



## 2. Studienprojekt

# Die Welt der Nachrichten und die Nachrichten der Welt

von E-Mail bis Telegram

Name, Vorname: Knothe, Marvin und Zhang, Yüxi  
Matrikelnummer: 640199 und 684163  
Studienjahrgang: 2020  
Fachbereich: Duales Studium Wirtschaft • Technik  
Studiengang: Informatik  
Modul: Studienprojekt II - 5. Semester  
Betreuer Hochschule: Prof. Dr. Arthur Zimmermann  
Anzahl der Wörter: 5517

20.02.2023,

*Knothe*

20.02.2023,

.....  
(Datum/Unterschrift Marvin Knothe)

.....  
(Datum/Unterschrift Yüxi Zhang)



*Kurzzusammenfassung (Abstract)*

---

**Kurzzusammenfassung**

Das Ziel dieser wissenschaftlichen Arbeit besteht darin, die wichtigsten Charakteristiken jeder Art von Nachrichten herauszuarbeiten. Aufgrund der Tatsache, dass Nachrichten heutzutage immer über Netzwerke übertragen werden, wird auf die verschiedenen Übertragungsprotokolle eingegangen. Es wird die Funktionsweise und der Anwendungszweck der Protokolle erläutert. Ein besonderes Augenmerk wird dabei auch auf die Aspekte der Sicherheit gelegt, weshalb zwei Verschlüsselungsmethoden kurz vorgestellt werden. Abschließend wird anhand eines praktischen Beispiels ein Übertragungsprotokoll detaillierter erläutert.

**Abstract**

The aim of this scientific work is to elaborate the main characteristics of each type of messages. Due to the fact that nowadays messages are always transmitted over networks, the different transmission protocols will be discussed. The functioning and the application purpose of the protocols will be explained. Special attention is also paid to the aspects of security, which is why two encryption methods are briefly presented. Finally, a transmission protocol is explained in more detail using a practical example.



## **Inhaltsverzeichnis**

<b>I. Abbildungsverzeichnis .....</b>	<b>II</b>
<b>II. Abkürzungsverzeichnis .....</b>	<b>II</b>
<b>1. Einleitung .....</b>	<b>1</b>
<b>2. Theoretische Grundlagen von Nachrichten .....</b>	<b>2</b>
2.1 Definition.....	2
2.2 Arten von Nachrichten.....	3
2.2.1 Short-Message-Service (SMS) .....	4
2.2.2 E-Mail.....	6
2.2.3 Instant Messenger .....	7
<b>3. Übertragungsprotokolle.....</b>	<b>8</b>
3.1 HTTP .....	8
3.2 SMTP.....	10
3.3 POP3.....	11
3.4 IMAP .....	12
3.5 SSH.....	14
3.6 XMPP .....	15
3.7 MTPProto .....	15
<b>4. Sicherheit und Verschlüsselung .....</b>	<b>16</b>
4.1 Transportverschlüsselung .....	17
4.2 Ende-zu-Ende Verschlüsselung .....	17
<b>5. Anforderungsanalyse .....</b>	<b>18</b>
<b>6. Konzept.....</b>	<b>19</b>
<b>7. Durchführung .....</b>	<b>20</b>
<b>8. Evaluation .....</b>	<b>24</b>
<b>9. Fazit und Ausblick.....</b>	<b>25</b>
<b>10. Literaturverzeichnis .....</b>	<b>26</b>
<b>11. Eidesstaatliche Erklärung.....</b>	<b>29</b>



## **I. Abbildungsverzeichnis**

Abbildung 1: Verlauf einer versendeten SMS eines Handys (bzw. Mobiltelefon) .....	4
Abbildung 2: Informationsaustausch bei einer SSH-Verbindung .....	19
Abbildung 3: PuTTY Konfiguration mit Verbindung auf den Stratoserver.....	20
Abbildung 4: Log-Datei der Schlüsselaustauschmethode .....	21
Abbildung 5: NTRU-Prime / Curve 25519 – Paketaustausch zwischen SSH-Client und SSH-Server.....	22
Abbildung 6: Prozess der Serviceanfrage zwischen SSH-Client und SSH-Server .....	22
Abbildung 7: Befehl "who" in der Kommandozeile nach erfolgreicher SSH-Verbindung .....	23

## **II. Abkürzungsverzeichnis**

Base Station Controller - BSC.....	4
Home Location Register - HLR.....	4
Instant Messengern - IM.....	7
Internet Message Access Protocol - IMAP.....	6
Mail Transfer Agent - MTA .....	10
Post Office Protocol - POP .....	11
Short-Message-Service - SMS.....	4
Simple-Mail-Transfer-Protocol - SMTP .....	6
SSH - Secure Socket Shell .....	1
Transaktionsnummer - TAN.....	4
Transport Layer Security - TLS.....	16



## *1. Einleitung*

---

### **1. Einleitung**

In den letzten Jahren hat im Zuge der Digitalisierung die Anzahl der verschickten Nachrichten aufgrund der Verbreitung von mobilen Messaging-Apps einen beeindruckenden Anstieg erfahren. Eine der am häufigsten genutzten Apps in diesem Bereich ist WhatsApp. Sie bieten einen kostenlosen, werbefreien und kommerziellen Messaging-Dienst und hat somit einen wichtigen Anteil an der zunehmenden Popularität von mobilen Messaging-Apps. Die Anwendung wird von über einer Milliarde Nutzern in 180 Ländern verwendet. [Kau19] Laut einer Studie von Statista wurden im Jahr 2011 weltweit ungefähr eine Milliarde WhatsApp-Nachrichten täglich verschickt. Diese Zahl ist neun Jahre später bereits auf 100 Milliarden gestiegen. [Rab21] Diese Entwicklung zeigt deutlich, wie wichtig die Kommunikation in der digitalen Welt geworden ist.

Aufgrund dieser Tatsache wird, im Rahmen eines Studienprojektes an der Hochschule für Wirtschaft und Recht Berlin wird die Welt der Nachrichten und die Nachrichten der Welt von E-Mail bis Telegram untersucht. Dabei werden die Transportprotokolle, die für die Übertragung dieser Nachrichten verwendet werden, betrachtet und deren Bedeutung und Anwendung diskutiert. Das SSH-Protokoll wird an einem Beispiel ausgeführt und dessen einzelnen Komponenten detailliert erläutert. Durch die Untersuchung dieser Protokolle wird ein tieferes Verständnis für die Technologien, die hinter der Übertragung von Nachrichten stehen, erlangt.



## *2. Theoretische Grundlagen von Nachrichten*

---

## **2. Theoretische Grundlagen von Nachrichten**

### **2.1 Definition**

In verschiedenen Fachgebieten hat der Begriff „Nachricht“ unterschiedliche Bedeutungen. Im Bereich des Journalismus bezieht sich der Begriff auf Neuigkeiten und die Vermittlung von relevanten Informationen und Fakten eines Ereignisses. [Spr10] In der Informatik bezieht sich der Begriff auf die Menge an Daten, die als Signal und Bedeutungsträger von einem Absender ausgesendet werden. [Ben20] (S.37)

In dieser wissenschaftlichen Arbeit wird der Begriff „Nachricht“ als Mitteilung definiert, die von einer Person oder einem System an eine andere Person oder ein anderes System übermittelt wird. [Rup14] (S. 1) Der Fokus liegt auf digitalen Nachrichten, die in Form einer Textnachricht, Sprachnachricht, E-Mail, Mediendatei oder anderen Art von Daten vorliegen.

In Bezug auf die Übertragung von Nachrichten wird zwischen synchroner und asynchroner Übertragung unterschieden. Bei synchroner Übertragung sind Absender und Empfänger gleichzeitig online und die Nachricht wird in Echtzeit übertragen, beispielsweise bei einem Telefonat oder einer Videokonferenz. Im Gegensatz dazu bedeutet eine asynchrone Übertragung, dass Absender und Empfänger nicht gleichzeitig online sind und die Nachricht zu einem späteren Zeitpunkt gelesen werden kann, wie zum Beispiel bei E-Mails oder Nachrichten in sozialen Medien. [Bru06] (S.10)



## *2. Theoretische Grundlagen von Nachrichten*

---

### **2.2 Arten von Nachrichten**

In diversen Kontexten werden unterschiedliche Arten von Nachrichten verwendet, um Informationen und Botschaften auszutauschen. Zu beachten ist, dass jede Art von Nachricht eine Form der Kommunikation darstellt. Kommunikation ist ein Vorgang bei dem mindestens zwei Partner beteiligt sind und Nachrichten übergeben oder ausgetauscht werden. Diese Partner können Menschen, Tiere, Maschinen und andere Individuen und Objekte sein. [Rup14] (S. 1)

Verbale Nachrichten, bei denen Worte zur Übertragung von Informationen genutzt werden, sind eine der wichtigsten Formen von Kommunikation. [Bru06] (S.10)  
Diese Art der Informationsvermittlung kann in mündlicher oder schriftlicher Form stattfinden. [Arg13] (S.11-13)

Nonverbale Kommunikation hingegen beschreibt die Übertragung von Informationen ohne Worte, beispielsweise durch Gesten, Mimik, Körpersprache oder andere Formen von nonverbalem Verhalten. Diese Art der Kommunikation kann bewusst als auch unbewusst erfolgen und spielt eine wichtige Rolle bei der Vermittlung von Bedeutungen und Emotionen. [Arg13] (S.11-13)

Neben anderen Arten von Nachrichten wie medialen Nachrichten, die im Fernsehen oder Radio übertragen werden, liegt der Fokus dieser wissenschaftlichen Arbeit auf digitalen Nachrichten wie E-Mails, SMS und Instant Messenger-Diensten. Diese Art des Informationsaustausches ermöglicht es Menschen effizient und komfortabel miteinander zu kommunizieren, unabhängig von zeitlichen oder räumlichen Einschränkungen.

