet oder wurden mit Hinweisen auf fehlende Möglichkeiten der Beantwortung zurückgewiesen.

Fest steht jedoch, dass deutsche Telekommunikationsanbieter erst nach Inkrafttreten des Gesetztes zur Unterbindung deutscher Absenderufnummern von ausländischen Anschlüssen diese blockiert haben. Ein Erklärungsansatz hierfür könnte die Unsicherheit über den Vertrauenszustand ausländischer Anbieter sein. Eine pauschale Ablehnung von Anrufen aus dem Ausland unter Verwendung einer deutschen Rufnummer, auch mittels der *P-Asserted-Identity*, könnte hier nicht gewollt gewesen sein. Des Weiteren bedeutet ein Abgleich der *IP-Adresse* des Absenders mit der im Datenpaket enthaltene *Header*-Zeile der *P-Asserted-Identity* einen zusätzlichen Aufwand durch die Implementierung eines entsprechenden Filters parallel zu den dadurch entstehenden Verzögerungen bei der Übermittlung der Datenpakete.

Ein großes Problem bei der Unterbindung von **Caller ID Spoofing** ist allerdings die unterschiedliche Rechtsauslegung zur Durchführung von Anrufen mittels einer frei gewählten Rufnummer. Während in Deutschland prinzipiell das Durchführen eines Telefonanrufes nur dann erlaubt ist, wenn für die dabei verwendete Rufnummer ein Nutzungsrecht besteht, kann in den Vereinigten Staaten von Amerika jede Rufnummer übertragen werden, sofern dahinter keine böswilligen Absichten stecken, siehe 2.8. Rein technisch besteht dabei somit auch kein Verhinderungsversuch von **Caller ID Spoofing** seitens der dortigen Verantwortlichen für die Abwicklung sämtlicher Telekommunikationsverbindungen. Anrufe unter Verwendung einer falschen Rufnummer können demnach auch erst mit Übertritt in das deutsche Netz unterbunden werden. Ein weiterer, in diesem Kontext zu betrachtender Aspekt ist die missbräuchliche Nutzung des in 3 beschriebenen *[display-name]*. Denn während die Übertragung des *[display-name]* auf der selben technischen Ebene wie eine gefälschte Rufnummer steht, ist im *TKG* jedoch lediglich die Rufnummer Teil des Sprachgebrauchs.

Ursache für die aufgetretenen Probleme bei der Erstellung dieser Arbeit lagen zunächst bei der Erarbeitung eines generellen Grundverständnisses über den Aufbau moderner Telekommunikationsinfrastrukturen, welche sich mittlerweile fernab des gesellschaftlichen Wissens bewegen. Im Rahmen dessen konnte auch nur bedingt Wissen im Wirkungsbereich der deutschen Telekommunikationsanbieter, wie die tatsächlich verwendeten Protokolle, Infrastrukturen und Abläufe innerhalb derer, generiert werden. Zwar greifen diese mit einer hohen Wahrscheinlichkeit ebenfalls auf standardisierte Protokolle wie *SS7*, *SIP* und *H.323* zurück, inwiefern diese allerdings innerhalb der Systemgrenzen übermittelt werden, gerade bei der Übergabe aus und in andere Netze, bleibt unklar.

Dazu kommt weiterhin der nach wie vor bestehende Parallelbetrieb verschiedener Generationen von Telekommunikations- und Netzwerktechniken wie *ISDN*, DSL und *VoIP*, welche alle mittels Gateways miteinander verbunden. Dazu kommt die Anbindung an das Mobilfunknetz, welches ebenfalls von verschiedenen Anbietern unter Verwendung weiterer technischer Komponenten betrieben wird.

Mit Sicherheit erfolgt die Übertragung innerhalb und zwischen den mittlerweile auf Servern basierenden Betriebsstellen der Telekommunikationsanbietern digital über Glasfaserkabel. Inwiefern diese allerdings über Gateways die nach wie vor an bestehenden analogen Netze angebunden sind, ist nicht öffentlich dokumentiert.

Ob es also demnach allein die *P-Asserted-Identity* oder der *From-Header* sind, welche sich die Täter zunutze machen, bleibt mit Abschluss dieser Arbeit nicht vollständig geklärt. Wie genau die unter 4 verwendeten *SIP*-Anbieter und deren *SIP-Proxy-Server* jene gefälschte Rufnummer tatsächlich übermitteln, welche beispielsweise, wie in diesem Anwendungsfall, im Skript übergeben wurde bleibt ebenso unklar wie das Wissen darüber, wie die *SIP-Proxy* der deutschen Telekommunikationsanbieter mit den ankommenden Daten verfahren und diese gegebenenfalls weiterleiten. Denkbar wäre hier beispielsweise auch die direkte Manipulation der Rufnummer in Form der *SIP*-Adresse, welche durch den genutzten *SIP*-Anbieter künstlich erzeugt und weitergegeben werden kann. Mit der Übertragung in das deutsche Netz mit Weitergabe über diverse Zwischenstationen und *Gateways*, möglicherweise in das *ISDN*-Netz wäre die wahre Absenderidentität mit Übernahme der in der *SIP*-Adresse eingebetteten Rufnummer erheblich schwieriger. Diese Möglichkeit sollte mit der generellen Blockierung deutscher Rufnummern aus ausländischen Netzen jedoch stark eingeschränkt sein.

