# Fraud Attacks in VoIP-Based Communications Systems
## *Risk Analysis, Prevention, Protection, Detection*

Benedikt Machens[1], Olaf Gebauer[2] and Diederich Wermser[1,2]
[1]*IANT - International Applied NGN Technologies GmbH, Salzdahlumer Str. 46/48, D-38302, Wolfenbüttel, Germany*
[2]*Research Group IP-Based Communication Systems, Ostfalia University of Applied Sciences,*
*Salzdahlumer Str. 46/48, D-38302, Wolfenbüttel, Germany*
*benedikt.machens@iant.de, {ola.gebauer, d.wermser}@ostfalia.de*

Keywords: Fraud, VoIP, PBX, Honey Pot, SIP, SIPX, SBC.

Abstract: This paper explains how fraud on modern VoIP-Systems works and which attacks are executed. This was examined practically by the example of a honey pot PBX, which ran for about 3 months and was monitored accordingly. Furthermore, this paper presents possibilities of how to protect productive VoIP systems against Fraud and to examine the fraud vulnerability.

# 1 INTRODUCTION

Fraud in general is the attempt to obtain a paid service. In the times of the analogue- or ISDN telephony, the obtained service often was a subscription or a simple telephone Advertisement like e-mail spam. By shutting down ISDN and the newly wide use of VoIP-Technologies, every telephone system is now affected by this danger. The user must be aware of the fact that he must accept losses in security due to the better availability of the VoIP-Service and thus become a fraud target. The communication system is now also vulnerable, similar to e-mails or websites. At the technical level, the conversion from ISDN to VoIP means that a previously closed system, which could only be attacked by physical manipulation or by the provider, is now more or less accessible on a logical level. The main goal of VoIP fraud is thereby the billing of a telephone call at the expense of the fraud victim, in order to make as much profit as possible for an Attacker.

The type of profit generation in VoIP that is the Obtainment of a chargeable service (telephone conversation) is a unique feature of VoIP compared to other IP services. As a result, VoIP systems, in addition to the usual threats to IP services, require a special way of thinking. The permanent availability of the system transfers the problems of a service provider on the Internet to every user of a VoIP system. Regardless of whether this user is a provider, a company or a private individual.

This paper addresses the topics of risk, prevention, detection, analysis and defense of fraud in VoIP and intends to uncover the danger for VoIP systems. The aim of this paper is to examine the risks and the expected costs of fraud-attacks in the field of VoIP systems. Therefore, a honey pot was set up for several months, which monitored most of the incoming attacks. In addition to these results, this paper shows which attacks can be repelled without hindering the normal operation of a VoIP infrastructure.

# 2 FRAUD IN VOIP-SYSTEMS

In the case of a fraud experiment, different participants are involved together as shown in Figure 1. On the one hand, there is the VoIP user with his system, which is typically connected to the VoIP provider via a WAN. On the other hand, there is the attacker, who looks for an access to the VoIP system and finally the internet service provider (ISP). No detailed statement can be made about the connection of the attacker, since he can make a fraud attempt at every point in the system.

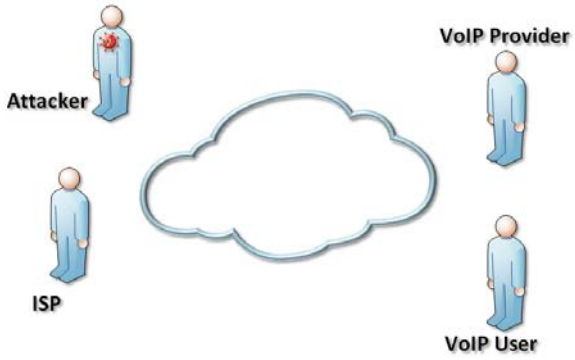


Figure 1: General fraud environment in VoIP.

In this consideration, the network service provider has a small influence on the VoIP level since the service is limited to the transport of IP packets and the possibilities only extend to OSI layer 3. Typical VoIP-Protocols are shown in Figure 2 (Sisalem, et al., 2009).

In the specific case of VoIP, an economic motive can be clearly defined, which consists in the negotiation of conversations without paying the costs for these. In this scenario, the attacker is someone who is himself a VoIP provider for another person. This untrustworthy Provider tries to arrange the handling of his calls through another VoIP system in order to let this fraud Victim pay the costs of the VoIP Call. In the same way, the fraud VoIP Provider keeps the cash from his subscriber. For this purpose, the surroundings are extended by Subscriber A and B, see Figure 3.

