VoIP SPAM and a Defence against this Type of Threat

MIROSLAV VOZNAK – FILIP REZAC
Department of Telecommunications
CESNET, z.s.p.o.
Zikova 4, 160 00 Prague 6
CZECH REPUBLIC
miroslav.voznak@vsb.cz , filip.rezac@vsb.cz

Abstract: - This paper deals with VoIP Spam and various techniques of defence against this threat. First of all we gave attention to the security in IP telephony and we divided the threats in several categories according to their specific behaviour and their impact on the affected system. Then we focused our work on Spam over Internet Telephony (SPIT) as a real threat for the future. We have developed both a tool generating SPIT attacks and AntiSPIT tool defending communication systems against SPIT attacks. AntiSPIT is based on our new approach evaluating call detail records and can be easily implemented to any communication system. AntiSPIT represents an effective protection based on statistical blacklist and works without participation of the called party which is a significant advantage. We implemented our method into Asterisk under GNU general public license.

Key-Words: **-** VoIP, SIP, SPIT, Security, Attack, SPITFILE, AntiSPIT

1 Introduction

Voice over Internet Protocol is without any doubts a step ahead in communication technologies. But similarly to other technologies, there should be certain specific rules and security measures otherwise the technology does not work properly. Nowadays, SIP protocol is the most frequently used signaling protocol in IP telephony, however it is prone to attacks as described below. We can divide these attacks into several categories based on the threat behavior [1]:

- Scanning and Enumerating a VoIP Network.
- Exploiting the VoIP Network.
- VoIP Session and Application Hacking.
- Social Threats.

We provide a brief and concise description of the most frequently used attacks. We tried to focus on finding out which of the attacks offers the biggest potential as a future threat and if there is an effective defence against it. It is reason why the two chapters (4 and 5) deal with two tools, SPITFILE and AntiSPIT. While we developed the first one to demonstrate a way to implement and launch SPIT, the latter illustrates the implementation of protection against SPIT into Asterisk (open-source PBX) which is based on ideas of authors originating in the statistical blacklist method. The final section provides our conclusions and summarizes the acquired knowledge.

2 Security Risks in IP telephony

All telecommunication channels, including VoIP, are subject to attacks. These may include interception, modification, or even a data loss during transport. SIP protocol is in particular very susceptible to redirection, modification, or termination of the calls. Moreover in IP telephony, it is not possible to line up individual packets to front and analyze them by return because the communication happens in real time. This is the main difference between the proposed security mechanisms for classical Internet services and VoIP.

2.1 Scanning and Enumerating a VoIP Network

This is not a case of a true VoIP attack. However, if someone wants to attack the individual components of VoIP infrastructure, he has to locate them in the network and try to get as much information about these VoIP elements and infrastructure as possible. This is how scanning and enumerating tools work. If an attacker is able to obtain information about individual devices then he can plan the next steps of attack. VoIP infrastructure also comprises elements other than just VoIP phones and servers. Because the availability and security of VoIP networks relies so heavily on supporting infrastructure, an attacker could focus only on devices running VoIP services. It behoves him to identify and map out other core network devices, including routers and VPN gateways, web servers, TFTP servers, DNS servers, DHCP servers, RADIUS servers, firewalls, intrusion prevention systems, and session border controllers to name a few. For instance, if an attacker was able to locate and disqualify TFTP server, several models of phones trying to download configuration files on bootup might crash or stall. If we should mention specific tools which can be used for realization this type of attacks we can choose Nmap for network scan and Sipscan to get the list of SIP accounts from SIP server.

2.2 Exploiting the VoIP Network

This category includes attacks which enable obtaining detail information about the VoIP component, restrict its function, or eavesdrop calls/data that was made between the components. These types of attacks are the most widespread and include Denial of Service (DoS), or Man-in-the-Middle (MITM). DoS [2], [3] affects various types of IP networks services. Subscribers are not able to use their services properly or the function of services is limited and marked as unusable. First, we will describe the implementation of the DoS flaw. In this case, the attacker send modified packets, or sequence of packets, through a “flaw” in VoIP component implementation.