Zur Umgehung dieser wäre hier beispielsweise aber auch das Verwenden mehrerer Zwischenstationen mit einer einfachen Weiterleitungsfunktion des Anrufes denkbar und möglich. Die Täter könnten so mehrere *SIP*-Anbieter hintereinander schalten, mit dem Ziel, ihre eigene Identität noch weiter zu verschleiern. Weiterhin können damit möglicherweise die Filterfunktionen der deutschen Telekommunikationsbetreiber umgangen werden, indem eine der zwischengeschalteten *SIP-Proxy* sowohl eine echte, als auch die gefälschte Rufnummer in das deutsche Netz übergeben wird, welche von den Telekommunikationsanbietern akzeptiert werden sollte.

In Hinblick darauf ist auch eine Manipulation von bestehenden, privaten *(VoIP-)* Telefonanlagen durch bislang unbekannten Sicherheitslücken denkbar. Durch Einschleusen von Schadsoftware in fremde Telekommunikationsinfrastrukturen, insbesondere die *SIP-Proxy-Server*, sowohl privater als auch professioneller Bauart, können Täter diese übernehmen und darüber manipulierte Anrufe abwickeln. [110]

Nach Aussage der Polizeiinspektion Göttingen lässt sich im Rahmen einer bei potentiellen Opfern durchgeführten *TKÜ* keine Ableitung auf die wahre Identität eines Anrufers ableiten. Dies dürfte aller Wahrscheinlichkeit nach am Aufbau der verwendeten Protokolle *SIP* und *RTP* liegen. Da die ermittelnden Behörden dieselben Kommunikationsdaten wie das Opfer selbst von dessen Telekommunikationsanbieter erhalten, ist demnach an dieser Stelle bereits die Übernahme der falsch übergebenen Telefonnummer erfolgt. Weiterhin sei im Rahmen dessen auch denkbar, dass bei der Durchführung einer *TKÜ* lediglich die Daten des Mediastreams, sprich die *RTP*-Verbindung zwischen Anrufer und Angerufenem aus dem System, ausgeleitet und betrachtet werden, ohne die eigentlichen für die Untersuchung von **Caller ID Spoofing** relevanten Signalisierungsdaten zu betrachten. Diese Detailbetrachtung war jedoch nicht Teil der vorliegenden Arbeit, kann aber in möglichen Folgebetrachtungen, gerade aus ermittlungstaktischer Sicht, weiter vertieft werden.

7 Fazit und Ausblick

Caller ID Spoofing lässt sich abschließend nicht als klassischer Angriff auf ein IT-System betrachten, sondern versteht sich vielmehr als ein geschicktes Ausnutzen bestehender Schwachstellen im Aufbau des *SIP*-Protokolls an sich, unter der Akzeptanz der vermittelnden Telekommunikationsanbieter.

Gerade technische Neuerungen eröffnen kriminelle Akteuren immer neue Vorgehen und Modi Operandi. So berichtet die New York Post zuletzt von einem Betrugsversuch, bei welchem mittels künstlicher Intelligenz die Stimme eines angeblichen Entführungsopfers nahezu identisch nachgesprochen wurde [111]. Eine mögliche Kombination dessen mit Techniken des **Caller ID Spoofing** ist gleichermaßen offensichtlich wie besorgniserregend.

Aufgrund dessen ist und wird **Caller ID Spoofing** in Betrachtung der vorliegenden Arbeit auch in Zukunft eine stetig präsente Gefahr darstellen. Die Vielzahl an unterschiedlichen wissenschaftlichen Ansätzen und anwendungsorientierten Lösungen auf verschiedenen Ebenen zur Abwehr unterstreichen dies ebenso, wie die bereits vorgenommenen Gesetzesanpassungen. Ermittlungsbehörden und Verantwortliche müssen darauf eingestellt sein, in Zukunft immer häufiger mit derartigen digitalen Bedrohungsszenarien konfrontiert zu werden.

Gleichzeitig zeigen diese Maßnahmen jedoch auch die Hürden bei der Entwicklung und sinnvollen Implementierung von Abwehrmechanismen gefälschter Anrufe auf, dessen Ursache sowohl im unsicheren Aufbau des internetbasierten Telefonnetzes unter Verwendung der beschriebenen Protokollen als auch dem unregulierten Umgang mit ausländischen Anbietern von Telefoninfrastrukturen liegt.

In Hinblick auf die unter Kapitel 5.1.2 vorgestellte Methode des *CEIVE* könnte man hierbei über die Einrichtung gemeinsamer Infrastrukturen, von Behörden und Telekommunikationsanbietern, zur Eindämmung von **Caller ID Spoofing** nachdenken. Die nötigen Ressourcen an Technik und Personal würden jedoch einen immensen finanziellen Aufwand verursachen, sodass an einer Praktikabilität dieser Variante zur Bekämpfung eines einzigen Phänomens des **Caller ID Spoofing** bezweifelt werden darf. Gleichwohl hat allerdings auch die in Kapitel 5.1.1 beschriebene Gesetzesanpassung zur Einführung der STIR/SHAKEN Mechaniken geführt, welche verpflichtend durch die Netzbetreiber im amerikanischen Raum umgesetzt werden musste.

Nichtsdestotrotz stehen staatliche Akteure wie die Bundesnetzagentur gemeinsam mit den hiesigen Telekommunikationsgesellschaften in der Verantwortung, durch geeignete, netzseitige Maßnahmen, den kriminellen Akteuren Einhalt zu gebieten. Parallel dazu muss ebenfalls die Politik des deutschen Rechtsstaates auf die sich ständig anpassenden Bedrohungslagen, gerade im digitalen Bereich, in einem angemessenen Zeitrahmen reagieren und geeignete Gesetzesanpassungen vornehmen können. Zur Durchsetzung dieser bedarf es entsprechend ausgestatteter polizeilicher Ermittlungsbehörden, welche die Wahrung der Gesetzmäßigkeiten wahrnehmen und Verstöße entsprechend verfolgen können.