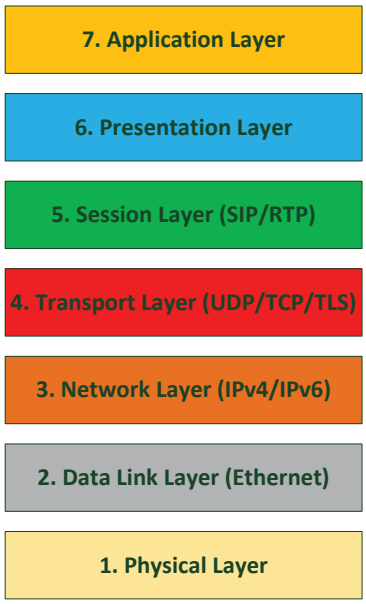


Figure 2: OSI layer with some VoIP protocols.

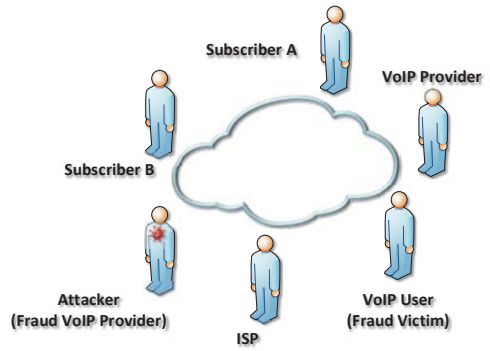


Figure 3: Extended fraud environment with all involved instances in VoIP.

The cost is very low for the attacker because of the IP-based communication. The fraud Provider just needs e.g. a virtual server, which can be hosted in any data center and manages the SIP communication. In general, this works with every call, but international calls are much more attractive in terms of the margin.

Figure 4 shows the path from subscriber A to subscriber B through the different SIP elements in the fraud scenario. The call is routed through the system of a fraud victim. In the legal case, the calls would be charged to the subscriber of the fraud victim but this does not apply to the fraud case. Here, the cash flow between fraud provider an fraud victim is not existent.

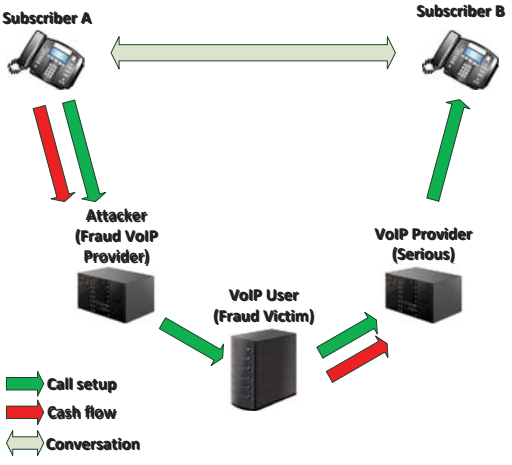


Figure 4: Cashflow in VoIP fraud.

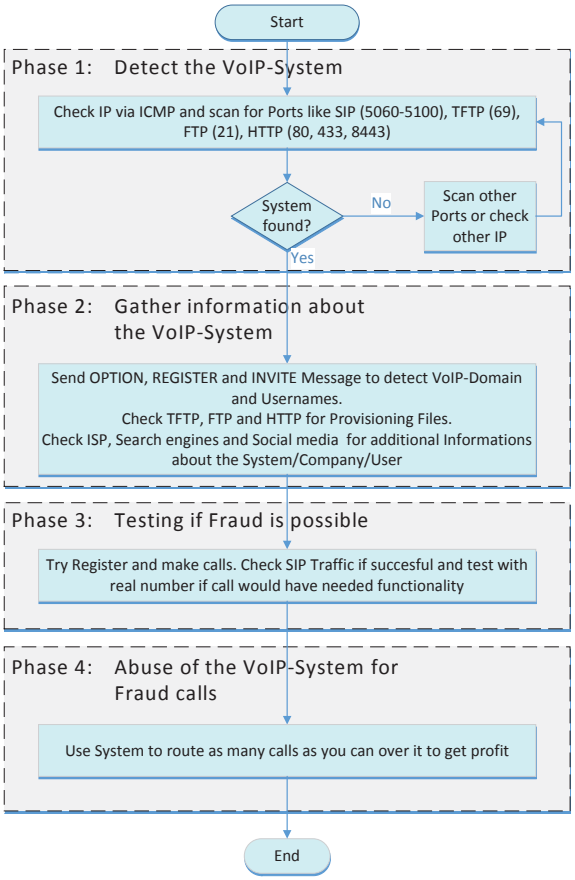


Figure 5: Fraud phase model.

