FAKULTÄT FÜR !NFORMATIK
Faculty of Informatics

Risk Evaluation and Security Threats Affecting Communication Channels of Corporate IT Systems

DIPLOMARBEIT

zur Erlangung des akademischen Grades

Diplom-Ingenieur

im Rahmen des Studiums

Wirtschaftsinformatik

eingereicht von

Michael Gissing, BSc
Matrikelnummer 0828426

an der
Fakultät für Informatik der Technischen Universität Wien

Betreuung: Thomas Grechenig
Mitwirkung: Christian Schanes

Wien, 29.11.2013

(Unterschrift Verfasser) (Unterschrift Betreuung)

FAKULTÄT FÜR !NFORMATIK
Faculty of Informatics

Risk Evaluation and Security Threats Affecting Communication Channels of Corporate IT Systems

MASTER'S THESIS

submitted in partial fulfillment of the requirements for the degree of

Diplom-Ingenieur

in

Business Informatics

by

Michael Gissing, BSc
Registration Number 0828426

to the Faculty of Informatics
at the Vienna University of Technology

Advisor: Thomas Grechenig
Assistance: Christian Schanes

Vienna, 29.11.2013

(Signature of Author) (Signature of Advisor)

Erklärung zur Verfassung der Arbeit

Michael Gissing, BSc
Schönbrunner Straße 282/12, 1120 Wien

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit - einschließlich Tabellen, Karten und Abbildungen -, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.

(Ort, Datum) (Unterschrift Verfasser)

Acknowledgements

I would like to express my gratitude to my advisers Thomas Grechenig and Christian Schanes for the continuous support during writing my thesis.
Furthermore I would like to thank Doris Puchner for her precise and detailed proofreading as well as for her motivations.
I also want to thank my whole family who supported me mentally and financially and often helped me to raise my motivation.
Especially I want to thank my girlfriend Verena Puchner who motivated me when I had problems with the thesis and who did everything for me to make the writing easier for me.

Abstract

Nowadays the focus of security specialists lies on securing the content of messages and on the identification of technical problems or vulnerabilities. Actual newspaper articles show that also traffic data and conceptual flaws can be vulnerabilities of computer systems. There are only a few publications which investigate this aspect explicitly. Therefore the focus of this thesis lies on the analysis of corporate communication components regarding traffic data and conceptual flaws. First of all potential attackers get analysed. Furthermore an overview of actual communication components is given. For further analysis, it is focused on email and voice over IP. These components are analysed regarding the used technologies and the processed data. Based on the results of these analyses, risks and threats regarding the communication components are determined. In the last step, a proper protection from the threats and risks is developed, in form of possible countermeasures. The analysis has shown that there are many possibilities for attackers to attack communication components. The waypoints on the transport route, data packets have to pass, provide good attacking possibilities. There are good security mechanisms for securing the transport route, but often such mechanisms aren't used. Encryption mechanisms don't always provide a proper protection, because attackers like the police and organized crime have their own ways to find out the key. Therefore it is important to analyse whether sensitive data should be stored and in which manner. The analysis has also shown, that traffic data can even reveal more information than content data and that not always technically high sophisticated attacks are necessary to gather valuable information. The result of the thesis is a list of the discovered risks and threats regarding traffic data and conceptional flaws of email and voice over IP. Furthermore the thesis compromises a list of possible countermeasures which provide a protection from the discovered risks and threats. These lists should be a compendium for companies to identify the listed risks and threats in their components and to implement the corresponding presented countermeasures.

Kurzfassung

Heutzutage liegt der Fokus von Security-Spezialisten auf der Sicherung von Nachrichteninhalten und der Identifikation von technischen Problemen und Schwachstellen. Aktuelle Berichte in den Medien zeigen, dass auch Verkehrsdaten und konzeptionelle Mängel Schwachstellen von Computersystemen sein können. Es gibt noch sehr wenige Studien, die explizit diesen Aspekt untersuchen. Deswegen liegt der Schwerpunkt der vorliegenden Arbeit auf der Analyse von betrieblichen Kommunikationskomponenten bezüglich Verkehrsdaten und konzeptionellen Schwachstellen. Dazu wird zunächst eine Analyse der potentiellen Angreifer durchgeführt und ein Überblick über weit verbreitete Kommunikationskomponenten gegeben. Danach wird der Schwerpunkt auf detaillierte Analysen von verwendeten Technologien sowie verarbeiteten Daten bei Kommunikation mittels email und voice over IP gelegt. Basierend auf den Ergebnissen dieser Analysen werden Risiken und Bedrohungen dieser Kommunikationsmechanismen ermittelt. Im letzten Schritt werden mögliche Gegenmaßnahmen erarbeitet, die einen angemessenen Schutz vor den beschriebenen Risiken und Bedrohungen bieten können.

Die Analyse hat gezeigt, dass Angreifer sehr viele Möglichkeiten haben, Kommunikationskomponenten anzugreifen. Besonders die Zwischenstationen auf dem Transportweg der Datenpakete bieten erfolgsversprechende Angriffsmöglichkeiten. Es gibt zwar Sicherheitsmaßnahmen, um den Transportweg abzusichern, aber diese werden oft nicht verwendet. Darüber hinaus ist das für verschlüsselte Informationen erreichbare Sicherheitsniveau vom Schutz der verwendeten Zugriffsschlüssel abhängig. Angreifer räumen der Beschaffung derartiger Schlüssel naturgemäß einen hohen Stellenwert ein, welcher direkt proportional zur Bedeutung verschlüsselter Inhalte ist. Kriminelle Organisationen schrecken dann im Zweifelsfalle auch vor körperlicher Gewalt nicht zurück. Überlegungen über angemessene Schutzmaßnahmen für das Schlüsselmaterial sind somit gleichermaßen relevant wie die Frage, ob reale Risiken sowie der Wert der zu verschlüsselnden Information überhaupt eine elektronische Speicherung zulassen.

Neben der Notwendigkeit eines risikobewussten Umganges mit der Vertraulichkeit von Inhalten hat die Analyse aber deutlich zwei oftmals unterschätzte Bereiche aufgezeigt. Zum einen können Verkehrsdaten für Angreifer oftmals mehr nutzbringende Informationen preisgeben als die eigentlichen Dateninhalte, und zum anderen ist oftmals ein Angriff auf technische Systeme gar nicht notwendig, wie obiges Beispiel der Schlüsselbeschaffung andeutet. Das Ergebnis der vorliegenden Arbeit ist ein allgemeines Bedrohungsprofil von Verkehrsdaten sowie ein Katalog von Risiken sowie die Identifikation konzeptioneller Schwachstellen der Kommunikation über email und voice over IP. Mittels konkreter erarbeiteter Empfehlungen wird die Grundlage für einen Unternehmensleitfaden zur Bedrohungs- und Risikoanalyse sowie zur Auswahl angemessener Gegenmaßnahmen geschaffen.

Contents

CHAPTER 1

Introduction

Nowadays IT is becoming more and more important for companies. Almost no company can make business without a sound IT infrastructure, because critical business processes often rely on the IT systems. Because of that development and the constant growth of the IT, systems are very complex and even get more complex. According to Bruce Schneier who said “Complexity is the worst enemy of security”, this is getting a big issue. Think about confidential data of a law office, which gets eavesdropped and used to gain advantage during trial.

At the time of increasing integration, especially communication is getting more and more important. Nowadays companies are communicating internally, with each other, with their customers and with their partners over IT systems. A factor which increases complexity is the high number of possible methods to communicate (IP telephones, email, chats, etc.). This development is not limited to a special industry; a metalworking company needs communication like a fashion company.
Communication is very vulnerable against security related risks. Due to that risk, most companies are already secured from well known threats like viruses, trojans, hacks and so on. But in fact these attacks are mainly aimed at the content part of messages. Actually there are also other parts of messages which can get attacked and therefore need to get protected.
Basically, when speaking about computer security, one thinks about a hacker who tries to hack into a computer system. But there are several other possible individuals who can attack such systems. A company may infiltrate the competitor to get sensitive information about a new product, the police can confiscate the infrastructure (or part) of a company and so gets access to sensitive data, terrorists may destroy the whole infrastructure and the press may eavesdrop conversations to find good stories [77].
These attackers are endangering many different security needs like integrity, confidentiality, authenticity, anonymity and so on, which are not always same important for every company. Depended on the core business, the security needs have to get prioritized, because there is a trade off between them.

1.1 Problem Description

As described in the introduction, nowadays the most communication components are already well secured against attacks on content data. This is especially very important for companies. These often often have a lot of business secretes whose exposure would arise high costs. Considering actual incidents, securing content data is not enough. This thesis concentrates on the risk evaluation of the communication components regarding traffic data and conceptual risks. An example attack would be the confiscation of an email server by the police, which then would have access to all emails stored on it. Companies also have to protect themselves from such attacks. Of course additional costs arise when implementing countermeasures, but the costs of a secret exposure could be much higher. Therefore also possible countermeasures are described within this thesis.

1.2 Methodological Approach

The thesis consists of two parts. The first part is an intensive research and theoretical analysis, to find answers to the questions mentioned in section 1.3. For this part mainly literature research was needed (attackers, security needs, resulting threats, countermeasures).

At first the common IT components of common companies are identified, with focus on communication components. Then the thesis deals with the possible attackers on a system. Then the security needs for common companies are defined. For these parts intensive literature research was needed. Additionally the criticality of different data is analysed and described to find out the protection requirements for the respective data. For this part a mixture between literature research and existing expertise were required. Out of the attackers and the security needs some threats arose. These are also described. In the last section of the first part some countermeasures are described.

Additionally for the first part an exemplary security analysis is made. That means to analyse the technique of communication components, the processed data as well as the resulting risks and threats. Data can get split up additionally, in personal data, confidential business data and public data. Based on that information the protection requirements get identified. A risk analysis helps to assess the threats and the required countermeasures.

The practical, second part deals with exemplary scenarios. There it will be shown that the described attacks are possible. It will also be shown that the defined countermeasures can protect the system from such attacks. This part is written inform of a discussion of the researched, theoretical thesis.

1.3 Aim of the Thesis

The aim of the thesis is to perform a risk analysis of common communication components in companies. Thereby the focus lies on the analysis of traffic data as well as on the analysis of conceptual risks. An analysis of the criticality of the processed data is necessary. The main questions which are answered by the thesis are:

- Which attackers are attacking communication channels of company IT systems?
- How critical is the processed data in communication channels?
- Which security threats and risks arise in communication channels?
- What countermeasures can be taken to secure the communication channels?

1.4 Composition of the Thesis

To understand the analysis described in the thesis some fundamental knowledge of security and networks is necessary. Therefore chapter 2 deals with this basic knowledge and the possible attackers. Chapter 3 deals with the role of the IT in common companies and the most common communication components. In chapter 4 a technical analysis as well as a data analysis of selected communication components are described. In chapter 5 the analysis of the attackers and the technical analysis are used to determine the risks and possible countermeasures of the respective communication components. In chapter 6 the results get discussed in form of showing that the found risks and threats are exploited by attackers. It is also shown that the found countermeasures could have been a proper protection. Chapter 7 sums up the most important parts of the thesis and deals with future possibilities.

CHAPTER 2

Security Basics for Company IT

In this chapter the basic security related terminology, which is required for understanding the thesis, is described.

2.1 Security Needs

To establish security in a system, at first the security needs have to get specified. If there are no special security needs for a system, it is difficult to define a proper security strategy. Furthermore the relevance and importance of security needs vary for different systems. Imagine a wiki page, where everybody should have access to read and write some articles with no limitation. It would make no sense to concentrate the security measures for such a page on confidentiality, as anyway everybody should have access to all data. Before discussing the importance of the different security needs, these need to get specified. Bruce Schneier describes in [77] a long list of security needs. Some of them are described in this section.

The most important security needs, also known as the *CIA Triad* are confidentiality, integrity and availability [3]. But also the security needs authenticity and reliability have to get considered for this thesis. There are also other security needs, like non-repudiation and non-propagation, which can be important for some scenarios. Nevertheless they are not important for this thesis and are therefore not described in this section.

2.1.1 Confidentiality

Confidentiality is an essential security need. It states, that confidential information must only be accessible to the individuals (persons, applications, processes, etc.) who have the right to do so. For most companies confidentiality is very important, as customer data or business secrets have to get protected. [3] [8] [77]

2.1.2 Integrity

Integrity states, that data must not be modified by an unauthorized individual. Sometimes such a protection is not possible. In such cases, an unauthorized modification has to be detectable. If an authorized modification is done, which is not desirable, it will have to be possible to restore the modified data [3]. Bishop states in his book [8], that also preventing improper change belongs to integrity.

2.1.3 Availability

Availability states, that data or systems have to be accessible every time an access is needed [3] [77]. Some systems may have a higher availability rate as other systems. For example, a bank, where thousands of customers access their money daily, must have a higher availability rate, as a private homepage [3] [77].

2.1.4 Authenticity

Authenticity means, that data has to come only from the creator or owner of it [3]. Data which comes from the wrong individual, that means not from the owner, has to get identified. So systems must be able to determine if data comes from a specified individual and not from an attacker. For example, if an email gets sent from Alice to Bob, but it is modified so that it looks like it comes from another email address, the authenticity is violated [3].

The article [68] from The Washington Post and the article [4] from the Augsburger Allgemeine show why the authenticity of data is very important. According to these articles, hackers hacked the Twitter account of the Associated Press and posted a fake tweet: “Breaking: Two Explosions in the White House and Barack Obama is injured”. As a reaction to this tweet, the stock exchange prices, the commodity market and others fell down immediately.

2.1.5 Reliability

Reliability is the percentage of time, the system works as specified [8]. So if a system works and is 100% available, but in 50% of the cases it doesn’t work correctly, it has a high availability, but it is not 100% reliable.

2.1.6 Trade-Offs

It is important to consider, that there is a trade-off between the different security needs [28] [73]. It is not always reasonable or possible to implement or consider all of the available security needs. Therefore at first a company has to think about their special systems and requirements. Based on that, a company can choose matching security needs [73].
[74] gives a good example for a trade-off. This trade-off is between availability and confidentiality. If the data of a system is completely encrypted, the confidentiality might be fulfilled (of course also other measures would have to be taken to ensure confidentiality). But if the key which is necessary for decrypting the data gets lost, then the availability of the system suffers.

2.2 Kind of Attacks

An attack on a system can always be categorized in one or more categories. There are four different categories. These categories are *interception*, *interruption*, *modification* and *fabrication* [3] [89]. Furthermore attacks can be distinguished between *criminal attacks*, *attacks on confidentiality*, *publicity attacks* and *judicial attacks* [77]. Interested readers can have a further look at [77].

2.2.1 Interception

Interception is an unauthorized access of data or services [3] [89]. It includes copying, viewing and eavesdropping data. Thus interception is an attack on confidentiality.

2.2.2 Interruption

Aim of an interruption attack is to make data or services unavailable/inaccessible [3] [89]. That includes making the data or services temporarily unavailable, or making them unusable or destroying them [89].

2.2.3 Modification

Modification is an unauthorized change or tampering of data or services [89]. When data gets modified from an unauthorized individual this is an attack on integrity. When a service gets modified in a way that it isn't available anymore, this is an attack on availability. When access rights get modified so that an attacker has access to confidential data, this is an attack on confidentiality [3].

2.2.4 Fabrication

With fabrication, additional data or activities (e.g. processes) get generated in a system [3] [89]. This could be additional data in databases, which is an attack on integrity. Generating additional processes making a service unavailable is an attack on availability [3].

2.2.5 Criminal Attacks

Often criminal attacks have the goal to maximize financial win. To reach that goal attackers use different types of attacks [77]:

Scams is aimed to convince persons to transmit confidential information or money to an attacker. Special emails or websites are used for it. For example a user views a web page which prompts him to transfer money to an account, so that he can receive a prize [77].

Destructive attacks are an example to show that not every attack aims to maximize financial win. Such attacks have only one goal: destruction. Mostly such attacks are carried out by terrorists or revengeful employees [77].

Theft of intellectual property is often done between competitors and it also includes pirate copies of software, CDs and digital print media as well as theft of business or private databases [77].

Identity theft aims at stealing someones identity and, for example, to obtain credit cards in the name of the victim. Nowadays more and more people reveal personal information imprudently which makes it easier to steal an identity [77].

Brand theft aims at using the brand of another company to make capital out of it. This could be a simple redirect of phone calls to the attackers number. So if a person actually wants to call a company with a special brand, this call will get redirected to the attacker [77].

2.2.6 Attacks on Confidentiality

There can be two kinds of attacks on confidentiality. On the one side there could be a directed attack on a person, on the other side there is data harvesting. Such attacks can be done with eavesdropping and analysis of data traffic. There are also attacks on confidentiality which at a first glance don't look like an attack on confidentiality. For example if an attacker collects single data which on its own doesn't reveal much information, but connected to each other this data can endanger confidentiality. Nowadays there are many different databases which contain information about individuals. On its own such a database can already reveal much information about someone. But when the databases get connected, even more information could get derived and there could be a big confidentiality loss [77].

2.2.7 Publicity Attacks

Also publicity attacks don't have the goal to maximize financial win. This fact is important to consider when implementing security for a system. So a system can be designed in a way, that for an attacker whose goal is to maximize financial win, it is not worth to attack it. But such systems are still vulnerable to publicity attacks. Such attacks only have the goal to get public attention [77].

2.2.8 Judicial Attacks

Goal of judicial attacks is to find security holes in exhibits. An attacker could break in a system and get accused based on his activities which got logged. If the attacker can prove that such logging can get tampered, such an evidence will be less significant [77].

2.3 Threat, Vulnerability and Risk

For the next parts of the thesis it will be important to understand the difference between *threat*, *vulnerability* and *risk*.

Threat A threat can cause harm to a system [3].

Vulnerability can lead to a threat if an attacker uses this vulnerability. Vulnerabilities are weaknesses or defects in a system. Such defects can be *bugs* or *flaws*. Whereas bugs are basically coding errors, flaws are design errors [3] [52].

Risk Flaws and bugs, respectively vulnerabilities and threats lead to risks. A risk is the likelihood that something will happen [3] [52].

2.4 Traffic Data vs. Content Data

In the following parts of the thesis it will be dealt with traffic and content data. Therefore this section should help to understand the difference between them. Furthermore it deals with the problem of classification in traffic or content data.

Content data is defined in TKG 2003 §92 paragraph 3 numeral 5 as contents of transferred messages. Whereas message is defined in TKG 2003 §92 paragraph 3 numeral 7 as information that is transferred over a public communication service between an endless number of parties [1]. Traffic data is defined in TKG 2003 §92 paragraph 3 numeral 4 as data which is processed for transferring a message to a communication network or for billing [1].

On the technical point of view this means, that content data is the actual content of the messages which are transferred. Traffic data is the data which is needed to transfer a message from one party to another (or many others) and to make billing.

The differentiation of traffic and content data is often very difficult. Freiling and Heinson wrote an article [35] which deals with this topic. It seems logical to define traffic data as the data which is located in the headers and content data as the data which is located in the body of data packets. The first problem with this definition is, that then only the header of the lowest layer will be seen as traffic data. That means only the header of the physical layer. So the header of IP or TCP packets respectively IP addresses and ports would not be seen as traffic data. The second problem is, that for example the subject of an email is located in the header section. Some would see the subject of an email already as part of the content of the message [35].
To solve the first problem a border is needed. Till this border the data can be seen as traffic data. Assuming the border is at the IP layer, then all data till the header of the IP packets is seen as traffic data. That leads to another problem. If the border is defined in a way so that email addresses are traffic data, then according to the TCP/IP reference model, also addresses of web pages are traffic data, because they are at the same level as email addresses. The law states that traffic data have to be stored [35] [34]. It also states, that email addresses should be stored, but not addresses of web pages. This example shows the difficulty of differing and also that a border is not a complete solution of the classification problem [35].
Another reason why a border is not sufficient, is that for example future protocols could be completely different. Even now it would be possible to send an IP address in the body of an email. In such a case traffic data becomes content data [35].
Freiling and Heinson state another example in [35], why a classification is difficult. The term

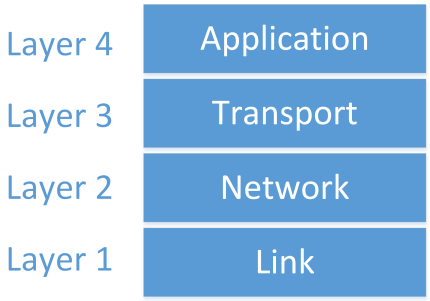

Figure 2.1: TCP/IP reference model [85] [66]

electronic mail is precisely defined in law. There terms like SMPT, IMAP, POP3, header and body are used. Regarding this terminology, a message sent over facebook is no electronic mail, and therefore traffic data regarding this message must not be stored [35].

In the last years many professionals concentrated only on securing the content data. Only a few thought about the attacking potential on traffic data and therefore neglected the protection of it. Therefore the security mechanisms for protecting content data are already sophisticated. The latest eavesdropping incidents of NSA have shown the potential of traffic data. There is an article [36], which describes that a telecommunication company has to transfer traffic data to the NSA. So much the worse is, that the protection of traffic data is not that much sophisticated.

Traffic data is used by the public authorities to find out communication patterns of criminals. Primarily traffic data is used in the evaluation phase to convict criminals. At court it is less used [34]. According to Freiling [34] in the future it will be better possible to deduce content data out of traffic data.

2.5 TCP/IP - Reference Model

For further understanding of the thesis, the basics of network communication are needed to be understood. For that reason in this section the TCP/IP reference model will be described. It is based on the Open Systems Interconnection Model (OSI model) [66]. Each layer of the TCP/IP reference model sums up more layers of the OSI model. For this thesis one would not need to understand the details of the OSI model [85].