Gerade in Bezug auf Letzteres hat der Austausch mit den Behörden gezeigt, vor welchen Hürden die ermittelnden Beamten stehen. Dass keine der befragten Institutionen eine generelle Handhabe gegenüber des Phänomens **Caller ID Spoofing** bei einer gleichzeitig hohen Zahl an auftretenden Fällen hat, kann und darf nicht den Anspruch eines rechtsstaatlichen Systems darstellen. Ein wichtiger Aspekt bei der Eindämmung von **Caller ID Spoofing** ist demnach der Auf- und Ausbau des technischen Handlungsspielraumes der ermittelnden Behörden, sowie die Schulung der eingesetzten Beamten.

Zu diesem Ausbau hinzu kommt ein zwingend benötigter Austausch zwischen Ermittlungsbehörden, wissenschaftlichen Instituten und in Bezug auf **Caller ID Spoofing** auch mit der Bundesnetzagentur, den Netzbetreibern und Telekommunikationsanbietern. Ein generelles Verständnis über die verwendeten Technologien, welche sich Täter zunutze machen, kann bereits ein entscheidender Schritt zu deren Verfolgung darstellen.

Allumfassend ist abschließend die permanente Aufklärung und Schulung der Gesellschaft nicht zu vernachlässigen. Unabhängig des aktuellen technischen Standes der Abwehrmaßnahmen als auch der Aufklärungsmöglichkeiten, ist *Security Awareness* auch in Betrachtung von **Caller ID Spoofing** das zur Zeit nach wie vor das geeignetste Mittel zur Abwehr gefälschter Anrufer und den daraus entstehenden Nachteilen. Unabhängig der technischen Abwehrmaßnahmen werden Täter immer Möglichkeiten zur Umgehung dieser finden und diese bis zu deren Anpassung ausnutzen. Während Gesetze, Staat und Ermittlungsbehörden den Taterfolgen hinterher arbeiten und eher proaktiv wirken, ist eine aufgeklärte Gesellschaft mit einem entsprechenden Wissensschatz über die für Sie relevanten Bedrohungen der wichtigste Baustein bei der Abwehr von Cyberkriminalität.

In Bezug auf einer Fortführung des in dieser Arbeit vermittelten Grundlagenwissens sind weitere, zumeist praktische Ansätze denk- und umsetzbar. Dabei sollte vor allem analysiert werden, welche Daten und Informationen tatsächlich wie und auf welchem Weg in Bezug auf die dabei verwendeten Algorithmen und Protokolle übertragen werden Die Veränderbarkeit der übertragenen Daten durch die genutzten Zwischenstationen (*Proxy*, *Gateways*) ist hierbei von besonderer Relevanz.

Zunächst kann sich dabei auf den Aufbau eines praktischen Versuchsaufbaus analog der im Kapitel 4 vorgestellten Komponenten, unter Zuhilfenahme eines nach den beschriebenen Kriterien nutzbaren *SIP-Anbieters* konzentriert werden. Unter Einsatz verschiedener *SIP-Anbieter* kann in diesem die Übermittlung der Datenpakete unter Verwendung des *SIP-Protokolls* mitgeschnitten und nachvollzogen werden. Der Fokus sollte dabei insbesondere auf die *INVITE*-Botschaften in Zusammenhang mit der Nutzung unterschiedlicher Übertragungswege (*VoIP*, *ISDN*) gelegt werden. Auch ein Vergleich zum im anschließend übertragenen *Media-Stream* in den verwendeten Datenpaketen ist hierbei möglich. In jedem Fall sollte allerdings bei der Durchführung von **Caller ID Spoofing** im deutschen Rechtsraum auf den durch das TKG geschaffenen Gesetzesrahmen geachtet werden.

In Verbindung dazu könnte es auch aus ermittlungstaktischer Sicht sinnvoll sein, die Möglichkeiten der *TKÜ* neu zu eruieren, um gegebenenfalls im Rahmen einer solchen sich nicht nur auf die Auswertung des akustischen Inhaltes eines Telefongespräches zu konzentrieren, sondern eine erweiterte Analyse der Sprachdaten auf Basis der eigentlichen Datenpakete durchzuführen.

Literaturverzeichnis

[1] A-Z Quotes, *QUOTES BY BRET MORRISON | A-Z Quotes*, 3.02.2023. Adresse: https://www.azquotes.com/author/23173-Bret_Morrison.

[2] J.-P. Domschke, *Ströme verbinden die Welt: Telegraphie - Telefonie - Telekommunikation* (Einblicke in die Wissenschaft). Wiesbaden: Vieweg+Teubner Verlag, 1997, ISBN: 9783322996251. DOI: 10.1007/978-3-322-99625-1.

[3] 6. W. Bundeskriminalamt, „Bundeslagebild Cybercrime 2021“, 2021. Adresse: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2021.html?nn=28110.

[4] 6. W. Bundeskriminalamt, „PKS 2021 Bund - Falltabellen: T01 Grundtabelle - Fälle“, Jg. 2021, 2021. Adresse: https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/PKS2021/PKSTabellen/BundFalltabellen/bundfalltabellen.html?nn=194208.