## 2. Theoretische Grundlagen von Nachrichten

### 2.2.1 Short-Message-Service (SMS)

Eine Untersuchung in Deutschland im Jahr 2013 mit einer Stichprobe von 2000 Teilnehmern zeigte, dass 69% der Befragten den Short-Message-Service (SMS) als bevorzugte Art der Mobilkommunikation ansahen, gefolgt von E-Mail mit 37% und Mobile Instant Messaging mit 24% Beliebtheit. Allerdings hat im Jahr 2017 die Dominanz von Instant-Messenger-Diensten wie WhatsApp die SMS als beliebteste Form der Kommunikation abgelöst. Der Anteil der SMS ist auf 38% gesunken und E-Mails konnten einen Anstieg auf 60% verzeichnen. [Nie17] SMS werden heutzutage oft im Zusammenhang mit Login-Verfahren (Zwei-Faktor-Authentifizierung) oder bei Überweisungen zum Zusenden einer Transaktionsnummer (TAN) genutzt.

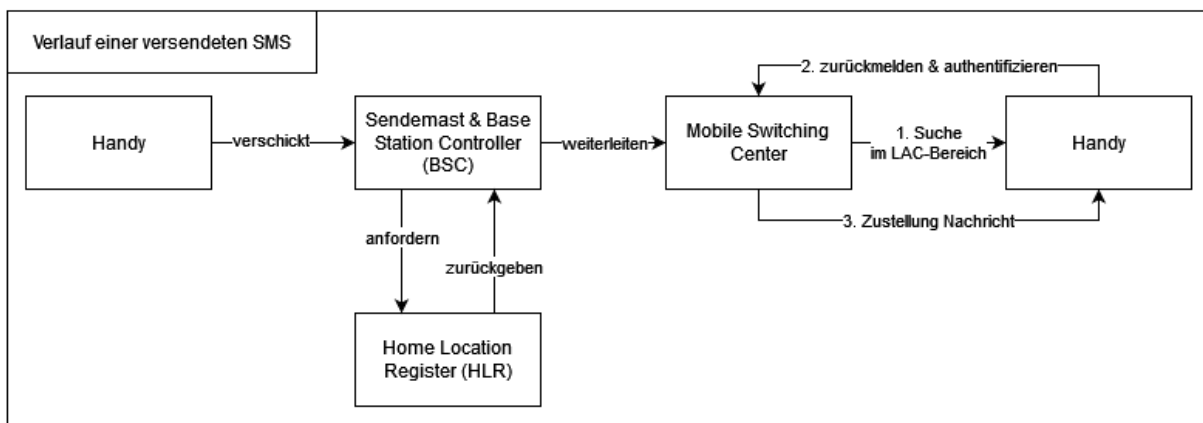


Abbildung 1: Verlauf einer versendeten SMS eines Handys (bzw. Mobiltelefon)

Die Übertragung von SMS erfolgt über Mobilfunkdienste und beginnt mit dem Versenden (siehe Abbildung 1, S.4). Die Nachricht gelangt zunächst zu einem Sendemast und wird von einem Base Station Controller (BSC) zum SMS-Center des eigenen Netzbetreibers weitergeleitet. Das SMS-Center fordert Informationen vom Home Location Register (HLR) an, um den Empfänger zu identifizieren. Die SMS und die Zusatzinformationen werden an das Mobile Switching Center weitergeleitet, welches den Empfänger bedient. Diese Vermittlungsstelle sendet einen Ausruf an mehrere Sendemasten, den sogenannten LAC-Bereich, um das Handy des Empfängers zu erreichen. Sobald das Handy sich zurückmeldet, authentifiziert es sich und erhält die SMS. Wenn die Zustellung nicht möglich ist, wird die SMS





## 2. Theoretische Grundlagen von Nachrichten

vom SMS-Center gespeichert und bei wiederhergestellter Netzverbindung erneut zugestellt.  
[Gaj]

Die Verwendung von SMS bietet sowohl Vorteile als auch Nachteile. Die Verwendung von SMS im Rahmen von Überweisungen oder Login-Verfahren sichert ab, dass die richtige Person die Nachricht erhält. Die Übertragung erfolgt über Mobilfunkdienste, wodurch eine hohe Netzabdeckung und Erreichbarkeit gegeben und keine stabile Internetverbindung notwendig ist. Eine hohe Erreichbarkeit ist für globale Unternehmen wie Airbnb oder Uber von großer Bedeutung, um Nutzer zu benachrichtigen. [Gaj] SMS werden zudem als seriöser wahrgenommen und werden laut Statistiken öfter geöffnet als andere Textnachrichten. [Ahr19] (S.164) Sehr alte Handys unterstützen diese Übertragungsmöglichkeit, sodass keine Abhängigkeit auf Software-Updates oder Betriebssystem-Support besteht. Im Vergleich zu Instant-Messengern werden keine Nutzerdaten für kommerzielle Zwecke genutzt.

Ein Nachteil von SMS kann in den anfallenden Kosten liegen, die allerdings im Laufe der Zeit deutlich gesunken und durch viele Mobilfunkverträgen abgedeckt sind. Eine chaotische Struktur in der Telekommunikationsbranche führt dazu, dass zahlreiche Netze keine Interoperabilität gewährleisten und somit eine Übertragung von SMS von einem Netz zu einem anderen nicht möglich sind. Darüber hinaus weist die Übertragung der Daten bei SMS ein unzureichendes Schutzniveau auf, wodurch die Möglichkeit für einen Missbrauch gegeben ist. Insbesondere bei der Übertragung sensibler Informationen stellt dies ein Problem dar. Zudem kann es zu Fehlzustellungen oder Verzögerungen bei der Übertragung kommen. Gerade bei wichtigen oder dringenden Nachrichten kann dieses Verfahren bedenklich sein. [Kla17]



## *2. Theoretische Grundlagen von Nachrichten*

---

### 2.2.2 E-Mail

Die elektronische Post, auch bekannt als E-Mail, kann als digitales Äquivalent der herkömmlichen Post betrachtet werden. E-Mails werden von einem Absender mit einer spezifischen Adresse an eine Adresse vom Empfänger gesendet, wobei die E-Mail-Adresse aus einem Lokalteil, einem Trennzeichen (meistens das @-Zeichen) und einer Domain besteht.

Der Zugang zum Mail-Server erfolgt in der heutigen Zeit in der Regel über einen Webbrowser, währenddessen früher Softwareclients der Standard waren. Bekannte Beispiele für Webmail-Programme sind Gmail von Google und Hotmail von Microsoft. [Cha14] (S.16-19) Für den Empfang von E-Mails können zwei Protokolle genutzt werden, das Internet Message Access Protocol (IMAP) und das Post Office Protocol (POP). Das Simple-Mail-Transfer-Protocol (SMTP) wird beim Versand von E-Mails verwendet. Weitere Informationen zu diesen Protokollen finden sich in den Kapiteln 3.2 bis 3.4. [Cha14] (S.30)

Die E-Mail bietet einige Vorteile, wie z.B. die kostenlose Registrierung, wodurch eine Versendung von Nachrichten an E-Mail-Adressen weltweit ermöglicht wird. Mittels Mailing-Listen können Nachrichten an mehrere und auch unbekannte Personen gleichzeitig verschickt werden. [Cha14] (S. 28)

Im Vergleich zu Instant Messengern kann der E-Mail-Service als langsamer betrachtet werden, da der Mail-Server nur in bestimmten Intervallen nach eingetroffenen E-Mails sucht und diese anschließend in die Mailbox des Empfängers legt. [Sch98] (S.29) Es gibt jedoch auch einige Nachteile wie z.B. Werbungsangebote und Spam-Mails, die Schadsoftware beinhalten können und nicht nur das eigene Gerät, sondern auch das gesamte Netzwerk in Gefahr bringen können.