These packets may be very long and syntactically incorrect which causes a VoIP component to fail as it is not implemented to handle such packets. Another example of an attack is Flood DoS. The primary feature of this attack is that the target component is flooded by many flood packets and then this component is not able to work with legitimate VoIP communication packets. Legitimate packets are either ignored or processed very slowly and the VoIP service becomes unusable. One variant of this type of attack is that the flood packets cause the target system to allocate resources or consume processing power while waiting for a response that will never be sent. Another variant is a Distributed DoS. Multiple systems are used to generate a massive volume of packets so that the target systems are flooded. Another type of DoS is Application-level DoS which consist of manipulation and changes to VoIP service properties. For example, hijacking the registration data for an IP phone can cause a loss of any inbound call. The next favorite attack is Man-in-the-Middle, in this case, the attacker is located between two communicating parties and is trying to intercept and alter the data stream direction between the subscribers. MITM attack can capture data between participants, and also eavesdrop intercepted calls. Nowadays the most used MITM method is called ARP Poisoning. The method works with the fact, that some systems receive and save an ARP entry in its ARP cache, regardless on the previously sent or not sent ARP request. This means that an attacker can fool one or both subscribers to think that the attacker MAC address is the address of the other computer or SIP server.

2.3 VoIP Session and Application Hacking

In this subchapter, we cover other attacks in which an attacker manipulates SIP signaling or media to hijack or otherwise manipulate calls. If the attacker wants to abort a built-up call, the SIP packet with SIP BYE method needs to be created. The client will receive this packet only if the call identification alias Call-ID is the same. The best packet for this modification is an ACK packet. This packet confirms a build-up call from the caller to the called subscriber. We only need to change one element in the packet: the ACK method for BYE. If the modified packet is sent to the called subscriber’s address, the phone will react as if the caller has ended the call. In case of RTP Data Redirecting we have to modify SDP packet content. SDP defines the IP address and the port which is used during the call. If the attacker has modified these data, subscriber’s VoIP client will send an audio stream to a different address and port which is a legitimate subscriber’s address.

2.4 Social Threats

Under this term we can imagine the attacks that are not focused to obtain informations about the users accounts, eavesdrop the sensitive data or attack VoIP components in order to disrupt its function. The attacks described in this chapter are designed to make a calls with advertising content and from theperspective of the victims are very annoying. Such an attack is for example SPIT (Spam over Internet Telephony), which is similar to e-mail Spam.

The first type of SPIT is applied by the call centres through which advertisement calls are managed by agents. Subscribers who answer the phone are systematically or randomly searched by computer and if they answer the call, they are redirected to agents. Most advertising messages are recited by agents. The volume of such advertisement calls is in direct proportion to the number of call agents. Another type of SPIT, so called ‘call bots’, uses the same principle as the call centres except that there are no call agents. The advertisement message is replayed automatically from a computer. There is no need to employ agents. Everything is administered by the computer. Certain VoIP phones may receive an “alert-info” SIP header. This header contains a internet link under which the advertising message is recorded. The message is played when the phone rings. When this type of attack occurs, the calls cannot be answered. The issue can be solved by turning off the internet ringing download on the telephone set. This attack is known as Ringtone SPIT.

3 Protection Against SPIT

In this section we describe theoretical methods of protection against SPIT, how far are effective is a topic of wide discussion.

A. Buddylist/Whitelist

Every subscriber has a list of subscribers. Those who are not on the list cannot initiate a call. The problem arises when the subscribers that are not on the list are regular callers and we would like to speak to them. To allow the calls from subscribers who are not on the whitelist is helpful to access a ’web of trust’. Each subscriber grants his trust to several other subscribers.

B. Blacklist

This is a reversed whitelist. In this case, the subscriber has a list of possible SPIT attackers and these contacts do not have access to subscriber’s phone.

C. Statistical Blacklist

Telephone providers carry out different analyses and apply different statistical methods to create a spammer list. If a caller makes hundreds of phone calls during a short time span, s/he is very likely to be a spammer.

D. Voice menu interaction

Before the caller is actually put through to the called subscriber, the caller is directed to the voice menu where he is asked to enter a numeric code (for example 123*) to be able to get through to the caller. This protection is effective against caller bots (relatively until the bots take up using a speech recognition).

E. Greylist

This is a modified blacklist (whitelist) under which the phone returns the engaged line tone to the caller who is making the call for the first time. This time, the phone does not actually ring on the called subscriber. If the caller attempts to make the connection again the call is connected. It increases a likelihood that the caller is a human person and not a SPIT bot.

