Risk analysis on VoIP systems

Knútur Birgir Otterstedt

Faculty of Industrial Engineering, Mechancial Engineering and Computer Science
University of Iceland
2011

Risk analysis on VoIP systems

Knútur Birgir Otterstedt

30 ECTS thesis submitted in partial fulfilment of a
Magister Scientiarum degree in Industrial Engineering

Advisors
Dr. Páll Jensson

Faculty Representative
Ebba Þóra Hvannberg

Faculty of Industrial Engineering, Mechanical Engineering and Computer Science
School of Engineering and Natural Sciences
University of Iceland
Reykjavik, June 2011

Risk analysis on VoIP systems
30 ECTS thesis submitted in partial fulfilment of a Magister Scientiarum degree in Industrial Engineering

Faculty of Industrial Engineering, Mechanical Engineering and Computer Science
School of Engineering and Natural Sciences
University of Iceland
Hjardarhagi 2-6
107, Reykjavik
Iceland

Telephone: 525 4600

Bibliographic information:
Knútur Birgir Otterstedt, 2011, *Risk analysis on VoIP systems*, Master's thesis, Faculty of Industrial Engineering, pp. 69.

Printing: Háskólaprent
Reykjavík, Iceland, July 2011

Útdráttur

Markmið þessarar ritgerðar var að framkvæma áhættugreiningu á VoIP kerfi fyrir þjónustuveitendur. Helstu ógnir kerfisins voru greindar og í kjölfarið var fjallað lauslega um hverja ógn. Eignir kerfisins voru greindar fyrir greininguna og einnig voru líkur á ógn og áhrif hverrar ógnar metnar (Á skalanum Lítil – Gríðarleg). Að þessu loknu var áhættugreiningin framkvæmd, í hugbúnaðinum RM-Studio, og niðurstöður hennar greindar. Sambærileg greining fyrir PSTN kerfið var framkvæmd til samanburðar. Loks voru gagnráðstafanir, við helstu ógnum VoIP kerfisins, kynntar.

Abstract

The goal of this thesis was to perform a risk analysis on a VoIP system for service providers. Main threats of the system were analysed and subsequently each threat was briefly introduced. Assets of the system were analysed, for the risk analysis, and probability of threat and impact of threat estimated (On the scale from low-immense). Next the risk analysis was performed, in software called RM-Studio, and the results analysed. Equivalent analysis was performed for the PSTN system for comparison. Finally countermeasures, to the main threats to a VoIP system, were introduced.

I want to dedicate this thesis to my newborn daughter.

Table of Contents

List of Figures

Tables

Abbreviations

CoS	Class of Service
CPU	Central Processing Unit
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS	Denial of Service
FMFM	Find-Me Follow-Me
GSM	Global System for Mobile Communications
HTTP	Hypertext Transfer Protocol
ID	Identity Document
IP	Internet Protocol
ISP	Internet Service Provider
kB	kilobyte
kb/s	kilobits per second
LAN	Local Area Network
MB	Megabyte
MitM	Man in the Middle
MPLS	Multiprotocol Label Switching
NGN	Next Generation Network
OS	Operating System
PC	Personal Computer
PIN	Personal Identification Number
POTS	Plain Old Telephone Service
PRS	Premium Rate Service
PSTN	Public Switched Telephone Network
QoS	Quality of Service
SIP	Session Initiation Protocol

SP	Service Provider
SPIT	Spam over Internet Telephony
UPS	Uninterupted Power Supply
URI	Uniform Resource Identifier
VoD	Video on Demand
VoIP	Voice over Internet Protocol
WAN	Wide Area Network

Thanks

First I would like to thank Síminn hf. for granting me the opportunity of working on this thesis and also for providing me with a workplace, resources and most appreciated meals every day.

Special thanks go to Sæmundur Þorsteinsson and Laufey Jóhannesdóttir, my contacts and advisors at Síminn. Your enthusiasm, opinions and advices regarding the project helped me a lot.

I would also like to thank my advisor, at the University of Iceland, Páll Jensson. Last but not least I want to thank my family for their endless support.

1 Introduction

VoIP stands for Voice over Internet Protocol and is a way to carry voice traffic over computer networks like the Internet. Over the last decade VoIP has become increasingly popular, gaining millions of subscribers every year and has certainly caught the eye of telecommunication service providers all over the world. Many service providers believe so strongly in the success of VoIP that they are starting to replace all PSTN based equipment, as it gets obsolete, with VoIP based equipment (Haselton, 2009).

The driving factor for the success of VoIP is cost reduction, both for users and providers. But VoIP doesn't only bring reduced costs it also brings threats and vulnerabilities unprecedented to the telephone industry. The classical PSTN is a robust, mature platform having been in place for well over a century. Threats to the system are relatively few and are well known. The opposite can be said about VoIP which is an inexperienced platform and since it is IP based it's susceptible to large number of threats.

This project is worked in collaboration with Síminn and aims at identifying the threats considered most important to VoIP and subsequently performing a risk analysis for VoIP service providers. Another risk analysis is performed for PSTN in order to establish foundation for comparison. The risk analyses are constructed in software called RM-Studio, developed by Stiki. Lastly, countermeasures are identified for some of the threats bearing the biggest security risk from the analysis.

The structure of this thesis is as follows: Chapter 2 introduces and compares VoIP and PSTN as well as briefly introducing MPLS. Chapter 3 identifies and describes the threats to the two platforms. Chapter 4 covers the risk analyses, shows how values were assigned, and the results from the analyses. In chapter 5 countermeasures are identified for those threats most vulnerable to VoIP. Chapter 6 concludes the thesis and presents main results.

2 Background

This chapter introduces and compares the two telephone systems in focus in this thesis, VoIP and PSTN. Brief introduction of MPLS, which is capable of supporting VoIP service, will also be given at the end of this chapter.

2.1 VoIP

VoIP is a way of delivering voice and multimedia sessions over Internet Protocol. In VoIP voice signals are converted into digital signals making them transferable over Internet Protocol. VoIP is packet switched meaning that the signals are divided into packets that travel via dynamic routing to their destination. The greatest benefit of being packet switched is that bandwidth efficiency is greatly enhanced as compared to circuit switching.

In 1995 a company called Vocaltec, Inc. marketed a product called InternetPhone which allowed users to call each other using a computer, sound card, microphone and speakers. Most acknowledge this as the birth of VoIP. At the time bandwidth was much more scarce than it is today. Lack of bandwidth resulted in bad quality of conversations compared to a regular telephone call which hindered VoIP's success significantly. Even though VoIP didn't become a great success in 1995, Vocaltec´s InternetPhone was a milestone. Others saw the future that VoIP offered and in 1998 VoIP switching software was included as a standard in three IP Switch manufactures' routing equipment. Despite this increased interest, VoIP usage only accounted for less than 1% of all voice calls (Hallock, 2004). Since then VoIP technology has evolved a lot and the number of VoIP users has grown enormously. VoIP users are estimated to be 250 million at the end of 2011, excluding calls between computers (Biggs, 2007).

As was stated above, VoIP service began as calls between two parties on separate computers. That is just one of the setups available as can be seen in Figure 1. The most popular ones are:

- **Scenario 1: PC ↔ PC**
  Users connect to an IP network through a computer. This scenario has grown very popular over the last years with the introduction of Skype, Messenger etc. A major reason for this setups popularity is that many VoIP providers offer their services free of charge within its own network making it popular e.g. in the gaming industry and for personal use. This scenario is sometimes referred to as VoIP over Internet. This scenario will not be the covered in this thesis.
- **Scenario 2: IP phone ↔ IP phone**
  Works the same way as scenario 1 except that users need special IP phones. As for scenario 1, VoIP providers sometimes offer service free of charge within their own network. One setup of this scenario is managed VoIP, which will be the setup examined in this thesis. Managed VoIP means that individuals and enterprises purchase VoIP

service from providers. In return they expect a reliable telecommunication service and a QoS agreement. The provider will provide the equipment, software etc. that is needed.

- **Scenario 3: IP phone/PC ↔ PSTN**
  After the success of scenarios 1 and 2, VoIP providers started offering calls between the two phone systems. Benefits of this scenario are that information travels through the network using VoIP until the very end where it is transferred into PSTN via a VoIP ↔ PSTN gateway. Thus VoIP providers can offer phone calls at a lower price, especially long distance ones.

There are other scenarios available e.g. IP ↔ PSTN ↔ IP, PSTN ↔ IP ↔ PSTN and some other variations of the scenarios but circumstances rarely require any other setup than those three mentioned above.

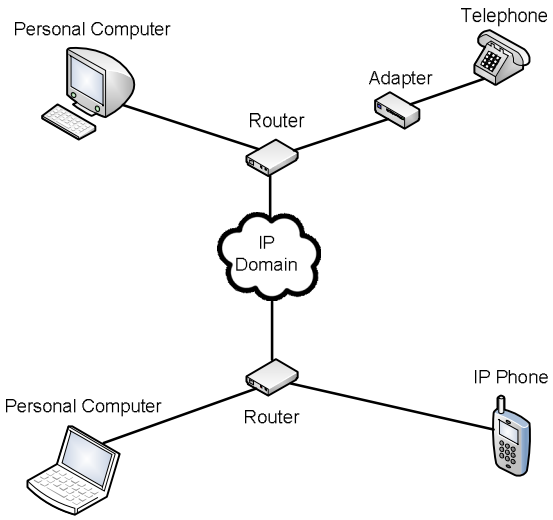

Figure 1: Possible VoIP scenarios

To be able to initiate a VoIP call, many protocols are needed. In relation to security two protocols stand out as important, SIP and H.323 as each one has vulnerabilities exploitable by attackers. These protocols are competing signalling protocols for VoIP systems responsible for setting up and tearing down calls, user registration, authentication and more. These two protocols will now be studied further.

2.1.1 H.323

When the idea of IP telephony started gaining popularity, around 1996, the telecom industry demanded that some protocol would be developed so that users and service providers could choose between vendors and products that would interoperate. The International Telecommunication Union (ITU) recommended H.323 which was a protocol developed for multimedia communication over packet data networks, such as LANs[1] or WANs[2] (Goode, 2002).

H.323 is actually an umbrella of four protocols which are:

- Registration Admission and Status (RAS)
- Q.931 (Connection control Protocol)
- H.245 (Control Channel Protocol)
- Real-time Transport Protocol (RTP)

Other protocols are needed for H.323 to successfully work but they may vary between applications or uses for H.323. A typical protocol stack for VoIP is shown in Figure 2.