## 2. Theoretische Grundlagen von Nachrichten

### 2.2.3 Instant Messenger

In den letzten Jahren hat die Verbreitung von Instant Messengern (IM) zu einem deutlichen Wandel in der Kommunikationslandschaft geführt. Dieser Trend setzt sich im Jahr 2022 fort, wobei WhatsApp in Deutschland als klarer Marktführer unter den Instant Messaging-Diensten hervorsticht. Darauf folgen der Facebook Messenger, FaceTime, Skype, Zoom und Telegram. [Kun22]

IMs sind Echtzeit-Kommunikationsmethoden, die es ermöglichen, Text- und Sprachnachrichten, Fotos, Kontakte, Videos und Audio sowie Standortinformationen zu übertragen. [Meh19] (S.12) Es gibt verschiedene Arten von IMs, darunter klassische Instant-Messaging-Programme wie Slack, mobile Messaging-Lösungen wie WhatsApp, Telegram, Signal oder Facebook Messenger, integrierte Kommunikationsplattformen wie Skype oder Discord und Social-Media-Plattformen wie Facebook, Instagram, Snapchat, Twitter und TikTok. [Gre08] (S. 2 -3)

IMs bieten verschiedene Vorteile, wie zum Beispiel die Möglichkeit, den Online-Status von Empfängern anzuzeigen, Nachrichten an Offline-Empfänger zu senden und mehrere Empfänger gleichzeitig zu kontaktieren. Es kann eine Vielzahl an verschiedenen Dateiformaten übertragen werden. IMs sind einfach und schnell zu nutzen und haben eine weite Verbreitung. [Gre08] (S. 2 -3)

Ein Nachteil einiger Instant Messenger kann die unzureichende Datensicherheit- und Verschlüsselung sein. Zudem sind sie nicht optimal für formelle oder geschäftliche Kommunikation geeignet, da es dazu verleitet, ihre privaten Nachrichten zu überprüfen und zu beantworten, anstatt sich auf andere Dinge zu konzentrieren. Es müssen auch oft die Allgemeinen Geschäftsbedingungen akzeptiert werden, wobei Nutzerdaten für kommerzielle Zwecke verwendet werden können und gespeicherte Telefonnummern unverschlüsselt an Dienstleister-Server übertragen werden. [Tec23]



### *3. Übertragungsprotokolle*

---

## **3. Übertragungsprotokolle**

Übertragungsprotokolle sind essenziell, um die Kommunikation zwischen zwei Systemen zu ermöglichen. Sie liefern die Gesamtheit der Steuerungsverfahren und Betriebsvorschriften einer Datenübertragung. Dies umfasst die Festlegung der spezifischen Formatierung, zeitlichen Abfolge und verwendeten Datenleitungen während des Informationsaustauschs. [wis23]

### **3.1 HTTP**

Hypertext-Transfer-Protocol (HTTP) ist das weitverbreitetste Anwendungsschicht-Protokoll im Internet. Es wird für die Kommunikation zwischen einem Webserver und einem Webbrowser verwendet und entspricht dem klassischen Client-Server-Modell. Es wird eine Verbindung vom Browser (Client) zum Server hergestellt, um eine Anfrage zu stellen. Der Client wartet, auf eine Antwort vom Server, woraufhin anschließend die Verbindung geschlossen wird. Da der Server zwischen den Anfragen keine Daten speichert, wird HTTP auch als "stateless protocol" bezeichnet. [MDN221]

Eine Anfrage an den Server besteht aus mehreren Bestandteilen, darunter eine Anfangszeile mit einer HTTP-Methode, einem Pfad und der verwendeten HTTP-Version. Die Methode beschreibt die Absicht der Anfrage, wobei die am häufigsten verwendeten Methoden GET, POST, PUT und DELETE sind. Eine GET-Anfrage deutet darauf hin, dass zum Beispiel Daten vom Server bereitgestellt werden sollen, um sie im Browser anzuzeigen. Währenddessen werden bei einer POST-Anfrage in der Regel Daten mitgeschickt, um sie auf dem Server zu speichern oder weiter zu verarbeiten.

Der Pfad kann ein absoluter Pfad sein, der auf eine Datei verweist oder direkt aus einer vollständigen URL bestehen. Zusätzlich kann am Ende des Pfades noch ein Query-String angehängt werden, um weitere Parameter anzugeben. Die Trennung zwischen Pfad oder URL und dem Query-String erfolgt durch ein Fragezeichen-Symbol („?“). [MDN22] (Abschnitt HTTP Requests)



### *3. Übertragungsprotokolle*

---

Ein weiterer Bestandteil ist der HTTP-Header, welcher die Möglichkeit bietet, weitere Informationen zwischen dem Client und dem Server auszutauschen. Ein Header besteht aus einem String, gefolgt von einem Doppelpunkt Symbol (,,:“) und einem Inhalt, dessen Format vom Header selbst abhängt [MDN22] (Abschnitt Headers in HTTP Requests)

Der letzte Bestandteil einer Anfrage ist der Body, der jedoch nicht von allen HTTP-Methoden verwendet wird, wie zum Beispiel GET oder DELETE. Der Body kann aus einer einzigen Datei bestehen oder aus mehreren Ressourcen, die durch die Header "Content-Type" und "Content-Length" näher definiert werden. [MDN22] (Abschnitt Body in HTTP Requests)

Eine HTTP-Antwort besteht aus mehreren Bestandteilen, darunter einer Statuszeile, die aus der HTTP-Version, einem dreistelligen Statuscode und einem kurzen Statustext besteht. Der Statuscode kann anhand der ersten Zahl in mehrere Gruppen unterteilt werden. Statuscodes, die mit einer eins beginnen, beschreiben informative Antworten. Wenn der Statuscode mit einer zwei beginnt, wurde die Aufgabe erfolgreich ausgeführt, während ein Statuscode mit einer drei auf eine Umleitung hinweist. Wenn ein Statuscode mit einer vier oder fünf anfängt, trat bei der Verarbeitung ein Fehler auf, wobei die vier einen Client-Fehler und die fünf einen Server-Fehler beschreibt. [MDN22] (Abschnitt Status line in HTTP Responses)

Es gibt Situationen, in denen nur Ressourcen auf dem Server erstellt werden, ohne dass diese an den Client zurückgegeben werden müssen. Falls es einen Body gibt, können die beiden Arten, die es auch bei Anfragen gibt, zum Einsatz kommen. Allerdings besteht ein Unterschied darin, ob die Länge der Datei bekannt ist oder nicht. Wenn die Länge bekannt ist, werden wie bei Anfragen die Header "Content-Type" und "Content-Length" verwendet. Falls die Länge jedoch nicht bekannt ist, wird die Datei in "chunks" verschlüsselt und der "Transfer-Encoding"-Header auf "chunked" gesetzt. [MDN22] (Abschnitt Body in HTTP Responses)



### 3. Übertragungsprotokolle

---

#### 3.2 **SMTP**

SMTP oder auch als „Simple Mail Transfer Protocol“ bekannt, ist ein E-Mail-Transferprotokoll, welches wie HTTP zur Familie der Anwendungsschicht-Protokolle gehört. SMTP stellt ein essenzieller Bestandteil der heutigen E-Mail-Kommunikation dar. Dadurch wird einem Server, E-Mails von einem Client zu empfangen und anschließend an den Zielservers weiterzuleiten.

Jeder E-Mail-Anbieter wie Gmail, Web.de oder Yahoo verfügt über einen Postausgangsserver, der auch als SMTP-Server bezeichnet wird. Auf diesen Servern werden die E-Mails vom SMTP-Client, also dem Absender, geladen. Anschließend kontaktiert der SMTP-Server den DNS-Server, um die IP-Adresse des Ziel-SMTP-Servers zu ermitteln, der anhand der Empfängeradresse der E-Mail bestimmt wird. Ein Mail Transfer Agent (MTA) ist ein Mail-Server, der sicherstellt, dass die E-Mail an ihren Ziel-Server gelangt. Der Austausch der Daten zwischen den MTAs erfolgt ebenfalls über das SMTP-Protokoll. [JKI08] (Abschnitt 2.1) Sobald die E-Mail ihr Ziel erreicht hat, wird sie temporär im Nachrichtenspeicher des Servers gespeichert, bis sie vom Empfänger per IMAP oder POP3 abgerufen wird.

Eine SMTP-Session bezeichnet die Verbindung zwischen Client und Server. [JKI08] (Abschnitt 3.1) Jeglicher Datenaustausch findet innerhalb einer Session statt, die bei Abschluss des Austauschs wieder geschlossen wird. Um mit dem Server zu kommunizieren, verwendet der Client SMTP-Kommandos wie zum Beispiel „HELO“, „MAIL FROM“ oder „DATA“. Einige der Kommandos benötigen zusätzliche Parameter. Das „MAIL FROM“ Kommando benötigt zusätzlich noch die E-Mail-Adresse des Empfängers, während „DATA“ nicht mit weiteren Informationen an den Server übermittelt wird. Der Server antwortet nach der Verarbeitung eines Kommandos mit einem dreistelligen Statuscode, welchem dem des Webservers ähnlich ist, dort aber andere Bedeutungen hat. Zusätzlich zu dem Statuscode gibt der SMTP-Server auch eine passende Meldung als Klartext wieder. Ein Statuscode, der mit einer zwei beginnt, gibt an, dass das Kommando erfolgreich ausgeführt wurde. Ein häufiges Beispiel ist der Statuscode 205, der signalisiert, dass das Kommando erfolgreich ausgeführt wurde. Wenn ein Statuscode mit einer drei beginnt, benötigt der Server weitere Informationen zur Verarbeitung des Kommandos. Der Code 354 gibt an, dass der Server den Mail Empfang



### 3. Übertragungsprotokolle

vom Client startet und wird immer dann verwendet, wenn der Server das „DATA“ Kommando erhält, da der E-Mail-Inhalt erwartet wird. Statuscodes, die mit einer vier beginnen, geben an, dass der Server einen temporären Fehler festgestellt hat. Das Kommando wurde möglicherweise trotzdem verarbeitet. Ein Beispiel für einen Statuscode dieser Gruppe ist der Code 452, der auftritt, wenn nicht genügend Systemspeicher vorliegt und das Kommando nicht ausgeführt werden konnte. Statuscodes, die mit einer fünf beginnen, signalisieren, dass der Server einen schwerwiegenden Fehler festgestellt hat und das Kommando nicht verarbeiten konnte. Ein Beispiel für einen Statuscode dieser Gruppe ist der Code 502, der zurückgegeben wird, wenn der Server ein Kommando erhält, das nicht existiert. Zusammenfassend besteht eine SMTP-Session aus einer Abfolge von Kommandos, die vom Client an den Server gesendet wird und im Gegenzug jeweils einen Statuscode mit einer Meldung zurückgibt. [JKI08] (Abschnitt 4.2.3)

### **3.3 POP3**

Das Post Office Protocol (POP) ist ein weiteres Protokoll, das in der E-Mail-Kommunikation verwendet wird. Die aktuelle Version von POP ist POP3. Im Gegensatz zu SMTP, welches zum Senden von E-Mails vom Client des Senders über den SMTP-Server des Senders zum Ziel-Server des Empfängers verwendet wird, ermöglicht POP3 das Herunterladen von E-Mails vom Server auf den Client.