The TCP/IP reference model allows computers of all kinds to communicate standardized with each other. It consists of four different layers, which are shown in figure 2.1. Each layer performs a special task to provide a solid communication facility. A lower layer provides it functionality to the higher layer [85]. When, for example, a message should get sent over a network, this message goes down from layer 4 to layer 1 at the sender and at the recipient it gets up from layer 1 to layer 4. Each layer adds his own header to the data, when it runs down the protocol stack. More on that is described in section 2.5.1 [85].

Layer 1: Link In the link layer, the device driver of the OS and the network card are located. The functionality of this layer is, to provide a link to the physical media which are used for the communication. These media could be cable based or wireless based. In the header of this layer, amongst others the mac address of the device is stored. The mac address identifies a single device locally [35]. The link layer sums up the OSI layers: physical layer and data link layer [66].

Layer 2: Network The network layer handles the movement of packets around the network [66] [85]. Amongst others, the IP address of the sender and of the recipient are stored in the header of this layer. This layer provides a global identification with help of the IP addresses [35]. This layer is also responsible for the routing of the packets in the network. The IP is connectionless. That means that once a packet is sent, it cannot be guaranteed that the packet really reaches the recipient. No acknowledgements are sent within the IP. This functionality is provided by layer 3 [85]. The network layer complies with the OSI layer: network layer [66].

Layer 3: Transport This layer provides a reliable connection between two hosts [85]. For this functionality the Transmission Control Protocol (TCP) is used. At this layer also the, more simple, User Datagram Protocol (UDP) can be used. UDP has no guarantee that the data reaches the recipient [85]. The transport layer provides more detailed addressing possibilities in addition to the IP address of the network layer. With the help of so called ports, special parts of the recipient (e.g. individual applications) can be reached [35]. The transport layer complies with the OSI layer: transport layer [66].

Layer 4: Application At this layer, the protocols for the applications are located [66]. Such protocols can be SMTP, HTTP, POP and so on. The application layer sums up the OSI layers: session layer, presentation layer and application layer [66].

For further reading of the OSI reference model have a look at [41].

2.5.1 Encapsulation

The data of the different layers gets encapsulated. That means, when data should get sent over a network (with TCP), the data flows from layer 4 to layer 1 through the protocol stack. Each layer adds additional information in form of a header to the data. In layer 1 additionally trailer information is added. After the data has passed layer 1, it is transferred over the network to the recipient. There the data flows from layer 1 to layer 4 [85].
At layer 2 the data package is called IP datagram, at layer 3 the data package is called TCP segment and at layer 1 the data package is called Ethernet frame [85].
As one can see in figure 2.2, the data gets bigger at every layer. The lower layer, takes the data from the higher layer and puts it in the body section. The additional information gets added in the header section. That's why this process is called encapsulation [85].

In their article [35], Freiling and Heinson presented encapsulation with an analogy to a post office. In this analogy, data packets are envelopes. The first layer is an envelope with

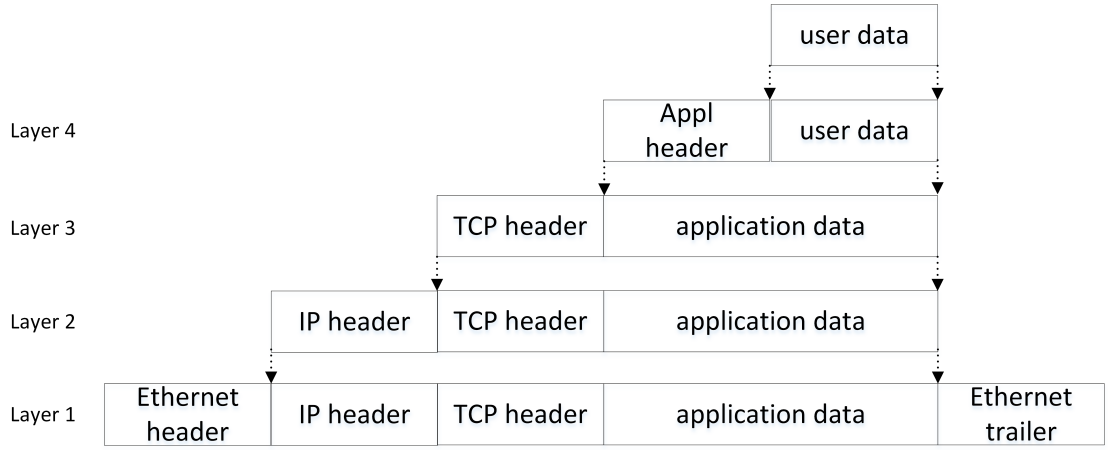

Figure 2.2: Encapsulation of data as it goes down the protocol stack [85]

a room number written on it, which represents the mac address. A second envelope with the concrete information about the way it should take (represents IP addresses) is put into the first envelope. Then another envelope with information about the responsible person written on it (represents port number) is put into the second envelope. Then the "real" data is put into the last envelope. When using for example email, this "real" data can again be an envelope. The text on it represents the header of an email and the message in it represents the body.

2.6 Types of Security Attackers

When analysing attacks on IT infrastructures, first one has to think about the different individuals which have the motivation to attack. In general, according to Sean Convery [21], there are three types of attackers.

Script Kiddies often have less experience in attacking systems. Therefore they use tools and guidelines for their attacks. They often don't differ between the targets they attack, and try out their attacks to find several vulnerable systems [21].

Crackers are more experienced and more dangerous opponents [21]. In contrast to the skript kiddies, they have the ability to think about and develop new attacks [21].

Elite have in general very specific targets. For example terrorists and spies can be assigned to this type of attackers [21]. Mostly these persons are highly developed and experienced.

Figure 2.3 shows the distribution of the different attackers. Whereas there are many Script Kiddies, there are only few persons which can be seen as Elite.

There are several different motivations why one attacks. Bruce Schneier describes in his book [77] a list of different attacker types, which might want to attack an IT infrastructure. Some descriptions are supplemented with more or less actual practical examples.

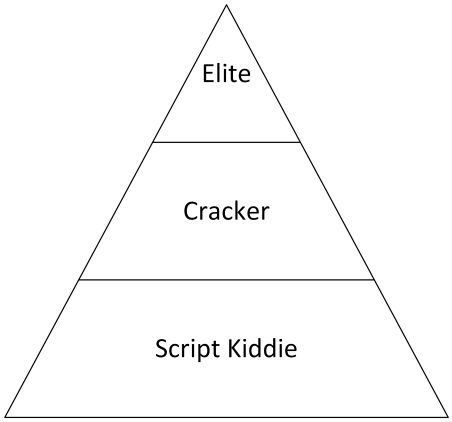

Figure 2.3: Types of Attackers according to [21]

2.6.1 Hacker

Nowadays many use the term hacker as a description for the good guys, and cracker for the bad ones [77]. Bruce Schneier defines a hacker as a person with certain skills and not with certain intentions. Only a small subset of the hackers are very good. Very good means, that they have a fundamental technological understanding and have the wish to learn more. Because of that, hackers often have much more expertise than the original system developers [77].

On the 18^{th} of August 2013 CNET published an article [18] about a researcher who detected a vulnerability in Facebook. According to the researcher, he has tried to report the vulnerability a couple of times to the security team. After being ignored, he exploited the vulnerability to publish a description of it on the Facebook wall of the founder of Facebook, Mark Zuckerberg. The question arises, if this "attack" has been done by a good hacker? Anyway, for reporting fundamental bugs, discoverer will get $500 from Facebook. Or maybe this guy just wanted to get some publicity?

According to [17], a group of hackers offered companies to buy instagram followers and likes, to get a higher "coolness" factor. Therefore they created a botnet with millions of computers which did the following and liking. The interesting thing is, that followers and likes were sold for more money than credit card numbers.

2.6.2 Single Perpetrator

Single perpetrators mostly attack commercial systems, because there they can steal a lot of money. Usually they don't have much expertise and money and make often dump faults which help to catch them. Anyway, such attackers can cause a high amount of damage to a company, especially if it is an insider attack. It can get very dangerous if an insider detects a vulnerability and decides to exploit it (see section 2.6.3) [77].

2.6.3 Malicious Insider

Insiders can be very dangerous if they decide to attack the system. They are seen as trustworthy and have access rights to the system. So they are already in the system and don't have to overcome some security measurements [77]. There are several attacking scenarios [77]:

- Insiders can help an attacker in granting access to the system
- Insiders can abuse the system for their own needs (e.g. sale of their own goods)
- Insiders can modify some system parameters for their advantage (e.g. salary increase)
- Insiders can just be careless and make unintentionally mistakes

Also external employees like consultants can be a malicious insider, because they often get some access rights to the system [77].

According to the article from the infosecurity magazine [39], 58% of the security incidents are related to an insider threat. Guy Bunker, Senior vice president of products at Clearswift, states that the problem is that nowadays IT is everywhere and accessible to so many persons.

On 17^{th} of December 2012, darkreading.com published an article [24] with five significant insider attacks of 2012. One disgruntled senior IT technician took terabytes of sensitive information from the swiss intelligence agency. He had unrestricted access rights, which enabled him to do that. Till now they don't have information that the employee had transferred or published some of the information - but they can never be sure.
In this article there is also a record of an inadvertent insider. An employee of the South Carolina Department of Revenue was taken in by a spearphishing attack and released his credentials. The attackers had access to 3.6 million social security numbers and to 387,000 credit- and debit-card numbers.

2.6.4 Industrial Espionage

Goal of industrial espionage is to steal business secrets to gain a competitive advantage. It may be much cheaper to steal a new technology from a competitor than developing the technology. Industrial spies have a high amount of money at their disposal, what makes them very dangerous. If a company which does industrial espionage gets caught, its image will be damaged forever. For that reason companies take a high risk when spying [77].

USNews published an article [97] which is concentrated on industrial espionage affecting the United States. It states that the damage from industrial espionage in the U.S. is at least $250 billion a year. It also states that "[...] since 2006, a single Chinese army cyberattack unit has compromised 141 companies spanning 20 major industries, from information technology and telecommunications to aerospace and energy, using a well-defined attack methodology, honed over years and designed to steal large volumes of valuable intellectual property."

In [69] one can find an article about industrial espionage in 1981. Hitachi got one of IBM's workbooks with sensitive information in it. This is a very good example, that industrial espionage is done since a long time.

2.6.5 Press

When the press attacks, it's kind of an industrial espionage. The difference is, that press isn't looking for business secrets, but for good stories. Such attacks can be very dangerous, because often journalists don't hesitate to publish sensitive information (like state secrets). For their attacks, the press has a high amount of money and, if they are committed of their job, might take a high risk [77].

2.6.6 Organized Crime

On the one hand organized crime is abusing technology for attacking valuable systems like banks and customer databases. On the other hand, technology is used for better coordinating the crime (e.g. mobile phones and online banking for money laundering). Criminals often don't have technological knowledge, but they have a lot of money. So knowledge and even access to systems can get bought [77].

2.6.7 Police

Police is a kind of national intelligence service, but with lower resources [77]. They attack systems, for fighting against crime. Things can be done at a lower risk, because the law is on their site. But for certain actions a court order is needed. Because of that reason in general honest people mustn't have fear of such attacks. A problem arises, when the resources of the Police get abused. A corrupt police officer with access to attacking systems can cause a high damage [77].

CNET published an article [19] which states that the Russian police developed a device which helps them to gather data from SIM cards of mobile phones in a radius of five metres. The purpose of this device is to catch mobile phone thieves.

2.6.8 Terrorists

When terrorists attack computer systems, the only goal of them is to make damage. If they are successful, the consequences can be fatal. They may harm the economy, or community facilities with simple denial of service attacks. To reach their goal they take a high risk (till death). With few exceptions, in general they don't have much money and expertise and tend to make faults. Nevertheless, terrorists are a serious opponent.

2.6.9 National Intelligence Service (NIS)

National intelligence services are probably the strongest attackers. In general they belong to the military and get all money which is needed. Goals of NIS are military information, weapons, diplomatic information and also other goals not everyone thinks about. NIS sometimes does

industrial espionage and leaks the information to national companies. Also often Hackers get recruited to help NIS to reach its goals. All in all NIS is a very dangerous and effective opponent [77].

Recently there was an incident which showed the problem what happens when the activities of national intelligence services get public. On the 6^{th} of July 2013, the guardian published an article [92] about an observation program of the American national intelligence service NSA. After some further publications of the guardian, on 9^{th} of July 2013, the informant, Edward Snowden, got presented. He was an employee of a company that worked for the NSA. Because of that, this is also a very good example for a malicious insider attack.
As a reaction to such an observation program many protests where organized and many criticism raised. That was really bad publicity for NSA.
According to [60], as a reaction, the NSA planned to release 90% of its system administrators after the incident with Edward Snowden. They had fear, that some other employees would also publish sensitive information.

The article [61] from ORF shows that national intelligence services can do nearly everything with their unlimited amount of money. According to this article, NSA has payed millions of dollars to companies like Microsoft, Google and Yahoo, for adjusting their technology on requirements of the NSA. A normal hacker wouldn't have the money and persuasiveness for reaching that.
A later published article from ORF [62] stated, that the NSA even got further. They paid millions of dollars to software companies, for opening up backdoors only for NSA. That means that even encryption of emails or VPN tunnels don't provide a proper protection from the NSA.

2.6.10 Infowarriors

Infowarriors are kind of soldiers. Their goal is to diminish the clout of the opponent. Therefore they have the same resources as the NIS. The difference to the NIS is, that infowarriors are not risk averse. Their spectrum covers the simple change of a system up to the complete destruction of it [77].

Table 2.1 sums up the different attackers and provides a good overview of the different motivations and resources of the different attackers.

Attacker	Motivation	Money	Willingness to take Risk
Hacker	Learning	Little	Low to High
Single Perpetrator	Money	Little	High
Malicious Insider	Revenge, money, publicity	Little	Low to High
Industrial Espionage	Information gain	Much	High
Press	Information gain	Much	High
Organized Crime	Criminal activities	Much	High
Police	Fight against crime	Much	Low
Terrorists	Destruction	Little	High
NIS	Information gain	Very much	Low
Infowarriors	Military attack	Very much	High

Table 2.1: Motivation, resources and risk aversion of different attackers

CHAPTER 3

Common IT Components in Corporate Environments with Focus on Communication Systems

This chapter gives an overview of the role of the IT in companies. Furthermore common communication components of common companies are getting described. These components will later get analysed regarding security.

3.1 IT in Companies

Nowadays companies collect more and more information during their daily business [72]. It isn't possible anymore to handle this huge amount of information manually with pen and paper. Instead proper IT systems are needed for handling. Furthermore information can and should be used by companies to adjust their business processes and to gain a competitive advantage. For such warehousing tasks, IT systems are necessary [72].

According to Gutenberg, production factors are all goods, which are needed for the process of production of goods and services [72]. Therefore also IT respectively information is a production factor. It is actually a very special factor. According to [72], information and its processing (which is IT), is a link between the elements of the model of Gutenberg.

IT is used in companies for several different purposes. But in general IT is used to actively support business and to carry out a contribution to the business goals [100].

IT for enhancing productivity is the most important purpose. Productivity can be enhanced in many ways, for example either by automating processes or by just supporting business processes. Often IT is used to analyse and optimize business processes [10].

IT for communication is used broadly. Nowadays many parts of communication take place over IT systems. Even, more and more phones get replaced by IP phones, which allow to talk over IP. Most companies use email instead of letters and instead of publishing a company newspaper manually, an internal company wiki is used [9].

IT for administration A lot of administrative work is done with the help of IT systems. Nearly every company is using software for accounting. This can be a powerful software like SAP or a simpler one like Excel.
With the amount of digital information which can be analysed with tools, IT enables decision makers to use this information for strategic decisions [72].

IT for fulfilling legal requirements Often it is required by law, that companies have to document their activities. Also some security issues are often given by law. These could be, for example requirements on personal data, data security or requirements on health authorities. For implementing such requirements IT is often used [72].

3.2 Common IT Communication Components of a Company

Before the appearance of the Internet and email, communication already was an essential part in companies. Basically two different communication channels were used:

- Telephone
- Fax

With the help of these components, at that time the whole communication was possible. Because of the growing interconnection between and within companies and the therefore growing communication demands, nowadays such communication components would not be sufficient. Instead the following components are now used:

- Voice over IP and mobile phones
- Instant messaging
- Email
- Wikis
- Cloud Computing

Voice over IP (VoIP) services have replaced or are currently replacing the classical telephone infrastructure [98]. Also Skype, which is working with VoIP, is used. Often even telephone isn't used anymore. Instead mobile phones are used.
Instant messaging (e.g. Spark, ICQ) has partly replaced short telephone calls and personal conversations. When one employee wanted to ask small questions, formerly he always had to call or visit the person he needed. Often the said person had no time and the point in time was adverse. Nowadays, instant messaging can be used for such scenarios. With instant messaging, one can

answer a little bit later when he has time.
Email has almost fully replaced fax. Some companies are still using fax as an alternative to email, but almost every company is using email nowadays.
Nowadays, also Wikis and Cloud Computing are used as communication components, although they are not communication components in classical sense. If used in a special way (for communicating), also these components can be seen as communication components.

This thesis concentrates on VoIP and email communication. To get an overview, these two and the other communication devices are described basically in the following sections.

3.2.1 Email

Email stands for electronic mail. It enables the users to send messages and all kinds of data over the Internet to one ore more recipients [48]. Nowadays email can be used from many different (mobile) devices [95]. Some of them are:

- Personal computers
- Laptops
- Tablets
- Mobile phones

3.2.2 Voice over IP

Voice over IP enables users to make phone calls over IP respectively the Internet or another network. This enables the users to save costs. Special IP phones with LAN connections are necessary. With the help of special adapters, even classical phones can be made usable for VoIP [5].

3.2.3 Instant Messaging

For instant messaging all participating users must have installed a client which supports the functionality. It works like a chat. So when one user sends a message to another user with the help of push, the message immediately pops up at the recipient. Many clients also support the transfer of multimedia data like images, music and so on [102].

3.2.4 Mobile Devices

Mobile Devices became very powerful in the last years. They developed from simple mobile phones with telephone and SMS functionality to multimedia devices called smartphones. Nowadays, with the help of mobile devices people can nearly do everything, they can do at home, including receiving and sending emails and using instant messaging. Some mobile devices are:

- Mobile phones
- Smartphones

- Tablets
- Laptops

3.2.5 Wikis

Wikis are used for building knowledge bases. Every user can read and write all articles. That means, if one article is written by a user, another user will be able to rework on it. In companies wikis are often used for placing guidelines, instructions, documentations and so on [31]. That makes it kind of a communication component [31].

3.2.6 Cloud Computing

With the help of cloud computing resources can be shared over the internet. There are many different resources which can be shared, also communication resources. One simple example for communication over a cloud is: One employee places instructions on the cloud. Some reviewers have a look, and comment it. After a rework, all other employees read it. This can also get implemented with a wiki. [11].

3.3 Definition of Communication Channels

In this section the term "communication channel" gets defined. Therefore the whole communication model has to get described briefly. The description will take email as an example.

According to Shannon [80], communication systems consist of essentially five parts:

1. Information source:
   The information source states the producer of one or more messages. This is the person or computer who writes the email.

2. Transmitter:
   The transmitter states the system which actually sends the information over the channel to the receiver. In case of email this is a computer which processes the written text as an email.

3. Channel:
   According to Shannon, the channel is the medium which is used to transfer the information from the transmitter to the receiver. In this thesis a channel stands for a whole communication system (e.g. email, VoIP).

4. Receiver:
   The receiver converts the information in a readable format for the destination. In case of email this is the email server or the computer of the person which receives the email.

5. Destination:
   The destination states the person or computer "[...] for whom the message is intended" [80]. This is the person which receives the email.

3.4 Business Data in Communication Channels

Nowadays every company uses email and other communication channels for communicating with partners, competitors and customers. A lot of information gets transferred this way. Often this information is sensitive business data. The problem is, that an email or a message over instant messaging is written and sent fast. Often people don't bear in mind that the content is confidential and that the information is possibly accessible to untrusted third parties.
PhoneFactor did a survey [65], in asking people how they and their companies use email. 73% of the participants stated, that they send sensitive information over email. With 59% proprietary company information is transferred mostly over email. On the second place with 54% email is used for sales communications. With 49% and 48% sensitive information about customers and intellectual property are also very often transferred via email.
Taking into account these points, the communication channels have to get protected properly. For protecting the contents of messages in communication channels already several security measures exist. Later on one will see that even the traffic data can reveal sensitive information.
Especially when taking into account email and VoIP privacy is a big issue. Often emails and calls should not be traceable. If an attacker eavesdrops traffic data of an email or a VoIP call, he must not be able to retrace back to the sender respectively the caller. This requirement on communication channels might be interesting for contract negotiations, where it should not be possible to reveal a connection between two parties.
Furthermore, often confidential business data can also get revealed when attacking traffic data. The subject field, for example is part of the traffic data of emails. Employees often already write confidential information in this field.

CHAPTER 4

Technical and Data Analysis of Communication Systems

In this chapter the technology of the mostly used communication components, which are described in chapter 3 get analysed. For each communication component, at first the general composition, the protocols and standards as well as the used message format get described. Additionally the processed data in the respective communication component gets analysed and classified according to the information value. Therefore the data is distinguished in traffic and content data.

4.1 Analysis of Email Communication

4.1.1 General Composition of Email

For sending an email, a sender address and a recipient address are needed. Each address consists of two parts. The first part, which is called *local part*, identifies the recipient at his mail server. The second part, which is called *domain part*, identifies the mail server in the Internet and it is a DNS name which has an IP entry [22].