[5] Arne Dreißigacker, Bennet von Skarczinski, Gina Rosa Wollinger, „Cyberangriffe gegen Unternehmen: Ergebnisse einer Folgebefragung 2020“, Nr. 162, Adresse: https://kfn.de/wp-content/uploads/Forschungsberichte/FB_162.pdf.

[6] Bundesnetzagentur, *Bundesnetzagentur - Presse - Tätigkeitsberichte Telekommunikation und Post 2020/2021*, 2021. Adresse: https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2021/20211216_PK-Monopolkommission.html.

[7] Statistisches Bundesamt, *Daten aus den Laufenden Wirtschaftsrechnungen (LWR) zur Ausstattung privater Haushalte mit Informationstechnik*, 27.10.2022. Adresse: https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Einkommen-Konsum-Lebensbedingungen/Ausstattung-Gebrauchsgueter/Tabellen/a-infotechnik-d-lwr.html.

[8] Bundesverband deutscher Banken e.V., *Krautscheid: Der Mensch ist das häufigste Angriffsziel*, 10.01.2023. Adresse: https://bankenverband.de/newsroom/zitate/mensch-angriffsziel-fur-cyber-kriminelle/.

[9] *Cyber-attacks set to become more targeted in 2021, according to HP Inc*, 6.01.2023. Adresse: https://press.hp.com/us/en/press-releases/2020/cyber-attacks-to-become-more-targeted-in-2021.html.

[10] Microsoft, „Microsoft Digital Defense Report 2022“, 2022. Adresse: https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022.

[11] „cyber-“, *Duden.de*, 17.05.2018. Adresse: https://www.duden.de/rechtschreibung/cyber_.

[12] Bundesministerium des Innern und für Heimat, „Cyberkriminalität“, *Bundesministerium des Innern und für Heimat*, 25.09.2017. Adresse: https://www.bmi.bund.de/DE/themen/sicherheit/kriminalitaetsbekaempfung-und-gefahrenabwehr/cyberkriminalitaet/cyberkriminalitaet-node.html.

[13] A. Brockhaus, „Cybercrime as a Service (CaaS) – So funktioniert die professionalisierte Cyberkriminalität“, *isits AG International School of IT Security*, 2.11.2021. Adresse: https://www.is-its.org/it-security-blog/cybercrime-as-a-service-caas-so-funktioniert-die-professionalisierte-cyberkriminalitaet.

[14] C. Hadnagy, *Die Kunst des Human Hacking: Social Engineering* (EBL-Schweitzer), Dt. Ausg., 2. Aufl. Heidelberg u. a.: Mitp-Verl., 2011, ISBN: 9783826686870. Adresse: http://swb.eblib.com/patron/FullRecord.aspx?p=1458222.

[15] Stefan Schumacher, „Die psychologischen Grundlagen des Social Engineerings“, *Magdeburger Journal zur Sicherheitsforschung*, Nr. Bd. 1, S. 1–26, 2011. Adresse: http://www.wissens-werk.de/index.php/mjs/article/viewFile/74/40.

[16] Dirk Labudde, *OSINT und Social Engineering*, 2020.

[17] 6. W. Bundeskriminalamt, „Bundeslagebild Cybercrime 2020“, 2020. Adresse: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2020.html?nn=28110.

[18] Bundesamt für Sicherheit in der Informationstechnik, *Darknet und Deep Web*, Bundesamt für Sicherheit in der Informationstechnik, Hrsg., 28.09.2021. Adresse: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Darknet-und-Deep-Web/darknet-und-deep-web_node.html.

[19] 6. W. Bundeskriminalamt, *Lageprodukte aus dem Bereich Cybercrime - QR Code 4: Eintrittsvektoren*, 6. W. Bundeskriminalamt, Hrsg., 13.01.2023. Adresse: https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/2021/Code4.html.

[20] Statista, *Anzahl der entdeckten Phishing-Webseiten weltweit 2022 | Statista*, 13.01.2023. Adresse: https://de.statista.com/statistik/daten/studie/73876/umfrage/anzahl-der-gemeldeten-phishing-webseiten-weltweit/.

[21] Kaspersky, Hrsg., *Was ist Spear-Phishing? | Definition und Risiken*, 18.04.2023. Adresse: https://www.kaspersky.de/resource-center/definitions/spear-phishing.

[22] Proofpoint, *Was ist Vishing? Phishing-Anrufe einfach erklärt*, 2021. Adresse: https://www.proofpoint.com/de/threat-reference/vishing.

[23] Proofpoint, *Was ist Smishing? Definition, Erklärung, Beispiele*, 2021. Adresse: https://www.proofpoint.com/de/threat-reference/smishing.

[24] LEO, Hrsg., *spoofing - LEO: Übersetzung im Englisch ⇔ Deutsch Wörterbuch*, 11.03.2023. Adresse: https://dict.leo.org/englisch-deutsch/spoofing.

[25] Ivan Belcic & Ellie Farrier, „Was ist Spoofing und wie lässt es sich verhindern?“, *Avast*, 3.06.2021. Adresse: https://www.avast.com/de-de/c-spoofing.

[26] *Was ist Spoofing? | IP- und Mail-Spoofing-Angriffe*, 10.01.2023. Adresse: https://www.kaspersky.de/resource-center/definitions/ip-and-email-spoofing.

[27] *What is Typosquatting?*, 20.01.2023. Adresse: https://www.kaspersky.com/resource-center/definitions/what-is-typosquatting.

[28] Prof. Dr. Dirk Pawlaszczyk, *Geonavigationssysteme / Geoforensik*, 2020.