Der Austausch von Kommandos und Antworten zwischen dem Client und dem Server erfolgt über den Port 110. Ein POP3-Kommando besteht aus einem Schlüsselwort, das klein- oder großgeschrieben werden kann und in einigen Fällen einen oder mehrere Parameter hat. Jedes Kommando wird mit "CRLF" abgeschlossen, um das Ende des Kommandos zu signalisieren. Beispiele von POP3-Kommandos sind „DELE“, „NOOP“ oder „QUIT“. Das „DELE“-Kommando markiert eine E-Mail zum Löschen, während „NOOP“ keine direkte Funktion besitzt, sondern den Serverstatus überprüft. Das „QUIT“-Kommando wird verwendet, um alle markierten E-Mails zu löschen und die Verbindung zu beenden.



### 3. Übertragungsprotokolle

Während einer Verbindung zum POP3-Server gibt es mehrere Zustände. Der erste Zustand ist der Authentifizierungszustand, in dem der Client seinen Benutzernamen und sein Passwort eingibt. Wenn die Authentifizierung erfolgreich war, sperrt der Server das Postfach und ordnet jeder vorhandenen E-Mail eine Nummer zu. Zusätzlich wird in den Übertragungszustand gewechselt. In diesem Zustand kann mit den E-Mails interagiert werden, um sie zum Beispiel auszulesen oder auch als „zu löschen“ zu markieren. Der Updatezustand tritt ein, wenn das QUIT-Kommando ausgeführt wird und löscht die markierten E-Mails. Der Server antwortet auf Kommandos entweder mit "+OK", wenn das Kommando erfolgreich ausgeführt wurde oder mit "-ER", wenn ein Fehler aufgetreten ist. Bei einer mehrzeiligen Antwort zum Beispiel bei der Rückgabe einer E-Mail gibt der Server ein "." als Signal, sodass die Antwort beendet ist. [Mye96]

### **3.4 IMAP**

Das Internet Message Access Protocol (IMAP) ist ein Protokoll, das ähnlich wie POP3 verwendet wird, um E-Mails vom E-Mail-Server auf den Client zu übertragen. Es besitzt Ähnlichkeiten zu POP3. Es werden Kommandos an den Server gesendet, der daraufhin eine spezifizierte Aufgabe ausführt und anschließend eine Rückmeldung zurück an den Client gibt.

Im Gegensatz zu POP3 hat jedes Kommando, das an den Server gesendet wird, einen Bezeichner in Form eines kurzen alphanumerischen Strings als Präfix (auch Tag genannt). Das kann zum Beispiel „A001“ sein und dieser erhöht sich beim folgenden Kommando vom selben Client, sodass der String „A002“ lautet. Dieser Bezeichner wird verwendet, um die Antworten vom Server den Kommandos vom Client zuzuordnen. Die Antwort des Servers startet mit demselben Tag, wobei alle vorherigen Zeilen, die zur selben Antwort gehören, mit dem Stern-Symbol („\*“) starten, um zu zeigen, dass die Antwort noch nicht abgeschlossen ist. [Cri03] (Abschnitt 2.2.1)

Jede Nachricht an den Server besteht neben dem Tag als Präfix aus einem Kommando und gegebenenfalls noch weiteren Parametern. Als Beispiel werden hier die Kommandos „login“ und „logout“ verwendet. Das „login“ Kommando wird verwendet, um sich beim Server zu





### 3. Übertragungsprotokolle

authentifizieren und besitzt als Parameter den Benutzernamen und das Passwort. Eine vollständige Authentifizierungsnachricht an den Server, kann wie folgt aussehen: „A001 login mark haus123“. [Cri03] (Abschnitt 6.2.3) Das „logout“ Kommando beendet die Serververbindung und benötigt keine Parameter. Es kann solch eine Form haben: „A002 logout“. [Cri03] (Abschnitt 6.1.3)

Eine Antwort vom Server beginnt entweder mit einem Tag, einem „\*-Symbol oder einem „+“-Symbol. Der Tag gibt an, dass das Kommando beendet wurde und die Antwort komplett ist. Das „\*-Symbol signalisiert, dass das Kommando noch in Bearbeitung ist und die Antwort zu diesem Kommando nicht die Letzte ist. Das „+“-Symbol zeigt an, dass der Server weitere Eingaben anfordert, um die Bearbeitung fortzusetzen.

Es gibt verschiedene Schlüsselwörter als Antwort auf ein Kommando, wie z.B. „OK“, „NO“ oder „BAD“. „OK“ wird als Antwort gesendet, wenn das Kommando erfolgreich ausgeführt wurde, während „NO“ gesendet wird, wenn das Kommando nicht erfolgreich ausgeführt wurde. „BAD“ wird zurückgegeben, wenn es einen Fehler im Protokoll gibt. Dies ist der Fall, wenn ein Kommando verwendet wird, welches nicht existiert oder ein Syntaxfehler aufgetreten ist. Zusätzlich gibt es häufig eine Nachricht, welche weitere Informationen geben soll, wie z.B. der Inhalt einer E-Mail. [Cri03] (Abschnitt 2.2.2)

Ähnlich wie bei POP3 gibt es auch bei IMAP verschiedene Zustände während einer Verbindung. Der erste Zustand ist der „Not authenticated“ Zustand oder der „Authenticated“ Zustand, je nachdem, ob die Verbindung bereits beim Aufbau authentifiziert wurde oder nicht. Wenn nicht, kann der „login“-Befehl verwendet werden, um in den „Authenticated“-Zustand zu wechseln. Die Verbindung muss jedoch in den „Selected“-Zustand übergehen, um auf E-Mails zugreifen zu können. Der Übergang in den „Selected“-Zustand erfolgt durch das Ausführen des „select“-Befehls, der den Namen des E-Mail-Postfachs angibt. Wenn der Client die Verbindung schließen möchte, kann dies durch das „logout“-Kommando erreicht werden. Der Server antwortet daraufhin mit einer „BYE“- und „OK“-Nachricht und schließt die Verbindung. Die „BYE“-Nachricht signalisiert dem Client, dass die Verbindung beendet wird und kann zusätzliche Informationen zum Grund der Antwort enthalten. [Cri03] (Abschnitt 3)



### 3. Übertragungsprotokolle

---

#### 3.5 SSH

Die Secure Shell (oder Secure Socket Shell) auch bekannt als SSH, ist ein Netzwerkprotokoll, das für den Einsatz in Remote-Zugriffen auf Systeme entwickelt wurde. Es existieren zwei Hauptversionen des Protokolls: SSH1 und SSH2, die untereinander nicht kompatibel sind. SSH2 bietet im Vergleich zu SSH1 eine höhere Sicherheit, bessere Leistung und mehr Funktionalität. Das SSH-Protokoll wird typischerweise verwendet, um sichere Remote-Sitzungen mit anderen Systemen herzustellen, beispielsweise mit virtuellen Maschinen, wobei der Zugriff und die Kommunikation in der Regel über eine Konsolenschnittstelle erfolgt. Das Hauptziel des Protokolls besteht darin, sicherzustellen, dass Daten während der Verbindung nicht von unbefugten Dritten abgefangen werden können.

Eine verbreitete Alternative zu SSH war früher das TELNET-Protokoll, das ebenfalls Remote-Sitzungen mit anderen Systemen ermöglicht. Der Vorteil von SSH gegenüber TELNET besteht jedoch darin, dass jegliche Daten, inklusive Anmeldeinformationen für den Server, die in der Konsole eingegeben werden, verschlüsselt übertragen werden. Letztlich wird dadurch eine bessere Sicherheit zu gewährleisten. [Hua23] (S. 90-91)

Die Sicherheit des SSH-Protokolls wird durch symmetrische Verschlüsselung und die Verwendung von Verschlüsselungs- und Integritätsschlüsseln gewährleistet. Diese Schlüssel werden sowohl auf dem Client als auch auf dem Server gespeichert und dienen dazu, die Vertraulichkeit und Echtheit der übertragenen Daten zu gewährleisten. Die Integritätsschlüssel werden verwendet, um sicherzustellen, dass die aktuelle Sitzung nicht von Dritten modifiziert wurde. Wenn die Integrität der Daten während der Übertragung verletzt wurde, können die Daten verworfen werden, um das Empfängersystem vor Schäden zu schützen. [Hua231] (S. 269)