For illustrating we are assuming that Alice, who has the address Alice@mailA.at, wants to send an email to Bob, who has the address Bob@mailB.at.
When an email gets sent, it is first transferred to the mail server of the sender. For this transfer the *Simple Mail Transfer Protocol (SMTP)* is used. More on that in section 4.1.3. In the example first the email is sent to the mail server of Alice which is mailA.at [22] [79].
Then the mail server tries to find the mail server of the recipient, which is the mail server mailB.at in that case. The address of the recipient, the mail server gets from the header part of the email message. At first eventually available local DNS servers are queried to get the IP address of the recipient's mail server. If none can be found locally, DNS servers in the Internet will be queried for the MX Resource Record [44]. MX Resource Records are entries for SMTP services. When

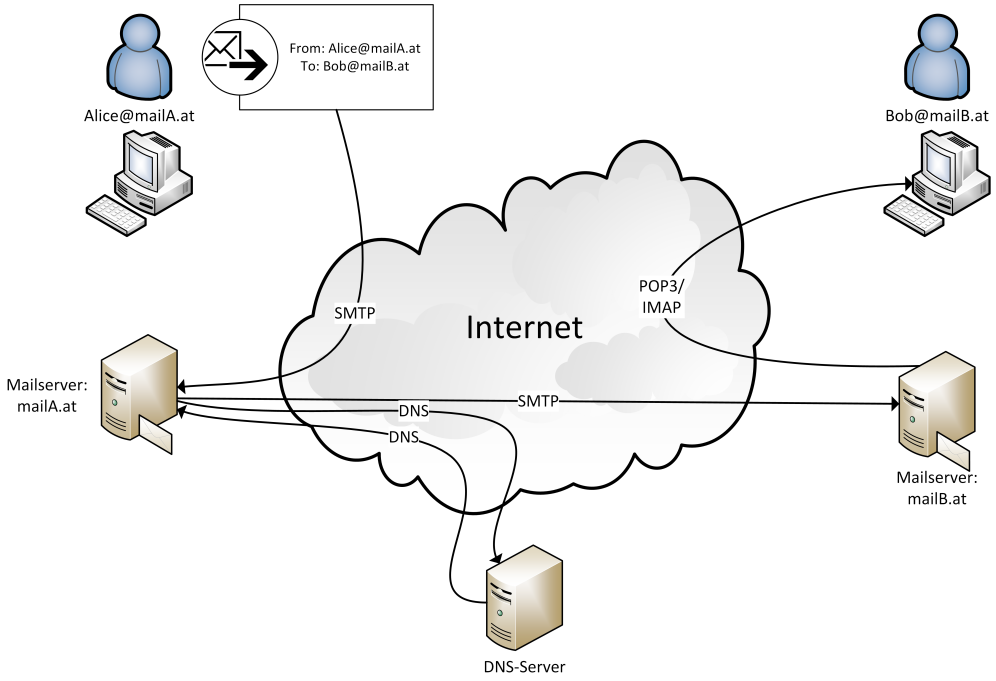

Figure 4.1: General components of Email communication [79] [22]

the mailsever has the IP address, then the message is transferred over SMTP to the mail server of the recipient [22] [79].
Now the local part of the email is needed. The mail server of the recipient will check if there is an entry for the recipient. If not, the original email message and an error message will be sent back to the sender [22]. If there is an entry, the message will get stored for the recipient [22].
For reading the email the recipient has three possibilities. The easiest one is to have a look in the webmail account at the mail server and read the email in the browser. For this method the *Hyper Text Transfer Protocol (HTTP)* is used. The next possibility is using the *Post Office Protocol version 3 (POP3)* for downloading the email to the computer of the recipient. When using POP3, the emails have to get fetched from the mail server and then they are only available locally on the computer. The emails are not remotely accessible [22]. The most powerful possibility to read emails is the Internet Message Access Protocol (IMAP). In contrast to POP3, with IMAP the emails stay stored on the mail server in general. More of the protocols one can find in section 4.1.3. The whole description of the general composition is illustrated at figure 4.1 [22].

4.1.2 Email Message Composition

An email consists of two parts. The first part is the header. As the header includes control information of the email, it can be seen as traffic data. The second part is the body. It includes the human readable text or data for the recipient. This part can be seen as content data [70].

4.1.2.1 Email Message Header

RFC 5322 [70] differs between header-field and header section. A header-field is one single header entry (e.g. the to field). The header section names the whole header of the email.

The only fields in the header, which must always be set, are the origination date field and the originator address field(s). All other fields are, theoretically, optional. In practice more than the two required fields are set [70].

According to [70] and [43] an email can have the following header-fields. The category in table 4.1 corresponds to the more detailed description later on.

Field	Min. Number	Max. Number	Should Occur	Category
received	0	unlimited		Trace
return-path	0	unlimited		Trace
resent-date	0	unlimited	yes	Resent
resent-from	0	unlimited	yes	Resent
resent-sender	0	unlimited	yes	Resent
resent-to	0	unlimited	yes	Resent
resent-cc	0	unlimited	yes	Resent
resent-bcc	0	unlimited	yes	Resent
resent-msg-id	0	unlimited	yes	Resent
orig-date	1	1		Originate Date
from	1	1		Originator
sender	0	1		Originator
reply-to	0	1		Originator
to	0	1		Destination Address
cc	0	1		Destination Address
bcc	0	1		Destination Address
message-id	0	1	yes	Identification
in-reply-to	0	1	yes	Identification
references	0	1	yes	Identification
subject	0	1		Informational
comments	0	unlimited		Informational
keywords	0	unlimited		Informational
optional-field	0	unlimited		Optional

Table 4.1: Header fields of email header [70]

Trace This field is a group of fields. It consists of one or more received fields and an optional return path field. So if the trace field is in use, at least one received field will have to be in the header [70].

Received This field gives information about the way the email took threw the Internet [44]. Each server which forwards the email adds an own received field with the IP address and a date time to this field [44].

return path After the final delivery of the email, that means, when the email is leaving the last SMTP server, the SMTP server adds the return path. The return path can be different from the sender (e.g. when errors should be delivered to another address) [70].

Resent When resent fields are used, it means that an email got reintroduced into the transport system by a user [70]. With these fields the email seems to come from the original sender for the recipient, because all other fields do not change. Each resent field corresponds to a matching field in the header. For example the resent-date field corresponds to the date field. When using resent fields, the resent-date and resent-from field must be used. When an email gets resent more times, for each time new resent fields will be added [70].

Origination Date The origination date field must always be in the email header. Its syntax is "Date:" date-time. The date field states the date and time, when the sender finished the mail and commits the email to be ready for transport. It isn't the time when the email is actually transported. The RFC 5322 [70] gives a good example: When someone writes an email and clicks the send button in the mail program, but is not connected to a network, the mail is put into a queue. In that case the date will be the date when the user has put the mail into the queue [70].

Originator Fields are for identifying the origination of emails. Three header fields belong to the group of originator fields [70]:

from The from field has to be present in every mail header. It specifies the mailbox(es) of the author(s) of the email. If there are specified more mailboxes, the sender field will have to be set [70].

sender The sender field specifies the mailbox of the person who is actually responsible for transmitting the email. RFC 5322 [70] gives a good example: If a secretary has to send an email for another person, the mailbox of the secretary will be in the sender field. Whereas the mailbox of the original author would be in the from field.

If the person who is responsible for transmitting the email and the person who actually writes the email are identical, then the sender field will not have to be set [70].

reply-to The reply to field is a suggestion from the author to the recipient. It states the address, to which the recipient should send a possible answer [70].

Destination Address Fields indicate the recipients of the email. Each field contains zero or more addresses. The usage of the different fields differ.

to The to field indicates the actual or main recipients of the email [70].

cc The cc (carbon coby) field indicates secondary recipients of the email [70].

bcc The bcc (blind carbon copy) states recipients who should receive the email, but must not be visible to other recipients [70].

Identification Fields As one can see in table 4.1 all identification fields are optional. But RFC 5322 [70] states that each email should have a message-id. It also states that each reply email should also have an in-reply-to and a references field.

message-id The message-id is a globally unique identifier which belongs to one particular version of an email. When the email changes, then a new message-id needs to get generated. The host, that generates the message-id, is responsible for the uniqueness [70]. For guaranteeing uniqueness several algorithms are possible. In RFC 5322 [70] section 3.6.4. an example algorithm is shown.

in-reply-to In contrast to the message-id field, the in-reply-to and references field can contain more than one unique identifier. The in-reply-to field contains the message-id of the email to which the actual email is a reply. If there are already some replies, then all parent message-ids will be contained in this field [70].

references The references field may be used to identify a "thread of conversation" [70]. For each email the message-id will be added to the references field [70].

Informational Fields The informational fields have no technical functionality. That means they are not machine readable, but human readable [70].

subject The, most common, subject field contains a short text which describes the topic of the content of the email [70].

comments The comments field contains additional information about the text in the body section of an email [70].

keywords "The "Keywords:" field contains a comma separated list of important words and phrases that might be useful for the recipient" [70].

Optional Fields The RFC 5322 [70] defines the optional fields for fields which are not specified in the RFC. All optional fields must not be identical to any other field which is specified in the RFC.

4.1.2.2 Email Message Body

The body of an email is very simple. RFC 5322 [70] only specifies some encoding issues regarding the body of an email. In general the body contains just text.

```
Received: from x.y.test ([195.3.96.112])
   by example.net
   via TCP
   with ESMTP
   id ABC12345
   for <mary@example.net>;  21 Nov 1997 10:05:43 -0600
Received: from node.example ([89.144.192.69]) by x.y.test; 21 Nov
1997 10:01:22 -0600
From: John Doe <jdoe@node.example>
Sender: Michael Jones <mjones@machine.example>
To: Mary Smith <mary@example.net>
Subject: Saying Hello
Date: Fri, 21 Nov 1997 09:55:06 -0600
Message-ID: <1234@local.node.example>

This is a message just to say hello.
So, "Hello".
```

Figure 4.2: Example email with trace information [70]

4.1.2.3 Example Email

This section should serve to get a better understanding of the theoretical concepts described before. The examples are taken out of the RFC 5322 [70]. The example in figure 4.2 is adjusted to match the needs of this thesis.

Figure 4.2 shows an email where trace fields (received) are set. In general such trace information must be read from bottom to top. So the IP *89.144.192.69* is the IP of the origin of the email. The next station, which has the IP *195.3.96.112*, also adds a received field.
Furthermore in this example, the author of the email(John Doe <jdoe@machine.example>) is not the actual sender (Michael Jones <mjones@machine.example>) of it. Therefore the sender field is also set.

Email headers can get analysed online with iptrackeronline.com [40].

Figure 4.3 shows an example where the resent fields are set. Mary receives this email from John. She wants to forward it to Jane, so that Jane thinks the email comes directly from John. Furthermore, when Jane replies to the email, the reply should go directly to John. Of course all original information in the email header should not be modified. For these three goals, resent fields have to be added to the email [70].

4.1.3 Protocols and Standards

In this section, the used protocols and standards of email, which are important for the understanding of this thesis, are described.

```
Resent-From: Mary Smith <mary@example.net>
Resent-To: Jane Brown <j-brown@other.example>
Resent-Date: Mon, 24 Nov 1997 14:22:01 -0800
Resent-Message-ID: <78910@example.net>
From: John Doe <jdoe@machine.example>
To: Mary Smith <mary@example.net>
Subject: Saying Hello
Date: Fri, 21 Nov 1997 09:55:06 -0600
Message-ID: <1234@local.machine.example>

This is a message just to say hello.
So, "Hello".
```

Figure 4.3: Example email with resent fields [70]

4.1.3.1 Multipurpose Internet Mail Extension (MIME)

The Multipurpose Internet Mail Extension (MIME) standard, introduces new header fields to the email header. It enables to send text encoded with other encodings than the American Standard Code for Information Interchange (ASCII). It also enables to send multimedia content like images and videos. The MIME standard is defined in RFC 2045, RFC 2046, RFC 2047, RFC 2048, RFC 2049, RFC 4288 and RFC 4289. The RFC 5322 still stays valid [79].

According to [79] essentially three extensions get included when using MIME for emails:

- When using MIME, five additional header fields have to get included in the email header. These fields describe the transferred content.
- The content formats are standardized.
- Standardization of transfer encodings.

The five header fields introduced by MIME are:

MIME-Version RFC 2045 [33] states that each email that implements MIME, has to have a "MIME-Version:" field set. For future versions of MIME, this field should help to differ between the different versions. Currently version 1.0 is used. Therefore the field looks like: "MIME-Version: 1.0" [33] [79].

Content-Type According to [79] this is the most important header field of MIME. It describes the content of the email, which is located in the body. With the help of this field, the email programs can start the matching display modules [79]. The content-type field specifies the nature of the data. For this specification a top-level type and a subtype are available. For example when the content-type field includes image/xyz, the email program knows that the content is an image. Xyz can mean anything program specific [33]. Another example can be found in [79]. If text/html is the content-type, then the email program will know

that the transferred content is text. Through the subtype the program knows that the text should be interpreted as html. Table 4.2 shows the most important content-types [79].

Content-Transfer-Encoding As the RFC 5322 is still valid, and therefore the content of an email should be still transmitted as a series of ASCII characters, MIME provides a set of algorithms, which convert the content into this form. MIME provides [79]:

- 7 Bit: In that case the text is already in the correct format.
- 8 Bit: The text contains only short rows (smaller 999 characters). No special encoding is done, but nevertheless the text can contain non ASCII characters.
- Binary: The text can contain long rows. Also here no special encoding is done, but the text can also contain non ASCII characters.
- Quoted-printable: Non ASCII characters get replaced by a series of three ASCII characters. This encoding is mainly used for German texts.
- Base 64: This encoding is used when transferring binary data.

According to the particular content the proper content-transfer-encoding has to get chosen.

Content-ID This field is optional with one exception: When using message/external-body as content type, then it is mandatory [33]. Content-ID is syntactically identical to the message-id. "The Content-ID value may be used for uniquely identifying MIME entities in several contexts [...]" [33].

Content-Description This field is also optional. It serves to describe the content of the email. For example if an image is in the body, the content-description field might contain: "this is a picture of a flower". It will help to understand the email or to find failures even if the image can't be displayed [33] [79].

4.1.3.2 Simple Mail Transfer Protocol (SMTP)

The Simple Mail Transfer Protocol (SMTP) is a very simple protocol which operates on top of TCP and IP [96]. It is used to transfer emails from the sender to the email server and to transfer emails between servers. Another protocol is used to retrieve received emails (POP or IMAP) [22].
Figure 4.4 shows a sample sequence with SMTP. The person with the email address test@exampleA.at wants to send an email to the person with email address test@exampleB.at. After identification to the mail server of the recipient, the email can be sent. Therefore the sender, recipient and the data get sent to the server sequentially. The end of data is marked with a line with only a single "." [79].
SMTP doesn't guarantee, that the email reaches the recipient. If not, the email is returned to the sender, which has to send it again [96].

The original version of SMTP doesn't provide any encryption of the data. Furthermore authentication isn't possible. Therefore the original version can't be categorized as secure [96].

Type	Subtype	Description
text	plain	unformatted text (e.g. ASCII)
	html	html data
multipart	mixed	independent parts which get transferred together. Parts have an order which needs to get met
	parallel	Same as mixed, but with no order
	alternative	Alternative versions of the same information get transferred [79]
	digest	Same as mixed, but as default Message/rfc822 is supposed
message	rfc822	The content (or body) of the email is an email itself [79]
	partial	Indicates an fragmented email [79]
	external-body	Indicates an email, whose body or parts of it is located somewhere else
image	jpeg	Body contains an image in JPEG format
	gif	Body contains an image in GIF format
video	mpeg	Body contains a video in MPEG format
audio	basic	Body contains an audio file in single-channel 8 Bit ISDN, 8kHz format
application	pdf	Body contains a pdf-file
	octet-stream	Body contains binary data consisting of 8-bit-bytes [79]

Table 4.2: Most important, possible content types [79]

Because of that there is an extended version of SMTP, called Extended SMTP (ESMTP). With this extension, SMTP can be used with authentication. Figure 4.5 shows a sample authentication sequence. Precondition for using authentication is, that the server supports ESMTP. The client has to state explicitly, that he wants to use ESMTP. Then the server returns the possible authentication mechanisms. The client picks one and informs the server about it. In figure 4.5 the client chooses a simple login for authentication. Then the server requests the username and password sequentially with Base64 encoding. When the credentials were incorrect, the server returns an authentication failure [37].
The extension of SMTP also enables the use of TLS (Transport Layer Security) for the transmission. This process is called SMTPS. TLS provides a secure communication between user and server and between the servers already on the transport layer. The problem with TLS is, that it is not guaranteed that the email is transferred over it the whole transportation route. Only one server not supporting TLS can restrict the confidentiality [57].

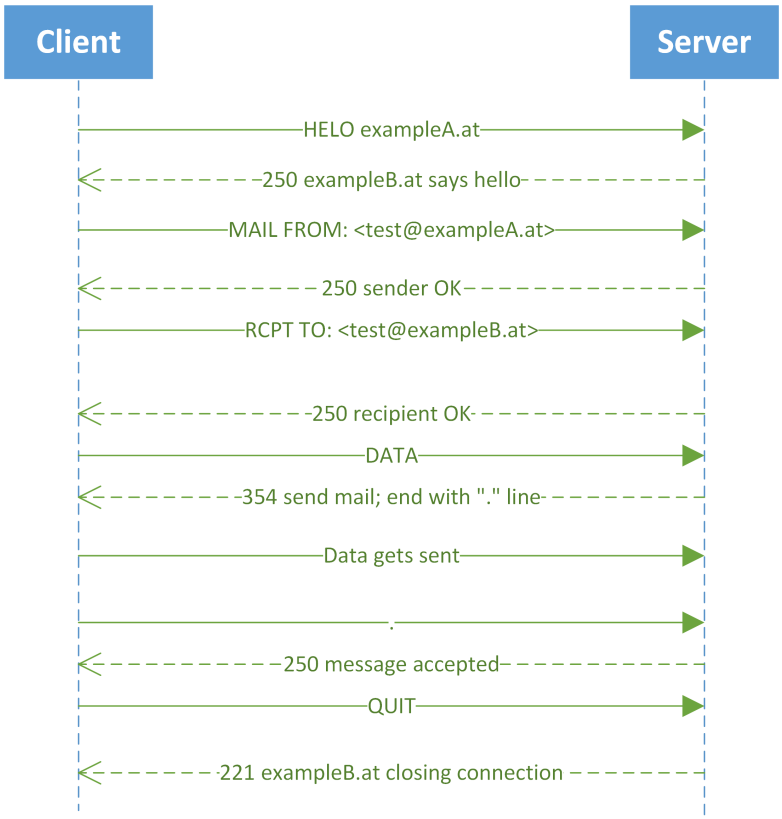

Figure 4.4: Sample sequence with SMTP [79]

4.1.3.3 Post Office Protocol Version 3 (POP3)

The emails which are transferred over SMTP, are not directly sent to the recipient of the email. Instead, the emails are stored temporarily on the email server of the recipient. If the recipient wants to view his emails, he has to retrieve them from the server. One possibility to do this is the Post Office Protocol (POP). The most recent version is 3, so it is called POP3. POP3 is a protocol for retrieving emails only. It cannot be used to send emails [37].

As default, POP3 uses the TCP port 110. Users who want to retrieve emails from the server have to authenticate. The implemented authentication mechanism of POP3 requires a username/password authentication. It is a big disadvantage, that the credentials are transferred unencrypted to the server per default. There is a possibility to cover this weakness. A challenge response protocol is offered. Therefore client and server need a shared secret. Both, client and server calculate an MD5 hash of the challenge combined with the secret. When the results are matching, then the authentication was successful. In practise this protocol is not practicable, because there is no mechanism to exchange the shared secret. Anyway, it may be practicable for smaller email servers [79].

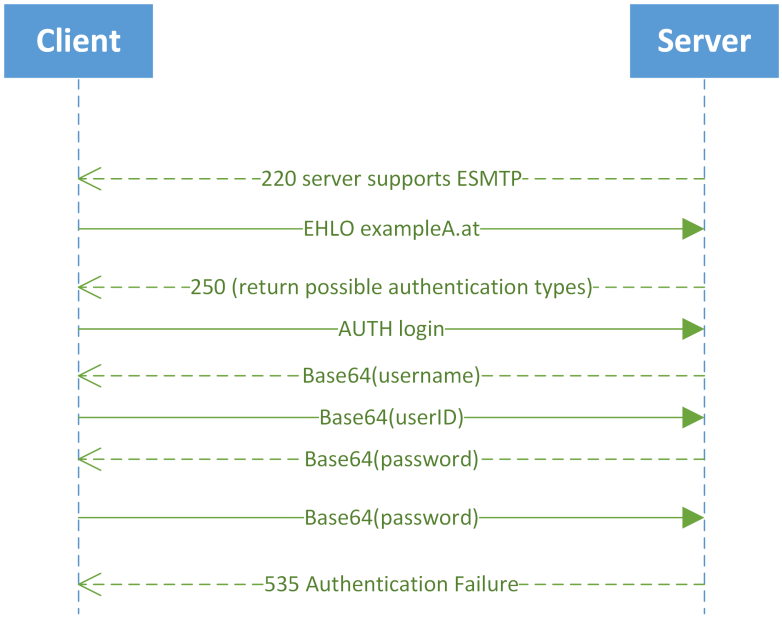

Figure 4.5: Sample SMTP authentication sequence [37]

TLS can also be used to make retrieving emails over POP3 more secure. This mechanism is defined in RFC 2595 [59]. For using TLS, the POP3 STARTTLS extension must be implemented. It is important to know, that TLS only secures the data over the network. For system administrators (e.g. on the mail server), the data is still available unencrypted. Therefore an end-to-end message security like S/MIME or PGP should be implemented additionally [59].