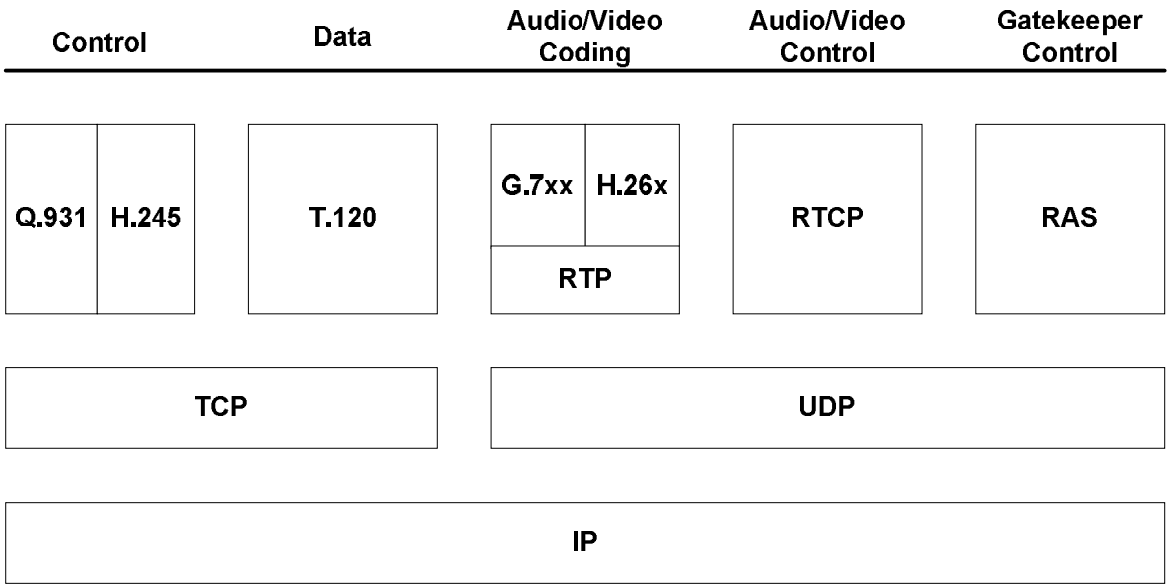

Figure 2: Possible protocol stack for H.323 (Liu & Mouchtaris, 2000)

An H.323 entity can be implemented in many different devices. For VoIP the most important ones are terminals, gateways and gatekeepers.

When H.323 calls take place they can be divided into seven phases. The phases and the protocols that are needed can be seen in Table 1 (Liu & Mouchtaris, 2000).

---

[1] Local area network is a compuer network that connects computers in a small geographical area (e.g. schools, work places)
[2] Wide area network covers broader area (e.g. regional zones, nations)

Phase	Protocol
Call Admission	RAS
Call Set-Up	Q.931
Capability Negotiation	H.245
Stable Call	RTP
Channel Closing	H.245
Call Teardown	Q.931
Call Disengage	RAS

Table 1: The seven phases of H.323 calls

2.1.2 SIP

The session initiation protocol or SIP is the other big signalling protocol for VoIP. SIP was originally designed by Henning Schulzrinne and Mark Handley in 1996 (Dehestani & Hajipour, 2010) but was later adopted by IETF. SIP is similar to HTTP and is a protocol that can set up and tear down any type of session (Goode, 2002).

Whilst H.323 has a formal and complex architecture, SIP is much simpler in both design and implementation. SIP only has two types of messages, request and response, and uses an URI to identify where requests shall be sent. SIP also offers many features unavailable in H.323. For example SIP supports instant messages and allows users to post status, such as "Busy" or "On a meeting", that other users can see. The design of SIP makes the addition of any third party service easy to implement so the possibilities for the implementation of further features is open. For this reason many vendors, especially in Europe and the US, choose SIP over H.323.

2.2 PSTN/POTS

PSTN is the traditional telephone system that has been used for over 100 years or since the telephone first became a success around 1875. At first the telephone network was fully interconnected, that is "*If a telephone owner wanted to talk to n other telephone owners, separate wires had to be strung to all n houses.*" (Tanenbaum, 2010). Figure 3 shows a interconnected network, where the dots represent telephone owners.

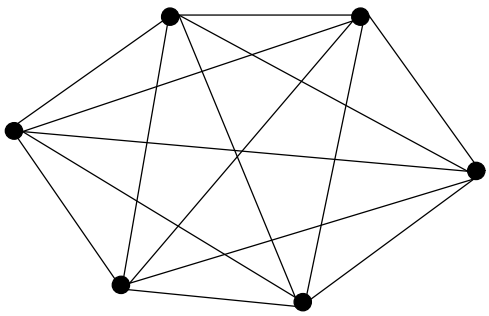

Figure 3: Fully interconnected network

It soon became obvious that connecting every telephone to every other telephone was not practical. Alexander Graham Bell, who is by most credited as the inventor of the telephone, acknowledged this problem early and formed the first switching office in 1878 where each phone was connected to a centralised switching office and human presence was required to switch and set up telephone calls, see Figure 4.

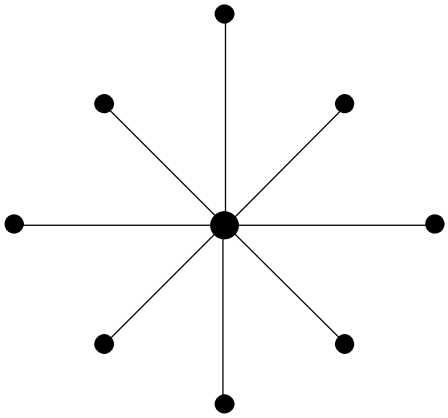

Figure 4: Centralised switch

To enable long distance phone calls, every switching station had to be connected to every other switching station. Therefore the original problem returned but was countered by the invention of second-level switching offices. One can imagine that after some time the same problem would occur with connecting second-level stations and so it did. Higher level stations were needed and the hierarchy eventually grew to five levels. In Figure 5 two level hierarchy setup is depicted.

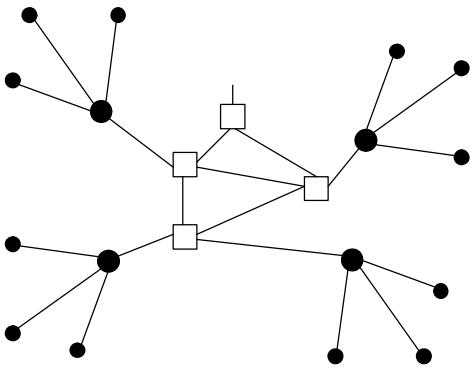

Figure 5: Two-level hierarchy

In 1891 a new technology was developed that enabled automated switching of phone calls. This technology took some time to be acknowledged and implemented but few decades later almost all manual exchanges had been replaced with this new technology. This system is currently known as POTS. The next revolutionary technology wasn't introduced until the 1970s when ISDN came around. In ISDN voice is converted to digital signals were before it had travelled as analogue. No major changes have been made to ISDN since then so the current state of PSTN is very mature.

2.3 VoIP versus PSTN

VoIP uses packet switching to transmit voice data while PSTN uses circuit switching. Therefore the two systems work in completely different ways and each has its advantages and disadvantages.

Table 2 shows a brief comparison between the two systems which will be studied further in this chapter.

PSTN	VoIP
Dedicated Lines	Multiple channels can be carried over the same connection
Each line is 64 kb/s (in each direction)	Audio compression can decrease bit rate significantly (Down to 5 kb/s)
Limited offer of extra features. The ones available such as call waiting, caller ID and so on are usually available at an extra cost	Many features available today with the opportunity to introduce new ones in the future. They are sometimes included free with the service
When placing an emergency call it can be traced to the callers location	Emergency calls cannot always be traced to a specific geographic location
Long distance calls are usually charged per minute or by bundled minute subscription	Long distance calls are often included in regular monthly price or cost the same as local calls
Hardwired landline phones (those without an adapter) usually remain active during power outage	If there is no backup power in place, phone service will go down during power outages

Table 2: VoIP vs. PSTN

2.3.1 Efficiency

In PSTN a connection is established between users participating in a phone call. During that session the line between the parties is completely occupied and can't be used by other users or for other activities. Usually only one user talks at a time in a phone call and sometimes even none which results in a low utilization of each phone line. Phone calls are transmitted at a fixed rate of 128 kb/s (64 kb/s in each direction) which translates into 16 kB each second the circuit is open or roughly 1MB per minute (Valdes & Roos, 2001). It is clear that much of the bandwidth is being wasted in every phone call which is one of the biggest reasons for the growing popularity of VoIP.

In VoIP voice data is packetised and sent over IP the same way as data is sent over the Internet. By being packet switched VoIP offers much improved utilization of bandwidth as data is only sent as soon as one/both parties make a sound. The sound is transferred into multiple packets that travel independently to their destination. Meanwhile parties can use the rest of their line capacity for other activities e.g. data transfer and browsing. Calls can be transmitted at a rate as low as 5 kb/s (in each direction) due to audio compression. Different codecs result in different bit rates and quality but the bit rate is almost always

lower than that for PSTN. Comparison of the bit rate achievable by some of the most common codecs is shown in Table 3 (Walker, 2002).

Codec	Bit Rate (Kbps)
G.711	64,0
G.729	8,0
G.7231.1-MPMLQ	6,3
G.7231.1-ACELP	5,3
G.726	32,0

Table 3: Bit rate comparison

2.3.2 Reliability

Besides advantages there are disadvantages with packet switching. As was mentioned above, packets travel through the network independent of each other which means that some might take longer time to arrive or get lost on the way resulting in a resend of those packets. This isn´t much of an issue in data transfers but for voice communication it is intolerable. No one wants to participate in a conversation where some of the speech gets lost or arrives too late resulting in long delays. Since VoIP users don't get their own lines for each conversation chances are that, during peak hours, traffic through the network is too high resulting in packet losses.

PSTN is much more reliable as its five nines availability confirms. The five nines availability stands for PSTN's 99,999% availability which is about 5 minutes of downtime per year (Zorpette, 1989). These numbers imply that reliability is at its best in PSTN. The same goes for quality as problems like jitter and delay are almost unheard of in PSTN. It´s evident that quality and reliability are far greater for PSTN than VoIP and improvements are required in order for VoIP to successfully replace PSTN.

Other factors relating to reliability are also in PSTN's favour. One thing worth considering is the case of power failures. Since data networks generally do not provide backup power, power failure leads to service interruption. For PSTN on the other hand the phone lines usually remain active during power outage. Another, more serious, issue is related to emergency calls e.g. 112 calls. When clients call 112 through a landline and are, for some reason, unable to give up information regarding their location, the call can be traced back to the client's location enabling a rescue team to be sent out. For VoIP users this is not a default feature. VoIP engineers are trying to find a solution to this problem but at the moment users will need to update their location regularly or risk being untraceable in case of emergency.

2.3.3 Costs and Features

When it comes to costs and features VoIP has a growing advantage over PSTN. Since VoIP transfers voice over IP it can offer cheaper calls, especially over long distance, as well as opening up many opportunities in service. Some examples of possible services with VoIP are

- Portability – Clients can, principally, use their phones anywhere there is access to IP.
- Rich media service – Clients are able to send instant messages, see if friends are online/offline, video calls and more.
- Integration with other applications – Makes click to call on websites available, voicemail over e-mail, call over e-mail and more.
- No geographical restrictions – Clients can be based in one country but still have their phone number registered in another.
- Rich features – Click to call, FMFM[3], personalised ringtones, call diverted to many phones at the same time and more.

These are only some of the services available with VoIP and with the continuous evolution of computer technology many other neat features and applications will become available in the future.

Some of the services available to VoIP users are also available for PSTN users but they more often than not come with extra charging fees. Many VoIP providers offer these services for free, resulting in lower cost for the user. Free or cheap features combined with lower charging fees can make monthly cost significantly lower for VoIP users than PSTN users. Since cost is often the most important factor for consumers, it has been one of the biggest incentives for people to switch over to VoIP.

[3] Feature that allows users to register list of numbers. If the called party can‘t be reached in the dialed number FMFM will try to rout the call to another number on the list.

2.4 MPLS

Internet activity has increased and evolved over the last few years enabling new applications and services in business and personal markets. Clients request services like e.g. VOD and VoIP to be available and work smoothly. This doesn´t only require greater bandwidth but also some guarantee of QoS or CoS. This is where MPLS comes into play as it is a protocol that was designed to meet the requirements of next-generation networks.

"*MPLS is an Internet Engineering Task Force (IETF)-specified framework that provides for the efficient designation, routing, forwarding, and switching of traffic flows through the network.*" (Trillium).