[29] C4ADS, „Above Us Only Stars: Exposing GPS Spoofing in Russia and Syria“, 2019. Adresse: https://c4ads.org/reports/above-us-only-stars/.

[30] Bundesnetzagentur, *Manipulation von Rufnummern*, 20.01.2023. Adresse: https://www.bundesnetzagentur.de/DE/Vportal/TK/Aerger/Faelle/Manipulation/start.html.

[31] 6. W. Bundeskriminalamt, „Warnhinweis des Bundeskriminalamtes: Bundesweite betrügerische Anrufe angeblicher Mitarbeiter verschiedener Polizeibehörden“, Adresse: https://www.bka.de/SharedDocs/Kurzmeldungen/DE/Warnhinweise/220411_AnrufeBehoerden.html.

[32] Federal Communications Commission, *Caller ID Spoofing*, 2011. Adresse: https://www.fcc.gov/spoofing.

[33] Ministerium des Innern des Landes Nordrhein-Westfalen, Hrsg., *Vorsicht: Falsche Polizeibeamte am Telefon!*, 1.04.2022. Adresse: https://polizei.nrw/artikel/betrueger-geben-sich-am-telefon-als-polizeibeamte-aus.

[34] B. Polizei, *Die Bayerische Polizei - Organisierter Callcenterbetrug - Falsche Polizeibeamte | Schockanruf*, Polizeipräsidium München, Hrsg., 2022. Adresse: https://www.polizei.bayern.de/schuetzen-und-vorbeugen/beratung/039355/index.html.

[35] 6. W. Bundeskriminalamt, *Enkeltrick: Betrug am Telefon mit neuer Masche*, 2020. Adresse: https://www.bka.de/SharedDocs/Kurzmeldungen/DE/Warnhinweise/200317_CoronaEnkeltrick.html.

[36] A. Henkel und L. Stuckenberg, *Tatort Telefon - Wie falsche Polizisten Millionen erbeuten*, 2023. Adresse: https://www.ndr.de/fernsehen/programm/epg/Tatort-Telefon-Wie-falsche-Polizisten-Millionen-erbeuten,sendung1314030.html.

[37] Microsoft, Hrsg., *Schützen Sie sich vor Betrugsversuchen im Zusammenhang mit dem technischen Support - Microsoft-Support*, 18.04.2023. Adresse: https://support.microsoft.com/de-de/windows/sch%C3%BCtzen-sie-sich-vor-betrugsversuchen-im-zusammenhang-mit-dem-technischen-support-2ebf91bd-f94c-2a8a-e541-f5c800d18435.

[38] Bundesamt für Sicherheit in der Informationstechnik, *APT*, 12.03.2021. Adresse: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Gefaehrdungen/APT/apt_node.html.

[39] A. Hatfield, „Phoney Business: Successful Caller ID Spoofing Regulation Requires More Than the Truth in Caller ID Act of 2009“, *Journal of Law and Policy*, Nr. 19, S. 827–865, 2011. Adresse: https://brooklynworks.brooklaw.edu/jlp/vol19/iss2/7/.

[40] Bundesrepublik Deutschland, *§ 3 Telekommunikationsgesetz - Begriffsbestimmungen: § 3 TKG - Begriffsbestimmungen*, 1.08.2022. Adresse: https://dejure.org/gesetze/TKG/3.html.

[41] Bundesnetzagentur, *Bundesnetzagentur - Aufgaben und Struktur*, 20.01.2023. Adresse: https://www.bundesnetzagentur.de/DE/Allgemeines/DieBundesnetzagentur/AufgabenStruktur/start.html.

[42] Bundesrepublik Deutschland, *§ 1 Telekommunikationsgesetz - Zweck des Gesetzes, Anwendungsbereich: § 1 TKG - Zweck des Gesetzes, Anwendungsbereich*, 1.08.2022. Adresse: https://dejure.org/gesetze/TKG/1.html.

[43] Bundesrepublik Deutschland, *Telekommunikationsgesetz: TKG*, 1.08.2022. Adresse: https://www.gesetze-im-internet.de/tkg_2021/TKG.pdf.

[44] Bundesrepublik Deutschland, *§ 120 Telekommunikationsgesetz - Rufnummernübermittlung: § 120 TKG - Rufnummernübermittlung*, 1.08.2022. Adresse: http://www.gesetze-im-internet.de/tkg_2021/__120.html.

[45] Bundesnetzagentur, *Ping/Lock-Anrufe*, 21.01.2023. Adresse: https://www.bundesnetzagentur.de/DE/Vportal/TK/Aerger/Faelle/Ping/start.html.

[46] Bundesrepublik Deutschland, *§ 123 Telekommunikationsgesetz - Befugnisse der Bundesnetzagentur: § 123 TKG - Befugnisse der Bundesnetzagentur*, 1.08.2022. Adresse: http://www.gesetze-im-internet.de/tkg_2021/__123.html.

[47] United States Congress, *Truth in Caller ID Act of 2009*, 22.12.2010. Adresse: https://www.congress.gov/bill/111th-congress/senate-bill/30.

[48] P. Watzlawick, J. H. Beavin und D. D. Jackson, *Menschliche Kommunikation: Formen, Störungen, Paradoxien*, 1. Aufl. s.l.: Hogrefe Verlag Bern (ehemals Hans Huber), 2016, ISBN: 978-3-456-85745-9. Adresse: http://ebooks.ciando.com/book/index.cfm?bok_id/2240200.

[49] Stadtarchiv Bonn, „Was willst du mir damit sagen? Die Geschichte der Kommunikation: Eine Austeilung zum Tag der Archive“, 2020. Adresse: https://www.bonn.de/medien-global/amt-41/stadtarchiv/Ausstellung_Geschichte_der_Kommunikation.pdf.