### 3. Übertragungsprotokolle

---

#### 3.6 XMPP

Das XMPP-Protokoll ist ein auf XML basierendes Protokoll, das für die Echtzeitkommunikation in Instant Messengern eingesetzt wird. Das Akronym XMPP steht für "eXtensible Messaging Presence Protocol". Ein wichtiger Bestandteil von XMPP ist der „presence indicator“, der dem Server anzeigt, ob der Benutzer online oder offline ist. Im Gegensatz zu E-Mail-Protokollen ermöglicht XMPP die Übertragung von Nachrichten in Echtzeit, was eine schnellere und effizientere Kommunikation ermöglicht. Darüber hinaus verursacht die Verwendung von XMPP für die Übertragung von Nachrichten weniger Netzwerklast als andere webbasierte Mechanismen. [XMP23] XMPP unterstützt auch Sprach- und Videoanrufe sowie Gruppenchats. Es ist plattformunabhängig und kann auf verschiedenen Betriebssystemen verwendet werden. XMPP ist auch erweiterbar und anpassbar, wodurch es für verschiedene Zwecke geeignet ist, wie zum Beispiel für den Messenger-Dienst WhatsApp. Jedoch bietet WhatsApp keine öffentlich zugängliche Dokumentation über ihre interne Infrastruktur. Neben den XMPP-Servern, welche die Kommunikation zwischen den XMPP-Clients ermöglichen, existieren auch XMPP-Gateways. Diese ermöglichen den Zugriff auf Nicht-XMPP-Domains, wie zum Beispiel SMTP-Domains und dienen als Übersetzer zwischen verschiedenen Internetprotokollen. [Jon09]

#### 3.7 MTPProto

MTPProto ist ein Protokoll, welches von dem Instant-Messenger Telegram für die Kommunikation zwischen dem Client und dem Server verwendet wird. Das Protokoll ermöglicht den Zugriff auf eine Server API und besteht aus drei Komponenten. Die erste („high-level“) Komponente ist für die Umwandlung von API-Queries und Responses in binäre Nachrichten zuständig. Die zweite Komponente dient zur Verschlüsselung der Nachrichten und die dritte Komponente für den Nachrichtentransport über bereits existierende Netzwerkprotokolle wie HTTP oder TCP. [Tel23] (Abschnitt General Description)

Die Kommunikation zwischen dem Client und dem Server findet innerhalb einer Sitzung statt, die an die Anwendung gebunden und durch eine ID authentifiziert ist. Die ausgetauschten



#### 4. Sicherheit und Verschlüsselung

Nachrichten werden in verschiedene Gruppen eingeteilt, wie zum Beispiel RPC calls und RPC responses. „RPC calls“ sind Nachrichten vom Client an den Server. „RPC responses“ sind die Antwort auf die „RPC calls“ vom Server an den Client. Neben diesen Gruppen gibt es Bestätigungen, dass Nachrichten vom Empfänger erhalten wurden. [Tel23] (Abschnitt High-Level Component)

Vor dem Versenden werden die verschlüsselten Nachrichten mit Hilfe von MTProtos Transportprotokollen in einen sekundären Protokollheader verpackt. Es gibt die vier Protokolle „Abridged“, „Intermediate“, „Padded Intermediate“ und „Full“. Diese unterscheiden sich in ihrer Komplexität und ihrem Overhead, wobei „Abridged“ den geringsten Overhead besitzt und „Full“ den höchsten. [Tel231] Anschließend wird zum Beispiel TCP oder HTTP verwendet, um die Nachricht zu versenden.

#### **4. Sicherheit und Verschlüsselung**

In der Welt der Nachrichten spielt die Sicherheit und Verschlüsselung eine zentrale Rolle, da diese die Basis für die heutige Kommunikation bildet. Ohne Verschlüsselung könnten sogenannte "Man-in-the-Middle"-Angriffe stattfinden, bei denen Daten und der Inhalt von Nachrichten zwischen dem Client und dem Server abgefangen und von Dritten ausgelesen werden könnten. Die verschiedenen Arten von Nachrichten nutzen je nach Anwendungsfall unterschiedliche Verschlüsselungsmethoden. Bei E-Mails wird üblicherweise Transport Layer Security (TLS) eingesetzt, um eine Transportverschlüsselung zu gewährleisten. Zudem können auch Schlüsselpaare erzeugt und ausgetauscht werden, um Nachrichten zu verschlüsseln und entschlüsseln. [Bun23] Bei SMS-Nachrichten wird oft das Signalling System No. 7 (SS7) im Mobilfunknetz verwendet. [Abb20] Ende-zu-Ende-Verschlüsselung wird hauptsächlich bei Instant-Messengern eingesetzt, bietet jedoch auch bei anderen Arten von Nachrichten einen höheren Schutz. [Eme18] Einige der genannten Verschlüsselungsmethoden werden im Folgenden näher betrachtet.



#### *4. Sicherheit und Verschlüsselung*

##### **4.1 Transportverschlüsselung**

Die Transportverschlüsselung ist eine Methode, um Daten bei der Übertragung zwischen zwei Systemen zu sichern. Ein gängiger Weg, um dies zu erreichen ist mit dem Protokoll TLS. Ein häufig eingesetztes Protokoll zur Umsetzung von Transportverschlüsselung ist das Transport Layer Security (TLS) das die Daten auf einem Sender-System wie beispielsweise einem Server verschlüsselt, bevor sie über das Netzwerk an ein Empfänger-System wie beispielsweise einen Client übertragen werden. Die Daten werden dabei in eine Folge von unverständlichen Zeichen umgewandelt und können nur am Empfänger-System wieder entschlüsselt werden. Falls die Daten noch nicht ihr tatsächliches Ziel erreicht haben, sondern noch unterwegs sind und durch Zwischenstationen laufen, werden sie erneut verschlüsselt, bevor sie an die nächste Station weitergeleitet werden. Der Nachteil bei diesem Verfahren liegt darin, dass die Daten an den Knotenpunkten, an denen sie weitergeleitet werden, dennoch als Klartext vorliegen und somit von Dritten manipuliert oder ausgelesen werden können. [Kne21] (S.189-190)

##### **4.2 Ende-zu-Ende Verschlüsselung**

Um die Datensicherheit zu erhöhen, kann die Ende-zu-Ende-Verschlüsselung eingesetzt werden. Diese Methode gewährleistet, dass Nachrichten beim Senden verschlüsselt und bis zum Empfänger verschlüsselt bleiben. Im Gegensatz zu der Transportverschlüsselung haben die Zwischensysteme an den Knotenpunkten keinen Zugriff auf die Nachrichten, da sie keinen Zugriff auf den benötigten Schlüssel haben. [von18] (S.93-94) Asymmetrische Verschlüsselung, die beispielsweise bei WhatsApp [Wha23] oder Telegram [Sup23] verwendet wird, nutzt einen öffentlichen Schlüssel, der es ermöglicht, eingehende Nachrichten zu entschlüsseln, während ausgehende Nachrichten mit dem privaten Schlüssel verschlüsselt werden. [Paa16] (Abb. 6.3)



*5. Anforderungsanalyse*

---

**5. Anforderungsanalyse**

In dieser wissenschaftlichen Arbeit müssen spezifische Vorgaben erfüllt werden. Es ist erforderlich, dass die Untersuchung der grundlegenden SSH-Prinzipien umfangreich, leicht verständlich und gut strukturiert erfolgt, um auch Personen mit geringem Vorwissen einen einfachen Zugang zu dem Thema zu ermöglichen. Zur Erreichung dieses Ziels ist es erforderlich, eine erfolgreiche SSH-Verbindung aufzubauen und alle relevanten Komponenten der Verbindung, einschließlich Befehle und Log-Dateien, detailliert zu analysieren und zu erläutern.

## 6. Konzept

### 6. Konzept

Im Rahmen dieser wissenschaftlichen Arbeit wird die Einrichtung einer SSH-Verbindung zwischen einem lokalen System (SSH-Client) und einem externen System (SSH-Server) beschrieben. Dabei werden die Struktur und Funktion des SSH-Protokolls sowie seine einzelnen Komponenten detailliert erläutert. Eine SSH-Verbindung wird aufgebaut, sobald der SSH-Client auf die IP-Adresse des Servers zugreift. Danach gibt der Client seine Anmeldedaten ein (siehe Abbildung 2. S.19). Diese werden durch das SSH-Protokoll über verschiedene Methoden verschlüsselt und vom SSH-Server entschlüsselt. Nach erfolgreicher Authentifizierung genehmigt der SSH-Server den Zugriff, was einen kontinuierlichen Datenaustausch zwischen dem Client und Server ermöglicht. Dabei können Außenstehende die übertragenen Daten nicht entziffern. Im folgenden Kapitel wird eine detaillierte Erläuterung über den Verbindungsaufbau gegeben.