Figure 4.6 shows a sample POP sequence. At first the user has to authenticate himself. If the authentication is successful, the server will respond with the amount of messages. The user can use the command STAT to check the status of the mailbox. With LIST the user can list his emails. With RETR single emails can get retrieved. Then the server sends the email to the client. The end of the data is marked with a line with a single ".". It is possible to retrieve only single emails and delete only single emails, but many implementations just retrieve and delete all emails [37].

4.1.3.4 Internet Message Access Protocol (IMAP)

The Internet Message Access Protocol (IMAP) is an alternative to POP3. IMAP has the same features as POP3, but some additional powerful extensions. In contrast to POP3, IMAP uses TCP-Port 143 as default port [79]. Some features, which can be additionally used with IMAP, are:

- Secure authentication mechanisms [22]: IMAP requires, as POP3, authentication. The client can propose different authentication mechanisms. RFC 1731 [58] proposes three

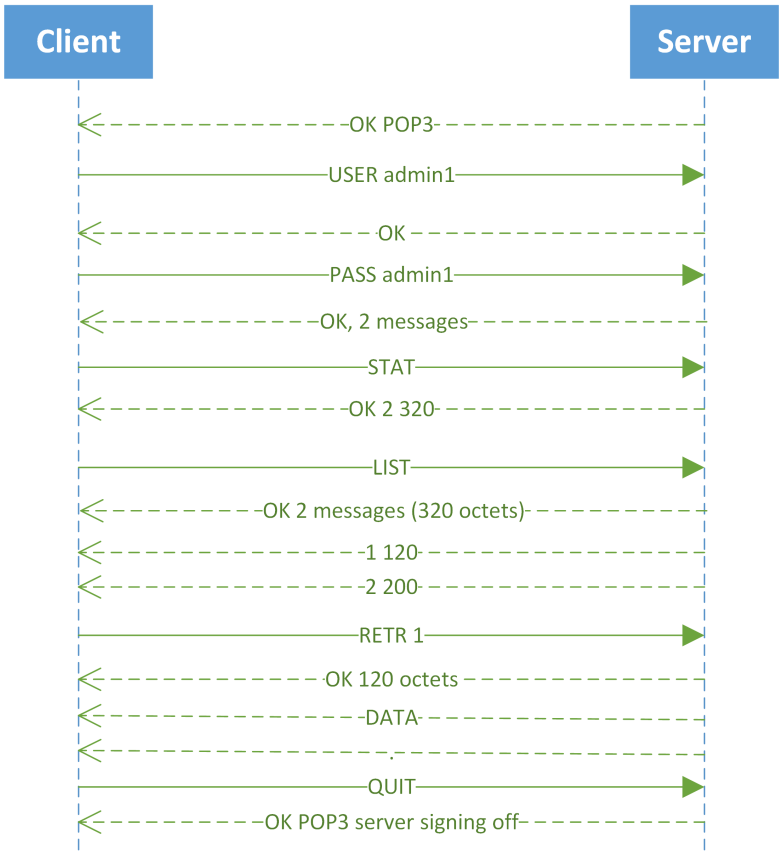

Figure 4.6: POP3 composed out of [37] and [79]

different authentication mechanisms. These are Kerberos, GSS-API and S/Key. But the authentication mechanisms can be extended to other methods [79].

- Multiple mailboxes can be managed at the same time, like it can be done with email programs like Outlook and Thunderbird [22] [79].
- Emails can be viewed remotely [22].
- Emails stay on the server and the client only has copies. That means, once an email is viewed, it gets marked as viewed on the server and on the client. Deleted emails are really deleted on the server. This enables consistent access, so that all clients with access, have the same information. That is a big difference to POP3. With POP3, when an email program crashes, and a new one is installed, all deleted emails (which were deleted in the program), will get retrieved again [79].

IMAP also allows the use of TLS. This mechanism is also defined in RFC 2595 [59], like for POP3.

4.1.4 Email Data Analysis

In this section, the data which is processed during an email process, is analysed. That means data gets classified according to the information value. Data with a high information value has a high risk, whereas data with a lower information value underlies a lower risk.

The data in the body of the emails is content data and therefore has a high information value. This is the data which potential attackers probably want the most. But in the last years the security developments [84] show, that the content of emails is getting more and more encrypted. In fact the encryption of emails is very simple and can be implemented by everybody. The article from Spiegel Online [84] states that since the NSA affair the amount of new uploaded PGP keys has increased a lot. According to the article from derStandard [27], the bigger email providers react to the NSA affair in encrypting the whole customer emails. This shows that the access to the content of emails is getting more difficult.

For attackers (for example NSA as recent occurrences showed), this is not a big problem as they can also concentrate on traffic data. The approval certificate [30] of Prof. Edward W. Felten as well as the article from Landau [49] show that the traffic data may be even more significant than the content data. Felten argues, that traffic data (he calls it metadata) is analysed easier than content data, because traffic data is structured. It is very easy to assign a telephone number or email address to a special facility or company [30]. For example if Alice writes an email to dr.bob@dentist.at, it will be easy to find out that she is communicating with Dr. Bob, who is a dentist. This information may be contained in the email address. If an address is not meaningful, a simple search for the owner of the email address will lead to a result. A pharmacy company for dentistry can use this information to infer, that Alice has tooth problems. Because of that, this company can send advertisements for dental care products to Alice.
With the help of powerful tools, correlations of more than one email or phone call can get detected and analysed. Such correlations may reveal more information than single communications [30]. Felten presents a good example for such a scenario [30]: "*A young woman calls her gynecologist; then immediately calls her mother; then a man who, during the past few months, she had repeatedly spoken to on the telephone after 11pm; followed by a call to a family planning center that also offers abortions.*"
Because of that, traffic data can also be classified as data with high information value. Some parts of the traffic data are more important than others.

4.1.4.1 Data in Email Body

In the body of an email, the whole content of it is stored. If an attacker is able to read the body of the email, the confidentiality of the email will be compromised. Depending on the content maybe other security needs would be endangered. If a system administrator sends credentials to an employee via email, an attacker will be able to intercept and read it. Then also the authenticity may be compromised.

4.1.4.2 Data in Email Header

Table 4.3 shows the classification of some header fields. In this section only those header fields are analysed which are relevant for the thesis. This is not an analysis of all available header fields.

IP address of sender In the header of an email the whole trace from the sender to the recipient is stored. Knowing from which IP address the email got sent, can be very valuable for attackers. The IP addresses in the header are classified as having high information value.

MIME content-type The MIME content-type of an email can reveal much information of the content. When viewing the content-type, an attacker can find out the type of the content. As this information on its own is not valuable, but already reveals some information about the content, this data can be classified as having a middle information value.

MIME content-description If the data in the body is described in this field, it won't be necessary for an attacker to decrypt the content. For example: A CEO sends his department chiefs a picture of a new organigram and describes it in the content-description field. An attacker can intercept the email and find out the new structure of the personnel. Therefore this field is classified as high information value.

Origination date The origination date of an email can be used to create a time line of events. It can be classified as middle information value.

From and to The originator and destination address fields provide a lot of information. With these fields an attacker can find out all communication participants. Therefore these fields get classified as data with high information value.

References field The references field can help to find connected emails of a conversation. This information may be very valuable. It is classified as data with high information value.

In-reply-to field This field can be used like the references field. But it does not reveal as much information as it. Therefore it is classified as middle information value.

Subject The subject field can already contain content data. Many people even write the whole content of an email in the subject field when it is a short email. Therefore the subject has a very high information value.

Comments Also the comments to an email can already contain sensitive information and are classified as high information value.

Keywords The keywords field is one of the most critical fields. It contains the words which describe the content of the email. If attackers search for some special emails with certain keywords, this list will help them to find the proper emails. This data has a high information value.

Data	Information value
IP address of sender	High
MIME content-type	Middle
MIME content-description	High
Origination date	Middle
From and to	High
References field	High
In-reply-to field	Middle
Subject	High
Comments	High
Keywords	High

Table 4.3: Classification of email header data according to the information value

4.1.4.3 Data in SMTP

Nowadays the transport route is often secured with TLS. Therefore the data in SMTP and POP3 isn't analysed in such a detail.

Basically the data processed in SMTP is the email itself. Additionally some control information is processed. The email address of the sender and of the recipient are transmitted before the actual email is sent. With this information a filtering of emails is possible. For example a possible attacker can intercept only emails transferred over SMTP which come from a certain sender. If SMTP authentication is enabled, the server will send a list of possible authentication mechanisms to the client. An attacker may make use of this list. Furthermore, the credentials are transferred unencrypted with Base64 encoded [37]. These data can be classified like shown in table 4.4.

Data	Information value
Sender address	Low
Recipient address	Low
List of authentication mechanisms	Middle
SMTP credentials	High

Table 4.4: Classification of SMTP data according to the information value

4.1.4.4 Data in POP3

Also POP3 has some control information which can be used by attackers. If the credentials used for retrieving emails with POP3 are transmitted unencrypted, they will have a high information value for attackers. Furthermore, other commands of POP3 like STAT and LIST can get eavesdropped. They reveal information about the size and amount of messages on the server.

Data	Information value
(Unencrypted) POP credentials	High
POP commands and returns	Low

Table 4.5: Classification of POP3 data according to the information value

4.2 Analysis of VoIP

4.2.1 General Composition - Voice over IP

Voice over IP (VoIP) is a notion for phoning over a network which is based on the internet protocol (IP). Therefore the used protocols for VoIP are located at the application layer (layer 4) of the TCP/IP reference model (see section 2.5). The devices which are used for phoning are called IP phones. An IP phone can be a special telephone set which is connected to an IP network. Also a normal computer can get extended, so that it can be used as IP phone. In that case an IP phone is called soft IP phone [5].

The general composition of an IP phone network looks like figure 4.7. It shows two users talking over the Internet. In fact it can be any IP network and must not be the Internet. In that case, the two users communicate with normal computers, adjusted for IP phoning [5].
For each call a RTP-Session (or VoIP-Session) must be established and after the call it must get terminated. RTP (Real-time Transport Protocol) is mainly based on UDP [88]. That means on layer 3, UDP is used. The resending mechanisms of TCP cannot be used, because VoIP is real time data. If the transmission of a single packet is faulty, it will make no sense to send it again, because the containing information would be outdated [5].
For each VoIP Session, two ports are used. The first port is used for exchanging digital speech. This virtual channel is a media channel and is called RTP-Channel. The second port is used for exchanging reports between the IP phones, including information about the phoning process. This control channel is called RTCP-Channel (RTP Control Protocol Channel) [5].

For establishing a VoIP Session, a signalling protocol is needed. Either Session Initiation Protocol (SIP) or the H.323 protocols can be used for that purpose [53]. According to [105] SIP is the dominant signalling protocol in deployed VoIP systems. Therefore it will only be dealt with SIP in the next parts. Furthermore the speech has to get digitalised. Therefore, several encoding mechanisms are possible. During the establishment of the session, the used mechanisms are turned out between the communication participants. It will not be dealt with the different encoding mechanisms in this thesis. [5].

Because VoIP has not fully replaced the classical (ISDN) telephone infrastructure (yet), some mechanisms which allow to combine both approaches are necessary. Such devices which take care of that, are called VoIP gateways [53]. These gateways must be able to assign telephone numbers to the appropriate IP addresses and vice versa. The gateway itself also must have an IP address and a telephone number. Figure 4.8 shows such a composition. That means, a ISDN

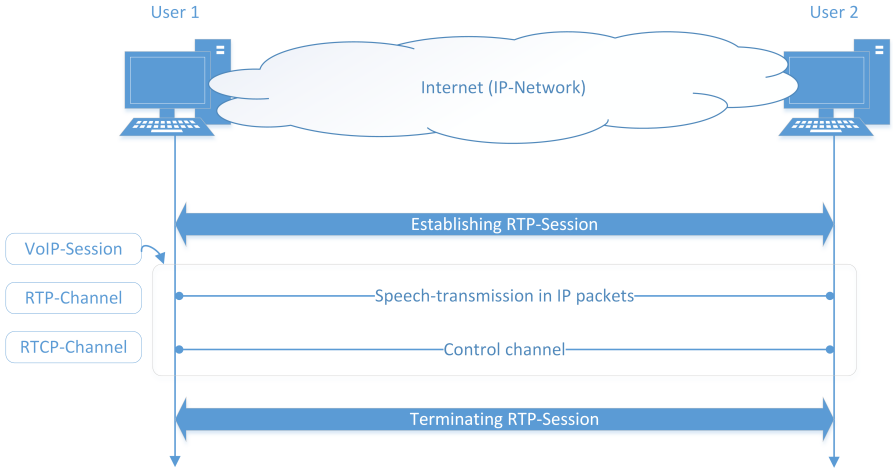

Figure 4.7: General composition of VoIP communication [5]

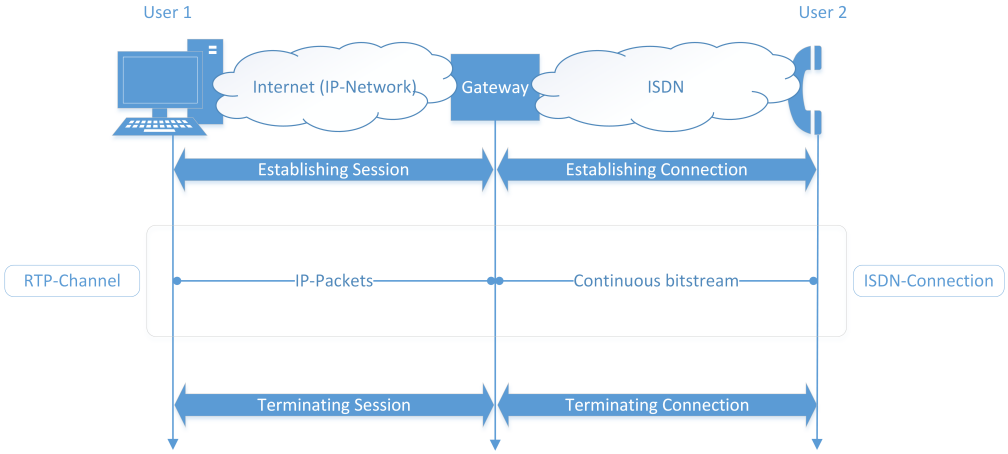

Figure 4.8: Extension of VoIP network with ISDN [5]

connection and a RTP channel have to get established for such a communication [5].

The possibility of extending VoIP with ISDN and vice versa, opens up many different scenarios [5]:

- Extension of ISDN with IP phone net [5].

- IP phone net as backbone for ISDN
  An ISDN network is established between two communication participants. There is also an IP network between them. They have an agreement, that phone calls go over VoIP. If one wants to call the other, he will enter the number. The gateways know about the

agreement and match the proper IP address to the number. Then the call goes over the IP network [5].

- IP phone net as connection between classical phone infrastructures
  [5] presents a good example for this scenario. If a company with several locations still uses classical ISDN devices in the different locations, there will be a possibility to connect the locations with VoIP. With help of that, the connection over the ISDN network can get eliminated and costs can be saved. Precondition is that the locations are connected over an IP network [5].

When spoken of VoIP, often only the terms SIP and H.323 occur. But these protocols are just signalling protocols. In fact, for VoIP also other protocols are needed. [5] defines the following classes of protocols:

- Protocols for speech transmission (RTP and RTCP)
  For transferring speech in real time, special protocols are needed [5].
- Signalling protocol (H.225.0 and H.245 out of H.323 or SIP)
  These are needed for establishing and terminating connections [5].
- Protocols for the control of media gateways (Media Gateway Control Protocol or Media Gateway Control)
  These protocols are needed for the integration of classical ISDN networks in VoIP [5].

4.2.1.1 Managed vs. Unmanaged VoIP

VoIP systems can be classified in managed and unmanaged systems. According to [14] residential and corporate VoIP systems are typically managed systems, whereas direct computer-to-computer VoIP systems are typical unmanaged systems. In managed VoIP systems, a call gets set up and managed by a service provider through its service gateways. Unique phone numbers get assigned to the customers who use “real“ VoIP phones. In unmanaged VoIP systems, a service provider isn’t used. Instead peer-to-peer technology can get used. The users of unmanaged VoIP systems mainly make use of user ids and soft VoIP phones [14].

4.2.2 Message Composition

4.2.2.1 SIP

A SIP message can be a request or a response message. RFC 3261 [71] defines the following request types:

- **INVITE**
  With this request, a session gets initiated. An INVITE message contains, amongst others, the addresses of the sender and recipient and the description of the session. This description is done with the Session Description Protocol (SDP) [71] [5].
- **BYE** signals that the session should be closed [71].

- **ACK** serves as positive acknowledgement [5]
- **CANCEL** is sent, when the session initiation should get aborted [71].
- **REGISTER** serves to inform the registrar, amongst others, about the location of users [5].
- **OPTIONS** serves to query the possible encodings and formats of IP phones [71].

RFC 3261 [71] defines also the possible response messages in response classes:

- **1xx: Provisional**
  These responses inform the sender that the request is continued processing [5] [71].
- **2xx: Success**
  These responses inform the sender that the request was received and accepted [5] [71].
- **3xx: Redirection**
  These responses inform the sender of a request, that further actions are necessary for processing [5] [71].
- **4xx: Client Error**
  These responses inform the sender of a request, that the request had a wrong syntax or can't be executed by the SIP server [5].
- **5xx: Server Error**
  These responses inform the sender of a request, that the SIP server can't execute the request [5].
- **6xx: Global Failure**
  These responses inform the sender of a request, that the request can't get executed at any server [5].

The SIP request and response messages have the same structure. They consist of three parts. The first part is the start line, the second part is the message header and the third part is the optional message body [71] [5]. "The body part is nothing more than a MIME body [...]" [42]. Figure 4.9 shows the difference between a request and a response message. For request messages, the start line is called request line. It includes three declarations [71]:

- *Method* states the request type.
- *Request-URI* states the SIP address.
- *SIP-Version*

A sample request line can look like `INVITE sip:bob@xyz.de SIP/2.0` [5]. For the response messages, the start line is called status line. It also includes three declarations [71]:

- *SIP-Version*

- *Status-Code* states the status code of the response.
- *Reason-Phrase* states the matching text to the status code.

[71] and [5] state the most important SIP header lines:

Allow The sender of a request can specify a list of supported requests in this header field. [5].

Call-ID This header field represents an identification of the call. It can be represented as a composition of a random number and the full hostname [5].

Contact represents the response address. All responses to this request have to get sent to this address [5].

CSeq serves to number the requests of a type. This field consists of a sequence number and the request type. For example if a request has the header field CSeq: 1234 INVITE, then the response to this request must also have this field [5].

From states the starter of the session. It can include a display-name, which identifies the caller name. When the caller name should not be displayed at the callee, the display-name must be "anonymous". The from field must contain the SIP address of the initiator. Furthermore there can be a tag field, which is used for dialogue identification [5].

Max-Forwards states the maximum number of proxies, the request is allowed to pass [5].

Via The via field can be compared with the received field of an email message. It serves to store the route, the request has taken. Each proxy, the request passes, adds its name and IP address. Therefore for responses, which adopt the via fields, it is easy to find the way back. A via field always starts with the SIP version and the used protocol [5].

Route This field serves to define a route. It includes a list of proxy servers, a request has to pass [5].

Record-Route A proxy can set this field, when a request passes. The proxy puts its name in the field. That means, that the rest of the signalling has to go over the proxy [5].

To has the same structure as the from field. It includes the address of the callee [5].

The body can include the description of the session based on SDP [5].

4.2.2.2 RTP-Packets

RTP packets consist of a RTP header, and a payload. This packet is encapsulated in the packet of the TCP/IP reference model. In that case RTP is the application data. In most cases, the transport protocol will be UDP. Figure 4.10 illustrates the encapsulation [5].

The RTP header consists of [5]:

Payload Type The payload type indicates the format of the payload data. That means it states if its audio or video and which encoding mechanism was used [5].

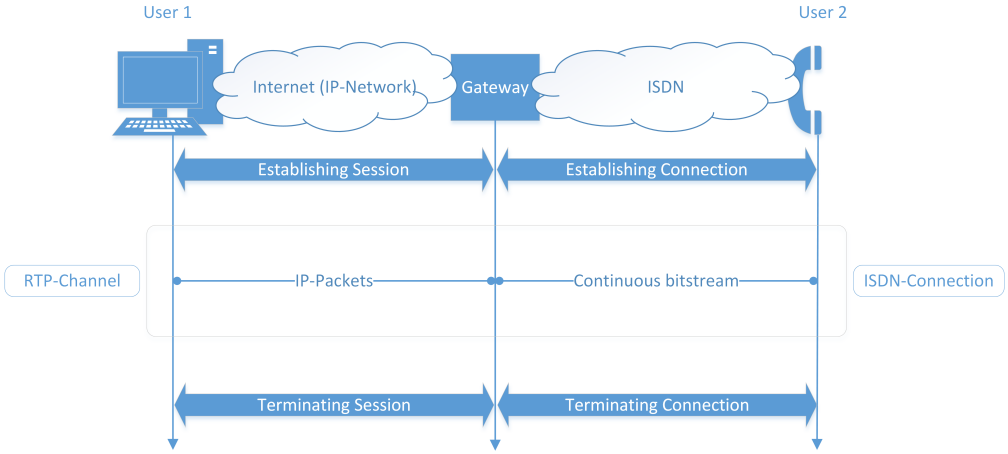

Figure 4.9: Structure of SIP Messages [5]

Ethernet header	IP header	UDP Header	RTP Header	Payload	Ethernet trailer

Figure 4.10: RTP Packet encapsulated [5]

Timestamp The timestamp is used for restoring the time intervals between the different RTP packets [5].