F. Law aspects

As telecommunication is protected by several laws, instances filtering mails or calls face several legal consequences (for example imprisonment). Therefore, it is mandatory not only to construct technical filtering mechanisms, but also to consider implications from telecommunication or privacy protection laws and regulation.

4 Implementation of SPIT

If we want to deal with a protection against SPIT we need to develope SPIT and show how works, how danger is and how easily can be implemented.

4.1 Motivation

Attacks on Internet services become a very frequent issue in the global IP network. Another threat is coming with IP telephony, SPIT. If we take the fact that Spam takes up 80-90% of the total number of attacks on Internet services, the threat of SPIT in the future is very real and dangerous. Many security experts also share this view. We can say that the only reason why the SPIT has no global impact yet is that it, as opposed to Spam, poses greater requirements on computing power, hardware and network connectivity. But this barrier will soon be removed by increasing technological development. SPIT also has a much greater annoying effect and impact on the victim than Spam. Just imagine, unlike an incoming emails with Spam, which you can easily ignore and delete, the new attack containing SPIT advertising message will ring again and again several times a day. That was the reason why we started developing and implementing our own tool. This tool is called SPITFILE [4] and it is based on well-known SIP packet generator Sipp. Next subchapter deals with SPITFILE application which is programmed in Python and it should demonstrate how easy it is to generate this type of attack.

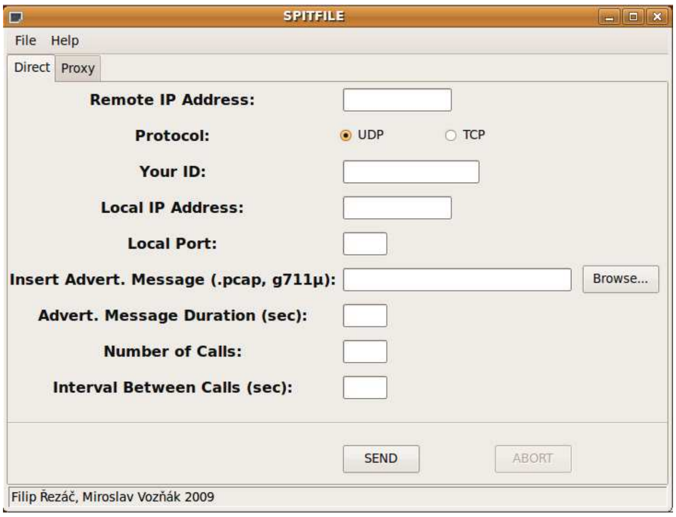
4.2 SPITFILE

During the development process, we put much emphasis on the simplicity of using and generating SPIT attacks. This decision was made on the ground of a study. We got acquainted with a few implementations of VoIP generators which were suitable for SPIT attack but they were mostly based on rather complex algorithms and demanded good knowledge of Linux-based systems. Therefore our aim was to design and then to implement a SPIT attack into an application which would be user-friendly and with an intuitive menu. We opted for Python to develop our SPIT application. Python is a high-level programming language similar to Perl or Tcl. The objective of designed application is to generate the phone calls and to replay a pre-recorded voice message.

We had to find a suitable SIP generator which we could modify. As an acceptable candidate was adopted an application SIPp which focuses on testing and simulating SIP calls in VoIP infrastructure. SIPp is a open-source test tool or traffic generator for the SIP protocol. SIPp can read custom XML scenario files describing from very simple to complex call flows and also send media traffic through RTP. Two methods were used for dynamic cooperation with parameters inserted into SIPp and XML. The variables corresponds to appropriate parameters inserted by user and they are sent to SIPp application to initialize a voice call. For the values which have to be dynamically inserted into XML file, a new function was created, enabling to search and to change a particular value. We use a library xml.dom.minidom for handling XML files. Our application called SPITFILE implements a graphic interface for SIPp and works with ready-made .xml diagrams. Thus, the simulation of a SPIT attack is much simpler. SPITFILE was programmed in Python using wxPython GUI. Its control is very intuitive – the requested values are submitted into relevant fields and the SPIT attack is launched by clicking the SEND button. For a proper operation of the SPITFILE application it is first necessary to install the following packages: Python ≥ v2.6 ,Sipp ≥ v2.1, Python-wxgtk ≥ v2.6. Our application can generate attacks in two modes: Direct and Proxy.

4.2.1 Direct Mode

It generates SPIT on IP phone directly in the local network without using the VoIP PBX (some IP phones can refuse a direct calls that avoid SIP Proxy, the Proxy mode is more suitable for such cases).