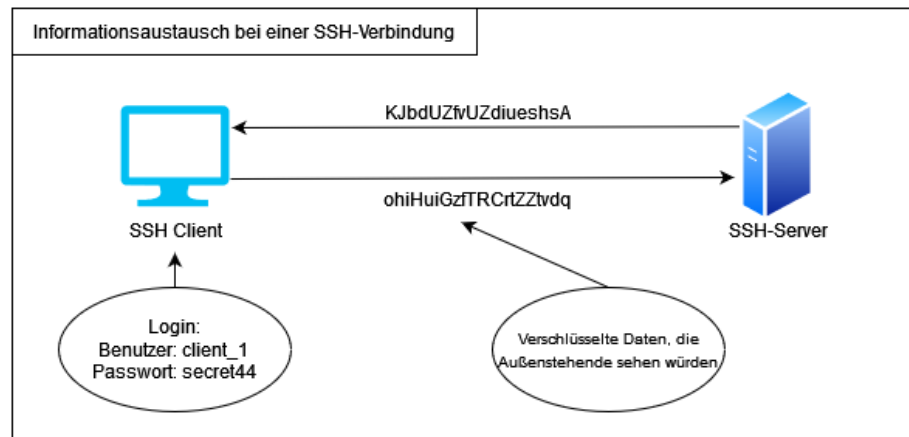


Abbildung 2: Informationsaustausch bei einer SSH-Verbindung

## 7. Durchführung

### 7. Durchführung

Im Rahmen dieser Durchführung wird das SSH-2.0-Protokoll verwendet, um eine sichere Verbindung zwischen einem lokalen Computer mit Windows 10 (64-Bit) und einem virtuellen Server herzustellen, der von dem Hosting-Dienstleister STRATO <sup>1</sup> gehostet wird. Der virtuelle Server verfügt über Ubuntu 22.04 LTS (64-Bit). Die Verbindung wird mithilfe des SSH-Clients PuTTY <sup>2</sup> in der Version „PuTTY\_Release\_0.78“ realisiert, welche auf dem lokalen Computer verwendet wird, während der virtuelle Server die „OpenSSH-Version 8.9p1 Ubuntu-3“ nutzt. Nachdem der Benutzer den Hostnamen oder die IP-Adresse des Servers in der PuTTY-Konfiguration angegeben hat, kann er durch die Eingabe seines Benutzernamens und Passworts eine Verbindung zum Server herstellen. Standardmäßig wird diese Verbindung über den Port 22 aufgebaut.

Sofern die Logging-Funktion in der Sitzung des SSH-Clients PuTTY aktiviert ist, kann der Benutzer anhand einer generierten Textdatei sämtliche SSH-Pakete einsehen, welche im Austausch zwischen dem Client und dem Server erfolgen. Hierbei sind sämtliche Daten in der Datei sowohl in ihrer ursprünglichen, verschlüsselten Form als auch in ihrer unverschlüsselten Form dargestellt.

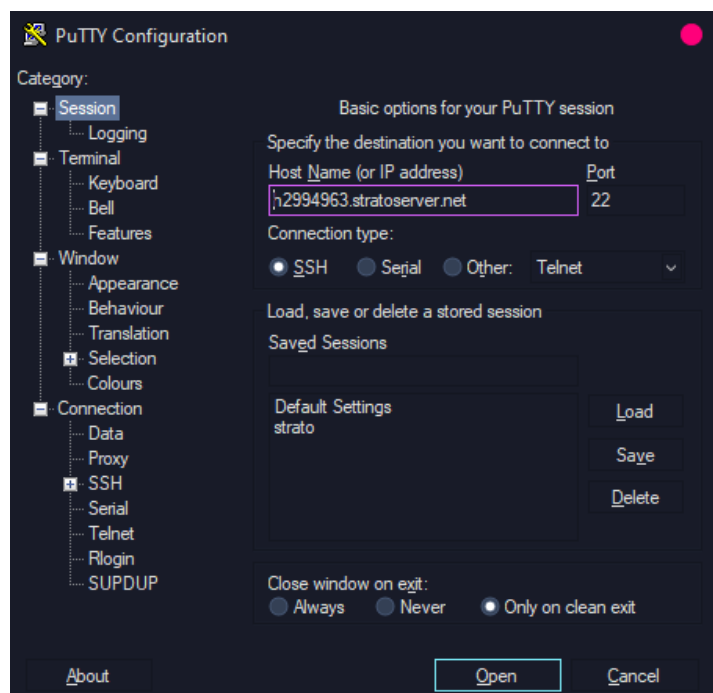


Abbildung 3: PuTTY Konfiguration mit Verbindung auf den Stratoserver

<sup>1</sup> <https://www.strato.de/> (Abrufdatum: 16.02.2023)

<sup>2</sup> <https://www.putty.org> (Abrufdatum: 16.02.2023)



## 7. Durchführung

Nachdem beide Parteien ihre SSH-Version erfolgreich ausgetauscht haben, initiiert der Client den Schlüsselaustausch, indem er das erste Paket vom Typ "SSH2\_MSG\_KEXINIT" an den Server sendet. Dieses Paket enthält eine Vielzahl von Algorithmen wie Verschlüsselungs- und Komprimierungsalgorithmen. [Ylo06] (Abschnitt 7.1 Der Server antwortet daraufhin mit dem gleichen Paket, da ein Schlüsselaustausch den Austausch identischer Pakete erfordert. Anschließend wird der Schlüsselaustauschalgorithmus ausgeführt, der je nach verwendeter Methode entsprechende Pakete zwischen den Parteien austauscht.

In diesem Fall wird der hybride Schlüsselaustausch namens „NTRU-Prime / Curve25519“ durchgeführt (siehe Abbildung 4, S. 21). Der Server sendet dem Client ein Paket vom Typ "SSH2\_MSG\_KEX\_ECDH\_INIT" mit dem Code 30 (siehe Abbildung 5, S. 22).

```
00000410 69 62 40 6f 70 65 6e 73 73 68 2e 63 6f 6d 00 00 ib@openssh.com..  
00000420 00 00 00 00 00 00 00 00 00 00 00 00 .....  
Event Log: Doing NTRU Prime / Curve25519 hybrid key exchange, using hash SHA-512 (unaccelerated)  
Outgoing packet #0x1, type 30 / 0x1e (SSH2_MSG_KEX_ECDH_INIT)  
00000000 00 00 04 a6 de 36 fb 51 cc 9f c4 06 d4 1d eb cc .....6.Q.....  
00000010 7b 3d d9 35 48 38 d0 ae ce d4 52 cf fb 05 d4 77 {=.5H8....R....w  
00000020 e8 57 63 3c 00 c7 14 56 0b df 43 df d2 6a 4a 0d .Wc<...V..C..j].  
00000030 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Abbildung 4: Log-Datei der Schlüsselaustauschmethode