Sequence Number The sequence number is used for detecting the loss of packets and for bringing the packets back in the correct order if they got mixed up [5].

Synchronization Source Identifier (SSRC) RTP packets have a source. This source can be a microphone or a camera, for example. The recipient groups the packets for each source. Therefore the SSRC serves for identifying the different sources. The SSRC is also important, because the sequence numbers and the principle of the timestamp calculation are valid for one source [5].

Contributing Source Identifiers (CSRC) This field is optional. It will be used, if the payload does not come directly from the original source. That means it got forwarded from a system between. This system can be a mixer. CSRC is a list of original sources and gets determined by a mixer [5].

Version names the used version of RTP [5].

Padding is a boolean value. If true, padding bits are used in the payload. Padding can be necessary for encryption [5].

eXtension is a boolean value. If true, the field header extension is set [5].

CSRS Count states the number of sources listed at the CSRC field [5].

Marker The meaning of the marker, is determined by the transported payload [5].

Header Extension The optional header extension gives space for new classes of applications. It serves for extending the RTP packet [5].

4.2.3 Protocols and Standards

In this section, the used protocols and standards of VoIP, which are important for understanding this thesis, are described.

4.2.3.1 Real-time Transport Protocol (RTP)

RTP is used for transferring the speech data. It doesn't provide any mechanism for establishing a session. For that reason, a signalling protocol like SIP is used [67] [7]. A session can be seen as a state, where the participants of the communication have established some agreements. In general a VoIP session is a singlemedia session. That means that only one RTP channel and one RTCP channel are established. Therefore only one media can get transferred. But there is also the possibility to establish multimedia sessions. In such a case, more RTP and RTCP channels get established and more than one media can get transferred [5].

The main functions of RTP, according to [5], are:

- Transmission of real time data in RTP packets
- Guarantee of the order of RTP packets
  The RTP packets are numbered to restore the correct order when the packets got mixed up during the transmission.
- Guarantee of isochronicity
  Timestamps are used to restore the correct time intervals between the packets.
- Transport of different real time data formats
- Translator- and mixer usage
  Translators are used to transfer data from one format into another. Thereby a translator can also be used for guaranteeing the confidentiality. Therefore two parties use a private format, which is only known by them. A translator converts the bitstream in this format, before the stream enters the Internet. On the site of the recipient, a translator converts the stream back into a standard format. Mixers, receive bitstreams from different sources, merge them and forward them [5].

There is a possibility to encrypt the RTP channel. This alternative is called Secure Real-time Transport Protocol (SRTP) and is an extension of RTP. This protocol encrypts the transferred real time data and also provides mechanisms to check if the data really comes from the true sender [5].

4.2.3.2 RTP Control Protocol (RTCP)

RTCP is used for the control channel of the VoIP session. It serves to transfer status and control information. Mainly quality information is transferred with RTCP. But also information about the sources get transferred [5]. [5] lists the main tasks of RTCP in detail:

- Monitoring of the transmission quality
  Sender and recipient periodically exchange information about the transmission quality. The sender can so adjust the bitstream on the current conditions.
- Identification of the source
  The source of the bitstream can get identified with a canonical name (CNAME).
- Support of multipoint communication
  Status information about new participants and left participants gets exchanged periodically with RTCP. With that one can see a list of the actual communication participants.

[5] specifies 5 different RTCP packets:

- Sender-Report
  This packet is used for describing the transmission quality from the view of the sender. It can be used for transmitting the data rate to the recipient to avoid overload.
- Receiver-Report
  This packet is used to describe the transmission quality from the view of the recipient. Reports of packet loss, time interval errors and so on are possible.
- Extended-Report
  This packet allows the transmission of additional parameters.
- Source-Description
  This packet allows to assign textual names to sources.
- Log-Out
  This packet indicates the end of a communication.

The header of the RTCP packets are mainly equal to the header of the RTP packets. Therefore they are not separately discussed.

4.2.3.3 Session Initiation Protocol (SIP)

The Session Initiation Protocol (SIP), is a signalling protocol which is used in a broad area. Beside the usage for VoIP, it is also used for instant messaging, emergency services and many other applications [67]. It can be used with TCP, UDP, SCTP or DCCP. The term SCTP is used, when SIP is used over TLS. DCCP (Datagram Congestion Control Protocol) is, like UDP, a connectionless protocol, but with overload control. UDP is mainly used [5].
SIP defines two components. First is the user agent client (UAC), which is implemented by the client. Calls always get initiated by the UAC. The second component is the user agent server

(UAS) [5] [67].
SIP is a request/response protocol. That means that the initiator sends a request. The recipient sends a response after he received the request [5].
SIP uses its own address, called SIP address, for addressing. There are several different SIP addresses which can be used [5]:

- `sip:user@domain`

  This address identifies a special user (or the IP phone of this user) in a domain. For resolving this address, a SIP proxy is needed. This kind of SIP address is often used [5].

- `sip:user@hostname`

  A sample address would be sip:alice@moon.xyz.de. This means, that the host "moon" is the IP phone of the user alice in the domain xyz.de. For this address no SIP proxy is needed [5].

- `sip:user@hostname;transport=tcp`

  This address is the same as the one directly before. The difference is, that SIP uses TCP in this case [5].

- `sip:phone-number@hostname`

  This address indicates, that a user with a certain phone-number, is reachable over a certain host [5].

- `sip:phone-number@gateway.abc.de`

  This address states, that a certain phone-number is reachable over a certain gateway of the domain abc.de. This addressing allows the integration of classical ISDN networks [5].

- `sip:user@ipv4address`

  This address indicates that a certain user's IP phone is reachable over a certain IP address [5].

Figure 4.11 shows the, in [5] defined, so called SIP trapezoid model. This model consists of 3 layers. The first layer is the session level. At this level, there is the established session, where the users can exchange their real time data. The second layer, is the proxy layer. At this layer, the proxies of the different domains are located. A proxy is a representative for the IP phones of a certain domain. This proxy is called SIP proxy. Such a proxy is necessary to resolve the SIP addresses to IP addresses. Depending on the implementation and configuration of the SIP proxy, it logs all packets which it processes [16]. Later on one can see that this can be a big security issue.
The basic resolving process is carried out in two steps [5]:

1. Assuming that a user initiates a call over an IP phone to the address sip:bob@abc.de. At first the IP address of the SIP proxy of the abc.de domain has to get gathered. This is done with the help of DNS. DNS provides the matching IP address of the SIP proxy to the domain part of the SIP address [5].

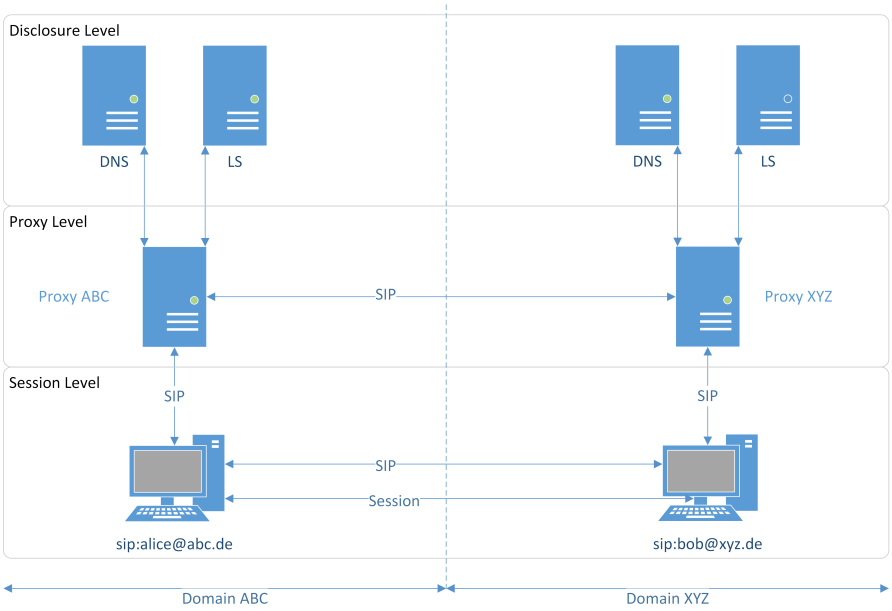

Figure 4.11: The SIP trapezoid model [5]

2. In the second step, the SIP proxy determines the IP address of the IP phone "bob". This allows a high user mobility. Because of the identifier (bob) of the IP phone, it can be located in the whole domain. Therefore it can be located at any computer or phone. The location can be entered at the SIP proxy or at a location server (LS). If a request enters the SIP proxy, it will have to query the location server for the current location of the IP phone [5].

Figure 4.12 shows how a basic initiation of a VoIP session looks like. The figure represents a scenario, where Alice with the SIP address `sip:alice@abc.de` calls Bob with the SIP address `sip:bob@xyz.de`. The initiation starts with an *INVITE* message. This message represents an invitation to a session. The INVITE is sent to the SIP proxy of the domain of the sender (in this case abc.de). This proxy queries a DNS server for the IP address of the SIP proxy of the domain of the recipient and forwards the INVITE to this proxy. Then the SIP proxy sends a *100 Trying* to the IP phone of the sender for acknowledgement. The SIP proxy of the domain xyz.de queries a location server for the current location of the IP phone of the recipient (bob). Then it queries the IP address of the location from a DNS server and forwards the INVITE to the IP phone. Then the SIP proxy sends a 100 Trying to the SIP proxy of the sender domain for acknowledgement [5].

If the IP phone of Bob and the IP phone of Alice are compatible, the IP phone of Bob will start to ring. This is signalled by sending a *180 Ringing* the whole route back to the IP phone of Alice. If the IP phone of Alice receives the 180 Ringing, a ringing tone will get generated [5].

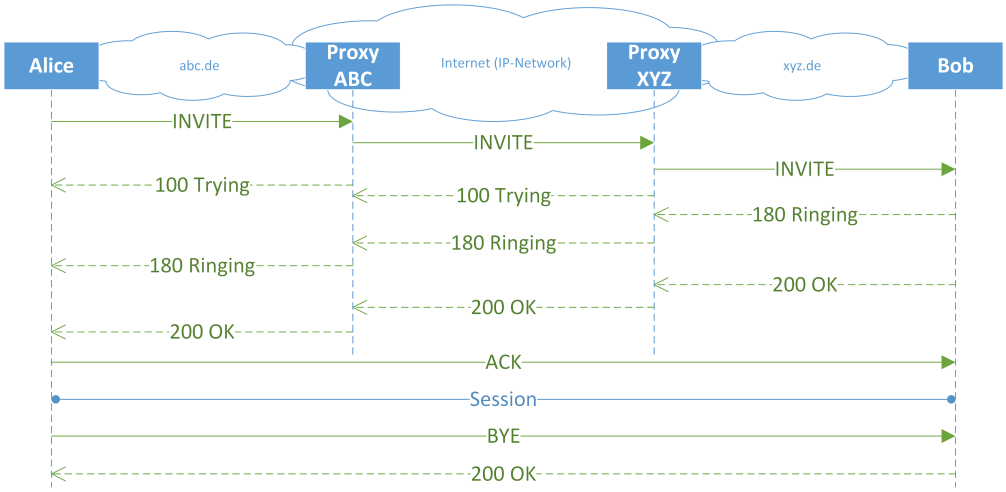

Figure 4.12: Typical SIP Sequence with two proxies [5]

If Bob accepts the call, a *200 OK* will be sent back the route to the IP phone of Alice. When the 200 OK arrives at the IP phone of Alice, an *ACK* is sent to the IP phone of Bob. After receiving the ACK, the session is established. Note that the ACK message is already sent directly to the IP phone of Bob [5].

The session can get closed by both parties. This is signalled by *BYE*, which is sent directly to the other party. This gets confirmed with 200 OK [5].

The whole process can also take place without proxies. In that case, the messages are sent directly between the IP phones [5].

4.2.3.4 Session Description Protocol (SDP)

This protocol is part of SIP. It serves to describe the requirements of the initiator of the session. If the recipient cannot fulfil these requirements the session will not be able to get established. This description is located at the body of a SIP message [5].
The initiator states his requirements in the body of the INVITE message. The recipient answers with a response and, in the body of it, with the description how he can fulfil the requirements [5].

Some SDP fields are [5] [38]:

- Session initiator
- Start and end time of the session
- Session name
- Connection information

- Media type
- Encoding mechanisms
- Encryption key

The encryption key is used by SRTP, when the session is established [2].

4.2.3.5 S/MIME for SIP

SIP can be used, like email, with the security standard S/MIME, because the body of a SIP message is a MIME body [42]. S/MIME is based on a public key infrastructure (PKI) and is used to guarantee confidentiality, integrity and authenticity. To protect the confidentiality with S/MIME the header fields which don't need to get interpreted by waypoints, can get transferred encrypted in the body of a SIP message [5] [42] [71]. That means, the sender encrypts the body with the public key of the recipient. To decrypt the body, the recipient can use his private key. The encrypted parts of the header (which are located in the body) are building a MIME object. Now the SIP message consists of two parts. The outer and inner part. The inner part is the MIME object which is encrypted. It consists of a header and a body. The outer part is the SIP header, which is unencrypted. It contains all parts of the original SIP header, which have to get interpreted on the transportation route [5]. These are: call-id, contact, cseq, from and to [5] [42] [71]. To protect the identity of the sender, the from field can be anonymous. Therefore the from field in the outer part will be set to `sip:anonymous@anonymizer.invalid`. The real sender can be stored in the encrypted MIME body. If S/MIME is used for signing, then the from field has to get set, because the recipient will have to find the correct public key of the sender [71].

To protect the integrity and authenticity, S/MIME can be used for signing SIP messages. Therefore the private key of the sender is used to sign the body of the message. This signature is appended to the body of the SIP message. The body contains information about what exactly got signed. So the SIP message consists of three parts. The header, body part 1 and body part 2 (signature). The recipient takes the identity of the sender from the from field, finds the matching public key and uses it to calculate the signature for the received body part 1. If the calculated signature and the one out of body part 2 are equal, the signature check was successful [5].

4.2.4 VoIP Data Analysis

As for email communication, in this section the data which is processed during an VoIP process, is analysed. Here also the data gets classified according to the information value.

In section 4.1.4 the criticality of traffic data got described, especially for email. In fact this is also valid for VoIP. Also phone numbers can get assigned to individuals very easy. The simplest way to do this would be to look up in a phone book. So if someone calls the number of a drug advisory service, the match of the number to the service would be easy. The person who called this number, or one of his friends or relatives, probably have a drug problem. When analysing the traffic data of that person one could find out which of his friends or relatives has the problem.

4.2.4.1 Data in SIP Header

Call-ID The call id identifies a special call. As this information can already contain the full hostname, it has a middle information value.

Contact The contact address provides information about the location of the caller. Therefore it has a middle information value.

From and to The from and to fields in SIP are as critical as the IP address and the from and to fields of emails. The used SIP addresses in these fields are unique and can be used to identify individuals. Therefore this data has an high information value.

Via This field is comparable to the received field of email. It stores the whole route of the SIP message. This data can be used to identify the SIP proxies which are passed during transmission. This information can be used to search for special proxies. The information value can be classified as middle.

Route This field is similar to the via field. It contains the predefined route and therefore tells which proxies the SIP message will pass. This information can be valuable for attackers and is classified as middle.

Record-route This field states that further signalling has to go over a certain proxy. When manipulated this field can get very dangerous. Furthermore this field, similar to the route field, provides information about one proxy where the future signalling will go over. The field can be classified as middle information value.

Table 4.6 shows the classification of the SIP header fields summed up.

Data	Information value
Call-ID	Low
Contact	Middle
From and to	High
Via	Middle
Route	Middle
Record-Route	Middle

Table 4.6: Classification of SIP header data according to the information value

4.2.4.2 Data in RTP Header

Like for email, the data in RTP header, RTP, SIP and SDP isn't analysed in such a detail, because it is often secured with TLS.

The data which is processed in the RTP header can be classified as data with low information value. Two fields should be considered: The SSRC field identifies the source where the data

comes from. This information can be used to filter out packets which come from a certain source. The CSRC field identifies waypoints which might be vulnerable. But nevertheless also these two fields are classified as low information value.

Data	Information value
SSRC	Low
CSRC	Low

Table 4.7: Classification of two RTP header fields according to the information value

4.2.4.3 Data in RTP

RTP is the protocol for transmitting the voice or video data. In contrast to the data in the RTP header, the communication data in the RTP body, has a very high information value.

Data	Information value
Communication data in RTP	High

Table 4.8: Classification of RTP data according to the information value

4.2.4.4 Data in SIP

SIP is a signalling protocol for VoIP. That means it transfers connection information between the caller and the callee. This data is traffic data. If an attacker looks just at traffic data (because other data is well secured), then the first look might be at SIP. With SIP the caller and callee addresses, the media type (audio or video), routing information and many other "interesting" data get transferred. Especially the SIP addresses can provide a lot of information including, the domain, user id, phone-numbers and IP addresses. Summing up the data in SIP, it is classified as having a high information value.

Data	Information value
Data processed in SIP	High

Table 4.9: Classification of data in SIP according to the information value

4.2.4.5 Data in SDP

The very critical encryption key for the SRTP channel is transferred with SIP and SDP during the initiation of the session. This key is used later on for the encryption of the session, ergo the phone call. This key is transferred unencrypted, when no security measurement like S/MIME is used. The problem is, that this key has a high information value [2].
Also other fields like the start and end time of a session can be interesting, indicating the time

which is left for an attack. The session name is kind of indicating the topic of the session, comparable to the subject field by emails. The connection information field provides information about the destination IP address.

Data	Information value
Encryption key	High
Start and end time of session	Low
Session name	Middle
Connection information	Middle

Table 4.10: Classification of important SDP fields according to the information value

CHAPTER 5

Risk Evaluation of Corporate Communication Channels

In this chapter, the technical and data analysis and the analysis of the potential attackers are used for a risk evaluation. Potential attackers may use some weaknesses and vulnerabilities in the technical infrastructure of the respective communication medium. Depending on the information value on the data this can lead to a higher or a lower risk.

Note, that this chapter doesn't compromise all possible attacks on the respective communication components. It only covers a subset of them. Rather this chapter should give an overview of the broad possibilities to attack such systems. It should make clear, that there are many different points in communication systems, where attackers can attack and that many of them are often not considered when establishing a security strategy. Actually this chapter includes an exemplary listing of some attacks to show the broadness of the topic.

As this chapter should just give an overview of the broadness of the topic, for further work the respective countermeasures have to get analysed in more detail. For example, a company has to make sure that with a delete operation the data gets safely deleted. So that data cannot get restored when making a forensic analysis.

5.1 Risk Evaluation of Email Communication

Some of the vulnerabilities described in this section could have been eliminated by encrypting emails. But because of the still bad usability most emails are still unencrypted. Whitten and Tygar [101], Sheng et al. [81] and Farrell [29] discussed this topic. The article from Schwartz [78] shows that till now Google has not encrypted traffic data between its data centres.

The analysis of the technical infrastructure, the data and the attackers lead to several weaknesses which can be extended to threats:

Persistent storage on email server One of the biggest weaknesses of email communication is the persistent storage of emails on the email server. Especially when using IMAP for email retrieving, the received emails stay stored on the server. This is getting a big problem, when the emails are not encrypted. Even the usage of TLS would be senseless, because this only secures the transmission. That means that each unencrypted email can be read. Even end-to-end encrypted emails can be usable for attackers, because the header of the email is not encrypted. As analysed in section 4.1.4 the header fields can reveal a lot of information (How attackers can use the header fields is analysed in the next points). Many attackers, if they can get access to the server, will be able to exploit that:

Malicious insider A malicious insider can access all the emails stored on the servers and do anything with it. For example, possible scenarios are selling data to a competitor, searching for credit card data or just spying on friends. A malicious insider can even get more dangerous. Imagine a mail provider has encrypted all emails stored on the servers for security reasons. This security measure would be senseless against such an attacker, as he has or can get access to the decryption key.

Industrial espionage For industrial spies this is a paradise. He would have access to all emails of competitors or partners of competitors which use this server. This could bring a big advantage.

Police It is easy for the police to get access to such servers. They don't have to hack in, they just need a court order to confiscate the whole equipment. Then they have access to all emails to search for criminals. Also here encryption would be senseless, as the police has the right to get the keys.

National intelligence service It is easy to get access for national intelligence services due to the high amount of resources they have. They can scan for emails with suspect contents. Furthermore they may have access to all information which got gathered by any police confiscation. So if an email server got confiscated, all content and traffic data could get analysed.

Press If the press can gain access to such email servers, they can search for "interesting" information which can get published. By nature they will search for emails of famous persons or bigger companies.

Terrorists are also a big threat. They can steal the whole server. By threatening the keepers with torture and death, they can extort the necessary keys to decrypt the emails. So they can get very sensitive information.

Organized crime The organized crime can act like the terrorists.

In fact this vulnerability can be interesting for any kind of attacker. But the described ones have the biggest interest.

Processing on email server Emails can be transferred over TLS to protect from eavesdropping. But TLS encrypts the email only for the transport. If an email reaches a server, it is not protected anymore unless the server encrypts it again with its own mechanism. This is the point where attackers can attack. They can gain access to the server and do the same things like can be done when emails are stored persistently. Even if the emails just get forwarded by the server and are only stored temporarily. Here of course the exception is the confiscation of the police.

Police Articles like [104] state that the police is even allowed to insert malware on confiscated devices in the UK. So after a confiscation, an email server could automatically send traffic information or even content data to the police.