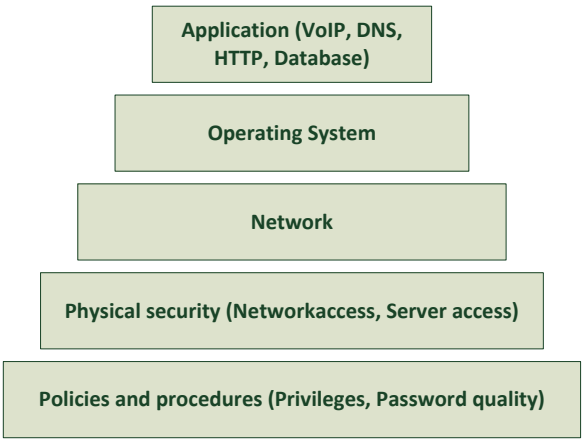


Figure 6: IP service security pyramid.

Technically a fraud attack on a VoIP system can be divided into several phases as shown in Figure 5. The aforementioned switching chain corresponds to the flow of information and cash within phase 4.

The attack scenarios on VoIP systems are similar to other IT services, such as DNS or HTTP. Figure 6 shows the different levels on which an attack can occur (Brennecke, 2009). If, for example, the password quality is poor at the lowest level or the authorization concept is insufficient or not available, safety precautions on higher levels are almost ineffective.

A general overview of the attack methods and threats typically affecting a VoIP system is shown in Figure 7. Many of these methods of attack are used in fraud experiments, and one has to protect the VoIP system against each of these.

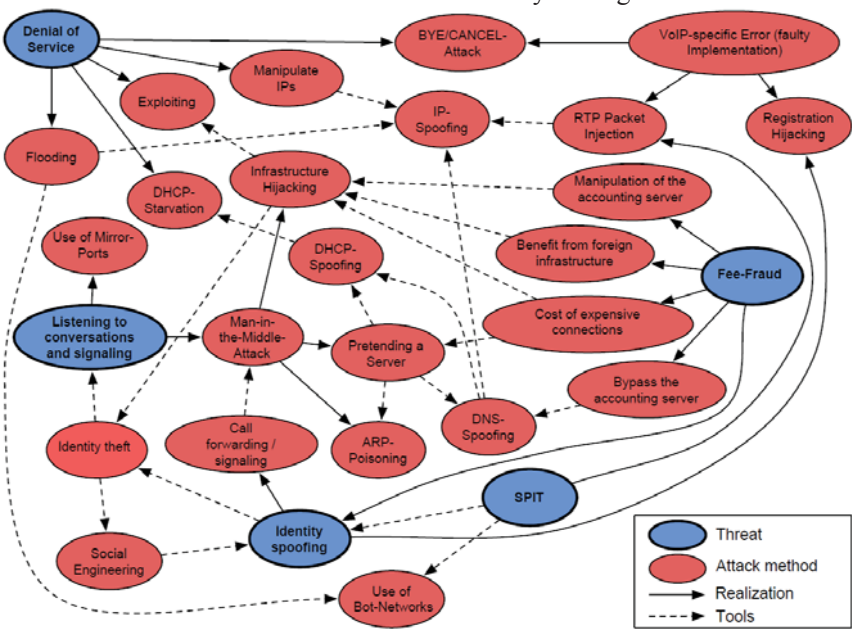


Figure 7: Overview of attack methods in VoIP systems (Brennecke, 2009).

# 3 HONEY POTS

In order to analyze attacks on VoIP systems more closely, the use of a honey pot is a good idea. This method is widely used in IP services, e.g. for e-mail systems. In that case e-mail addresses are provided, which receive spam mails in order to evaluate them. After a SPAM mail has been detected, the global lists of the mail providers are updated and can be used to protect the regular e-mail accounts.

The main difference in the detection of unwanted e-mails and unwanted telephone calls is that content analysis is much easier with e-mails than with calls because of a better pattern recognition. There are only a few parameters for deciding whether a connection request is a "fraud call" (Endler & Coller, 2007).