Die Pakete von Code 30 bis 49 sind für Schlüsselaustauschmethoden reserviert und können von Methode zu Methode variieren. Das Paket enthält den öffentlichen Teil eines kurzlebigen Schlüsselpaars als Oktett-String, das ebenfalls vom Client generiert wird, bevor das Paket gesendet wird. Der Server überprüft die Gültigkeit des Schlüssels, erstellt ein kurzlebiges Schlüsselpaar und berechnet dabei das gemeinsame Geheimnis (Secret). Darüber hinaus generiert und signiert er einen Austausch-Hash. Daraufhin sendet er ein "SSH2\_MSG\_KEX\_ECDH\_REPLY" Paket, das sowohl den öffentlichen Hostschlüssel des Servers als auch den Oktett-String des öffentlichen Schlüssels des kurzlebigen Schlüsselpaars enthält, das vom Server erzeugt wurde. Das Paket enthält zusätzlich die Signatur des Austausch-Hashes. Der Client überprüft, ob der Hostschlüssel zum Server gehört und ob der Schlüssel des kurzlebigen Schlüsselpaars gültig ist. Abschließend berechnet der Client das gemeinsame Geheimnis (Secret), erstellt einen Austausch-Hash und überprüft die Signatur des Servers. [Ste09] (Abschnitt 4)

## 7. Durchführung

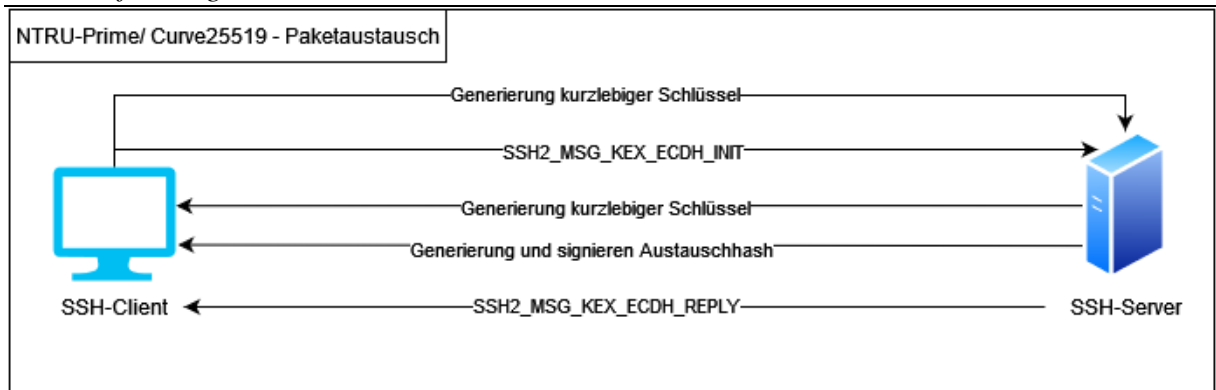


Abbildung 5: NTRU-Prime / Curve 25519 – Paketaustausch zwischen SSH-Client und SSH-Server

Nachdem der hybride Schlüsselaustausch erfolgreich durchgeführt wurde und die Schlüssel überprüft wurden, senden sowohl der Server als auch der Client ein "SSH2\_MSG\_NEWKEYS" Paket (siehe Abbildung 6, S.22). Dieses Paket enthält die alten Schlüssel und Algorithmen. Ab diesem Zeitpunkt müssen alle nachfolgenden Nachrichten die neu generierten Schlüssel und Algorithmen verwenden (aus Abbildung 5). Danach sendet der Client ein "SSH2\_MSG\_SERVICE\_REQUEST" Paket mit dem Servicennamen "ssh\_userauth" versendet, welches ebenfalls aus dem Log ausgelesen werden kann. Der Server antwortet daraufhin mit einem "SSH2\_MSG\_EXT\_INFO" Paket, das dem Client die erforderlichen Informationen zur Authentifizierung liefert. [Bid18] (Abschnitt 2.4) Als nächstes liefert der Server ein "SSH2\_MSG\_SERVICE\_ACCEPT" Paket, um zu signalisieren, dass er diesen Service unterstützt und dem Client die Nutzung ermöglicht. [Ylo06] (Abschnitt 10) Ein Teil des Pakets ist dabei nochmals der Servicename „ssh\_userauth“.

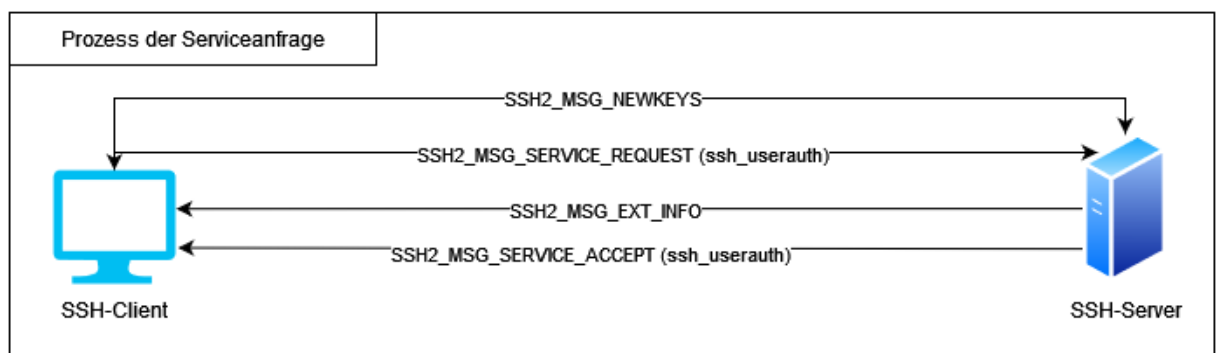
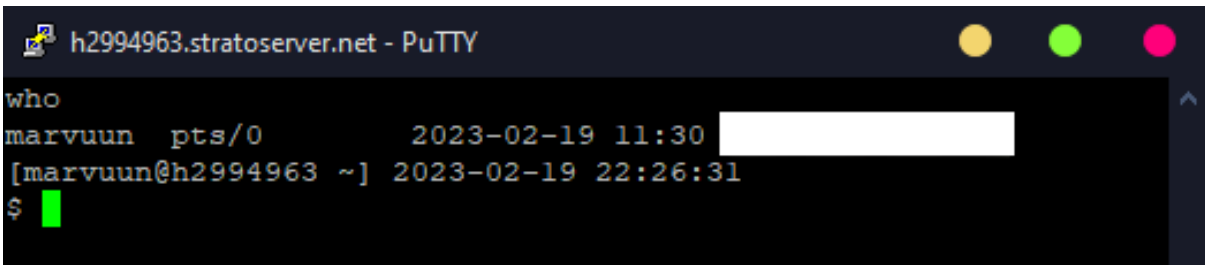


Abbildung 6: Prozess der Serviceanfrage zwischen SSH-Client und SSH-Server

## 7. Durchführung

An diesem Punkt des Verbindungsaufbaus besteht die Möglichkeit für den Benutzer, sich am Server anzumelden. Hierbei sendet der Client nach Angabe des Benutzernamens ein "SSH2\_MSG\_USERAUTH\_REQUEST"-Paket an den Server, um sich zu authentifizieren. Dieses Paket enthält den Benutzernamen, den Servicenamen "ssh\_connection" und die gewünschte Authentifizierungsmethode, in diesem Fall "none". Da der Server diese Methode nicht unterstützt, sendet er ein "SSH2\_MSG\_USERAUTH\_FAILURE"-Paket als Antwort und informiert den Client, dass nur die Methoden "publickey" und "password" unterstützt werden. Folglich wird der Benutzer zur Eingabe seines Passworts aufgefordert. Sobald das Passwort eingegeben wurde, sendet der Client erneut ein "SSH2\_MSG\_USERAUTH\_REQUEST"-Paket, dieses Mal mit der Methode "password" und dem eingegebenen Passwort. Der Server antwortet daraufhin mit einem "SSH2\_MSG\_USERAUTH\_SUCCESS"-Paket, um zu signalisieren, dass die Authentifizierung erfolgreich war. [Ylo061] (Abschnitt 5.1)

Nach erfolgreicher Authentifizierung tauschen Client und Server weitere Pakete aus, um einen Nachrichtenkanal zu öffnen, über den die Kommunikation stattfindet. Über diesen Kanal werden Eingaben, die in die Konsole eingegeben werden, übertragen und ausgegeben.