[50] A. Badach, *Voice over IP - Die Technik: Grundlagen, Protokolle, Anwendungen, Migration, Sicherheit, Notrufdienste, Videotelefonie* (Hanser eLibrary), 5., erweiterte Auflage. München: Hanser, 2022, ISBN: 9783446471504. DOI: 10.3139/9783446471504. Adresse: https://www.hanser-elibrary.com/doi/book/10.3139/9783446471504.

[51] D. Linnemann und J. Gerchow, Hrsg., *Damenwahl! 100 Jahre Frauenwahlrecht* (Schriften des Historischen Museums Frankfurt am Main). Frankfurt am Main: Societäts-Verlag, 2018, Bd. Band 36, ISBN: 978-3-95542-306-3. Adresse: https://portal.dnb.de/opac/mvb/cover?isbn=978-3-95542-306-3.

[52] Deutsche Telekom AG, *Vom Hebdrehwähler bis zum Smartphone: Meilensteine aus 150 Jahren Telefon*, 2011. Adresse: https://www.telekom.com/de/medien/medieninformationen/detail/vom-hebdrehwaehler-bis-zum-smartphone-meilensteine-aus-150-jahren-telefon-333532.

[53] M. Sauter, *Grundkurs mobile Kommunikationssysteme: LTE-Advanced Pro, UMTS, HSPA, GSM, GPRS, Wireless LAN und Bluetooth*, 7. Auflage. Wiesbaden und Heidelberg: Springer Vieweg, 2018, ISBN: 978-3-658-21646-7.

[54] Deutsche Telekom AG, *LTE: Wie es funktioniert. Was es kann. Wo es verfügbar ist*, 2020. Adresse: https://www.telekom.com/de/konzern/details/die-neun-wichtigsten-fakten-zu-lte-604990.

[55] Deutsche Telekom AG, *Telekom erklärt, wie eine Vermittlungsstelle funktioniert*, Deutsche Telekom AG, Hrsg., 2016. Adresse: https://www.telekom.com/de/blog/netz/artikel/telekom-erklaert-wie-eine-vermittlungsstelle-funktioniert-65588.

[56] International Telecommunication Union, Hrsg., *Integrated Services Digital Network (ISDN) Service Capabilities: Definition of Supplementary Services*, Melbourne, 1988. Adresse: https://www.itu.int/rec/T-REC-I.250/_page.print.

[57] U. Trick und F. Weber, *SIP und Telekommunikationsnetze: Next Generation Networks und Multimedia over IP - konkret*, 5., überarb. und erw. Aufl. München: De Gruyter Oldenbourg, 2015, ISBN: 978-3-486-77853-3.

[58] International Telecommunication Union, Hrsg., *Stage 3 description for number identification supplementary services using Signalling System No. 7 – Calling line identification presentation*, 2019. Adresse: https://www.itu.int/rec/T-REC-Q.731.3.

[59] International Telecommunication Union, Hrsg., *Stage 3 description for number identification supplementary services using Signalling System No. 7 – Calling line identification presentation*, 2019. Adresse: https://www.itu.int/rec/T-REC-Q.731.4.

[60] fonial, „CLIP no-screening“, *Fonial*, 28.09.2018. Adresse: https://www.fonial.de/wissen/begriff/clip-no-screening/.

[61] M. Ehlers, *CLIP no screening schnell und einfach erklärt*, easybell, Hrsg., 2021. Adresse: https://www.easybell.de/wissen/clip-no-screening-erklaert/.

[62] P. Schnabel, *Netzwerktechnik-Fibel: Grundlagen Netzwerktechnik, Übertragungstechnik, TCP/IP, Anwendungen und Dienste, Netzwerk-Sicherheit*, 4., überarbeitete Auflage. Ludwigsburg: Patrick Schnabel, September 2016, ISBN: 9783833416811.

[63] Elektronik-Kompendium, Hrsg., *H.323 (Voice over IP)*, 18.04.2023. Adresse: https://www.elektronik-kompendium.de/sites/net/0905101.htm.

[64] Elektronik-Kompendium, *AES - Advanced Encryption Standard*, Elektronik-Kompendium, Hrsg., 6.04.2023. Adresse: https://www.elektronik-kompendium.de/sites/net/1901171.htm.

[65] *Bundesnetzagentur - Verzeichnisse zu Ortsnetzen*, 23.03.2023. Adresse: https://www.bundesnetzagentur.de/DE/Fachthemen/Telekommunikation/Nummerierung/ON_Verzeichnisse_RNB/ONverzeichnisse_node.html.

[66] J. Schmitz, „Das Geheimnis der VoIP Rufnummern“, *Fonial*, 17.10.2016. Adresse: https://www.fonial.de/blog/artikel/lesen/das-geheimnis-der-voip-rufnummern-240/.

[67] iana, *ARPA Domain*, iana, Hrsg., 10.03.2023. Adresse: https://www.iana.org/domains/arpa.

[68] RIPE NCC, *About Us — RIPE Network Coordination Centre*, RIPE NCC, Hrsg., 10.03.2023. Adresse: https://www.ripe.net/about-us.

[69] I. Lazar, „H.323 versus SIP: Was ist der Unterschied?“, *ComputerWeekly.com/de*, 11.05.2017. Adresse: https://www.computerweekly.com/de/antwort/H323-versus-SIP-Was-ist-der-Unterschied.