In other words it is a standards-approved technology that enables QoS by specifying paths through which packets travel. This is done by assigning labels to each packet's header so that routers need less time to identify the next node the packet is forwarded to. Labels can be created and designed by different criteria but that is beyond the scope of this thesis. Here it´s sufficient to know that MPLS is capable of handling VoIP packets.

3 Threats

This chapter introduces the taxonomy used for the VoIP analysis. Few threats, from the taxonomy, were considered redundant since they offered little to no threat to either providers or consumers. These threats were therefore omitted in the analysis but those used will be briefly introduced in this chapter. Threats to the PSTN system will be briefly introduced.

3.1 Threats to VoIP

3.1.1 Threat taxonomy

When constructing a risk analysis for a system one needs to know all possible threats to that system. Threats to VoIP are quite a few and outnumber those of PSTN. People and organisations have, over the last few years, constructed taxonomies for VoIP threats. Most of those taxonomies agree on the threats but the categorisation within the taxonomy may differ.

VoIPSA (Voice over IP security association) is a non-profit organisation that aims at increasing VoIP security. In 2005 VoIPSA released a comprehensive threat taxonomy that defined threats to VoIP deployments, services and end users. The biggest downside of VoIPSA's taxonomy is that it isn´t focused on either users or vendors. Therefore some of the threats may apply strongly to users but are not serious to the vendors and vice versa. Although other taxonomies are available, most of them are built with the guidance of VoIPSA's taxonomy and often only differ in the categorization of the threats.

In VoIPSA's taxonomy threats are divided into six categories:

- Social Threats
- Eavesdropping
- Interception and Modification
- Service Abuse
- Intentional Interruption of Service
- Other Interruptions of Service

VoIPSA's taxonomy will be used for the risk analysis in this thesis. Each category and the threats within each one[4] will be covered in the following chapters.

[4] Few threats from the taxonomy have been left out of the risk analysis for this thesis and will therefore not be covered.

3.1.2 Social Threats

Patrick Park defines social threats in the following way: *„It focuses on how to manipulate the social context between communication parties so that an attacker can misrepresent himself as a trusted entity and convey false information to the target user.“* (Park, 2008). This definition describes threats categorised under misrepresentation but theft of service and unwanted contact are also categorised as social threats. These threats can be seen in Figure 6.

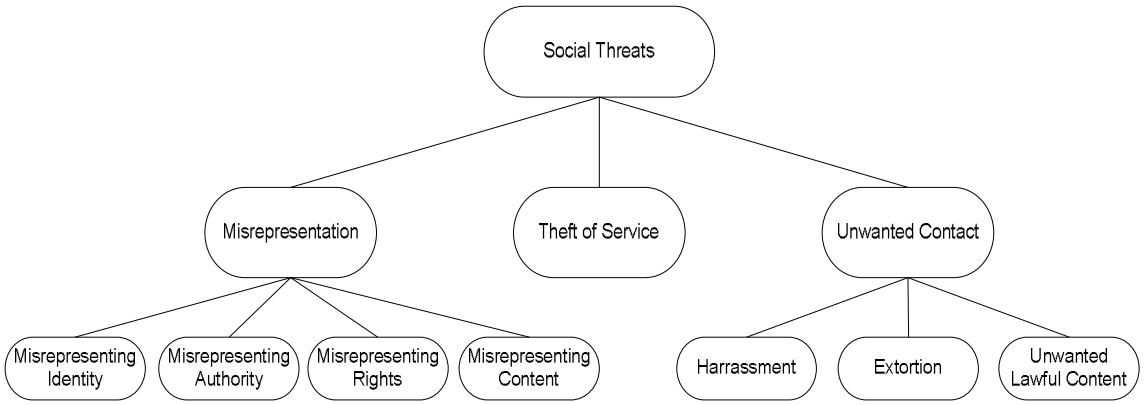

Figure 6: Social Threats

Misrepresentation:

The legal definition of misrepresentation is "*an assertion or manifestation by words or conduct that is not in accord with the facts*".

As can be seen in Figure 7 the attacker claims to be User A by presenting false information to User B (the victim). This is done e.g. in order to gain access to otherwise unreachable information, gain access to toll calls, call logs, files and for phishing purposes. The attacker may misrepresent his identity, authority, rights and/or content in order to fulfil his achievements.

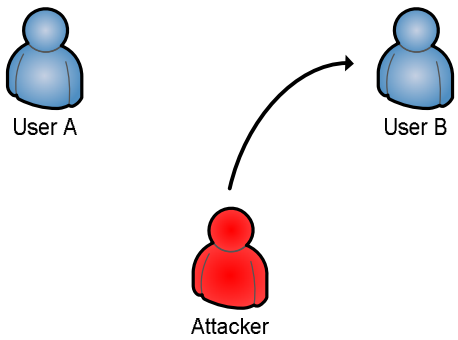

Figure 7: Misrepresentation

Theft of Service:

Theft of service stands for any use of service without proper payment. Toll frauds have been a part of the telephone system almost from start and VoIP is no different. Typical theft of service is placing calls without payment. This may be done e.g. by hacking the system or changing billing information. More serious attack is the unlawful taking of service provider property. Over the last years many cases have come up where computer criminals hack a service provider and sell his phone minutes on the black market. Attacks on private telecommunication stations are also increasing in number and magnitude. The number of minutes sold can be in thousands or even millions (Antonopoulos, 2006) so the financial loss for the victim can be significant.

Unwanted Contact:

Unwanted contact is any contact that either requires prior affirmative consent for incoming calls or bypasses a refusal of consent for outgoing calls (VoIPSA, 2005). Harassment, extortion and unwanted lawful content fall under this category. The biggest issue, of those three, for service providers and users is the unwanted lawful content.

Unwanted lawful content may include lawful pornography, advertisements and/or other unwanted messages. In many cases the attacker sends out a bulk of session initiation attempts to the user in order to spam messages to him as can be seen in Figure 8. Everybody is familiar with the annoying e-mail spams that count for up to 95% of all e-mail traffic (Trend, 2010, p. 27). They have been countered with filters, which are capable of blocking about 90% of all spams, and the awareness of users. With VoIP came the possibility of spam over IP telephony or SPIT. SPIT is somewhat comparable to PSTN-call spam in the form of telemarketer calls. The main difference is that through VoIP those sorts of calls are made much easier due to lower call cost, spam applications and so on. Attackers can even infect other users with viruses and utilise their bandwidth to generate spam.

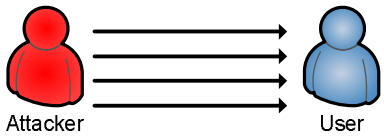

Figure 8: SPIT Attack

SPIT is getting more popular due to the fact that it's much harder to counter than e-mail spam. Since voice is real-time media users can't recognize spam until they have listened to its content.

3.1.3 Eavesdropping

Eavesdropping is when an attacker intercepts a data stream between two or more users without altering the data. The attacker does however gain access to the conversation between the users, as can be seen in Figure 9, making users vulnerable to the threats shown in Figure 10.

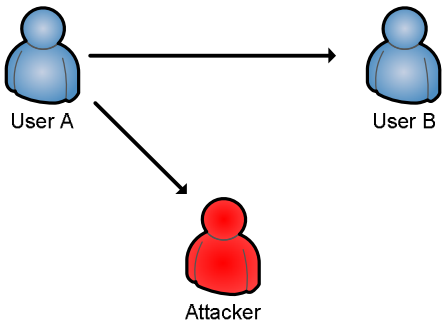

Figure 9: Eavesdropping attack

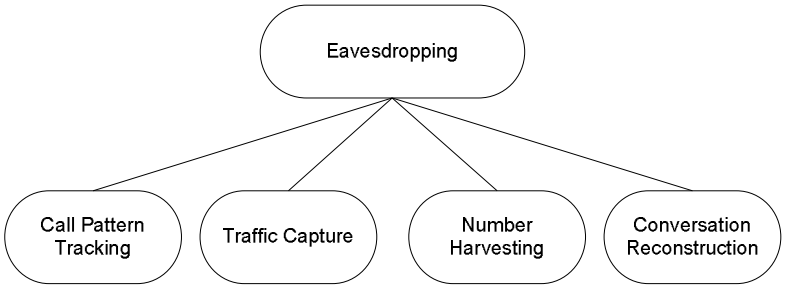

Figure 10: Eavesdropping Threats

Call Pattern Tracking

Call pattern tracking is the unauthorised tracking of users' call pattern. This enables the attacker to capture and analyse victims' phone records and use it to his advantage. This means the attacker can see who the victim has been calling which can be helpful in many situations. Reasons for these attacks may include theft, extortion and espionage.

Traffic Capture

In traffic capture, the attacker can capture ingoing/outgoing traffic and eavesdrop it. He however can't alter the traffic in any way.

Number Harvesting

Number harvesting is the unauthorised collection of IDs, usually in the form of phone numbers. The attacker monitors incoming/outgoing calls in order to build a database of legitimate IDs. The databases can be used for other attacks such as SPIT, toll fraud calls and DoS attacks (Endler & Collier, 2006, p. 149).

Reconstruction

Reconstruction refers to any unauthorised monitoring, recording, storage, reconstruction, recognition, interpretation, translation and/or feature extraction of any portion of a media session without consent of the owner (VoIPSA, 2005).

3.1.4 Interception and Modification

Threats in this category describe attacks where the attacker can intercept and modify the traffic between two or more endpoints. In Figure 11 a scenario is depicted where the attacker has intercepted traffic between two endpoints. The attacker now has the power to implement the threats shown in Figure 12. These attacks are also known as MitM attacks.

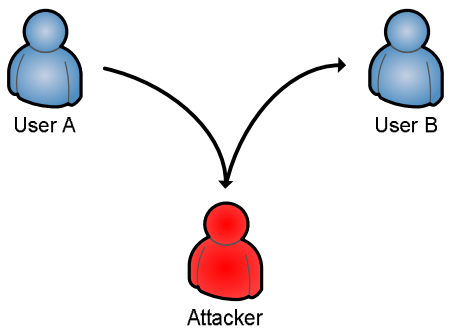

Figure 11: Interception and Modification attack

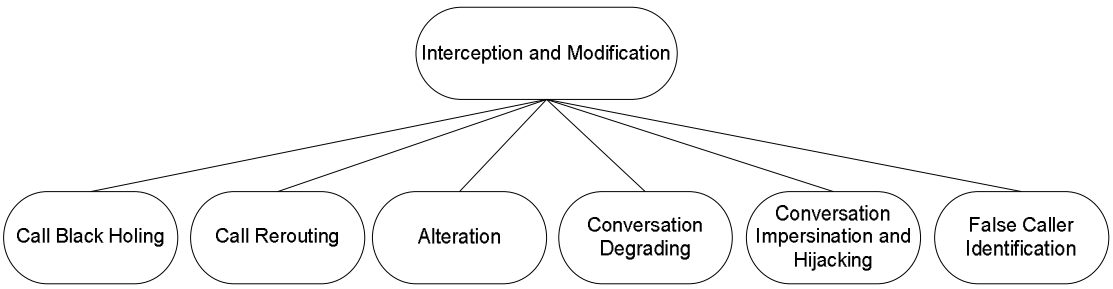

Figure 12: Interception and Modification Threats

Call Black Holing

Call black holing stands for any unauthorized method of redirecting essential elements of any VoIP protocol, usually SIP or H.323. This results in delayed call setups, errors in applications, dropped calls and other denial of service. One example of a black holing attack is when an attacker denies all incoming calls to a specific organisation such as hospitals, banks or police stations.