Eavesdropping unsecured email transfer This vulnerability is based on the assumption, that TLS is not used for the transport. There are two possibilities: The user uses PGP or another end-to-end encryption. In that case, only the header of the email can get analysed. When there is no end-to-end encryption, also the body can get analysed. It is important to know, that servers must not support TLS. That means if the connection from the sender computer to the mail server is protected with TLS, it does not necessarily mean that the connection from the "sender server" to the "recipient server" is also protected with TLS. Also here the same attackers which are interested in the persistent storage are also interested in this vulnerability.

National intelligence service The fact, that the eavesdropping stays unrecognised, can be very interesting for national intelligence services, as they want to work in the background.

Industrial espionage Also for industrial espionage actions, staying unrecognised is very important.

Press The press might have a big interest, if the email is not end-to-end encrypted. Then they would have access to sensitive information. If an end-to-end encryption is present, the traffic information might be still interesting for a good story (e.g. Apple is negotiating with Samsung).

Single perpetrator A single perpetrator may have interest in emails which are not encrypted as they may contain sensitive information which can be sold.

Persistent storage on client When using an email client program, emails get stored on the client computer or also on smartphones.. Of course attackers can also attack the computer of the client or his smartphone. Here it also needs to be distinguished between encrypted emails and not encrypted emails which are stored. In general all attacks, like for the persistent storage on the email server, can be done. The difference is, that here only data in correlation with the users of the client and their communication partners can get analysed. The police has additional possibilities:

Police The police can also confiscate a single client. This is, for example, regularly done at the border control in the United States and United Kingdom. Articles like from the

guardian [94] show that this is reality. Furthermore the article from Bruce Schneier [75] shows that even encrypted emails are not secure, as the police might ask for the key. The article [63] shows, that the police can get the key in extorting the owner with threatening him with jail. If employees are allowed to use the company laptops privately and the police confiscates all devices at the home of one employee, this vulnerability will get an issue. Sensitive company data can get revealed in that case.

Industrial espionage Spies can steal computers of the competitor and look for sensitive information. Even if there aren't interesting documents on it, some emails can reveal a lot of information. For example, the survey of PhoneFactor [65] shows, that 76% of the managers send budget planning data over email to the employees. Furthermore, if the emails are encrypted, the traffic data can get gathered.

Terrorists can easily steal a client computer. They have their methods to get the key when the emails are encrypted. The police can ask more or less legally for the keys and threaten with jail. Terrorists or other criminals can also ask for the keys. But they will threaten with torture or death and so extort the key.

Organized crime The organized crime can act like terrorists.

Backup server Often companies make use of backup systems. There email and other data get regularly transferred to a backup server [103]. In such a case, the whole information from the emails are also stored at a backup server. Even if the emails are already deleted from the live system, they are still available at the backup system. Attackers can also get their data from there. Traffic data and content data analysis would be enabled by this threat. Here the same attackers like for persistent storage on client and email server are interested.

National intelligence service Especially experienced attackers like national intelligence services may attack backup systems, if they don't find valuable information at the live systems.

Single Perpetrator Also other attackers may search for backups if no data can be found at the live systems.

Log files Email servers often make us of log files. In such files, the traffic data of emails are stored. Basically this is the information which gets exchanged at SMTP [54]. Analysing log files can also reveal a lot of information [87]. Actually also the sender and the recipient are stored in such log files. Therefore also with log files user profiles and big pictures can get created. The most dangerous fact of log files is, that even if the emails are deleted, the log files are still there. This is comparable to the threat of a backup server.

Police If the police has confiscated an email server, they can analyse the log files.

National intelligence service can have a look at log files, if no valuable emails are available anymore.

Intrusion detection systems One functionality of intrusion detection systems is logging [50]. It can occur, that if on an email server such a system is implemented, that emails get logged. This leads to the same problem which occurs with "normal" log files. Also the

same attackers like for log files, may be interested in the logging of intrusion detection systems.
One can see that there are many different systems which may log email traffic and that there are probably more which are not considered in this thesis.

Analysing addressing fields in header The addressing fields are those fields, that provide information of the sender and recipient of the email as well as for the servers which where passed on the route. These fields are "from", "to" and "received". This information can be used to find out communication patterns, communication participants and communication habits. They can be used to filter out interesting emails. If one email is interesting, then further analysis (e.g. trying to decrypt the content) can be done. Furthermore this information can be used to get a big picture of the communication. The traffic data of many emails can reveal much more information than the content of a single email, like the example of Felten in section 4.1.4 shows. Another reason why such data gets analysed can be, because the content of the email is encrypted. In each email, the IP address of the sender is stored. This address can be used to find out the location of the sender, but not 100 percent accurate [6]. But accurate enough to find out in which country the sender is operating [49]. Articles like [99] show that for example the NSA is analysing traffic data. This weakness can be exploited by:

- **Industrial espionage** Industrial spies can take advantage of this vulnerability. With the help of the addresses a spy can find potential partners and contract partners of the competitor. As stated in section 4.1.4 it is easy to match an email address to a facility or company. It is also possible to assign names to IP addresses, but this is more difficult. Tools like Domain Dossier [12] can be used for that. IP addresses can't get matched to single persons. Therefore a court order would be needed. This is very interesting, when a spy wants to find out with which companies the competitor is communicating respectively negotiating. Especially when more than one email gets analysed communication patterns can get detected. Out of them a spy may detect correlations and deduce a new product, the competitor is working on.
- **National intelligence service** use this kind of traffic data to get a big picture to detect suspicious persons. Out of the communication pattern (e.g. if a person communicates with known criminals or terrorists) these persons can be found. Once found, the national intelligence services can "zoom" in and start further investigations. It would not be possible to analyse each single communication in such a detail.
- **Police** The police can make use of that information like the national intelligence services. The difference is, that the police uses this information especially for law enforcement.

Analysing MIME content-types If an attacker already knows what kind of content he is searching for, this vulnerability might be very interesting for him. With the help of the MIME content-type an attacker can find out what type of data is included in the body of the email. So an attacker can filter out the emails which might be interesting for him. It can also be used to draw conclusions on the content.

Industrial espionage A spy can have a look at which kind of data the competitors are exchanging with whom and when. A single email may not be significant, but once a big picture is gathered, some findings are possible.

National intelligence service The national intelligence services can also use the MIME content-type to find correlations. So first to get an overview and then zoom in.

Single perpetrator A single perpetrator may analyse emails based on the content-types and attack only these, which have an interesting one. For example if Apple sends a secret product presentation video per email, this can get caught by an attacker. A single perpetrator can make money in selling this video to the press.

Hacker A hacker may have a similar interest like a single perpetrator. The difference is that a hacker may not make money out of the vulnerability. He may even inform Apple about this vulnerability. A bad hacker may do the same like a single perpetrator.

Subject and Comments field The subject field of an email can already contain valuable information. Often the whole content of an email will be written in the subject field, if it is a short email. In that case an attacker wouldn't even have to look at the content. Furthermore, the subject field can be used as a filter for interesting emails. The comments field can even reveal more information than the subject field.

National intelligence service The filtering possibility can be used by national intelligence services. The subject and comments field can additionally be used as intermediate step. So if the traffic data analysis unfolds that the person is suspect, a look at the subject or comments field can clarify if this assumption is correct or not and if further steps have to be taken.

Industrial espionage Industrial spies can use these fields to get information about the content and try to draw conclusions.

Press The press can look for interesting information in the fields which are worth publishing.

Single Perpetrator A single perpetrator can also use these fields as a filter. If the subject field includes for example "Credit Card", then maybe credit card data will be in the content of the email and therefore it is worth attacking.

References and in-reply-to field With the help of these fields it is possible to correlate emails without looking at the content section.

National intelligence service This vulnerability may be used to create user profiles and big pictures. Correlating emails give information to whole conversations. So a large amount of emails can be grouped in conversations with certain persons.

Eavesdropping POP3 authentication When the POP3 authentication mechanism doesn't go over TLS, then the credentials are transmitted unencrypted. Every attacker who sniffs the network traffic, can so read the credentials. The credentials open up boundless possibilities. An attacker can log in to the mail account of the victim, can read all emails, send

emails in the name of the victim and so on. Furthermore the victim may have used the credentials on other websites. The attacker can get access to these, too.

National intelligence service This vulnerability can also get exploited, for example, by the NSA even if TLS is used. An article from DailyTech [23] shows, that the FBI and NSA asked for the TLS keys from companies. Although the article also states that the legal circumstances are not fully cleared, many companies will give out the keys. Another article from Bruce Schneier [76] states, that the NSA is able to break TLS with a man-in-the-middle attack under special circumstances.

Single perpetrator This is a classical vulnerability which gets exploited by a single perpetrator. This attacker can do anything he wants with the email account. Primarily he will have a look for information which he can use for making money.

Hacker A hacker can use this vulnerability like the single perpetrator, without the necessarily to make money.

Intercepting POP3 authentication As mentioned in the sections before, in POP3 a list of possible authentication mechanisms is returned to the client, who picks one out of the list. A potential attacker can intercept the list and answer for the client. The weakest authentication mechanism can get selected out of the list, so that it is easier to break. This kind of attack is called man-in-the-middle attack [51].

Single perpetrator A single perpetrator can use this vulnerability to log in into the mail account of the victim.

5.1.1 Countermeasures for Email Communication

In this section, possible countermeasures to the email vulnerabilities discovered above get described.

Using end-to-end encryption Like described in [101], [81] and [29] many people don't make use of TLS and end-to-end encryption. Thereby such encryptions can make the work for attackers much more difficult and discourage them. End-to-end encryption can protect from attacks on the storage of emails. Attackers who have access to the emails can only analyse the traffic data in that case. This is a countermeasure against:

- Persistent storage on email server
- Persistent storage on client
- Eavesdropping unsecured email transfer
- Eavesdropping POP3 authentication
  Of course the end-to-end encryption cannot hinder the attacker from eavesdropping the POP3 authentication, but it can protect from the consequences.

- Intercepting POP3 authentication
  This countermeasure also cannot protect from the interception itself, but from the consequences.

Using TLS Also the usage of TLS would make email more secure. With the use of TLS, all eavesdropping would not be possible. Indeed it would be possible, but the network packets would not be readable. Therefore both, content and header of the emails would be protected. All header analysis during the transport would not work. When an attacker likes to analyse the header information, he would have to attack a waypoint or an end device. This is a countermeasure against:

- Eavesdropping unsecured email transfer
  - Analysing addressing fields in header
  - Analysing MIME content-types
  - Subject and Comments field
  - References and in-reply-to field
- Eavesdropping POP3 authentication
- Intercepting POP3 authentication

Note that the header analysis would be still possible. The point is, that it is not possible by simply eavesdropping the communication.

Encrypting whole emails on servers When presenting the countermeasure end-to-end encryption, the fact was mentioned that the header of the emails could still get analysed. To protect against this vulnerability, the email providers could encrypt the whole emails including the headers. The systems, of course, may get slower because of the encrypting and decrypting processes, but also more secure. This is a countermeasure against:

- Persistent storage on email server
  - Analysing addressing fields in header
  - Analysing MIME content-types
  - Subject and Comments field
  - References and in-reply-to field

Note, again this protects from the analysis of the header fields, but only for the persistent storage on email servers.

Reset devices after confiscation After the police has returned confiscated devices, these should get reset. This reset should remove all modifications done by the police. This is a countermeasure against:

- Processing on email server
- Persistent storage an client (confiscation of the police)

Give out journey devices If possible, a company should provide own journey devices for their employees. These devices should be a journey laptop and a journey smartphone. Employees should not be allowed to take other devices with them which include or once included business data. The laptops and smartphones shouldn't have sensitive data on them. This is a countermeasure against:

- Persistent storage an client (confiscation of the police)

Leave optional MIME header fields As described above, the MIME header fields can reveal a lot of information. The fields content-ID and content description are optional. These fields should not be used, unless it is absolutely necessary. An attacker has so as few information as possible. This is a countermeasure against:

- Analysing MIME content-types

Encrypting encryption key As described above, one might be urged to give out the encryption keys of the encrypted emails on the laptop when crossing border control. Bruce Schneier presents in [75] a good way to secure oneself against that. If one does not know the key, he will not be able to give it out. So before starting the journey, the key get encrypted itself with a random key which cannot get memorized. One gives out this key to a trusted person. If border control is passed, the trusted person will send the key and the emails will be accessible again. This is a countermeasure against:

- Persistent storage on client

Deleting emails from server No email should be stored on the server of the email provider, even if the provider ensures that the emails are encrypted. If an attacker gets access to the server, he won't find emails. Imagine, the police confiscates the server. In that case it doesn't matter if the emails are protected, because the police will urge to give out the key. This is a countermeasure against:

- Persistent storage on email server
  - Analysing addressing fields in header
  - Analysing MIME content-types
  - Subject and Comments field
  - References and in-reply-to field

Only store necessary emails All emails which are not necessary anymore, should get deleted immediately. When an email contains important information, someone still needs, this information should be copied into a file on the file system. If an attacker gets access to the email server, then he will only have access to few emails; maybe too few emails to develop a user profile (big picture). This is a countermeasure against:

- Persistent storage on client
  - Analysing addressing fields in header

  - Analysing MIME content-types
  - Subject and Comments field
  - References and in-reply-to field

Considering backup systems When only necessary emails are stored and emails are deleted from an email server, also possible backup systems have to be considered. If emails are deleted from a live system, but not from the backup system, the information is still available and a potential threat. Therefore the emails also have to get deleted from the backup system. This is a countermeasure against:

- Backup server

Considering log files When using an external mail server, a company should urge the service provider, to not log email traffic or at least to regularly delete the log files. If an own mail server is used, the logging can get deactivated directly. With this countermeasure the amount of exposed information can get limited if log files get attacked. This is a countermeasure against:

- Log files

Limit information in subject field Subject fields should never contain the whole content. This is annoying for the recipient and reveals too much information. The information included in this field should be limited and just be an overview. Maybe it can be a term which is only meaningful for the communication participants.This is a countermeasure against:

- Subject and Comments field

Don't use comments field If the comments field is not used, it cannot be a vulnerability. As it is optional, it can be left out. This is a countermeasure against:

- Subject and Comments field

Eliminate unnecessary header fields Header fields which are not needed for the transport can get eliminated. For example the IP address of the sender is not used for the transport. So there is no additional benefit. In contrast, it provides an attacker with the position of the sender.

Don't send confidential data imprudently It should be clear now: Don't send confidential data over email imprudently. Of course often it is necessary to communicate confidential data with other companies especially when they are negotiating about an offer. But in such cases the communication participants should be aware of the confidential data they are sending and should use end-to-end encryption to protect the content of the emails. Data, like a financial report of a company, which doesn't necessarily have to get send over email shouldn't be sent. Unfortunately, the survey of PhoneFactor [65] showed, that still many people send all kind of confidential information imprudently.

Developing policies All countermeasures which should get implemented, should be presented in a policy. Employees have to read and sign the policy. This policy should include explanations of the vulnerabilities and rules, the employees have to follow. One rule could be, that employees are not allowed to store emails older than one week in the email client. Older emails have to get transferred to a encrypted archive system.

It is not really possible to protect something from getting confiscated with a court order. If the police asks for the keys, one will have to give them out. But in general, legal companies don't have to be afraid of the police if they use their own servers in their own server rooms. Even after a search by the police, the gathered data won't find the way to competitors, under the assumption that the police isn't corrupt. The easiest way to protect oneself is to store as few confidential information as possible.

5.2 Risk Evaluation of VoIP

Also for VoIP there are already some security measures which can be countermeasures to some of the following vulnerabilities. But also these are not broadly used. According to [105], TLS, IPSec or S/MIME should be used to protect the integrity and confidentiality of the transferred data, but in deployed VoIP Systems, IP phones are only required to support SIP authentication mechanisms. That means that these security mechanisms are mostly not implemented.

Hacking translator A translator is used to convert the bitstream in the needed data formats. A potential attacker can hack into a translator and modify the transformation. This can have several reasons. As a translator can also be used for guaranteeing confidentiality, an attacker can attack this mechanism. For example he can modify the bitstream, so that the recipient is not able to convert the stream into a readable format. For the recipient that would mean that the integrity is violated and would be a kind of denial of service (DoS) attack. For the attacker this is an attack on the availability. A translator can also be modified in a way, that every stream which goes over it, gets modified, so that nobody can read it. The attacker types which may exploit this vulnerability are mainly out to destroy something.

Terrorists may attack a government installation and destroy a complete branch of the communication infrastructure.

Single perpetrator can block the VoIP infrastructure of a whole company. He can hold up this block until the company pays some money (or eliminates the vulnerability).

Malicious Insider As an act of revenge a malicious insider can modify a translator to harm his ex-company.

Organized crime To interfere the police with the evaluation, organized crime can harm the communication infrastructure.

Infowarriors can destroy the VoIP infrastructure of the opposing army for example.

Hacking mixer A mixer can be similarly attacked like a translator. The difference is, that a mixer doesn't serve to convert data formats, but to mix bitstreams from more than one source into one bitstream. If attackers manipulate such a mixer, it will be possible to bring the VoIP system to breakdown.

Hacking SIP proxy The SIP proxy is also a device which VoIP packets pass between the sender and the recipient. Therefore it is a potential attacking possibility. The problem is, that even when TLS is used to encrypt the transfer of the packets, the packets are not encrypted on the proxy. If an attacker can gain access to the proxy, he will have access to all VoIP packets and the headers which include the interesting fields. According to the data analysis in section 4.2.4 the data in the header of SIP messages partially has a high information value. Several attackers can exploit this attacking possibility.

Police If the police confiscates a SIP proxy, it will not route any packets anymore. So real time analysis isn't possible. But, for example, the CISCO SIP proxies [16] can be configured in a way, that they log the headers of all processed packets. In that case, the police has access to all traffic data till the day of confiscation.

Malicious insider In principle a malicious insider can do the same things as the police. The difference is, if he does it "correctly", nobody will recognize it. He can sell sensitive information to competitors or other interested parties. Furthermore, a malicious insider can also perform a real time analysis because the server will still be running.

Industrial espionage As header information reveals information about the communicating parties, this attacking possibility is also very interesting for industrial espionage. A spy can gather information from a competitor and find out negotiation partners, suppliers and so on.

National intelligence service As the national intelligence services are gathering as much traffic data as possible, this attacking possibility is very valuable for them. They can use the header data to filter for interesting data.

Organized crime The organized crime doesn't even have to hack into the SIP proxy. They can extort the keepers of the server and force them to give out the server and the, eventually necessary, keys. Furthermore organized crime can force the provider to install additional software, which provides them with valuable information. This can also be done be terrorists.

Manipulating SIP Proxy Attackers can also get access to the SIP proxy in order to manipulate it in a way, that calls get forwarded to them. For example, the CEO of company A wants to call the CEO of company B to arrange a deal. An attacker manipulates a SIP proxy between them and the call of company A gets forwarded to attacker A. Attacker A impersonates the CEO of company B. So the attacker could get access to sensible information. Also other manipulations are possible. For example an attacker could instruct the proxy to forward the traffic data.

National intelligence service will be able to collect a lot of traffic data, if they have manipulated several SIP proxies.

Police Like for email, also here the police can insert malware on the server after confiscation. The server then periodically provides the police with traffic data.

Single perpetrator A single perpetrator can also collect traffic data and then sell this data to interested individuals. Such individuals could be other attackers who want to create user profiles and scan for interesting persons.

Press If the press is on the track of an interesting story, they may even manipulate a proxy.

Voice mail server There is a possibility to forward calls to a voice mail server [5]. There the data gets stored, till the recipient retrieves and deletes it. In the meantime, an attacker will be able to get access to such a server and access all voice mails, if they are not protected.

Police The police doesn't need to hack into a voice mail server. They just need a court order to listen to some voice mails. They use that for criminal prosecution. They may confiscate the server, or just access it remotely.

Malicious insider A malicious insider can sell sensitive voice mails to interested parties for much money.

Industrial espionage Industrial spies may use this information for gathering information about negotiation status, company secrets, new products, offer prices and so on.

National intelligence service may hack into voice mail servers for special persons. These persons may have come out by analysing the big pictures with the help of the header data.

Press The press may search for interesting voice mails including information that is worth publishing.

Organized crime As for hacking the SIP proxy, also here organized crime can extort the keepers.

Managed VoIP systems As stated in the technical analysis in section 4.2.1.1, for managed VoIP systems a service provider is used. This service provider has all necessary addressing information about the caller and the callee. That means even if the header fields are encrypted, the service provider will have the addressing information [14]. This is a big security issue, as if the provider got hacked, the encryption of the header would be useless. All traffic data could get gathered from the server of the provider.

Malicious insider A malicious insider could sell all the traffic data to interested persons.

National intelligence service can use such a vulnerability, if the traffic data is encrypted. A provider would provide a well prepared list of traffic data (log file).

Police The police only needs a court order to get the necessary information and would probably not hack the provider. When confiscating the server, they can also get access to the voice mail data.

Single perpetrator A single perpetrator can use the gathered traffic data for looking for some communication pairs which might communicate some sensitive information. He can listen selectively for this special pair and then he can eavesdrop the communication.

Unmanaged VoIP When using unmanaged VoIP like Skype, the traffic information of calls and chats get logged locally [82]. If an attacker gets access to the computer which is used for calling, he also will have access to the whole log file. A traffic analysis of the calls and chats is possible. Additionally, the contents of the chats get also stored [83].

Police Here the same problem like for email occurs. The police can confiscate the laptops which are used as soft VoIP phones. This often happens in the course of the border control. Then the police has access to the whole traffic data.

National intelligence service can get access to the clients, too. Especially private clients are often not well secured and are therefore very easy to break. For national intelligence services, this traffic data is even more valuable than for the police.