[70] A. Donner und S. Luber, „Was ist SIP?“, *IP-Insider*, 1.08.2018. Adresse: https://www.ip-insider.de/was-ist-sip-a-663855/.

[71] M. Raußen, *Was ist eine PBX? Cloud-PBX? Hosted PBX? Vorteile, Funktion, FAQ*, Placetel, Hrsg., 18.04.2023. Adresse: https://www.placetel.de/ratgeber/cloud-ip-hosted-pbx-telefonanlage.

[72] B. Lutkevich und J. Scarpati, *SIP (Session Initiation Protocol)*, ComputerWeekly, Hrsg., 2022.

[73] I. Bauer, „Was ist ein Softphone?“, *heise online*, 13.11.2019. Adresse: https://www.heise.de/tipps-tricks/Was-ist-ein-Softphone-4585247.html.

[74] FRITZ!Box, *So funktioniert Voice over IP (VoIP)*, FRITZ!Box, Hrsg., YouTube, 2021. Adresse: https://www.youtube.com/watch?v=9-s4UVYs3VQ.

[75] Network Working Group, Hrsg., *Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks*, 2002. Adresse: https://www.ietf.org/rfc/rfc3325.txt.

[76] 3CX.de, *SIP-Telefonie: Gesprächsabwicklung per SIP*, 19.07.2022. Adresse: https://www.3cx.de/voip-sip/aufbau-sip-gespraech/.

[77] J. Peterson, *A Privacy Mechanism for the Session Initiation Protocol (SIP)*, Institute of Electrical and Electronics Engineers, Hrsg., 2002. DOI: 10.17487/RFC3323. Adresse: https://www.rfc-editor.org/rfc/rfc3323.html.

[78] A. Donner und S. Luber, „Was ist ein Router?“, *IP-Insider*, 15.08.2018. Adresse: https://www.ip-insider.de/was-ist-ein-router-a-751339/.

[79] C. Jennings, J. Peterson und Watson M., *Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks*, Institute of Electrical and Electronics Engineers, Hrsg., 2002. DOI: 10.17487/RFC3325. Adresse: https://www.rfc-editor.org/rfc/rfc3325.html.

[80] J. Song, H. Kim und A. Gkelias, „iVisher: Real-Time Detection of Caller ID Spoofing“, *ETRI Journal*, Jg. 36, Nr. 5, S. 865–875, 2014, ISSN: 1225-6463. DOI: 10.4218/etrij.14.0113.0798. Adresse: https://onlinelibrary.wiley.com/doi/full/10.4218/etrij.14.0113.0798.

[81] Oracle, *Oracle VM VirtualBox*, Oracle, Hrsg., 26.04.2023. Adresse: https://www.virtualbox.org/.

[82] Ubuntu, *Enterprise Open Source and Linux | Ubuntu*, Ubuntu, Hrsg., 26.04.2023. Adresse: https://ubuntu.com/.

[83] Asterisk, *Get Started ⋆ Asterisk*, Asterisk, Hrsg., 7.04.2021. Adresse: https://www.asterisk.org/get-started/.

[84] TechMaxim, *Easily Spoof Your Phone Number in Minutes - Setup Guide*, 2023. Adresse: https://www.youtube.com/watch?v=1jSNp9mBswA.

[85] CounterPath, *Products – Bria Solo*, CounterPath, Hrsg., 19.04.2022. Adresse: https://www.counterpath.com/bria-solo/.

[86] sipgate GmbH, *Wir sind sipgate*, 6.04.2023. Adresse: https://hello.sipgate.de/wir-sind-sipgate.

[87] sipgate Hilfecenter, *Verifizierung Ihres Unternehmensstandorts*, 2022. Adresse: https://help.sipgate.de/hc/de/articles/360019995317-Verifizierung-Ihres-Unternehmensstandorts.

[88] Bundesrepublik Deutschland, *§ 170 Telekommunikationsgesetz - Umsetzung von Überwachungsmaßnahmen, Erteilung von Auskünften: § 170 TKG - Umsetzung von Überwachungsmaßnahmen, Erteilung von Auskünften*, 1.08.2022. Adresse: https://www.gesetze-im-internet.de/tkg_2021/__170.html.

[89] TempMail, *Temporäre E-Mail - Einweg-Mail - Anonyme Mail*, TempMail, Hrsg., 27.04.2023. Adresse: https://temp-mail.org/de/.

[90] Receive SMS Online, *Receive SMS online | Temporary Phone Number*, Receive SMS Online, Hrsg., 27.04.2023. Adresse: https://receive-smss.com/.

[91] *About Us | SpoofCard*, 17.04.2023. Adresse: https://www.spoofcard.com/about.

[92] SpoofCard, *Terms of Service | SpoofCard*, 17.04.2023. Adresse: https://www.spoofcard.com/terms.

[93] D. Hayon, *App ersetzt SIM-Karte: mypio vergibt deutsche Nummer auf Knopfdruck - CHIP*, Chip Online, Hrsg., 2018. Adresse: https://www.chip.de/news/mypio-vergibt-deutsche-Nummer-auf-Knopfdruck-Neue-App-ersetzt-SIM-Karte_148497914.html.

[94] Elektronik-Kompendium, *eSIM - Embedded Subscriber Identity Modul*, Elektronik-Kompendium, Hrsg., 17.04.2023. Adresse: https://www.elektronik-kompendium.de/sites/kom/2109131.htm.

[95] Bundesnetzagentur, *Manipulation von Rufnummern*, 7.02.2023. Adresse: https://www.bundesnetzagentur.de/DE/Vportal/TK/Aerger/Faelle/Manipulation/start.html;jsessionid=9C02FD5C07C0212CA7B746F6C5E493CB.