Call Rerouting

In call rerouting the attacker changes the call direction from one or more endpoints by altering the routing information in the protocol message. Reasons for rerouting are to either

include illegitimate notes into a communication or exclude legitimate ones. Attacker can use this attack for scams. One example is when an attacker reroutes incoming calls, e.g. to a bank, to himself and attempts to gain critical information from the user in the process, e.g. PIN numbers.

Alteration

Alteration, as the name applies, refers to any unauthorised alteration of communication. The attacker will alter some or all of the communication between endpoints in order to e.g. misrepresent identity, or deliver undesired information. These attacks can be extremely dangerous for the users as, in many cases, they think they are talking to a trusted person and may give up critical information to the attacker.

Conversation Degrading

Conversation degrading stands for any unauthorised reduction in QoS of any communication. The attacker intercepts and manipulates the media packets in a communication in order to introduce latency, jitter and so on. Reasons for these attacks may be to frustrate users or undermine SP's reputation.

Conversation Impersonation and Hijacking

Conversation impersonation and hijacking includes any modification of a communication in order to impersonate a trusted user or hijack the traffic completely.

False Caller Identification

False caller identification is a threat where the attacker calls a user and manages to signal untrue identity. One example is where an attacker represents a bank employee, or other trusted person, and asks for a PIN number or any other critical information. The victim may be more likely to give out this information if he sees the banks phone number calling him.

3.1.5 Service Abuse

Service abuse covers threats regarding any kind of fraudulent activity regarding VoIP. List of threats can be seen in Figure 13.

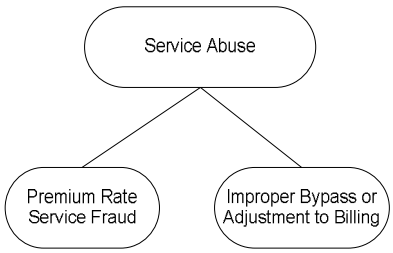

Figure 13: Service Abuse Threats

Premium Rate Service Fraud

Premium rate service fraud is the act of deceiving someone to call a premium rate number without offering some reward or service for the process. Premium rate numbers bear higher calling cost as portion of the fee goes to the owner of the number. Fraudsters have many

ways of enticing users to call these numbers and one popular way is by false advertisement.

Improper Bypass or Adjustment to Billing

This threat describes any unlawful method to avoid service charges or bills.

3.1.6 Intentional Interruption of Service

Threats in this category all aim at interrupting users from using VoIP and/or other service as depicted in Figure 14. In most cases the attacker has no personal gain from these attacks so the biggest motivation for attacks in this category is to annoy the victim. Intentional interruption can be carried out in many ways. DoS threats, especially VoIP specific ones, count for the largest part of intentional interruption threats.

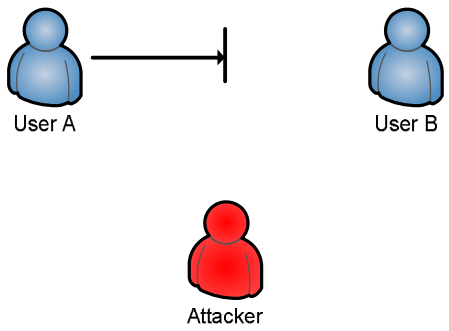

Figure 14: Interruption of Service attack

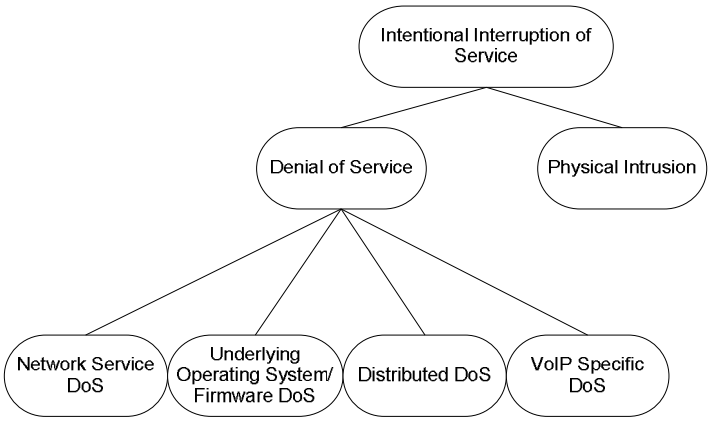

Figure 15: Intentional Interruption of Service Threats

Denial of Service

Denial of service or DoS attacks are well known in the computer world as hackers, through the years, have applied various ways to deny users of some sort of service. DoS attacks are defined as attempts to make computer resources unavailable to their intended users and this is precisely what they do. The hacker, through various measures, floods the system and makes it unable to function correctly in the process.

Since VoIP is IP based it is also vulnerable to DoS threats. There are number of ways that an attacker can deny VoIP service but the threats can be divided into four categories. These categories will now be studied further.

Distributed DoS

DDoS is an attack where number, often thousands or even millions, of computers are utilised to attack a single target. Usually the attacker utilises a number of computers without their owner consents to form a so-called botnet. These botnets are then controlled by one master computer and their forces combined to attack a single target, flooding it with countless number of packets.

Underlying operating system or firmware DoS

Most of the underlying OS and firmware for VoIP is run on popular operating systems or firmware that regularly becomes vulnerable to new threats, e.g. viruses. Vendors update their products regularly but hackers are quick to find and exploit any sort of vulnerability in the underlying systems.

Network services DoS

Network service DoS describes the threat that an attacker targets network components or services that the VoIP service depends on. For example the attacker can flood routers, switches, proxies, etc. making them unable to function properly and therefore close down any VoIP service passing through these network components. The attacker can also target services that VoIP depends on like DNS and DHCP with the same results.

VoIP specific DoS

Threats in this category are all VoIP specific i.e. they all utilise vulnerabilities in VoIP protocols, endpoint software, setup etc. to enable attacks.

Physical Intrusion

Physical intrusion describes the threat that an unauthorised person gains access to a protected premise. If that premise is accessed the attacker can cause serious damage to a VoIP system by various methods. The premise can be in the form of a tangible asset such as a building or a facility. It can also be in the form of an intangible asset such as the physical layer of the OSI model.

3.1.7 Other Interruptions of Service

This category hosts other threats that interrupt VoIP service but aren't necessarily intentional. The threats can be seen in Figure 16.

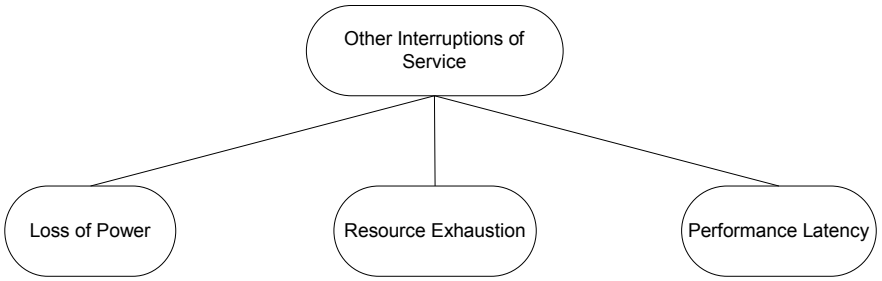

Figure 16: Other Interruptions of Service

Loss of Power

Since VoIP is data network based, power loss will deny users of any service unless they have some backup power in place. Power loss can have various causes, both intentional and unintentional. Intentional causes include vandalism, theft, terrorism etc. often in the form of direct physical damage to power stations or other power sources. Regular power outage will deny endpoint devices of service since they rely on external power sources and are seldom UPS-protected.

Resource Exhaustion

„Resource exhaustion is a simple denial of service condition which occurs when the resources necessary to perform an action are entirely consumed, therefore preventing that action from taking place." (OWASP, 2009). Resource exhaustion can origin from various causes. Attackers can flood a victim's system with various requests, depleting all CPU memory in the process. Faults in software/hardware and viruses may also cause resource exhaustion in various ways.

Performance Latency

Latency, or delay, is measured as the time it takes a packet to travel from its origin to its final destination. The delay can be divided into three categories: Propagation delay, handling delay and serialisation delay. Propagation delay is caused by the length that a signal has to travel in packet networks. Handling delay describes the delay caused by devices that forward the packet through a network (e.g. packetisation, compression, and packet switching). Finally serialisation delay is the time it takes to place a bit/byte onto an interface (Davidson, Peters, Bhatia, Kalidindi, & Mukherjee, 2006).

It's evident that the delay may have various sources. Latency >200 ms is, in most cases, considered unusable in normal conversations (VoIPSA, 2005). Providers need therefore to monitor the whole calling process and try to minimise delay at all sources.

3.2 Threats to PSTN

As has been previously stated, there are way fewer threats to the PSTN system. In fact only 9 of the 31 threats to VoIP were believed to apply to PSTN. These threats can be seen in Table 4 below.

#	Threat
4.5	Misrepresentation
4.6	Theft of Service
4.7	Unwanted Contact
7.2	Premium Rate Service Fraud
7.3	Improper Bypass or Adjustment to Billing
8.1.4	Distributed Denial of Service
8.2	Physical Intrusion
9.1	Loss of Power
10.1	Inability to Locate Emergency Calls

Table 4: Threats from VoIPSA that apply to PSTN

Seven other threats were identified for the PSTN system. These threats will not be given as detailed attention as the threats to VoIP. The aim of this thesis is to construct a risk analysis for VoIP and the one for PSTN will only be used for comparison. The threats, and the sources of each one, can be seen in Table 5.

Threat	Source
Personnel errors	Errors made by service providers personnel
Other human errors	Errors made by other people
Acts of Nature	Natural events/disasters
Hardware failures	Failure in hardware components
Software failures	Internal errors in software
Overloads	Service demand exceeds the system's capacity
Denial of Service	Any denial of service

Table 5: Other threats to PSTN

Threats in Table 4 have already been covered in section 3.1 and most of the threats in Table 5 are self explanatory, except possibly for the threat of an overload.

Overload refers to the threat that the phone system will be overloaded due to traffic reaching its limits. During an overload the system is unable to serve new clients. This sometimes happens during peak hours, such as new-year's eve.

4 Risk Analysis

4.1 RM Studio

The risk analysis, in this thesis, was performed in a software called RM Studio. RM Studio was developed by Stiki which is a leading provider of information and security solutions in the Nordic countries and was one of the first organisations to achieve ISO/IEC 27001 certification.

The software is divided into three processes:

- Risk Assessment
- GAP Analysis
- Risk Treatment

In the risk assessment process, assets and threats are identified. Impact and probability of each threat along with the vulnerability of assets from particular threats are assigned a value from low to immense. The risk associated with each asset is then calculated by examining the relationship between assets and threats. When the risk assessment is complete the user can see the security risk of the whole system and also the risk involved with each asset. The security risk is calculated based upon number of factors e.g. the impact and probability of each threat, vulnerability of assets and value of assets. The results are shown on a scale from 0-100%. The meaning of these numbers must be interpreted for each project and/or each threat. Sometimes a security risk of 50% is considered too high where in other cases it's acceptable.

The GAP analysis allows the user to compare the actual state of the entity to the standard he is trying to achieve certification of. The standard can be a built in standard, e.g. ISO/IEC 27001, or user defined.

If the user is in the process of implementing any standards, or plans to do so in the future, the risk treatment section of RM studio will calculate current-, future- and base security risk. Future risk takes into consideration any future implementation of standards or parts of them, defined by the user. Base security risk calculates the system risk given that no parts of the standard are implemented. That way the user gets some idea about the benefits of implementing a standard and can also see which parts of the standard benefit the system the most.