Attackers like the press and single perpetrators, will be able use this vulnerability, if they have already chosen a special person to attack.

Eavesdropping SIP signalling For analysing the header fields respective the traffic data of SIP messages, the messages have to get eavesdropped, except that one of the previous vulnerabilities are used. This vulnerability is based on the assumption, that either TLS isn't used for SIP or that the TLS protection can get bypassed (for example with extorting the key). So an attacker could simply eavesdrop all SIP messages which go over the network and analyse the addressing information. What he could do with that information and which attackers exploit this vulnerability, is described at the next point.

Analysing addressing fields in SIP header The addressing fields for SIP are "from", "to" and "via". They provide information of the caller and the callee, as well as of the transport route of the SIP messages. As like for email, this information can be used to create user profiles and big pictures of communication behaviour. This information can be used to identify interesting calls. For example it will be visible in the traffic data, if a person which is considered to be a terrorist, performs a call. This call would be interesting and should get eavesdropped. So analysing the addressing fields could be used to filter out interesting calls. Even if the analysed call itself cannot get eavesdropped immediately, further calls of the respective person can get captured. Manipulation of the SIP proxy can be interesting for that case. When a person should get eavesdropped, calls from and to this person should be immediately reported. The SIP proxy could be manipulated in a way, that it reports that. S/MIME could be used to encrypt some header fields. But the addressing fields, except of the from field, can't get encrypted. The from field can get encrypted and presented as anonymous. But as described in the beginning of this section, such measurements are rarely used.

Industrial espionage With the help of SIP addresses, industrial spies can find a matching company or facility and so detect potential partners. Furthermore correlations can

get detected and so help the spy to find out the status of negotiations or product developments. For example if Apple is communicating with many different companies which are producing fingerprint sensors, a spy may assume, that Apple will want to include a fingerprint sensor in one of its products. If the person who communicates, is the chief of smartphones, the device is likely to be the iPhone.

National intelligence service As for emails, the national intelligence services are collecting the traffic data of VoIP to get a big picture and find suspect persons. Once found, a SIP proxy can get manipulated like described above. Furthermore, also email communication of that person can get eavesdropped after the person got classified as suspicious.

Police The police is analysing the addressing information like national intelligence services, but maybe not in such a large scale.

Via field The via field is comparable to the received field of email messages. It includes the whole route of the SIP message and therefore also all passed SIP proxies. An attacker can use this field to identify vulnerable proxies. A vulnerable proxy can just be badly secured so that it can easily get hacked, or it just can't simply support TLS. That would mean that messages sent to and from that proxy would not be secured. These two points indicate proxies and connections which are vulnerable to eavesdropping SIP signalling and manipulating SIP proxies. Furthermore, the via field can reveal information about the service provider. In turn the service provider can reveal the identity of the person [64].

Single Perpetrator A single perpetrator may use this vulnerability to identify easy targets. For example if the conversation of two people goes over a proxy which does not support TLS this will be an easy target.

National intelligence service A national intelligence service is using each vulnerability to gather as much information as possible, therefore also this may be used.

Police The police may use the via field to identify the service provider of a suspect and then confiscate it.

Route field The route field serves to predefine a route which the SIP messages should take. An attacker could try to put himself into the route field so that all messages go over his computer. This is very difficult. But with the help of the route field an attacker could also identify the next proxies, which the packet will pass and prepare them for an attack. Precondition is, of course, that one of the proxies is vulnerable to a hack. After the proxy got hacked, the manipulation of the SIP proxy is possible.

Record route field The record route field indicates proxies, the SIP message has to pass. This is often used for proxies which have a firewall for VoIP which needs to get passed [5]. Also here an attacker can try to put himself into this field. He would probably not implement a firewall, but maybe a forwarding of traffic information to his computer. This vulnerability is comparable to the vulnerability "route field".

SDP - Session name The session name, which has to get set with SDP, is comparable to the subject field in the email header. It can reveal information about the topic of the call. This information can be used to filter out calls, which are worth eavesdropping. This vulnerability only exists, if SDP isn't encrypted using S/MIME.

National intelligence service The filter functionality can be used like for email. Furthermore this field can be used to develop user profiles easier.

Industrial espionage In combination with the addressing fields, the session name can reveal a lot of information to industrial spies. If a call from BMW to Magna BDW Technologies has the session name "offer of new aerodynamic autobodies", a spy will be able to draw the conclusion that Magna has offered some new parts to BMW, or that BMW is developing a new aerodynamic car.

Press Conclusions like for the industrial espionage, may be also interesting for the press.

Eavesdropping RTP channel Once an attacker has found a suspicious or interesting conversation, using a traffic analysis, it can get eavesdropped through the RTP channel. If the traffic analysis has put out a suspicious or interesting person, the future conversations of this person can get eavesdropped. The RTP channel can only get eavesdropped, if SRTP is not used. But according to [105], it is only rarely used. Eavesdropping the RTP channel means actually listening to the conversations.

National intelligence service The conversations of suspects will be eavesdropped by the national intelligence services. They could also eavesdrop conversations automatically and scan for suspicious words like terrorist, bomb, and so on.

Police The police is not allowed to eavesdrop a conversation without a court order. But once they have it, they will use this vulnerability.

Industrial espionage Eavesdropping a conversation of the competitor would be very valuable for industrial espionage. A call between the competitor and a customer for example can reveal useful information. Maybe they talked about a new order and the price. Then the company could offer a cheaper price without the danger to get too cheap.

Press If the press could do so, they would eavesdrop all conversations of famous people. With the help of traffic analysis and the filtering, they could concentrate on single calls.

Single Perpetrator For example a single perpetrator, is able to listen to calls of his wife and check if she is cheating on him. Or maybe he tries to eavesdrop conversations to get information he could sell.

5.2.1 Countermeasures for VoIP

In this section, the countermeasures to the VoIP vulnerabilities discovered above get described.

Regularly delete protocol Especially when using unmanaged VoIP, calling protocols may get stored on the computer. Eventually existing protocols (like in Skype) should get deleted regularly. If the calling information is needed, it can be stored somewhere else than in the protocols. For example at border control a police officer won't find any protocol data. Furthermore, if an attacker gets access to the client, he also won't find valuable information regarding VoIP. This is a countermeasure against:

- Unmanaged VoIP
  - Analysing addressing fields in SIP header

Encrypting encryption key As stated in section 5.1.1 for email, also the data of VoIP can get encrypted. The easiest way would be to encrypt the whole hard disk. For example at border control, the police may ask for this key. Therefore the key should get encrypted itself. For further information have a look at section 5.1.1.

Using S/MIME Goal number one, regarding traffic analysis must be to provide as few information as possible. Therefore everything that can be encrypted, should get encrypted. With S/MIME, the whole SIP message can get encrypted except of some addressing fields (see 4.2.3.5). Using S/MIME, the "from" field can get anonymised. That means an attacker analysing the traffic data wouldn't have information of the sender. This is a countermeasure against:

- Analysing addressing fields in SIP header

Using TLS When using TLS, the whole connection between the servers and clients would be encrypted. That would make eavesdropping more difficult. Attackers would probably concentrate on attacking servers or clients. This is harder to do. It is important to check, if all servers and clients on the transport route support TLS. This is a countermeasure against:

- Eavesdropping SIP signalling
  - Analysing addressing fields in SIP header
  - Route field
  - Record route field
  - Via field
  - SDP - Session name

Note, that analysing the addressing fields and using the route and record route fields would still be possible, but not by simply eavesdropping the SIP messages.

Correctly using route and record route field When used correctly, they can be used as countermeasures. Only proxies which are supporting TLS should get entered in these fields. Therefore no proxy can get passed, which does not support TLS and so breaks the encryption chain. This is a countermeasure against:

- Eavesdropping SIP signalling
  - Analysing addressing fields in SIP header
  - Via field
  - SDP - Session name
- Route field
- Record route field

Use providers supporting TLS When using managed VoIP, someone is dependent on some service provider. When choosing this service provider, only one should be chosen, which supports and uses TLS encrypted connections. This is a countermeasure against:

- Eavesdropping SIP signalling
  - Analysing addressing fields in SIP header
  - Route field
  - Record route field
  - Via field
  - SDP - Session name

Using SRTP A good way to protect a conversation of getting eavesdropped is using SRTP. An attacker could still eavesdrop RTP packets, but they would be encrypted and therefore useless for the attacker. As the connection information is already exchanged through the signalling process, SRTP has no effect to the traffic data. This is a countermeasure against:

- Eavesdropping RTP channel

Limit information in session description The session description field should never contain a description that reveals too much information about the actual content of the conversation. This is comparable to the subject field in emails. Also for VoIP the session description should be a term which is only meaningful for the communication participants. This is a countermeasure against:

- SDP - Session name

Encrypt voice messages When a company is using a voice mail server, then all voice mails which are stored on it should be encrypted. If an attacker gets access to this server, he won't find usable information. Furthermore, partners, customers and employees should get informed, that no sensitive information should be revealed in the voice mail. So that even if an attacker is able to break the encryption, there will be no "dangerous" information. This is a countermeasure against:

- Voice mail server

Deleting voice mails Retrieved voice mails should get deleted immediately. Information, which is not existing, cannot get captured by an attacker. Especially when voice mails are stored on external servers (e.g. the server of the provider), this would be very vulnerable as one has no control of the server. This is a countermeasure against:

- Voice mail server

Reset devices after confiscation Also the VoIP devices should get reset, when the police returns them after confiscation. This is a countermeasure against:

- Manipulating SIP Proxy
- Unmanaged VoIP (confiscation of the police)

Give out journey devices Like for email, also regarding VoIP vulnerabilities, a company should give out own journey devices (laptops and smartphones). This is a countermeasure against:

- Unmanaged VoIP (confiscation of the police)

Secure translator and mixer Translators and mixers have to get secured very well, so that no attacker can modify them. Classical security measurements like firewalls, access restrictions, virus scans and so on can be used. This is a countermeasure against:

- Hacking translator
- Hacking mixer

Secure SIP proxy Similar like the translator and mixer, also the SIP proxy has to get secured against hacking attacks. Also here classical security measurements are sufficient. This is a countermeasure against:

- Hacking SIP proxy
- Manipulating SIP proxy

Don't spread confidential information over VoIP Like for email, a general countermeasure is, that nobody should transfer confidential information over VoIP imprudently. Of course also here often it is necessary to communicate confidential data. But this should be done consciously. When communicating confidential data, the VoIP session should be encrypted with SRTP. This is a countermeasure against:

- Eavesdropping RTP channel

CHAPTER 6

Discussion of Real-World Scenarios in the Context of Corporate Communication Channels

In this chapter, the results will be discussed with the help of practical examples. The chapter serves to evaluate the results of chapter 5. These scenarios should show the practical relevance and criticality of the threats and vulnerabilities described in section 5.1 and section 5.2. Furthermore the scenarios should show that the threats and vulnerabilities can get secured with the countermeasures described in section 5.1.1 and section 5.2.1.

An article from Computerworld [20] shows that the police has powerful possibilities. The article states, that the Swedish police confiscated the servers of PRQ, which is a hosting service. Reason for the confiscation was, that one of the servers was once used by a criminal organization. The police had technical problems to identify a single server. Therefore they took all servers. They had the localisation problem, because the network of PRQ was formerly used for an DDos attack. The article demonstrates two problems. The servers of a company can get confiscated, because they were once used by a criminal organization. And, according to [20], if the server of a company shares the location with a server of criminals, this server can also get confiscated if the police has localisation problems. So the police can "unintentionally" come to sensitive information.
Assuming that a criminal organization has located a server in the same server room like a company has located its servers, a police operation also affects this company. Although this company hasn't committed a crime, the servers would get confiscated if the police has a localisation problem of the correct servers. The police would have access to all emails and calling protocols. They could analyse the traffic data of email and VoIP and create user profiles. Based on that, for the interesting users, the contents of the emails could get analysed.
This can also happen when using cloud computing. There many different virtual machines

(maybe of different companies) are located on one physical server. If such a server gets confiscated by the police, they have access to all of the virtual machines.
The described countermeasures can help against that scenario. If the company uses end-to-end encryption, the police cannot view the contents of the emails. If the whole emails are encrypted, that means inclusive traffic data, and if the calling protocols get regularly deleted, even user profiles can't be created. A policy of the company stating that "only necessary emails should be stored", can also help to limit the possibilities of the police. The countermeasure: encrypting the encryption keys would probably not be implemented in that short run. Anyway, in this scenario the police wouldn't have a basis for asking for the encryption keys. After the police has returned the servers, the company should reset all of them, to remove inserted malware.

The article from Chimpreports [15] states that the police "[...]confiscated four computers from the Red Pepper editorial department". One of the employees stated, that the detectives scanned through all his files and emails. ZDNet published an article [104] which describes the approach of the police at border control in the UK. They don't even need a reason to confiscate a laptop at border control. Also the article from Kravets [46] states the "suspicionless" confiscation. The police officers confiscate the laptop and jail the suspect for the time the laptop is searched. According to another article from Kravets [45], if the data is password protected, the police will ask for the password. The article from ORGZine [63] states, that the police will even threaten the suspects with jail if they don't give out the passwords. In such situations everyone would probably give out the password.
Assuming the employees of a company often have to travel to the US and UK. Therefore they will often be confronted with border control. That means that the laptops of employees are likely to get confiscated. The police would have access to all data available on them, including emails and the calling protocols of Skype. Additionally, the police can insert malware, which spies out the network of the company if the laptop gets connected to it after the journey.
If the company has implemented all of the countermeasures, the police will not get any valuable information. In some cases it will be necessary, that an employee also has sensitive data stored on the laptop. Then the data gets encrypted with a key. This key is encrypted with a random key, known only by the security department of the company. So if police officers confiscate the laptop at border control, they cannot extort the employee and sensitive data doesn't get exposed. When the employee has passed border control, the security department sends the needed random key to decrypt the actual key. If the company gives out own journey laptops, the police will also don't get valuable information. If the journey laptop was in use before border control, some emails and entries in the calling protocol could be available. For that reason, only necessary emails should be stored and the calling protocol should get deleted. Furthermore sensitive information shouldn't get sent over email. If such an email is received, it should get deleted immediately on a journey. The laptop should get reset before connecting to the company network, therefore malware couldn't cause damage.

As the article from techdirt [90] shows, it may also occur, that private laptops get confiscated. The article states, that a motorcyclist recorded himself during a police control. A few days later, the police confiscated all his computers and helmet camera, because it is not allowed

to record someone without his accordance.
This motorcyclist could be an employee of a company. In that case, the employee would not have a journey laptop, but a company laptop with possibly sensitive data on it. If the company has implemented all countermeasures, such a confiscation would be less damage.
If only necessary emails are stored, the police will have to few information to create user profiles. The same will be valid for the VoIP calling protocols, if they are deleted regularly. If all emails are end-to-end encrypted, the police won't get content data out of them, providing that they are not extorting the employee. All confiscated laptops should get reset before connecting to the company network.

The article from Miller [55] shows, that also criminals can get physical access to computers or servers. According to this article, some criminals dressed as policemen and "confiscated" servers of the Verizon data center. If a company implements all of the countermeasures described above, it can limit the damage.

Even if a company uses end-to-end encryption mechanisms or TLS to secure the transport, national intelligence services like the NSA can get to interesting data. The articles from ORF [62] and the guardian [93] state, that the NSA paid millions of dollars so that software companies implement backdoors for the NSA. Assuming that also encryption tools have backdoors, even strong encryptions are possibly no barrier for some attackers.
Assuming a company has implemented end-to-end encryption for email, encrypts all its transport data with TLS, takes care of only using servers which support TLS and uses SRTP for VoIP calls. All these mechanisms provide a good protection from many attackers, but they don't protect from the NSA if it has backdoors in them. Therefore additional security measures are necessary.
Of course, if NSA has its backdoors and gets access to confiscated devices, not all information can get protected. But the amount of damage can be limited. If only absolutely necessary emails are stored and if the calling protocols are deleted regularly, the NSA might have too few information to create user profiles. Regarding email, the content data can't get protected if there are backdoors in the encryption mechanisms. But if no confidential data is sent over email, the NSA will not get valuable information out of it. This is also valid for voice mails. If already retrieved voice mails are deleted, the amount of stored voice mails will be limited.

The article from derStandard [25] shows that also email providers can be an attacker. The article states that Google scans the content of emails to present proper advertisements to the users.
If a company makes use of Google Mail, all of their emails would get scanned by their provider. In that case a malicious insider at Google could cause damage to the company.
When end-to-end encryption is used, Google Mail wouldn't be able to scan the content of emails and therefore it would be a good protection.

Former scenarios have dealt with conceptual risks. But, as described in chapter 5, for all of the sample scenarios described above, the police, NSA, organized crime or other attackers could

analyse the traffic data respective the header fields. According to the article from Vaughan-Nichols [99], the NSA is making traffic data analysis. The article from the guardian [91] and the article from Bellovin et al. [6] states that after 9/11 2001 the NSA started a surveillance program. This program included the eavesdropping of email traffic data where at least one communication participant was outside the United States or where no participant was a United States citizen. The article from Moechel [56] states that the US telecommunication concern Verizon has to provide all traffic data of its customers to the NSA. Thereby a huge amount of data is coming up, so that even an own fibre glass line from Verizon to the NSA had to get established. According to Moechel this line is existing since 2003 with a very high probability.
The problem is that the information which is gathered by the NSA can be used for industrial espionage. An article from the Frankfurter Allgemeine [32] states that the databases of the NSA get operated and serviced by contract companies. It is very easy for those companies to query the databases and have a look at what their competitors are doing. According to the article the NSA wouldn't even recognize this. An article from Bruce Schneier [76] even states, that the NSA is doing industrial espionage itself (in the article a spy attack on Petrobras, a Brazilian oil company was mentioned).
Attackers have several ways to get access to traffic data. One possibility is to directly access the data on servers. How this can be done is described in the scenarios above. According to the article from Kumer [47], the NSA has the possibility to eavesdrop traffic data in real time. In this article also some slides of the exposed PRISM program are presented. One of these slides shows that also email and VoIP traffic data, as discussed in this thesis, can get eavesdropped.
When a company has locations in the United States, also every traffic data of email and VoIP communication to and from these locations gets eavesdropped by the NSA. With this data the NSA can create detailed user profiles and analyse communication patterns. If competitors of a company get in hold of this data, business secrets can get revealed. For example with which partners a company is negotiating.
With the help of the described countermeasures, the traffic data can get protected. Assuming that a company is using an implementation which doesn't include a backdoor for the NSA, TLS is countermeasure number one to protect traffic data. If the NSA would eavesdrop the traffic data of the company, through TLS no information would be revealed and no header analysis would be possible. Regarding VoIP, if S/MIME is used, the SIP messages will be protected additionally. Of course the company has to watch out that only servers are used which support TLS. When using SIP, the route and record route field can be used to specify only servers which fulfil the requirements. The problem with these technical countermeasures is, that according to the articles, telecommunication providers have to give out traffic data. In that case, it doesn't matter if the connection is protected with TLS as the data is directly transferred to the NSA. In fact, also conceptual countermeasures have to be taken. Regarding email, if the optional MIME header fields are left out and the subject and comments field don't contain meaningful information, as few information as possible will be provided. Regarding VoIP respective SIP, the information in the session description should be limited.

Other attackers have higher barriers than the NSA. They don't have backdoors and the telecommunication providers must not give out data to them. But they can also eavesdrop

communication data. This is shown in the article from Charette [13]. It states that hackers eavesdropped a call between the FBI and Scotland Yard.
Hackers could make a lot of money in providing the traffic data of a company to interested persons. Imagine a hacker eavesdrops traffic data of a hard disc company which includes evidence that the company has communicated regularly with Seagate and then he sells this information to Western Digital. This information could be an indicator for a cooperation of Seagate with this company.
Here, also the technical countermeasures can provide good security. It is not so easy for attackers to break a connection which is correctly encrypted with TLS or to decrypt a SIP message which is encrypted using S/MIME. In case that attackers are able to break the encryption, the described conceptual countermeasures provide additional protection.

The articles from tagesschau.de [86] and derStandard [26] state that the British newspaper News of the World eavesdropped the mobile boxes of about 800 people to gather interesting information. This example affects mobile devices, but it can also get adapted for VoIP respective voice mail. Assuming a company makes use of a voice mail server. Newspapers like the News of the World eavesdrop all voice mails which are located on the server to gather interesting information. Assuming that they find information about a revolutionary idea and publish it. This would cause a lot of damage to the company. When voice mails are deleted regularly, the amount of sensitive information can get limited. If the voice mails are encrypted additionally, attacks like the one from the News of the World would not cause damage.

CHAPTER 7

Conclusion

The analysis have shown that there are broad attacking possibilities for many different attackers with different motivations. But the different attackers can use the same vulnerabilities and analysis techniques to reach their goals. For example the NSA analyses the addressing information to create user profiles and industrial spies analyse the addressing information to identify potential contract partners of competitors. The analysis have shown that not always technically high sophisticated attacks are necessary to gather valuable information. Instead of that conceptual flaws and traffic data provide good attacking possibilities for every kind of attacker. Even well secured communication systems can get attacked when looking at conceptual flaws. Especially very powerful attackers like national intelligence services (e.g. NSA) and the police have additional possibilities. Software development companies have implemented backdoors for the NSA to enable them to analyse the data. In some countries, the police can request the encryption key for further analysis. Often the necessary keys get extorted by the police at border control or by criminals at an attack. In such cases, the even existing encryption mechanisms don't protect the data of a company from getting stolen. Countermeasures which help to fill conceptual security gaps help to protect the data in such cases.