[96] Elektronik-Kompendium, Hrsg., *Telefonnetz / Festnetz*, 20.04.2023. Adresse: https://www.elektronik-kompendium.de/sites/kom/0312101.htm.

[97] Federal Communications Commission, Hrsg., *Combating Spoofed Robocalls with Caller ID Authentication*, 24.04.2023. Adresse: https://www.fcc.gov/call-authentication.

[98] TransNexus, *Understanding STIR/SHAKEN*, TransNexus, Hrsg., 21.04.2023. Adresse: https://transnexus.com/whitepapers/understanding-stir-shaken/.

[99] H. Deng, W. Wang und C. Peng, „CEIVE“, in *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking*, R. Shorey, Hrsg., Ser. ACM Conferences, New York, NY: ACM, 2018, S. 369–384, ISBN: 9781450359030. DOI: 10.1145/3241539.3241573.

[100] H. Mustafa, W. Xu, A.-R. Sadeghi und S. Schulz, „End-to-End Detection of Caller ID Spoofing Attacks“, *IEEE Transactions on Dependable and Secure Computing*, Jg. 15, Nr. 3, S. 423–436, 2018, ISSN: 1545-5971. DOI: 10.1109/TDSC.2016.2580509.

[101] J. Li, F. Faria, J. Chen und D. Liang, „A Mechanism to Authenticate Caller ID“, in *Recent Advances in Information Systems and Technologies*, S. 745–753. DOI: 10.1007/978-3-319-56538-5{\textunderscore}75. Adresse: https://link.springer.com/chapter/10.1007/978-3-319-56538-5_75.

[102] M. Hansen, M. Hansen, J. Möller, T. Rohwer, C. Tolkmit und H. Waack, „Developing a Legally Compliant Reachability Management System as a Countermeasure against SPIT“, *Third Annual VoIP Security Workshop*, 2006. Adresse: https://www.semanticscholar.org/paper/Developing-a-Legally-Compliant-Reachability-System-Hansen-Hansen/03beaf08b0764e93a80834875b52bc2670620a54.

[103] J. Quittek, S. Niccolini, S. Tartarelli, M. Stiemerling, M. Brunner und T. Ewald, „Detecting SPIT Calls by Checking Human Communication Patterns“, in *2007 IEEE International Conference on Communications*, IEEE, 6/24/2007 - 6/28/2007, S. 1979–1984, ISBN: 1-4244-0353-7. DOI: 10.1109/ICC.2007.329.

[104] J. Chaudhry und C. Shafique, „Secure Calls and Caller ID Spoofing Countermeasures Towards building a Cyber Smart Societies“, *International Conference on Recent Advances in Computer Systems*, S. 169–172, 2015, ISSN: 2352-538X. DOI: 10.2991/racs-15.2016.29. Adresse: https://www.atlantis-press.com/proceedings/racs-15/25847802.

[105] K. Weber, A. Schütz und T. Fertig, *Grundlagen und Anwendung von Information Security Awareness: Mitarbeiter zielgerichtet für Informationssicherheit sensibilisieren* (Springer eBooks Computer Science and Engineering). Wiesbaden: Springer Vieweg, 2019, ISBN: 978-3-658-26257-0. DOI: 10.1007/978-3-658-26258-7.

[106] Bundesnetzagentur, *Aktueller Hinweis - Anstieg von Anrufen ohne angezeigte Rufnummer*, 2022. Adresse: https://www.bundesnetzagentur.de/DE/Vportal/TK/Aerger/Aktuelles/Hinweise_aktuell/AktHinw2022/Anstieg_unbekannte_Anrufe.html.

[107] Florian Meyer, Hrsg., *Masterarbeit Caller ID Spoofing: e-Mail*, 1.02.2023.

[108] Deutscher Bundestag, „„Auslandskopfüberwachung“ in der Telekommunikations- Überwachungsverordnung (TKÜV): Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Rainer Funke, Rainer Brüderle, Hans-Joachim Otto (Frankfurt), weiterer Abgeordneter und der Fraktion der FDP – Drucksache 15/5164 –“, *Drucksache 15/5199*, Adresse: https://dserver.bundestag.de/btd/15/051/1505199.pdf.

[109] „authentisch“, *Duden.de*, 24.04.2018. Adresse: https://www.duden.de/rechtschreibung/authentisch.

[110] D. Kochheim, *Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik* (Beck-online Bücher), 2. Auflage. München: C.H. Beck, 2018, ISBN: 9783406728686. Adresse: https://beck-online.beck.de/?vpath=bibdata/komm/KochheimHdbStrafR_2/cont/KochheimHdbStrafR.htm.

[111] Ben Cost, „AI clones teen girl's voice in $1M kidnapping scam: 'I've got your daughter'“, *New York Post*, 12.04.2023. Adresse: https://nypost.com/2023/04/12/ai-clones-teen-girls-voice-in-1m-kidnapping-scam/.

Eidesstattliche Erklärung

Hiermit versichere ich – Florian Meyer – an Eides statt, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Quellen und Hilfsmittel angefertigt habe.

Sämtliche Stellen der Arbeit, die im Wortlaut oder dem Sinn nach Publikationen oder Vorträgen anderer Autoren entnommen sind, habe ich als solche kenntlich gemacht.

Diese Arbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt oder anderweitig veröffentlicht.

Mittweida, 05. Mai 2023	
Ort, Datum	Florian Meyer, B.Sc.