4.2 Implementation

In order to construct the risk analyses, for VoIP and PSTN, assets and threats had to be defined. The threats, and descriptions of them, have already been covered in chapter three (3.1). The assets were chosen in guidance with employees of Síminn and were both in the form of tangible and intangible assets. The assets that were defined, as well as descriptions of each one, can be seen in Table 6.

Name	Description
Personal Privacy	Clients demand that their personal privacy is protected by the service provider. Breach of such privacy may result in lost customers, lawsuits etc.
Financial Assets	Any financial asset, other than phone minutes, belonging to service providers.
Phone Minutes	Hackers/Cyber-Criminals are stealing phone minutes from users or service providers with unprotected passwords or other vulnerabilities. In many cases clients are responsible for paying the bills that can be very expensive.
Critical Information	Critical Information refers to financial information, corporate information and any other information that is considered critical by the client.
Communication Service	Clients have paid for a way to communicate, in this case through VoIP and therefore consider this an asset. Any attacks that aim at blocking communication (e.g. DoS) are threatening this asset.
Information Services	As with communication services, information service is a service that the client has to pay for. Any attacks that block information are threatening this asset. Example: Some DoS attacks on VoIP may overflow to other devices such as routers and therefore block access to the Internet.
Welfare	The welfare of clients is considered an asset. This asset may be at risk if for example an attacker blocks communication and therefore takes away the ability to make emergency calls. Another issue is the inability to locate VoIP users that make emergency calls.
Reputation	Reputation is one of the most valuable assets of any company that offers service of some sort.
Revenue	Some attacks may hinder clients and/or service providers in making phone calls. This results in loss of revenue for the service provider.
Databases	Databases can include loads of private and/or delicate information. Failure to protect those databases can result in lost reputation, financial loss etc.
Hardware	All hardware belonging to service providers

Table 6: List of assets

The next step was to assign the impact and probability of each threat as well as assigning vulnerability to assets from particular threats. The values, as mentioned above, ranged from low to immense. Definitions of each value, low to immense, can be seen in the appendix.

The values given to each category were decided by studying various papers, discussion boards and web-seminars regarding VoIP/PSTN threats. The results were presented to a work group at Síminn and final values decided. Reasons behind the final values, for threats to VoIP, are presented in Tables 7 and 8. Reasoning behind PSTN values can be seen in Tables 17 and 18 in the appendix.

Threat:	Impact of Threat	Reason
Misrepresentation	**High**	Attacker can gain access to various information that can be harmful to the user. (PIN numbers, company information etc.)
Theft of Service	**Immense**	If attackers can implement the attack they can steal assets worth millions. (Example: Attackers from Romania stole phone minutes worth 11 million Euros from SPs all over the world)
Unwanted Contact	**Low**	This threat is mostly annoying to the user and denies phone activity while the user is being spammed.
Call pattern tracking	**Low**	Attacker only gains information about the numbers called by the user. He has to draw conclusions about the nature of the calls but has no concrete evidence about them. (Spying, extortion etc.)
Traffic Capture	**Medium**	Attacker can only listen in on the conversation but is unable to alter it. Therefore he could stumble upon important information but can't phish for them.
Number Harvesting	**High**	Information gathered in a database and used in other, more serious, attacks. (e.g. SPIT, DoS)
Reconstruction	**Very High**	Attacker can take over a conversation, add information or alter it in any way. He can misrepresent identity (Since User A thinks he is talking to User B) and therefore gain access to delicate information (ID, PIN number etc.)
Call Black Holing	**High**	The attack reduces QoS or denies service all together. (Companies unable to make outgoing calls, users can't make emergency calls etc.)
Call Rerouting	**Very High**	Attacker can take over a conversation, add information or alter it in any way. He can misrepresent identity (Since User A thinks he is talking to User B) and therefore gain access to delicate information (ID, PIN number etc.)
Alteration	**High**	Attacker can alter a conversation, gaining valuable information in the process.
Conversation Degrading	**Low**	Reduces QoS temporarily. Is annoying for users but not particularly threatening.
Conversation Impersonation and Hijacking	**Very High**	Attacker can gain access to valuable information.
Premium Rate Service Fraud	**Low**	If the attacker abuses this threat too much it will probably get noticed by the SP.
Improper bypass or adjustment to billing	**Low**	A single user can possibly get away with avoiding bills, which has minimum effect on SP's financial status.
User Call Flooding	**Low**	This attack only targets a single user at a time so the impact is minimal.
User Call Flooding Overflowing to other devices	**Medium**	This attack only targets a single user at a time so the impact is minimal. It can however deny other devices of service (Internet, PCs etc.)
Endpoint request flooding	**Medium**	This attack targets a single endpoint. If the attack arrives from PSTN it can impact the call processor.

Call controller flooding	**High**	This attack can deny all endpoints, connected to the call controller, of service.
Request looping	**High**	This attack can deny all endpoints, connected to the call controller, of service.
Directory Service Flooding	**Very High**	Attack takes out all endpoints connected to the attacked server.
Malformed Requests and messages	**Medium**	Attack targets single user at a time.
QoS Abuse	**Low**	Reduces QoS but doesn't deny or stop data stream altogether.
Spoofed Messages	**High**	Attackers can exploit vulnerabilities in protocols to send all sorts of messages (SIP BUY, SIP BUSY, etc.) that interrupt or shut down a conversation.
Call Hijacking	**High**	This attack can deny users completely of service.
Network Services DoS	**Very High**	Attack aimed at network components and/or services that VoIP depends on. Successful attack can shut down service for multiple users.
Underlying Operating System/Firmware DoS	**High**	Viruses, worms etc. that attack underlying OS can shut down VoIP service.
Distributed Denial of Service	**Immense**	100s/1000s of computers/phones used (often without their owners knowledge) to flood a system and shut it down completely. Especially dangerous if the target is a emergency call centre.
Physical Intrusion	**Immense**	If an attacker gains access to restricted area he can do great deal of harm.
Loss of Power	**Very High**	If there is no backup power in place, VoIP service will shut down completely.
Resource Exhaustion	**Low**	Faults in software/hardware can affect VoIP service temporarily. These faults are easily solved with updates or new firmware. Viruses can also cause resource exhaustion but they are likely to do greater harm in other areas.
Performance Latency	**Low**	Annoying for the user but has no other affects.
Inability to Locate Emergency Calls	**Very High**	Callers' welfare may be at risk. Inability to locate an emergency call can result in serious harm, or even death, of the caller.

Table 7: Reasons behind Impact of Threat values (VoIP)

Threat:	Probability of Threat	Reason
Misrepresentation	**High**	There are many ways to misrepresent identity. Users are, in many cases, unaware of the threats involved with IP systems.
Theft of Service	**Medium**	SP, most likely, has a strong security system in place. There are however many examples of attackers managing to steal phone minutes.
Unwanted Contact	**Very High**	Spamming through VoIP (SPITTING) is easy (Number of software available that allow attackers with little to no knowledge to implement SPAM). It´s hard to filter out SPIT since the nature of the call can't be known until the call is answered.
Call pattern tracking	**Medium**	Attacker has to gain access to the SP's network (that should be well protected)
Traffic Capture	**Medium**	Attacker has to gain access to the SP's network (that should be well protected)
Number Harvesting	**Medium**	Attacker has to gain access to the SP's network (that should be well protected)
Reconstruction	**High**	Many applications available, often free of charge, that make this attack easy to implement.
Call Black Holing	**Low**	The attacker has little to gain from the attack other than to annoy.
Call Rerouting	**High**	Many applications available, often free of charge, that make this attack easy to implement.
Alteration	**Medium**	It's harder to alter a part of a conversation than to take over the conversation completely.
Conversation Degrading	**Low**	The attacker has little to gain from the attack other than to annoy.
Conversation Impersonation and Hijacking	**Medium**	Attacker has to gain access to the SP's network (that should be well protected)
Premium Rate Service Fraud	**Medium**	It's harder to implement PRS scams in Iceland than on the International scene. (due to smaller customer base and fewer international clients)
Improper bypass or adjustment to billing	**Low**	SPs should keep good records on telephone records and accounting information.
User Call Flooding	**Medium**	Attacker has to gain access to the SP's network (that should be well protected)
User Call Flooding Overflowing to other devices	**Medium**	Attacker has to gain access to the SP's network (that should be well protected)
Endpoint request flooding	**Medium**	Attacker has to gain access to the SP's network (that should be well protected)

Call controller flooding	**Low**	Servers are well protected.
Request looping	**Low**	Servers are well protected.
Directory Service Flooding	**Medium**	Attacks on DNS, DHCP etc. are harder to implement than attacks on single users. (since they are better protected)
Malformed Requests and messages	**Medium**	Attacker has to gain access to the SP's network (that should be well protected)
QoS Abuse	**Medium**	Attacker has to gain access to the SP's network (that should be well protected)
Spoofed Messages	**Medium**	Attacker has to gain access to the SP's network (that should be well protected)
Call Hijacking	**Medium**	Attacker has to gain access to the SP's network (that should be well protected)
Network Services DoS	**Medium**	Attacks on DNS, DHCP etc. are harder to implement than attacks on single users. (Since they are better protected)
Underlying Operating System/Firmware DoS	**Low**	Operating systems are updated regularly, especially if there is a known vulnerability in the OS. So the timeframe for these attacks is narrow.
Distributed Denial of Service	**High**	If the attacker possesses enough computers/phones then there isn't much that can be done to avoid this attack.
Physical Intrusion	**Low**	SPs usually have a good security system in place. Entrance to important rooms (server rooms etc.) usually requires access key and these rooms are often guarded at all hours.
Loss of Power	**Low**	Power outages are rare. SPs should have some backup power but single users are likely to lose all service.
Resource Exhaustion	**Low**	Hardware/software constantly updated to correct flaws.
Performance Latency	**Very High**	Latency in calls can be the result of many different things. (bad service, servers, end devices etc.)
Inability to Locate Emergency Calls	**Immense**	Few VoIP providers guarantee traceability of emergency calls. In most cases the user is responsible for regularly updating the location of his phone (good chance that many users will ignore this duty)

Table 8: Reasons behind Probability of Threat values (VoIP)

4.2.1 VoIP results

The results from the risk analysis can be looked at in a number of ways, e.g. with respect to the risk involved with each asset or by looking at the total risk of the system. Since this thesis emphasises on the threats involved with VoIP, it is natural to look at the results with respect to the average security risk from each threat. These results can be seen in Table 9.

Threat Name	Security Risk
10.1 - Inability to Locate Emergency Calls	82%
5.4 to 5.8 – Reconstruction	69%
4.6 - Theft of service	68%
6.2 - Call Rerouting	65%
8.2 - Physical Intrusion	65%
8.1.4 - Distributed Denial of Service	63%
4.5 – Misrepresentation	62%
9.1 - Loss of Power	61%
8.1.1.1.7 - Directory Service Flooding	59%
6.6-6.7 - Conversation Impersonation and Hijacking/ False Caller Identification	58%
9.3 - Performance Latency	56%
8.1.1.5 - Call Hijacking	53%
8.1.2 - Network Services DoS	53%
8.1.1.1.5 - Call Controller Flooding	52%
6.1 - Call Black Holing	51%
8.1.1.1.2 - User Call Flooding Overflowing to Other Devices	51%
8.1.1.1.6 - Request Looping	50%
6.3-6.4 Message Alteration	49%
7.2 - Premium Rate Service Fraud	47%
4.7 - Unwanted Contact	47%
5.3 - Number Harvesting	47%
8.1.1.1.3/4 - Endpoint Request Flooding before/after Call Setup	47%
8.1.1.2 - Malformed Requests and Messages	47%
8.1.1.3 - QoS Abuse	47%
5.2 - Traffic Capture	45%
8.1.1.4 - Spoofed Messages	44%
6.5 - Conversation Degrading	44%
8.1.1.1.1 - User Call Flooding	41%
8.1.3 - Underlying Operating System/Firmware DoS	41%
7.3 - Improper Bypass or Adjustment to Billing	35%
5.1 - Call Pattern Tracking	32%

Table 9: Average risk of VoIP threats

As the table shows, inability to locate emergency calls bears the biggest risk factor. This is in accordance with the discussions in the VoIP community today. There are number of cases available where VoIP users failed to receive help due to the inability to locate VoIP calls. This has invoked questions about the responsibilities service providers have

regarding their users safety and has in some cases lead to lawsuits against providers (Gross, 2005). Telecommunication regulators all over the world are respectively demanding social obligations and/or imposing regulations requiring VoIP providers to deal with the emergency call problem (Lee, 2006).