- Caller
- Callee
- Time of the request
- Frequency of the request

The use of honey pots as a productive counterpart in addition to a running PBX is basically possible, but the expected benefits do not cover the resources and configuration costs. All the information that the honey pot could collect can be detected by a session border controller (SBC). Furthermore, the handling of traffic on the edge of VoIP systems mitigates the effects of DoS attacks.

In this case open-source solutions were used for the honey pot. The core is a SipX (http://www.sipxcom.org), which provides all services and functions of a modern VoIP PBX as seen in Table 1 (ProQuest, 2016).

Table 1: Relevant services of a SipX honey pot system.

| Dienst | Beschreibung |
|---|---|
| SIP Proxy | Exchange of SIP-packets |
| SIP Registrar | Management of registered SIP-Users |
| Call-Queue | ACD-Solution |
| TFTP | Provisioning of Telephones |
| HTTP | Platform for Management |
| DNS | Nameresolution for Services (e.g. SRV-Records) |
| NTP | Timeserver for Local Telephony |
| SNMP | Log-Server for Telephony |
| XMPP (OpenFire) | Instant Messaging Service |

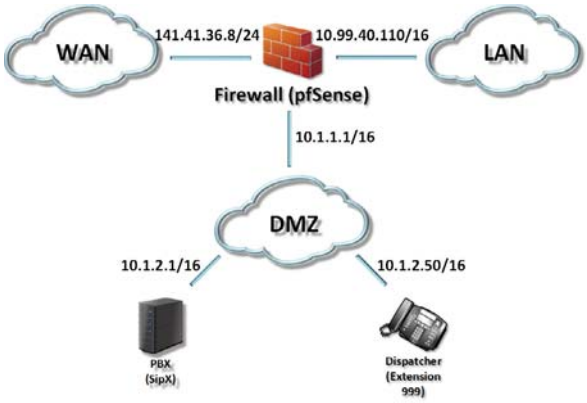


Figure 8: Architecture of the honey pot.

In order to create a controllable and manageable environment, it is necessary to place the SipX behind a firewall. For this, a pfSense (https://www.pfsense.org) was used. With appropriate firewall rules, the PBX is made completely accessible via the external IP. The only exception is port 22 for SSH access. An overview of the network structure is shown in Figure 8. The demilitarized zone (DMZ) network contains all the necessary components of the honey pot, while the LAN segment is intended for administrative access to the DMZ.

# 4 RESULTS

The goal of the first filtering of the raw data is to remove the internal traffic of the SipX and the internal network. This traffic plays a subordinate role for the search for fraud attempts and must only be taken into account in special cases. The recorded data shows that accessibility via ICMP is a critical point because attackers first check the general availability. After enabling ICMP and the external availability of UDP and TCP, approximately 90 minutes have elapsed until the first IP packet from an unknown source were received. This short time shows it is likely that a variety of port scanners and bots are looking for systems with security weaknesses.

The daily traffic summaries were scanned for external IP addresses and checked with the help of an online API (http://ip-api.com) to determine IP information. This data is from a database that is updated monthly. Therefore, the full validity of the information is not given. Dynamic IP addresses are not provided with the correct global position, but the

Figure 9: Location of the attacker's IP addresses.

IP ranges are usually assigned to an ISP and are thus located within a specific region. Static IP addresses, on the contrary, are indicated with the presumed current position.

Another critical point is the IP address itself. From the point of view of the honey pot, the IP is the last layer 3 device from which the packet was received. However, this does not necessarily have to be the attacker, but could be a pirated PC, a router or a spoofed IP. Considering the restrictions mentioned above, a world map with the potential attacker positions was drawn as seen in Figure 9.

The different IP addresses are evaluated, but not how often packets were received from these IP addresses. For a system which is connected in Germany, external IP addresses from Germany, for example NTP servers, should appear predominantly. The following Table 2 and Table 3 show the top 20 countries and Cities of the IP addresses. A total of 11956 IP addresses (as of 12.07.2016) were recorded.