```
h2994963.stratoserver.net - PuTTY
who
marvuun pts/0      2023-02-19 11:30 [REDACTED]
[marvuun@h2994963 ~] 2023-02-19 22:26:31
$
```

Abbildung 7: Befehl "who" in der Kommandozeile nach erfolgreicher SSH-Verbindung

Um zu verifizieren, ob eine SSH-Verbindung zum Server besteht, kann der Befehl „who“ in der Eingabekonsole verwendet werden, um anzuzeigen welche SSH-Verbindungen zum Server aktuell aktiv sind.

In dieser Ausgabe der Eingabekonsole können Informationen über die aktuelle SSH-Verbindung eingesehen werden. Es werden Angaben wie der Benutzername "marvuun", der verwendete Kanal - in diesem Fall eine Pseudokonsole "pts/0" - sowie das Datum und die Uhrzeit des Logins und die IP-Adresse (die hier aus Sicherheitsgründen unkenntlich gemacht wurde) angezeigt.



## 8. Evaluation

### 8. **Evaluation**

---

Es kann festgestellt werden, dass die Durchführung erfolgreich war, da die Verbindung zum Server erfolgreich hergestellt wurde. Es sollte jedoch beachtet werden, dass aufgrund des Umfangs der Untersuchung nicht alle Einzelheiten des Vorgangs im Detail beschrieben werden konnten. Zum Beispiel wurde die Erstellung eines Nachrichtenkanals nicht detailliert behandelt. Es ist außerdem anzumerken, dass die Verbindung zwischen beiden Parteien ohne weitere Anpassungen der Einstellungen funktioniert, hat In der Regel werden manuell Authentifizierungsschlüssel erstellt und ausgetauscht, was eine zusätzliche Sicherheitsebene bietet. Dabei müssen auch Anpassungen an der Firewall des Servers vorgenommen werden, um eine Verbindung zu ermöglichen. Es ist jedoch anzunehmen, dass der Hostdienstleister Strato bereits solche Anpassungen vorgenommen hat, um eine sofortige Verbindung per SSH zum Server zu ermöglichen.



*9. Fazit und Ausblick*

---

**9. Fazit und Ausblick**

Die heutige Kommunikation wird maßgeblich von digitalen Nachrichten beeinflusst, die einen unverzichtbaren Beitrag zur menschlichen Interaktion leisten. Diese Nachrichten können je nach Art und Inhalt unterschiedliche Anforderungen an die Übertragungsgeschwindigkeit, Komplexität und den Datenübertragungsweg stellen, wodurch eine Vielzahl von Kommunikationswegen und -plattformen entstanden sind.

Neben der Wahl der Übertragungsart spielt auch die Verschlüsselung von Nachrichten eine wichtige Rolle in der heutigen Kommunikation. Verschiedene Verschlüsselungsmethoden wie die Transportverschlüsselung oder Ende-zu-Ende Verschlüsselung sorgen dafür, dass Informationen sicher übertragen und vor unautorisiertem Zugriff geschützt werden.

Insgesamt lässt sich sagen, dass die moderne Kommunikation ohne den Austausch digitaler Nachrichten undenkbar ist. Die Vielfalt der Kommunikationswege und -methoden stellt sicher, dass die verschiedenen Anforderungen an die Übertragung von Nachrichten erfüllt werden können. Die zukünftige Entwicklung der Kommunikation wird weiterhin von neuen Technologien und Innovationen geprägt sein, die die Kommunikation noch schneller, effizienter und sicherer machen werden.



## 10. Literaturverzeichnis

### 10. Literaturverzeichnis

- [Abb20] Haider Abbas, Hammad Afzehl, Yawar A. Bangash, Mian M. W. Iqbal, Imran Rashid und Kaleem Ullah: *IEEE Xplore – SS7 Vulnerabilities—A Survey and Implementation of Machine Learning vs Rule Based Filtering for Detection of SS7 Network Attacks*. 05. Februar 2020. Abgerufen 17. Februar 2023. [online] <https://ieeexplore.ieee.org/abstract/document/8984216/authors#authors>
- [Ahr19] Dennis Ahrholdt, Goetz Greve und Gregor Hopf: *Online-Marketing-Intelligence - Kennzahlen, Erfolgsfaktoren und Steuerungskonzepte im Online-Marketing*, Bd. 1. Wiesbaden: Springer Gabler, 2019.
- [Arg13] Micheal Argyle: *Körpersprache & Kommunikation*, Bd. 1. Junfermann, 2013.
- [Ben20] Gerd Beneken, Hartmut Ernst und Jochen Schmidt: *Grundkurs Informatik - Grundlagen und Konzepte für die erfolgreiche IT-Praxis – Eine umfassende, praxisorientierte Einführung*, Bd. 7. Wiesbaden: Springer Fachmedien, 2020.
- [Bid18] D. Bider und Bitwise Limited: *RFC Editor*. März 2018. Abgerufen 19. Februar 2023. [online] <https://www.rfc-editor.org/rfc/rfc8308.html>
- [Bru06] Tobias Bruns: *TU-Dresden*. Diplomarbeit, Technische Universität, Institut für Systemarchitektur. Dresden, 2006. [online] [http://os.inf.tu-dresden.de/papers\\_ps/bruns-diplom.pdf](http://os.inf.tu-dresden.de/papers_ps/bruns-diplom.pdf)
- [Cha14] Tom Chatfield: *50 Schlüsselideen Digitale Kultur*, Bd. 1. Heidelberg: Springer Spektrum, 2014.
- [MDN221] MDN Contributors: *MDN Web Docs*. 13. September 2022. Abgerufen 16. Februar 2023. [online] <https://developer.mozilla.org/en-US/docs/Web/HTTP>
- [MDN22] MDN Contributors: *MDN Web Docs*. 11. Oktober 2022. Abgerufen 15. Februar 2023. [online] <https://developer.mozilla.org/en-US/docs/Web/HTTP/Messages>
- [Cri03] M. Crispin und University of Washington: *RFC Editor*. März 2003. Abgerufen 16. Februar 2023. [online] <https://www.rfc-editor.org/rfc/rfc3501>
- [Bun23] Bundesamt für Sicherheit in der Informationstechnik – E-Mail Verschlüsselung. Abgerufen 17. Februar 2023. [online] <https://www.bsi.bund.de/dok/11486416>
- [Eme18] Sinem Emeröz, Nina Gerber, Birgit Henhapl, Tobias Hilt, Melanie Volkamer und Verena Zimmermann: *Springer – Nutzerwahrnehmung der Ende-zu-Ende-Verschlüsselung in WhatsApp*. 10. November 2018. Abgerufen 17. Februar 2023. [online] <https://link.springer.com/article/10.1007/s11623-018-1024-z>
- [Gaj] Henning Gajek und Thorsten Neuhezki: *Teltarif – Hintergrund: So funktioniert das SMS-Versenden*. Abgerufen 12. Februar 2023. [online] <https://www.teltarif.de/mobilfunk/technik/sms.html>



## 10. Literaturverzeichnis

---

- [Gre08] Michael Greifeneder: *Einsatzmöglichkeiten von Instant Messaging*. Bachelorarbeit, Technische Universität, Institut für Gestaltungs- und Wirkungsforschung, Wien, 2008.
- [Nie17] Nier Hedda: *Statista – Wie sich die digitale Kommunikation verändert hat*. 11. Oktober 2017. Abgerufen 31. Januar 2023. [online] <https://de-statista-com.ezproxy.hwr-berlin.de/infografik/11426/wie-sich-die-digitale-kommunikation-veraendert-hat/>
- [Hua231] Huawei Technologies Co., Ltd.: *Construction, Operation and Maintenance of Network System (Junior Level)*, Bd. 1. Singapur: Springer Singapore, 2023.
- [Hua23] Huawei Technologies Co., Ltd.: *Data Communications and Network Technologies*, Bd. 1. Singapur: Springer Singapore, 2023.
- [Jon09] M. Jones: *IBM Developer*. 18. September 2009. Abgerufen 17. Februar 2023. [online] <https://developer.ibm.com/tutorials/x-xmppintro/>
- [Kau19] Katja Kaufmann und Corinna Peil: *Sage Journals*. 12. September 2019. Abgerufen 25. Januar 2023. [online] <https://journals.sagepub.com/doi/full/10.1177/2050157919852392>
- [Kla17] Thomas Klar: *CIO – Warum die SMS mehr als zeitgemäß ist*. 21. Dezember 2017. Abgerufen 17. Januar 2023. [online] <https://www.cio.de/a/warum-die-sms-mehr-als-zeitgemaess-ist,3572480>
- [JK108] J. Klensin: *RFC Editor*. Oktober 2008. Abgerufen 16. Februar 2023. [online] <https://www.rfc-editor.org/rfc/rfc5321>
- [Kne21] Ralf Kneuper: *Datenschutz für Softwareentwicklung und IT*, Bd. 1. Berlin Heidelberg, Deutschland: Springer Vieweg Berlin, Heidelberg, 2021.
- [Kun22] Alexander Kunst: *Statista – Beliebteste Messenger in Deutschland im Jahr 2022*. 02. Dezember 2022. Abgerufen 13. Februar 2023. [online] <https://de-statista-com.ezproxy.hwr-berlin.de/prognosen/999735/deutschland-beliebteste-messenger?locale=de>
- [Meh19] Matthias Mehner: *Messenger Marketing: Wie Unternehmen WhatsApp & Co erfolgreich für Kommunikation und Kundenservice nutzen*, Bd. 1. Springer Gabler, 2019.
- [Mye96] J. Myers, Carnegie Mellon, M. Rose und Inc. Dover Beach Consulting: *IETF Datatracker*. Mai 1996. Abgerufen 16. Februar 2023. [online] <https://datatracker.ietf.org/doc/html/rfc1939>
- [Paa16] Christof Paar und Jan Pelzl: *Kryptografie verständlich*, Bd. 1. Berlin Heidelberg, Deutschland: Springer Vieweg Berlin, Heidelberg, 2016.



## 10. Literaturverzeichnis

---

- [Rab21] L. Rabe: *Statista*. 09. Dez. 2021. Abgerufen 08. Dezember 2022. [online] <https://de-statista-com.ezproxy.hwr-berlin.de/statistik/daten/studie/868733/umfrage/anzahl-der-taeglich-verschickten-whatsapp-nachrichten-weltweit/>
- [Rup14] Werner Rupperecht: *Einführung in die Theorie der kognitiven Kommunikation - Wie Sprache, Information, Energie, Internet, Gehirn und Geist zusammenhängen*, Bd. 1. Wiesbaden: Springer Vieweg, 2014.
- [Sch98] Peter Schlobinski, Torsten Siever und Jens Runkehl: *Sprache und Kommunikation im Internet: Überblick und Analysen*. VS Verlag für Sozialwissenschaften, 1998.
- [Ste09] D. Stebila, Queensland University of Technology, J. Green und Queen's University: *RFC Editor*. Dezember 2009. Abgerufen 19. Februar 2023. [online] <https://www.rfc-editor.org/rfc/rfc5656.html>
- [Sup23] Telegram Support: *FAQ Telegram – F: Wie verschlüsselt ihr nun genau Daten?*. Abgerufen 13. Februar 2023. [online] <https://telegram.org/faq#f-wie-verschlusselt-ihr-nun-genau-daten>
- [Wha23] WhatsApp Support: *FAQ WhatsApp – Informationen zur Ende-zu-Ende-Verschlüsselung*. Abgerufen 13. Februar 2023. [online] <https://faq.whatsapp.com/820124435853543>
- [Tel23] *Telegram*. Abgerufen 17. Februar 2023. [online] <https://core.telegram.org/mtproto>
- [Tel231] *Telegram*. Abgerufen 17. Februar 2023. [online] <https://core.telegram.org/mtproto/mtproto-transports>
- [von18] Markus von Rimscha: *Datenschutz – Konzepte, Algorithmen und Anwendung*, Bd. 1. Wiesbaden, Deutschland: Springer Vieweg Wiesbaden, 2018.
- [Tec23] *Technikum Wien Academy – Was ist Instant Messaging?*. Abgerufen 16. Februar 2023. [online] <https://academy.technikum-wien.at/ratgeber/instant-messaging-was-ist-das/>
- [wis23] *wissen.de*. Abgerufen 14. Februar 2023. [online] <https://www.wissen.de/lexikon/uebertragungsprotokoll>
- [Spr10] Uwe Wolff: *Springer Link (Zusammenfassung)*. 30. Mai 2010. Abgerufen 01. Januar 2023. [online] [https://link.springer.com/chapter/10.1007/978-3-8349-8566-8\\_5](https://link.springer.com/chapter/10.1007/978-3-8349-8566-8_5)
- [XMP23] *XMPP*. Abgerufen 17. Februar 2023. [online] <https://xmpp.org/about/>
- [Ylo06] T. Ylonen, SSH Communications Security Corp, C. E. Lonvick und Cisco Systems, Inc.: *RFC Editor*. Januar 2006. Abgerufen 19. Februar 2023. [online] <https://www.rfc-editor.org/rfc/rfc4253.html>
- [Ylo061] T. Ylonon, SSH Communications Security Corp, C. E. Lonvick und Cisco Systems, Inc.: *RFC Editor*. Januar 2006. Abgerufen 19. Februar 2023. [online] <https://www.rfc-editor.org/rfc/rfc4252.html>





*11. Eidesstaatliche Erklärung*

**11. Eidesstaatliche Erklärung**

Wir erklären ehrenwörtlich:

1. dass wir unser Studienprojekt selbständig verfasst haben,
  2. dass wir die Übernahme wörtlicher Zitate aus der Literatur sowie die Verwendung der Gedanken anderer Autoren an den entsprechenden Stellen innerhalb der Arbeit gekennzeichnet haben,
  3. dass wir unser Studienprojekt bei keiner anderen Prüfung vorgelegt haben.
- Wir sind uns bewusst, dass eine falsche Erklärung rechtliche Folgen haben wird.

Luckenwalde, 20.02.2023

*Knothe*

\_\_\_\_\_  
Ort, Datum und Unterschrift

Marvin Knothe

Werder, 20.02.2023

\_\_\_\_\_  
Ort, Datum und Unterschrift

Yüxi Zhang