Other threats are significantly lower with the second biggest risk being reconstruction. Reconstruction poses various threats to the clients as it can threaten all sorts of information and privacy which will result in unsatisfied customers and bad reputation for VoIP providers. Close behind is the threat of service theft where theft of phone minutes contributes greatly to the security risk. Cyber criminals all over the world are increasingly focusing their attacks at VoIP providers with the goal of stealing, and reselling on the black market, phone minutes worth thousands or even millions of dollars (Constantin, 2010), (Barnard, 2009).

Close behind are the threats of call rerouting and physical intrusion. Call rerouting, just as reconstruction, doesn't pose a direct threat to the service provider but rather it can hurt the client in many ways resulting in unsatisfied clients and/or bad reputation for the provider. Physical intrusion on the other hand does threat the provider directly. Although this threat is very unlikely to occur, since most telephone providers defend valuable tangible assets, the consequences of such an attack can be devastating. If an intruder gains physical access to the right equipment he can cause great damage to the telephone system and even shut it down completely for some time. Intrudes can also hack into SPs network layer and deal harm to the telecommunication system from there.

The sixth biggest threat is DDoS. This kind of threat is unlikely to be targeted directly at the service provider but rather at big clients e.g. companies or big organisations. The biggest problem regarding this threat is that if an attacker can gather enough endpoint devices, for the attack, neither the client nor the service provider can do much to stop it.

The seventh biggest threat is misrepresentation which is, similar to reconstruction and call rerouting, directed at the client rather than directly at the service provider.

The last threat, that bears over 60% security risk, is the threat of power loss. As was stated in section 2.3.2 power loss will cause DoS for VoIP users unless they have some backup power in place. Service providers and bigger clients will probably take this into consideration, by installing a UPS backed up by a gasoline generator, but it's unreasonable to expect single users to do the same. They will therefore be denied of all service in case of a power loss.

The rest of the threats bear lesser security risk and will not be covered further. They may however not be overlooked by the service providers. In many cases measures against one threat can reduce the security risk involved with another one. Service providers can therefore reduce security risk for most threats by actively fighting the eight threats above.

4.2.2 PSTN results

In Table 10 the average security risk of each threat to the PSTN system is shown.

Threat Name	Security Risk
#6 - Overloads	62%
8.2 - Physical Intrusion	59%
10.1 - Inability to Locate Emergency Calls	59%
4.5 - Misrepresentation	50%
5 - Communication Service	50%
#3 - Acts of Nature	49%
#2 - Other human errors	47%
7.2 - Premium Rate Service Fraud	47%
8.1.4 - Distributed Denial of Service	47%
#4 - Hardware Failures	47%
#5 - Software failures	47%
#1 - Personnel Error	46%
4.6 - Theft of service	44%
7.3 - Improper Bypass or Adjustment to Billing	35%
9.1 - Loss of Power	35%
#7 - Denial of Service	29%
4.7 - Unwanted Contact	29%

Table 10: Average risk of PSTN threats

The threat of a system overload is considered the biggest threat to PSTN. Although the capacity, at least in Iceland, manages to fulfil all demand in nearly all cases, there is always a chance of it exceeding capacity. This results in denial of service to all potential new users during an overload. Since this happens during peak hours, where many users want to place a call, service providers' reputation is compromised during the overload.

The second biggest threat is physical intrusion. This threat isn't directly dependant on a particular telephone system so it is to no surprise that the security risk is similar between the two analyses.

Inability to locate emergency calls does still bear considerable security risk. Reasons are similar to those for an overload. There is a minimum likelihood of calls from PSTN being untraceable but if that happens, consequences can be severe and can cause damage to the users' welfare. Since the impact is so severe, this threat can't bear lover security risk.

These three threats stand out regarding security risk. Other threats are all on or under 50% security risks and will not be covered further in this thesis.

4.2.3 Comparison

As can be seen in Table 10, in section 4.2.2, there's only one threat that bears over 60% security risk, compared to eight for VoIP. Every threat, included in both analyses, is lower for PSTN than for VoIP with the exception of threat 7.3, improper bypass or adjustment to billing, which is equal between the two systems.

Even though inability to locate emergency calls bears significant security risk in the PSTN analysis, it is much lower than in VoIP. This threat is considered by many to be one of the biggest hurdles that VoIP has to overcome.

Social threats apply to both systems. These threats are however easier to implement and/or more severe for VoIP systems. When misrepresenting, VoIP attackers can signal untrue identity by various means, such as signalling untrue phone number, while PSTN attackers have to rely on deception. Theft of service can also be much more severe in case of VoIP, where attackers can steal phone minutes worth millions. Attacks of this significance are unheard of in PSTN.

Eavesdropping threats are of little worry to PSTN users. There are certainly ways to unlawfully capture traffic between two PSTN parties but this requires the attacker to connect himself to a phone line/station of one of the participants, tap the victims' phone etc. These measures require much effort and will usually leave the attacker exposed. In VoIP however, the attacker can eavesdrop a victim in the comfort of his own home. The attacker needs not expose himself directly to implement this attack and can even be stationed in another continent.

Interception and modification threats do not apply to the PSTN system. Meanwhile they can cause serious harm and/or discomfort to VoIP users. VoIP therefore introduces a whole set of threats that users didn't need to worry about before.

Examining the average security risk involved with each asset, for the two systems, further supports that PSTN is safer than VoIP. Every asset bears lesser risk in PSTN than in VoIP, ranging from 6%-21%. Tables 11 and 12 show the average security risk to each asset.

Name	Security Risk
1 - Personal Privacy	52%
2 - Financial Assets	59%
3 - Phone Minutes	44%
4 - Critical Information	57%
5 - Communication Service	57%
6 - Information Services	59%
7 - Welfare	41%
8 - Reputation	57%
9 - Revenue	55%
10 - Databases	50%
11 - Hardware	59%

Table 11: Average risk to assets in VoIP

Name	Security Risk
1 - Personal Privacy	41%
2 - Financial Assets	50%
3 - Phone Minutes	34%
4 - Critical Information	47%
5 - Communication Service	50%
7 - Welfare	32%
8 - Reputation	51%
9 - Revenue	48%
10 - Databases	29%
11 - Hardware	49%

Table 12: Average risk to assets in PSTN

This chapter has shown that threats that apply to both systems always bear equal or larger security risk for VoIP. One must also take into consideration all the other threats that are only threatening to VoIP. All these results imply that VoIP still has a long way to go in order to become as reliable as the PSTN system.

5 Countermeasures

If VoIP is to successfully replace PSTN some measures need to be taken in order to approach the reliability that PSTN offers. It's somewhat unrealistic to demand PSTN's 99,999% availability for VoIP, since IP based systems are exposed to larger threat pool than public switched ones, but there are actions available that can significantly reduce risks involved with VoIP. Some of those actions are general and don't counter any specific threat directly while other actions are strictly aimed at countering specific threats. In this chapter some of those actions will be studied.

5.1 General actions

5.1.1 Software Updates

Keeping software up to date is always a good way of limiting the probability of vulnerabilities. This goes for any software needed to keep the service up and running as well as the software needed for end devices.

VoIP servers are often run on operating systems which may have some vulnerability (SNAC, 2006). By making sure that the operating system is up to date many vulnerabilities can be avoided. Although this is a direct counter to threat 8.1.3, Underlying Operating System/Firmware DoS, it also reduces other risks and is therefore considered a general action.

The provider should also take end users' safety into consideration. VoIP phones can include flaws, exploitable by attackers, so keeping the software up to date reduces the risk as newly discovered threats are often corrected through patches (Contreras, Doswald, Ehrensberger, Hahn, Litzistorf, & Ventura, 2007). Many users are unaware of the risk involved with outdated software making them vulnerable in the process. Service providers can inform users of these threats and/or monitor any software updates by major VoIP telephone vendors and forward them to users through a website, newsletters etc.

5.1.2 Anti-virus systems

Every computer system benefits from having a good anti-virus system in place. Worms and viruses are getting more complex and attackers are constantly figuring out new ways of infecting users. Many VoIP threats benefit from having the victims' computer infected with a virus before the attacker carries out the threat (e.g. unwanted contact, DoS attacks and resource exhaustion). Cyber-criminals release new viruses every day and since VoIP is getting more attention new VoIP viruses are likely to be developed and released in the future. VoIP providers and users should therefore always have a good, and regularly updated, anti-virus system in place.

5.2 Specific actions

5.2.1 Emergency Calls

The inability to locate emergency calls made from VoIP is a problem that needs to be issued if VoIP is to become a leading telephone system in the future. Unfortunately there's no solution that works as well as for PSTN, where the operator can easily link an address to the caller's number due to the E112/E911[5] capabilities. Instead VoIP users need to manually update the address linked to a VoIP number. VoIP providers need therefore to keep their clients informed of the capabilities and limitations of emergency calls through VoIP, in order to keep a good reputation and/or avoid lawsuits, upkeep social obligation, fulfil regulations etc. This can be done by including detailed information regarding emergency calls with every purchased VoIP service, place information and links on providers' website etc.

5.2.2 Eavesdropping

"*Preventing eavesdropping and impersonation requires good network security, and enabling strong encryption and authentication on the phones and servers.*" (SNAC, 2006).

Good network security is a wide concept and isn't directly related to VoIP and will not be discussed further. Encryption and authentication can be implemented by many different techniques. The level of encryption and authentication depends on the importance of information being protected. For regular users open source encryption software or VoIP phones with built in encryption may suffice. Other clients, e.g. corporations or companies, may demand better protection. In that case there are number of options available. The user can choose to encrypt the signalling messages, media stream or both. Figure 17, from (SNAC, 2006), shows three different setups.

[5] Enables emergency call centres to determine the general location from where a call originates.