Remote IP Address:

Protocol: ● UDP ○ TCP

Your ID:

Local IP Address:

Local Port:

Insert Advert. Message (.pcap, g711µ):

Advert. Message Duration (sec):

Number of Calls:

Interval Between Calls (sec):

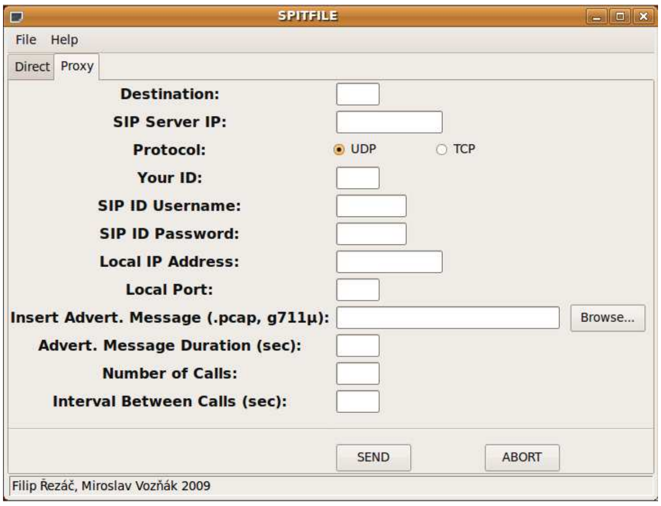
Filip Řezáč, Miroslav Vozňák 2009

Fig. 1. SPITFILE in Direct Mode

SPITFILE in Direct mode is depicted in Fig. 1. It is necessary to fill in mandatory information which is used to launch the prepared attack.

4.2.2 Proxy Mode

It generates SPIT via VoIP PBX (SIP Proxy) and the attack thereupon can run against anything that is available behind the Proxy, theoretically involving not only IP phones but also ordinary phones and the whole telephone world. As well as in Direct mode in Proxy mode on Fig. 2, it is also necessary to fill in compulsory information needed to create the SPIT attack. In addition, it is necessary to obtain a user account because a successful registration at SIP Registrar is required before the calls via SIP Proxy can be performed. It is the main difference between Direct and Proxy modes. The attacker should obtain a valid account at SIP Proxy. There exist many ways how to obtain the username and password, for example applications Cain and Abel or SIPcrack. Both applications are a tool for sniffing and cracking the digest authentication [3] which is used in the SIP protocol.



Destination:

SIP Server IP:

Protocol: ● UDP ○ TCP

Your ID:

SIP ID Username:

SIP ID Password:

Local IP Address:

Local Port:

Insert Advert. Message (.pcap, g711µ):

Advert. Message Duration (sec):

Number of Calls:

Interval Between Calls (sec):

Filip Řezáč, Miroslav Vozňák 2009

Fig. 2. SPITFILE in Proxy Mode

Before SPITFILE can be opened, preconfigured .xml diagrams (direct.xml and proxy.xml) should be imported into /etc/ directory. Afterwards we can launch SPITFILE and choose one of the two above mentioned attacks that we want to carry out.To run SPITFILE, just type the following command to the terminal *python <location of the SPITFILE.py file>*. The called phone rings after the attack has been sent and a pre-recorded voice message will be played after the incoming call is answered.

SPITFILE has been tested with HW Grandstream IP phones (GXP 2000, 3000) and with SW IP phones (Sjphone and X-Lite). The Proxy mode has additional fields such as the required account which is consequently used for registration, such as SIP number, username and password. The other fields are the same as in the case of previous Direct type. We have tested Asterisk PBX and Siemens hipath4000 PBX.

5 AntiSPIT

In chapter 3 we described several theoretical methods how to defend against SPIT, everyone can assess how useful they are and whether they are suitable for a practical implementation.

Irrespective of the types of defence mentioned in the chapter 3,we tried to design and create our own model of security application based on Blacklist which would provide an efficient defence against SPIT, the name AntiSPIT [4] has been given to the new application. AntiSPIT is able to analyse and process input data from Call Detail Records (CDR's) and consequently determine whether the used source will be inserted into blacklist. CDR's are an integral part of every PBX and we decided to implement AntiSPIT into Asterisk PBX. The application gives an output which is inserted as a command which can control the blacklist. Asterisk provides CLI interface enabling us to create or delete the particular records in the blacklist database.