Table 2: List of external IP addresses by country that communicated with the honey pot.

| Number of Different IP Addresses | Country |
|---|---|
| 1805 | USA |
| 1482 | China |
| 1113 | Taiwan |
| 568 | Russia |
| 559 | Brazil |
| 502 | Venezuela |
| 379 | Germany |
| 379 | France |
| 371 | India |
| 267 | Vietnam |
| 264 | South Korea |
| 218 | Netherlands |
| 216 | Canada |
| 204 | Mexico |
| 187 | United Kingdom |
| 173 | Turkey |
| 172 | Italy |
| 167 | Argentinia |
| 150 | Indonesia |
| 149 | Romania |

Table 3: List of external IP addresses by town that communicated with the honeypot (The World Bank, 2016).

| Number of Different IP Addresses | Town |
|---|---|
| 751 | Taipei |
| 237 | Fremont |
| 184 | Peking |
| 172 | Hanoi |
| 169 | Roubaix |
| 145 | Ann Arbor |
| 138 | Montreal |
| 137 | Moscow |
| 111 | Fen-chi-hu |
| 110 | Nanjing |
| 101 | Guangzhou |
| 100 | Caracas |
| 98 | Paris |
| 96 | Seoul |
| 95 | Shanghai |
| 94 | São Paulo |
| 93 | St. Louis |
| 92 | Caracas (Los Palos Grandes) |
| 89 | Maracay |
| 88 | San Francisco (Financial District) |

The evaluation of cities (Table 3) shows that Taipei leads the list by far. On closer examination of the background, the IPs can be traced back to the "Data Communication Business Group". This is the Asia Pacific Network Information Center (APNIC), which is responsible for IP management for the Asia and Pacific region. Since APNIC is a central administration, the identity of the attacker is probably concealed here or the WHOIS entries in the APNIC database are not completely maintained.

The configuration of the honey pot allows to monitor the SIP behavior, especially the SIP calls. Figure 11 shows the time course of the SIP requests recorded by the honey pot. In addition to the daily OPTION messages with which attackers are looking for a potential target, several INVITE and REGISTER brutforce attacks were registered. The analysis of SIP traffic per day shows that attacks are independent of the daytime. The attacks from 30$^{th}$ of May to the 7$^{th}$ of June were continuous inquiries with about a few hundred requests per minute. In contrast to this, the data of June 24$^{th}$ shows 200,000 SIP REGISTER requests during the lunch time within 200 minutes. In general, the assertion is that attacks occur primarily outside of business hours, e.g. on holidays or on weekends. However, this can not be confirmed by the recorded data. Thus, in a VoIP system which is reachable 24 hours a day and 7 days a week, fraud attempts should always be expected.

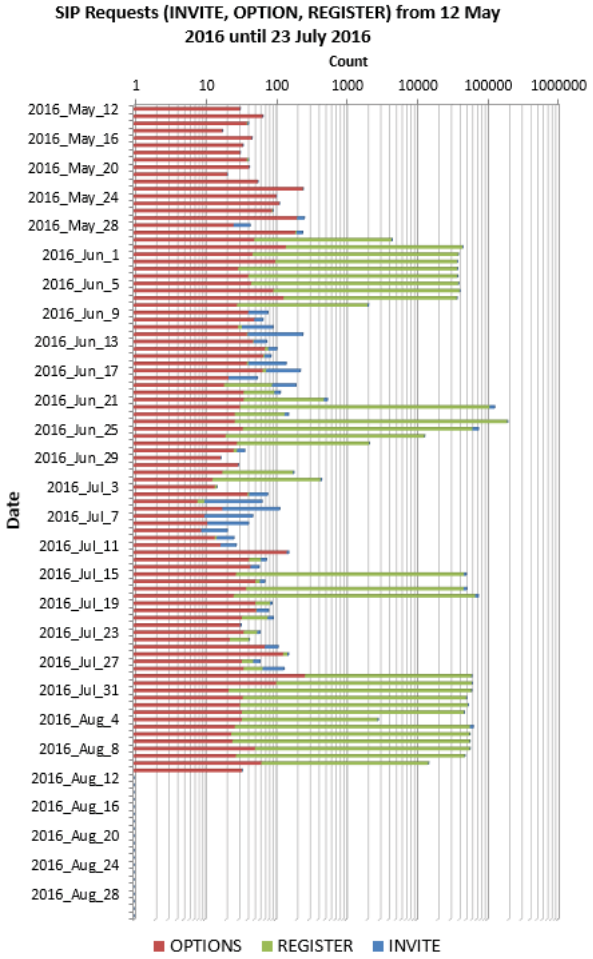


Figure 10: SIP requests of the honey pot from 12th of may until 23rd of july 2016.

# 5 FRAUD-VULNERABILITY

The verification of a VoIP system on its strength against fraud attacks can not be summarized in a single scenario. There is a large amount of attack points and various factors depending on the used PBX solution as well as the architecture and the specific installation. These points make it difficult to develop an automated tool that would allow people with no significant knowledge of the subject to check their own VoIP system.