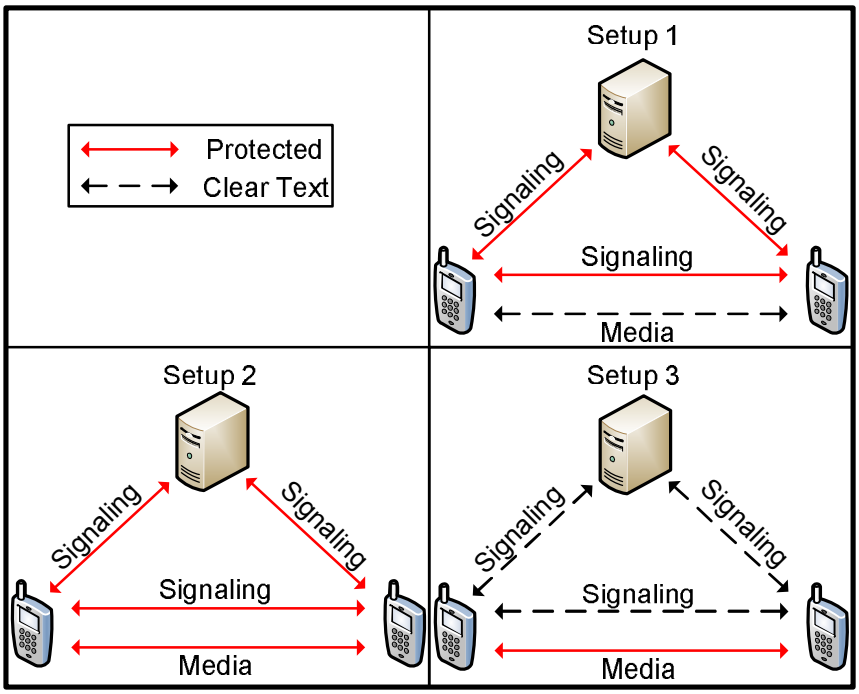

Figure 17: Encryption and authentication setups

In "setup 1" signalling messages are encrypted, protecting them from message spoofing and compromise of sensitive information. The media stream is however unprotected so it's vulnerable to eavesdropping and spoofing.

In "setup 2" both the signalling message and media session are protected so message spoofing, compromise of information and eavesdropping are prevented.

"Setup 3" is the inverse of "setup 1" so now eavesdropping and spoofing are no longer threats but the VoIP system is susceptible to message spoofing and call hijacking.

As was stated above, the level of protection depends on each user. Service providers can offer technical advices and/or setup assistance to bigger clients in order to find appropriate level of encryption needed in each case.

5.2.3 Interception and Modification

Threats in this category all involve some sort of ID spoofing, where the attacker causes the victims phone to display a number which is not that of the actual originating station.

Unfortunately, there is no effective way to prevent caller ID spoofing. The best solution so far is not to trust caller ID at all (Jianqiang, 2007). Distrusting caller IDs will however only work in certain circumstances. If the receiver isn´t familiar with the caller he has no way of confirming his credentials.

The risks of ID spoofing attacks can be limited by proper use of firewalls, configured to filter out the unwanted contact. Intrusion detection/prevention systems are also available

but just like the firewalls they limit interception and modification attacks but can´t prevent them completely (Herculea, Blaga, & Dobrota, 2008).

5.2.4 Intentional Interruption of Service

Intentional interruption of service can have different causes so there is no measure that tackles all the threats at once. Instead different actions have to be taken in order to effectively secure VoIP systems from threats in this category.

Physical intrusion has to be countered by implementing strict physical security scheme with restricted areas, access control, security guards, lock etc (Jianqiang, 2007).

DoS attacks aren't much of an issue for the service providers, since the attacker has to gain access to the provider's network, that should be extremely well protected, but users are ideal targets since their networks often lack security. Good computer security can prevent many DoS attacks as well as many other threats. VoIP users should therefore strive at keeping their computer security up to date at all times. This involves implementing and updating anti-virus software, set up firewalls, update software and so on.

This may not be sufficient to protect against all DoS attacks. There is always a possibility that SPs or users become victims of DoS attacks. In that case VoIP networks can be configured so that limited number of external calls will be accepted simultaneously. That way the victim can still make internal calls during the attack (SNAC, 2006).

6 Conclusions

If Voice over IP is to be a successor to PSTN much work must be done to enhance its security. PSTN has been in place for over a century so clients are used to a certain level of security and reliability. These users expect the same security performance of VoIP.

This thesis has shown that this is not the case today. VoIP is susceptible to a larger number of threats than PSTN and these threats are usually more severe for VoIP. All hope is not lost since there are indeed measures that can be taken in order to increase security for both VoIP users and providers. This is however far from a perfect solution to the problem. Most of these measures require a combination of time, money and IT knowledge to be successfully implemented. This will not be an issue for service providers and large companies but the general customer can't be expected to take such drastic measures only to achieve a properly secure telephone service.

Currently there is little to no legal framework regarding protection of transmission in VoIP. Therefore providers are not obligated to provide any kind of security to clients. Telecommunication regulators need to bring VoIP under a legal framework. Providers also have social responsibilities they need to honour since their destiny is intertwined with the users as there will not be a need for VoIP providers if the general public rejects the system. Providers need therefore uphold social obligations such as providing clients with appropriate security; inform them of main threats; maintain help centres etc.

Emergency calls in VoIP are another big issue. Similar to protection of transmissions, there has to be a legal framework regarding providers' responsibility in this matter. In many countries providers are required to inform all new clients of the limitations inherent in the VoIP emergency service.

As has previously been stated, many of the threats can be limited and/or avoided. Interception and modification will however still be a threat to the system. Firewalls and intrusion detection systems only go so far as limiting some of the threats in this category. Other measures have been suggested such as black/white listing (Baumann, Cavin, & Schmid, 2006) and voice authentication (Lawecki, 2007). All these measures have their limitation as they either lack in effect and/or are too troublesome to implement.

In summary, service providers will not be directly affected by most of the threats to VoIP, since they have the resources to defend against most of them. Their biggest concern will be the security of the average customer and finding ways to avert users getting exposed to these threats.

References

Anonymous. (n.d.). *Voice Over IP Information*. Retrieved May 10, 2011, from VoIP Laws and Legal Issues: http://www.voiceoveripinfo.com/voip-laws-legal-issues.php

Antonopoulos, A. M. (2006, June 16). *Nemertes*. Retrieved Mars 15, 2011, from VoIP Security: Theft of Service: http://www.nemertes.com/impact_analyses/voip_security_theft_of_service

Barnard, P. (2009, April 8). *TMCnet*. Retrieved April 25, 2011, from Men Charged with Stealing More Than 120 Million VoIP Minutes from Verizon, AT&T: http://hosted-voip.tmcnet.com/feature/articles/53861-men-charged-with-stealing-more-than-120-million.htm

Baumann, R., Cavin, S., & Schmid, S. (2006). *Voice Over IP - Security and SPIT.* Berne: University of Berne.

Biggs, P. (2007). *The status of voice over internet protocol (VoIP) worldvide, 2006.* ITU.

Chen, Z., Guo, S., Zheng, K., & Li, H. (2009). Research on Man-in-the-Middle Denial of Service Attack in SIP VoIP. *Networks Security, Wireless Communications and Trusted Computing, 2009. NSWCTC '09. International Conference on* , 263 - 266 .

Constantin, L. (2010, February 4). *Softpedia*. Retrieved May 6, 2011, from Fraudster Pleads Guilty to Stealing Millions of VoIP Minutes: http://news.softpedia.com/news/Fraudster-Pleads-Guilty-to-Stealing-Millions-of-VoIP-Minutes-134101.shtml

Contreras, S., Doswald, A., Ehrensberger, J., Hahn, X., Litzistorf, G., & Ventura, S. (2007). *Best Practices for VoIP-SIP Security.* Hesso; Ict.

Davidson, J., Peters, J., Bhatia, M., Kalidindi, S., & Mukherjee, S. (2006). *Voice over IP Fundamentals.* Cisco Press.

Dehestani, A., & Hajipour, P. (2010, April). Comparative Study of M/Er/1 and M/M/1 Queuing Delay Models of the two IP-PBXs. *JCIT: Journal of Convergence Information Technology, Vol. 5, No. 2* , pp. 36-42.

Endler, D., & Collier, M. (2006). *Hacking Exposed VoIP: Voice Over IP Security Secrets & Solutions.* McGraw-Hill Osborne Media.

Goode, B. (2002, September). Voice Over Internet Protocol (VoIP). *PROCEEDINGS OF THE IEEE, Vol. 90, No. 9* , pp. 1495-1517.

Gross, G. (2005, Mars 22). *PC World*. Retrieved April 26, 2011, from Texas Sues Vonage Over Emergency Service: Suit highlights VoIP's shortcomings on 911 emergency calls: http://www.pcworld.com/article/120141/texas_sues_vonage_over_emergency_service.html

Hallock, J. (2004). *A Brief History of VoIP Document One - The past* . Washington: University of Washington.

Haselton, T. (2009, December 31). *Mobile Burn*. Retrieved May 5, 2011, from AT&T asks FCC to drop required support for landlines: http://www.mobileburn.com/news.jsp?Id=8469

Herculea, M., Blaga, T., & Dobrota, V. (2008). *Evaluation of Security and Countermeasures for a SIP-based VoIP*. Cluj-Napoca: Editura U.T.PRESS.

Jianqiang, X. (2007). *Security Issues and countermeasure for VoIP.* SANS Institute.

Lawecki, P. (2007). *VoIP Security in Public Networks.* Stuttgart: University of Stuttgart.

Lee, J. (2006). *The policy implications of voice over internet protocol.* OECD.

Liu, H., & Mouchtaris, P. (2000, October). Voice over IP Signaling: H.323 and Beyond. *IEEE Communications Magazine, Vol. 38* , pp. 142 - 148.

Operations, D. F. (2006). *INTERNET PROTOCOL TELEPHONY & VOICE OVER: SECURITY TECHNICAL IMPLEMENTATION GUIDE.* DOD.

OWASP. (2009, February 28). *The open web application security project*. Retrieved April 20, 2011, from Resource Exhaustion: https://www.owasp.org/index.php/Resource_exhaustion

Park, P. (2008). *Voice over IP Security.* Cisco Press.

Rippon, W. J. (2006). Threat Assessment of IP Based Voice Systems. *1st IEEE Workshop on VoIP Management and Security* (pp. 17-26). IEEE.

SNAC. (2006). *Security Guidance for Deploying IP Telephony Systems.* National security agency: USA.

Tanenbaum, A. S. (2010). *Computer Networks.* Prentice Hall.

Trend, D. (2010). *Small Business IT Security For Dummies.* John Wiley and Sons, Inc.

Trillium. *Multiprotocol label switching.* IEC.

Unuth, N. (n.d.). *About.com*. Retrieved May 4, 2011, from What is Latency?: http://voip.about.com/od/glossary/g/latency.htm

Valdes, R., & Roos, D. (2001, May 9). *How Stuff Works*. Retrieved Mars 10, 2011, from How VoIP Works: http://communication.howstuffworks.com/ip-telephony2.htm

VoIPSA. (2005). *VoIP Security and Privacy Threat Taxonomy.* VOIPSA.

Walker, J. Q. (2002). *Assessing VoIP Call Quality Using the E-model* . NetIQ Corporation.

Zorpette, G. (1989, June). Keeping the phone lines open . *Spectrum, IEEE, Vol. 26* , pp. 32 - 36 .

Appendix

RM Definitions

The following two tables, 13 and 14, respectively show definitions of threat evaluation values and asset evaluation values as they are defined in RM-Studio.

	Impact of Threat	***Probability of Threat***	***Vulnerability of Asset***
Low	Minimal impact of threat.	The threat is likely to happen less than once a year.	Despite of the occurrence of the threat, the asset will be unchanged.
Medium	There is some impact of the threat.	The threat is likely to happen once a year.	If the threat happens the asset might be damaged or be unusable for some time.
High	Much disturbance in operation. Considerable time and investment required to go back to normal operation.	The threat is likely to happen once a month.	If the threat happens the asset might be damaged or be unusable.
Very High	Serious disturbance in nearly every part of the operation. Much time and investment to go back to normal operation.	The threat is likely to happen once a week.	If the threat happens the asset will be damaged to a great extent.
Immense	The consequences of threat are widespread and cause serious disturbance in operation. Very difficult to go back to normal operation.	The threat is likely to happen once a day.	If the threat happens the asset will cease to exist or be unusable.