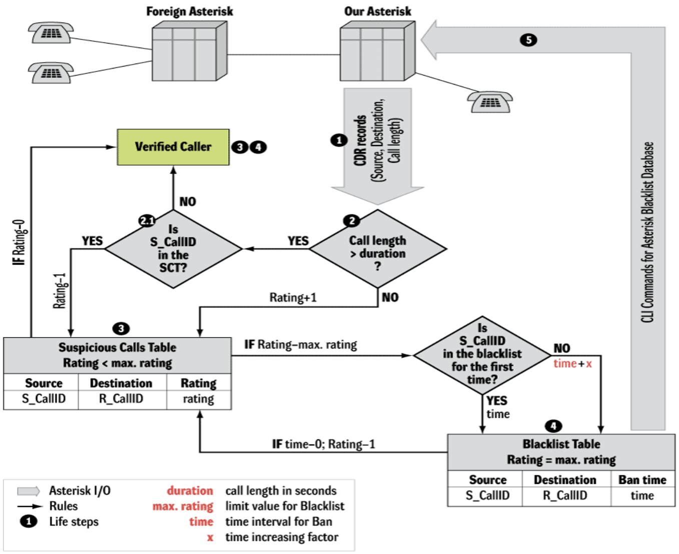
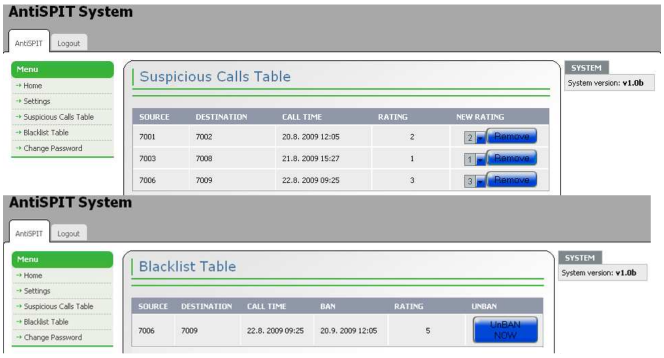

Foreign Asterisk
Our Asterisk
5
1
CDR records (Source, Destination, Call length)
CLI Commands for Asterisk Blacklist Database
Verified Caller
3 4
NO
2.1
Is S_CallID in the SCT?
YES
2
Call length > duration ?
YES
NO
Rating+1
IF Rating–0
Rating–1
3
Suspicious Calls Table
Rating < max. rating
Source | Destination | Rating
S_CallID | R_CallID | rating
IF Rating–max. rating
Is S_CallID in the blacklist for the first time?
NO
time+x
YES
time
4
IF time–0; Rating–1
Blacklist Table
Rating = max. rating
Source | Destination | Ban time
S_CallID | R_CallID | time
Asterisk I/O
Rules
1 Life steps
duration call length in seconds
max. rating limit value for Blacklist
time time interval for Ban
x time increasing factor

Fig. 3. AntiSPIT Concept

The whole concept acts as an effective tool and provides a SPIT recognition and consequently a protection against SPIT attacks. In principle, the main idea of this proposed method is based on the human behaviour in case of an unwanted call. The called party terminates the unwanted call early after the SPIT call is answered and the reaction gets quicker when it reoccurs. The called party terminates such repeating SPIT call in a substantially shorter time interval than in the previous case. This concept is shown in Fig. 3.

In this case, we can monitor the call duration from CDR's where every call has stored a record and if the call duration is less than a certain interval (duration), the source of the calls will receive the status of suspicious caller and a record with rating is created. In the case of repeated suspicious behaviour the rating will be increased. The record includes sender's called ID (S_CallID), receivers called ID (R_CallID), rating and will be listed in the table named Suspicious Calls Table (hereafter SCT). The maximum achieved rating factor represents a threshold limit value that makes a decision about whether the record from SCT is put onto Blacklist table (BLT). If this record is transferred into BLT then a caller stated in such a log can not carry out inbound calls for a specific time interval (time). The BLT record contains sender's called ID (S_CallID), receivers called ID (R_CallID), and time interval determining the ban (time). After expiration of the ban time the rating of the record is reduced by one and is transferred back to SCT.