There are several Linux-variants, which are good for fraud testing. For example "Kali" can be used . This distribution is freely available and specifically designed to perform "penetration testing" on IT systems. Kali provides hundreds of programs to perform attacks that target the goal of cracking passwords, manipulating DNS servers, or intercepting data as a “man-in-the-middle”.

A test plan should be based on the fraud-phase model (Figure 5) and be tested against a system, which is directly accessible. This scenario represents the greatest possible failure of firewall and SBC and offers a variety of possible attacks. In the first Phase, the goal is to detect the VoIP-System. Therefore, Tools like “nmap” for ICMP- and UDP/TCP-Port-scanning can be used. Especially the Port 5060 is important. In the next phase, the system under test should be confronted with several SIP messages. The information in the answers are essential for the next steps. This information can include details like the branch of the User Agents, the VoIP domain and the location of a TFTP server. Tools like “cURL” can now be used to download configuration data from a TFTP-Server. This is possible with the knowledge of the MAC addresses of the manufacturer. With the configuration file, it is often possible to register phones at the VoIP System. The tasks in the last phase is to get to know the necessary format of actually making calls. Therefore, “SIPp” test cases can be used to detect the prefix with a brutforce like method. Another possible way to get the format for making calls is to receive incoming calls because in most cases a recall is directly possible. After making an active outgoing call the fraud calls can be started.

# 6 CONCLUSION

The attempt to implement fraud over telephony is not a phenomenon of VoIP. It was already present with analog and ISDN telephones and as VoIP extended these old technologies, the fraud problem was also extended. The use of an open and strong network like the Internet requires new considerations of securing your own telephone system. The past thinking of the ISDN world is not sufficient in the security scenario and must be combined with already established methods of the IP services, such as layer 7 firewalls (SBCs), in order to be able to effectively protect against fraud (Wallingford, 2005).

The architecture of the VoIP system is decisive for the realizable degree of control. With an open structure and easy accessibility, the comfort factor is very high and easy to use. This applies to both, the administrator and the users, but unfortunately also to the attacker. Network severing (e.g., VoIP and data LAN) creates hurdles and ways to build control without massively reducing usability. It is irrelevant whether the separation takes place at the physical or the logical level.

For the establishment of a secure VoIP system, it is useful to consider all levels of the system and to decide whether and how services of the PBX should be used. From a technical security perspective, the construction of an ISDN system is secure. It is completely self-contained and can only be compromised in a few places. In combination with firewalls, SBCs and the PBX it is possible to get this state also in VoIP systems. The VoIP trunk can not be built into this old construct due to the public connection. For the design decision, you can choose between these two extremes (complete shutdown or direct public connection) in order to achieve the desired usability / security ratio.

The honey Pot experiment has shown how the impact on a directly to the Internet connected VoIP system is. The plant is under massive and permanent attacks and is therefore strongly endangered. The registered attacks show that it can be considered as negligent to operate an installation with such an architecture. This paper has shown how easy and quick a VoIP system can be analyzed and abused for fraud. If there are no corresponding backup measures or a preventive maintenance system is used to alert an administrator to an ongoing attack in case of an emergency, it is possible to hack a VoIP system and execute fraud attacks within a day. Depending on whether there is a limit for outgoing calls or not, the potential damage, even for such a short period of time is enormous.

# REFERENCES

Brennecke, S., 2009. *Literaturgestützte und experimentelle Untersuchung zur Sicherheit vin Voice over IP in Unternehmensnetzwerken - Diploma Thesis.* Institute for communication and technologies - Ostfalia - Wolfenbüttel: s.n.

Endler, D. & Coller, M., 2007. *Hacking Exposed VoIP: Voice over IP Security - Secrets & Solutions. ISBN: 978-0072263640.* s.l.:Mc Graw Hill Professional.

ProQuest. *Products & Services - SIPX.* [Online] Available from: http://www.sipx.com/products/ 2016.10.19.

Sisalem, D., 2009. *SIP Security. ISBN: 978-0-470-51636-2.* s.l.:John Wiley & Sons Ltd..

The World Bank. *Data | The World Bank.* [Online] Available from: http://data.worldbank.org/ 2016.07.12.

Wallingford, T., 2005. *Switching to VoIP: A Solutions Manual for Network Professionals. ISBN: 978-0596008680.* 1. Hrsg. s.l.:O'Reilly Media.