National intelligence services like the NSA have already discovered the potential of traffic data. When developing user profiles and big pictures, traffic data can get even more significant than content data. Correlations between messages and persons can get exposed and reveal even more information than content data itself. The NSA and other attackers are using traffic data to look for suspicious persons. Once identified, further investigations, also regarding content data, can get started.
Especially waypoints on the transport route are making the communication channels very vulnerable against attacks. Security measurements like TLS are only protecting the transport route and not the waypoints. In email and VoIP communication there are many different waypoints which the data passes till it receives the target. These waypoints provide many different attacking vectors.

Regarding the possible countermeasures, there are already several established security measurements to protect communication channels. Especially the transportation route, which is very assailable is well secured when using TLS. Also the transportation route of real time data, like used in VoIP is well secured when using SRTP. The content data of emails can be protected when using end-to-end encryption mechanisms like PGP, whereas the content data of SIP messages can be protected when using S/MIME. The problem with all of these security measurements is, that there are still many people and companies, that don't implement these easy measurements and are therefore vulnerable to very easy attacks.

The outcome of the thesis is a compendium consisting of two lists. The first list compromises the discovered risks and threats regarding traffic data and conceptional flaws of email and VoIP. The second list includes the possible countermeasures which provide a protection from the discovered risks and threats. The compendium can be used by companies and security specialists to identify the discovered risks and threats in their components. Furthermore the compendium should help security specialists to identify proper countermeasures which should get implemented in their systems.

Future work should concentrate on conceptual flaws and traffic data and how the problem of backdoors for powerful attackers can get eliminated. Furthermore, further work can be done to analyse the described communication components in more detail and to analyse other communication channels than VoIP and email. Of course companies are also using communication channels like instant messaging and mobile phones. These also have to get analysed. Furthermore future work can analyse the vulnerabilities described in this thesis from a technical point of view.

Bibliography

[1] Österreichisches Telekommunikationsgesetz 2003.

[2] F. Andreasen, M. Baugher, and D. Wing. Session Description Protocol (SDP) Security Descriptions for Media Streams. RFC 4568 (Proposed Standard), July 2006.

[3] J. Andress. *The Basics of Information Security : Understanding the Fundamentals of InfoSec in Theory and Practice*. Elsevier Science & Technology, 2011.

[4] Augsburger Allgemeine. Börse stürzt nach Falschmeldung über Obama-Attentat ab. http://www.augsburger-allgemeine.de/wirtschaft/Boerse-stuerzt-nach-Falschmeldung-ueber-Obama-Attentat-ab-id24955661.html. Accessed: 2013-08-24.

[5] A. Badach. *Voice over IP - die Technik: Grundlagen, Protokolle, Anwendungen, Migration, Sicherheit*. Hanser, 4 edition, 2010.

[6] S. Bellovin, M. Blaze, W. Diffie, S. Landau, P. Neumann, and J. Rexford. Risking Communications Security: Potential Hazards of the Protect America Act. *Security Privacy, IEEE*, 6(1):24–33, 2008.

[7] S. Berthold and G. Zhang. Hidden voip calling records from networking intermediaries. In *Principles, Systems and Applications of IP Telecommunications*, IPTComm '10, pages 12–21, New York, NY, USA, 2010. ACM.

[8] M. Bishop. *Introduction to Computer Security*. Addison-Wesley Professional, 2004.

[9] G. Brebner. *Computers in Communication*. McGraw-Hill Ryerson, Limited, 1997.

[10] E. Brynjolfsson and L. M. Hitt. Computing Productivity: Firm-Level Evidence. *REVIEW OF ECONOMICS AND STATISTICS*, 85:793–808, 2003.

[11] Bundesamt für Sicherheit in der Informationstechnik. Cloud Computing Grundlagen. https://www.bsi.bund.de/DE/Themen/CloudComputing/Grundlagen/Grundlagen_node.html. Accessed: 2013-07-19.

[12] CentralOps.net. Domain Dossier - Investigate domains and IP addresses. http://centralops.net/co/DomainDossier.aspx. Accessed: 2013-09-18.

[13] R. Charette. Hackers Eavesdrop on FBI SScotland Yard Conference Call Discussing Hackers. http://spectrum.ieee.org/riskfactor/telecom/security/hackers-eavesdrop-on-fbi-scotland-yard-conference-call-discussing-hackers. Accessed: 2013-10-04.

[14] S. Chen, X. Wang, and S. Jajodia. On the anonymity and traceability of peer-to-peer VoIP calls. *IEEE Network*, 20(5):32–37, 2006.

[15] Chimpreports. Police Confiscate 4 Computers At Red Pepper. http://chimpreports.com/index.php/people/blogs/10245-police-confiscate-4-computers-at-red-pepper.html. Accessed: 2013-09-30.

[16] CISCO. GUI Administration Guide for Cisco Unified SIP Proxy Release 8.5. http://www.cisco.com/en/US/docs/voice_ip_comm/cusp/rel8_5/OLH/en_US.pdf. Accessed: 2013-09-23.

[17] CNET. Buying your biz a buzz: Hackers sell fake Instagram 'likes'. http://news.cnet.com/8301-1009_3-57599003-83/buying-your-biz-a-buzz-hackers-sell-fake-instagram-likes/. Accessed: 2013-08-17.

[18] CNET. Researcher posts Facebook bug report to Mark Zuckerberg's wall. http://news.cnet.com/8301-1023_3-57599043-93/researcher-posts-facebook-bug-report-to-mark-zuckerbergs-wall/. Accessed: 2013-08-18.

[19] CNET. Russian police spy on people's mobile data to catch thieves. http://news.cnet.com/8301-1009_3-57596063-83/russian-police-spy-on-peoples-mobile-data-to-catch-thieves/. Accessed: 2013-08-06.

[20] Computerworld. Swedish police confiscated three servers during raid on former Pirate Bay host. http://www.computerworld.com/s/article/9231979/Swedish_police_confiscated_three_servers_during_raid_on_former_Pirate_Bay_host. Accessed: 2013-09-30.

[21] S. Convery. *Network Security Architectures*. Cisco Press, 2004.

[22] J. Cowley. *Communications and Networking: An Introduction*. Springer, 2007.

[23] DailyTech. Fbi, nsa want master encryption keys from internet companies. http://www.dailytech.com/FBI+NSA+Want+Master+Encryption+Keys+from+Internet+Companies/article32046.htm. Accessed: 2013-10-20.

[24] Darkreading.com. Five Significant Insider Attacks Of 2012. http://www.darkreading.com/insider-threat/five-significant-insider-attacks-of-2012/240144559. Accessed: 2013-08-23.

[25] derStandard. Google wird illegales Abhören von E-Mails vorgeworfen. http://derstandard.at/1379292789234/Google-wird-illegales-Abhoeren-von-E-Mails-vorgeworfen. Accessed: 2013-11-23.

[26] derStandard. “Jahrhundertprozess” in Abhörskandal um “News of the World” beginnt. http://derstandard.at/1381370088234/Jahrhundertprozess-in-Abhoerskandal-um-News-of-the-World-beginnt. Accessed: 2013-11-23.

[27] derStandard. T-Online, GMX und Web.de verschlüsseln nun Kunden-E-Mails. http://derstandard.at/1375626143705/T-Online-GMX-und-Webde-verschluesseln-nun-Kunden-E-Mails. Accessed: 2013-09-17.

[28] G. Elahi and E. Yu. Modeling and analysis of security trade-offs - A goal oriented approach. *Data Knowl. Eng.*, 68(7):579–598, July 2009.

[29] S. Farrell. Why Don’t We Encrypt Our Email? *Internet Computing, IEEE*, 13(1):82–85, 2009.

[30] E. W. Felten. DECLARATION OF PROFESSOR EDWARD W. FELTEN. http://ia601803.us.archive.org/22/items/gov.uscourts.nysd.413072/gov.uscourts.nysd.413072.27.0.pdf. Accessed: 2013-09-17.

[31] M. Figura and D. Gross. Die Qual der Wiki Wahl: Wikis für Wissensmanagement in Organisationen, 2013.

[32] Frankfurter Allgemeine. Experte sieht NSA-Vertragsfirmen als Einfallstor für Industriespionage. http://www.faz.net/agenturmeldungen/adhoc/experte-sieht-nsa-vertragsfirmen-als-einfallstor-fuer-industriespionage-12573932.html. Accessed: 2013-10-19.

[33] N. Freed and N. Borenstein. *RFC 2045: Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies*. Internet Engineering Task Force, November 1996.

[34] F. Freiling. Zur Nutzung von Verkehrsdaten im Rahmen der Vorratsdatenspeicherung. Technical report, Universitüt Mannheim - Institut für Informatik, 2009.

[35] F. Freiling and D. Heinson. Probleme des Verkehrsdatenbegriffs im Rahmen der Vorratsdatenspeicherung. *Datenschutz und Datensicherheit - DuD*, 33(9):547–552, 2009.

[36] golem.de. NSA speichert Verkehrsdaten von Verizon. http://www.golem.de/news/ueberwachung-nsa-speichert-verkehrsdaten-von-verizon-1306-99667.html. Accessed: 2013-08-22.

[37] W. Goralski. *The Illustrated Network*. Elsevier Inc., 2009.

[38] M. Handley, V. Jacobson, and C. Perkins. SDP: Session Description Protocol. RFC 4566 (Proposed Standard), July 2006.

[39] Infosecurity-Magazine. 58% Information Security Incidents Attributed to Insider Threat. http://www.infosecurity-magazine.com/view/32222/58-information-security-incidents-attributed-to-insider-threat-/. Accessed: 2013-06-20.

[40] ipTRACKERonline.com. Email Header Analysis. http://www.iptrackeronline.com/email-header-analysis.php. Accessed: 2013-08-23.

[41] Information Technology — Open Systems Interconnection — Basic Reference Model: The Basic Model. ISO/IEC 7498-1:1994, ISO, Geneva, Switzerland, Nov. 1994.

[42] G. Karopoulos, G. Kambourakis, S. Gritzalis, and E. Konstantinou. A framework for identity privacy in SIP. *Journal of Network and Computer Applications*, 33(1):16 – 28, 2010.

[43] R. Khare. The spec's in the mail. *Internet Computing, IEEE*, 2(5):82–86, 1998.

[44] J. Klensin. Simple Mail Transfer Protocol. RFC 5321, October 2008.

[45] D. Kravets. ACLU Sues Over Laptop Border Searches. http://www.wired.com/threatlevel/2010/09/laptop-border-searches/. Accessed: 2013-09-30.

[46] D. Kravets. DHS Watchdog OKs "Suspicionless" Seizure of Electronic Devices Along Border. http://www.wired.com/threatlevel/2013/02/electronics-border-seizures/. Accessed: 2013-09-30.

[47] M. Kumar. NSA can eavesdrop traffic in Real Time, more PRISM slides leaked. http://thehackernews.com/2013/06/NSA-PRISM-slides-download-surveillance-snowden.html. Accessed: 2013-10-04.

[48] L. Lamb and J. Peek. *Was sie schon immer wissen wollten: alles über email*. Was Sie schon immer wissen wollten. O'Reilly, Internat. Thomson-Verlag, 1996.

[49] S. Landau. Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations. *Security Privacy, IEEE*, 11(4):54–63, 2013.

[50] H.-J. Liao, C.-H. R. Lin, Y.-C. Lin, and K.-Y. Tung. Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, 36(1):16 – 24, 2013.

[51] T.-H. Lin, C.-Y. Lin, and T. Hwang. Man-in-the-Middle Attack on "Quantum Dialogue with Authentication Based on Bell States". *International Journal of Theoretical Physics*, 52(9):3199–3203, 2013.

[52] G. McGraw. *Software Security: Building Security In*. Addison-Wesley Professional, 2006.

[53] P. Mehta and S. Udani. Voice over ip. *Potentials, IEEE*, 20(4):36–40, 2001.

[54] Microsoft. Aktivieren und Interpretieren der Datei Smtp.log. http://support.microsoft.com/kb/155455. Accessed: 2013-10-20.

[55] R. Miller. “Ocean’s 11” Data Center Robbery in London. http://www.datacenterknowledge.com/archives/2007/12/08/oceans-11-data-center-robbery-in-london/. Accessed: 2013-09-30.

[56] E. Moechel. Täglich eine Milliarde Datensätze an die NSA. http://fm4.orf.at/stories/1719553/. Accessed: 2013-10-04.

[57] C. T. Moecke and M. Volkamer. Usable secure email communications: criteria and evaluation of existing approaches. *Information Management & Computer Security*, 21:41–52, Jan. 2013.

[58] J. Myers. IMAP4 Authentication Mechanisms. RFC 1731 (Proposed Standard), December 1994.

[59] C. Newman. Using TLS with IMAP, POP3 and ACAP. RFC 2595 (Proposed Standard), June 1999. Updated by RFC 4616.

[60] ORF. Nicht schnell genug. http://orf.at/stories/2194108/2194109/. Accessed: 2013-08-09.

[61] ORF. NSA zahlte Millionen an Internetfirmen. http://orf.at/stories/2195940/2195939/. Accessed: 2013-08-24.

[62] ORF. Software mit absichtlichen “Hintertüren”? http://orf.at/stories/2197467/. Accessed: 2013-09-06.

[63] ORGZine. Seizing personal data without reasonable suspicion. http://zine.openrightsgroup.org/features/2013/seizing-personal-data. Accessed: 2013-09-30.

[64] J. Peterson. A Privacy Mechanism for the Session Initiation Protocol (SIP). RFC 3323, IETF, Nov. 2002.

[65] PhoneFactor. What’s in your email? https://www.phonefactor.com/two-factor-resources/assets/EmailSecuritySurvey2012.pdf. Accessed: 2013-09-24.

[66] J. Plate. Skript: Grundlagen Computernetze. http://www.netzmafia.de/skripten/netze/netz8.html. Accessed: 2013-08-23.

[67] T. Porter, B. Baskin, L. Chaffin, M. Cross, J. Kanclirz Jr., A. Rosela, C. Shim, and A. Zmolek. *Practical VoIP Security*. Syngress Publishing, 2006.

[68] T. W. Post. Market quavers after fake AP tweet says Obama was hurt in White House explosions. http://articles.washingtonpost.com/2013-04-23/business/38764770_1_twitter-account-stock-market-jay-carney. Accessed: 2013-08-24.

[69] B. Pundit. 10 Most Notorious Acts of Corporate Espionage. http://www.businesspundit.com/10-most-notorious-acts-of-corporate-espionage/. Accessed: 2013-08-23.

[70] P. W. Resnick. Internet Message Format. RFC 5322, October 2008.

[71] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler. RFC 3261: SIP: Session Initiation Protocol. Technical report, IETF, 2002.

[72] A. Rüter, J. Schröder, A. Göldner, and J. Niebuhr. *IT-Governance in der Praxis:Erfolgreiche Positionierung der IT im Unternehmen. Anleitung zur erfolgreichen Umsetzung regulatorischer und wettbewerbsbedingter Anforderungen*. Springer, 2010.

[73] R. Sandhu. Good-enough security. *Internet Computing, IEEE*, 7(1):66–68, 2003.

[74] C. Schanes and H. Brunner. Advanced Security for Systems Engineering - VO 05: Security Architectures. http://security.inso.tuwien.ac.at/advsecsyseng-ws2012/. Accessed: 2013-09-24.

[75] B. Schneier. Laptop Security while Crossing Borders. https://www.schneier.com/blog/archives/2009/07/laptop_security.html. Accessed: 2013-09-26.

[76] B. Schneier. New NSA Leak Shows MITM Attacks Against Major Internet Services. https://www.schneier.com/blog/archives/2013/09/new_nsa_leak_sh.html. Accessed: 2013-10-20.

[77] B. Schneier. *Secrets and Lies: Digital Security in a Networked World*. Wiley, 1 edition, Jan. 2004.

[78] M. J. Schwartz. NSA Fallout: Google Speeds Data Encryption Plans. http://www.informationweek.com/security/government/nsa-fallout-google-speeds-data-encryptio/240161070. Accessed: 2013-10-03.

[79] J. Schwenk. *Sicherheit und Kryptographie im Internet - Von sicherer E-Mail bis zu IP-Verschlüsselung*. Vieweg, 3 edition, 2010.

[80] C. Shannon. A Mathematical Theory of Communication. *Bell System Technical Journal*, 27:379–423, 623–656, 1948.

[81] S. Sheng, L. Broderick, C. A. Koranda, and J. J. Hyland. Why Johnny Still Can't Encrypt: Evaluating the Usability of Email Encryption Software. In *In Proceedings of the Second Symposium on Usable Privacy and Security, Poster*, 2006.

[82] skype. Wie kann ich mein Anrufprotokoll einsehen? https://support.skype.com/de/faq/FA3171/wie-kann-ich-mein-anrufprotokoll-einsehen. Accessed: 2013-09-26.

[83] skype. Wo finde ich in Skype für Windows Desktop mein Chat-Protokoll und was kann ich damit machen? https://support.skype.com/de/faq/FA392/wo-finde-ich-in-skype-fur-windows-desktop-mein-chat-protokoll-und-was-kann-ich-damit-machen. Accessed: 2013-09-26.

[84] SPIEGEL ONLINE. NSA-Überwachung: Nachfrage nach Mail-Verschlüsselung sprunghaft gewachsen. http://www.spiegel.de/netzwelt/web/nsa-ueberwachung-verschluesseln-sie-doch-selbst-wie-millionen-andere-a-915647.html. Accessed: 2013-09-17.

[85] W. R. Stevens. *TCP/IP illustrated (vol. 1): the protocols*. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 1993.

[86] tagesschau.de. "News of the World" ließ etwa 800 Menschen abhören. http://www.tagesschau.de/ausland/murdoch186.html. Accessed: 2013-11-23.

[87] D. Takahashi, Y. Xiao, and K. Meng. Creating user-relationship-graph in use of flow-net and log files for computer and network accountability and forensics. In *MILITARY COMMUNICATIONS CONFERENCE, 2010 - MILCOM 2010*, pages 1818–1823, 2010.

[88] K. Tam and H. L. Goh. Session initiation protocol. In *Industrial Technology, 2002. IEEE ICIT '02. 2002 IEEE International Conference on*, volume 2, pages 1310–1314 vol.2, 2002.

[89] A. S. Tanenbaum and M. v. Steen. *Distributed Systems: Principles and Paradigms (2nd Edition)*. Prentice-Hall, Inc., Upper Saddle River, NJ, USA, 2006.

[90] techdirt. Maryland Police Confiscate Biker's Computers After He Catches Questionable Activity On Helmet Cam. http://www.techdirt.com/articles/20100420/1041329109.shtml. Accessed: 2013-09-30.

[91] theguardian. NSA collected US email records in bulk for more than two years under Obama. http://www.theguardian.com/world/2013/jun/27/nsa-data-mining-authorised-obama. Accessed: 2013-10-04.

[92] theguardian. NSA Prism program taps in to user data of Apple, Google and others. http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data. Accessed: 2013-08-23.

[93] theguardian. Revealed: how US and UK spy agencies defeat internet privacy and security. http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security. Accessed: 2013-10-03.

[94] theguardian. Taking your laptop into the US? Be sure to hide all your data first. http://www.theguardian.com/technology/2008/may/15/computing.security. Accessed: 2013-09-26.

[95] O. Turel and A. Serenko. Is mobile email addiction overlooked? *Commun. ACM*, 53(5):41–43, May 2010.

[96] P. Tzerefos, C. Smythe, I. Stergiou, and S. Cvetkovic. A comparative study of Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP) and X.400 Electronic Mail Protocols. In *Local Computer Networks, 1997. Proceedings., 22nd Annual Conference on*, pages 545–554, 1997.

[97] USNews. It's Time for the U.S. to Deal with Cyber-Espionage. http://www.usnews.com/opinion/articles/2013/06/04/chinas-industrial-cyberespionage-harms-the-us-economy. Accessed: 2013-08-23.

[98] U. Varshney, A. Snow, M. McGivern, and C. Howard. Voice over ip. *Commun. ACM*, 45(1):89–96, Jan. 2002.

[99] S. J. Vaughan-Nichols. Big data, metadata, and traffic analysis: What the NSA is really doing. http://www.itworld.com/big-data/366825/big-data-metadata-and-traffic-analysis-what-nsa-really-doing. Accessed: 2013-09-30.

[100] R. Vogt. Swiss IT 2011: Die Rolle der IT im Unternehmen. http://www.computerworld.ch/marktanalysen/swissit/artikel/swiss-it-2011-die-rolle-der-it-im-unternehmen-56330/, 2011.

[101] A. Whitten and J. D. Tygar. Why Johnny can't encrypt: a usability evaluation of PGP 5.0. In *Proceedings of the 8th conference on USENIX Security Symposium - Volume 8*, SSYM'99, pages 14–14, Berkeley, CA, USA, 1999. USENIX Association.

[102] Z. Xiao, L. Guo, and J. Tracey. Understanding Instant Messaging Traffic Characteristics. In *Distributed Computing Systems, 2007. ICDCS '07. 27th International Conference on*, pages 51–51, 2007.

[103] Y. Xu, H. Yu, and W. Zheng. A Consistent Backup Mechanism for Disaster Recovery that Using Container Based Virtualization. In *ChinaGrid Annual Conference (ChinaGrid), 2012 Seventh*, pages 95–100, 2012.

[104] ZDNet. When authorities confiscate your electronics: The fate of David Miranda's computer and phone. http://www.zdnet.com/when-authorities-confiscate-your-electronics-the-fate-of-david-mirandas-computer-and-phone-7000019796. Accessed: 2013-09-30.

[105] R. Zhang, X. Wang, X. Yang, and X. Jiang. On the billing vulnerabilities of SIP-based VoIP systems. *Computer Networks*, 54(11):1837 – 1847, 2010.

List of Figures

List of Tables