However, if the inbound call is repeatedly marked as a suspicious and the threshold rating factor value is exceeded it will be put back onto the Blacklist table, this time for a longer period of the ban time (time + x). At the same time, as the record is inserted into the Blacklist table database put blacklist <number> command is generated for PBX Asterisk CLI. After the ban time expiration the record is returned to SCT and database del blacklist <number> command is sent Asterisk CLI. Callers who have a record in the SCT can also reduce their rating value and it is also possibly to fully remove them from SCT. Once the caller carries out a call with a longer duration than the set threshold limit (duration) and his S_CallID is a part of the record in the SCT, then the suspicion mark is consequently reduced by 1. If the caller does not have a record in the SCT then he is a certified subscriber and no action is required. The process is denoted in Fig. 3



Suspicious Calls Table

SOURCE	DESTINATION	CALL TIME	RATING	NEW RATING
7001	7002	20.8. 2009 12:05	2	2 Remove
7003	7008	21.8. 2009 15:27	1	1 Remove
7006	7009	22.8. 2009 09:25	3	3 Remove

Blacklist Table

SOURCE	DESTINATION	CALL TIME	BAN	RATING	UNBAN
7006	7009	22.8. 2009 09:25	20.9. 2009 12:05	5	UnBAN NOW

Fig. 4. Administration Menu

AntiSPIT has been created in LAMP environment – meaning Linux, Apache web server, MySQL databases and PHP. AntiSPIT offers user-friendly administration through a web front-end enabling a user to set the key parameters such as length of call interval (duration), maximum achieved rating factor (max rating), ban time (time). The web front-end also enables monitoring and the management of both SCT table and BLT table.The AntiSPIT can be downloaded and freely distributed under the GPL.

6 Conclusion

This paper dealt with VoIP attacks and especially SPIT. We divided threats into several categories and mentioned the specific techniques on how to apply these attacks in real-case. Our goal was to determine which of the attacks are currently the biggest threat for VoIP networks and analyse potential risks and defences against them. For this purpose, we developed a SPITFILE application and AntiSPIT. Some of the described security measures in chapter 3 or combination thereof should be implemented in every IP ready PBX. This should enhance the protection against SPIT attacks. However, as effective SPIT attack methods are being developed very fast, further intensive research is needed to guarantee the security of VoIP systems. Fortunately, most telephone calls are charged which functions as a brake but we cannot not rely on it. SPIT is a threat hanging over the telephony world like the sword of Damocles. We also made a model of an effective defence against SPIT which we implemented into software IP PBX Asterisk and it has been given a name AntiSPIT. AntiSPIT is based on a call rating factor and blacklist table, together it provides a good protection against SPIT. We hope that applications such as AntiSPIT will help us to define and develop the idea how to defend against the new SPIT attacks and how to break this imaginary sword.

Acknowledgement

This research has been supported by the “Optical Network of National Research and Its New Applications” (MSM 6383917201) research intent of the Ministry of Education of the Czech Republic.

References:

[1] Endler, D., Collier, M., *Hacking Exposed VoIP*, McGraw-Hill Companies, 2007, ISBN 978-0-07-226364-0

[2] Collier, M., *VoIP Denial of Service (DoS)*, White paper, SecureLogix Corp., May 2005

[3] Rezac, F., Voznak, M., Ruzicka, J., *Security Risks in IP Telephony*, CESNET Conference 2008 Security, Middleware and Virtualization, September, 2008 Prague, ISBN 978-80-904173-0-4

[4] Voznak, M., Rezac,F. *The implementation of SPAM over Internet telephony and a defence against this attack*, Telecommunications and Signal Processing (TSP) 2009, Dunakiliti, Hungary, August 2009, ISBN 978-963-06-7716-5

[5] Novotny, V., Komosny, D., *Large- Scale RTCP Feedback Optimization*, Journal of Networks, 2008, Volume 3, pp. 1-10, ISSN 1796- 2056

[6] Voznak, M. *Speech Bandwith Requirements in IPsec and TLS Environment*, 13th WSEAS International Conference on Computers, p.217-220. Rodos, Greece, July, 2009, ISBN 978-960-474-099-4

[7] Voznak, M., *Voice over IP*. VSB-Technical University of Ostrava, September, 2008, ISBN 978-80-248-1828-3

[8] Meggelen, J., Smith, J., Madsen, L., *Asterisk: The Future of Telephony*, O'Reilly, 2007, ISBN 978-0-596-00962-5