Table 13: Definition of threat evaluation values

	Integrity	***Availability***	***Value***	***Confidentiality***
Low	It is not important that the asset is accurate.	The asset is not necessary for operating the business entity.	Easy and inexpensive to regain the asset.	Public may be aware of the asset. It may be discussed and published.
Medium	It is important that the basics are accurate.	It is possible to operate the business entity without the asset. It has to be available again in 24 hours.	Possible to operate business entity for a time period if loss of asset occurs.	Employees have access to or are aware of the asset. Information must be treated with caution towards third party.
High	The asset has to be reasonably accurate.	If the asset is not available it is difficult but possible to proceed working for 2-3 days.	Difficult to continue operation without the asset. Difficult to regain the asset if loss occurs.	Most employees are aware or have access to the asset. Intended for use inside the business entity only. Must not be disclosed to third party.
Very High	The asset must be complete and accurate, but details are irrelevant.	The asset has to be available during working hours.	Very difficult to continue operation without the asset. Very difficult to regain the asset if loss occurs.	Key employees are familiar with the asset but many employees are aware of it.
Immense	The asset must be complete and accurate.	The asset has to be available 24 hours a day.	Not possible to operate the business entity without the asset. Immensely difficult to regain the asset if loss occurs.	Only key employees have access to and are aware of the asset.

Table 14: Definition of asset evaluation values

Results from the VoIP analysis

This table depicts security risk between assets and threats along with impact, probability and vulnerability evaluations.

Asset Name	Threat Name	Security Risk	Impact of Threat	Probability of Threat	Vulnerability of Asset
1 - Personal Privacy	5.4 to 5.8 - Reconstruction	65%	Very High	High	Very High
1 - Personal Privacy	4.5 - Misrepresentation	59%	High	High	Very High
1 - Personal Privacy	6.2 - Call Rerouting	59%	Very High	High	High
1 - Personal Privacy	6.6-6.7 - Conversation Impersonation and Hijacking/ False Caller Identification	59%	Very High	Medium	Very High
1 - Personal Privacy	4.7 - Unwanted Contact	53%	Low	Very High	Very High
1 - Personal Privacy	8.1.1.5 - Call Hijacking	53%	High	Medium	Very High
1 - Personal Privacy	6.3-6.4 Message Alteration	47%	High	Medium	High
1 - Personal Privacy	5.2 - Traffic Capture	41%	Medium	Medium	High
1 - Personal Privacy	5.1 - Call Pattern Tracking	29%	Low	Medium	Medium
2 - Financial Assets	4.6 - Theft of service	76%	Immense	Medium	Very High
2 - Financial Assets	5.4 to 5.8 - Reconstruction	71%	Very High	High	High
2 - Financial Assets	6.6-6.7 - Conversation Impersonation and Hijacking/ False Caller Identification	65%	Very High	Medium	High
2 - Financial Assets	7.2 - Premium Rate Service Fraud	59%	Low	Medium	Immense
2 - Financial Assets	4.7 - Unwanted Contact	53%	Low	Very High	Medium
2 - Financial Assets	5.2 - Traffic Capture	47%	Medium	Medium	Medium
2 - Financial Assets	7.3 - Improper Bypass or Adjustment to Billing	41%	Low	Low	High
3 - Phone Minutes	4.6 - Theft of service	76%	Immense	Medium	Immense
3 - Phone Minutes	4.7 - Unwanted Contact	47%	Low	Very High	Medium
3 - Phone Minutes	7.2 - Premium Rate Service Fraud	29%	Low	Medium	Low
3 - Phone Minutes	7.3 - Improper Bypass or Adjustment to Billing	24%	Low	Low	Low
4 - Critical Information	5.4 to 5.8 - Reconstruction	71%	Very High	High	Very High
4 - Critical Information	4.5 - Misrepresentation	65%	High	High	Very High
4 - Critical Information	4.6 - Theft of service	65%	Immense	Medium	High
4 - Critical Information	6.3-6.4 Message Alteration	59%	High	Medium	Very High
4 - Critical Information	6.6-6.7 - Conversation Impersonation and Hijacking/ False Caller Identification	59%	Very High	Medium	High
4 - Critical Information	8.1.1.5 - Call Hijacking	59%	High	Medium	Very High
4 - Critical Information	5.2 - Traffic Capture	47%	Medium	Medium	High
4 - Critical Information	5.1 - Call Pattern Tracking	35%	Low	Medium	Medium
5 - Communication Service	8.1.4 - Distributed Denial of Service	76%	Very High	High	Immense
5 - Communication Service	6.2 - Call Rerouting	71%	Very High	High	Very High

5 - Communication Service	8.2 - Physical Intrusion	71%	Immense	Low	Immense
5 - Communication Service	8.1.1.1.7 - Directory Service Flooding	65%	Very High	Medium	Very High
5 - Communication Service	8.1.2 - Network Services DoS	65%	Very High	Medium	Very High
5 - Communication Service	9.1 - Loss of Power	65%	Very High	Medium	Very High
5 - Communication Service	8.1.1.1.2 - User Call Flooding Overflowing to Other Devices	59%	Medium	Medium	Immense
5 - Communication Service	8.1.1.1.3/4 - Endpoint Request Flooding before/after Call Setup	59%	Medium	Medium	Immense
5 - Communication Service	8.1.1.1.5 - Call Controller Flooding	59%	High	Low	Immense
5 - Communication Service	8.1.1.1.6 - Request Looping	59%	High	Low	Immense
5 - Communication Service	8.1.1.5 - Call Hijacking	59%	High	Medium	Very High
5 - Communication Service	6.1 - Call Black Holing	53%	High	Low	Very High
5 - Communication Service	8.1.1.1.1 - User Call Flooding	53%	Low	Medium	Immense
5 - Communication Service	8.1.1.4 - Spoofed Messages	53%	High	Medium	High
5 - Communication Service	8.1.3 - Underlying Operating System/Firmware DoS	53%	High	Low	Very High
5 - Communication Service	6.6-6.7 - Conversation Impersonation and Hijacking/ False Caller Identification	47%	Very High	Medium	Low
5 - Communication Service	8.1.1.2 - Malformed Requests and Messages	47%	Medium	Medium	High
5 - Communication Service	8.1.1.3 - QoS Abuse	47%	Low	Medium	Very High
5 - Communication Service	9.3 - Performance Latency	47%	Low	Very High	Medium
5 - Communication Service	6.3-6.4 Message Alteration	41%	High	Medium	Low
5 - Communication Service	6.5 - Conversation Degrading	41%	Low	Low	Very High
6 - Information Services	8.1.1.1.2 - User Call Flooding Overflowing to Other Devices	59%	Medium	Medium	Immense
7 - Welfare	10.1 - Inability to Locate Emergency Calls	82%	Very High	Immense	Immense
7 - Welfare	9.1 - Loss of Power	53%	Very High	Medium	High
7 - Welfare	8.1.4 - Distributed Denial of Service	47%	Very High	High	Low
7 - Welfare	8.1.1.1.7 - Directory Service Flooding	41%	Very High	Medium	Low
7 - Welfare	8.1.1.5 - Call Hijacking	41%	High	Medium	Medium
7 - Welfare	8.1.2 - Network Services DoS	41%	Very High	Medium	Low
7 - Welfare	4.7 - Unwanted Contact	35%	Low	Very High	Low
7 - Welfare	8.1.1.1.2 - User Call Flooding Overflowing to Other Devices	35%	Medium	Medium	Medium
7 - Welfare	8.1.1.1.3/4 - Endpoint Request Flooding before/after Call Setup	35%	Medium	Medium	Medium
7 - Welfare	8.1.1.1.5 - Call Controller Flooding	35%	High	Low	Medium
7 - Welfare	8.1.1.1.6 - Request Looping	35%	High	Low	Medium
7 - Welfare	8.1.1.4 - Spoofed Messages	35%	High	Medium	Low
7 - Welfare	8.1.1.1.1 - User Call Flooding	29%	Low	Medium	Medium
7 - Welfare	8.1.3 - Underlying Operating System/Firmware DoS	29%	High	Low	Low

8 - Reputation	8.1.1.1.7 - Directory Service Flooding	65%	Very High	Medium	High
8 - Reputation	8.1.4 - Distributed Denial of Service	65%	Very High	High	Medium
8 - Reputation	9.3 - Performance Latency	65%	Low	Very High	Very High
8 - Reputation	8.1.1.1.5 - Call Controller Flooding	59%	High	Low	Very High
8 - Reputation	6.1 - Call Black Holing	53%	High	Low	High
8 - Reputation	8.1.1.1.6 - Request Looping	53%	High	Low	High
8 - Reputation	6.5 - Conversation Degrading	47%	Low	Low	Very High
8 - Reputation	8.1.1.3 - QoS Abuse	47%	Low	Medium	High
9 - Revenue	8.1.1.1.7 - Directory Service Flooding	65%	Very High	Medium	High
9 - Revenue	8.1.4 - Distributed Denial of Service	65%	Very High	High	Medium
9 - Revenue	9.1 - Loss of Power	65%	Very High	Medium	High
9 - Revenue	7.2 - Premium Rate Service Fraud	53%	Low	Medium	Very High
9 - Revenue	8.1.1.1.5 - Call Controller Flooding	53%	High	Low	High
9 - Revenue	8.1.1.1.6 - Request Looping	53%	High	Low	High
9 - Revenue	6.1 - Call Black Holing	47%	High	Low	Medium
9 - Revenue	7.3 - Improper Bypass or Adjustment to Billing	41%	Low	Low	High
10 - Databases	4.6 - Theft of service	53%	Immense	Medium	Low
10 - Databases	5.3 - Number Harvesting	47%	High	Medium	Medium
11 - Hardware	8.2 - Physical Intrusion	59%	Immense	Low	Very High

Table 15: VoIP Security risk between assets and threats

Results from the PSTN analysis

The following table shows the results from the PSTN risk analysis. The table shows security risk along with impact-, probability- and vulnerability values.

Asset Name	Threat Name	Security Risk	Impact of Threat	Probability of Threat	Vulnerability of Asset
1 - Personal Privacy	4.5 - Misrepresentation	47%	High	Low	Very High
1 - Personal Privacy	4.7 - Unwanted Contact	35%	Low	Low	Very High
2 - Financial Assets	#1 - Personnel Error	47%	Medium	Medium	Medium
2 - Financial Assets	#2 - Other human errors	53%	Medium	Medium	High
2 - Financial Assets	#3 - Acts of Nature	59%	High	Low	Very High
2 - Financial Assets	4.6 - Theft of service	53%	Medium	Low	Very High
2 - Financial Assets	4.7 - Unwanted Contact	35%	Low	Low	Medium
2 - Financial Assets	7.2 - Premium Rate Service Fraud	59%	Low	Medium	Immense
2 - Financial Assets	7.3 - Improper Bypass or Adjustment to Billing	41%	Low	Low	High
3 - Phone Minutes	#1 - Personnel Error	35%	Medium	Medium	Low
3 - Phone Minutes	#2 - Other human errors	35%	Medium	Medium	Low
3 - Phone Minutes	#3 - Acts of Nature	35%	High	Low	Low
3 - Phone Minutes	4.6 - Theft of service	53%	Medium	Low	Immense
3 - Phone Minutes	4.7 - Unwanted Contact	29%	Low	Low	Medium
3 - Phone Minutes	7.2 - Premium Rate Service Fraud	29%	Low	Medium	Low
3 - Phone Minutes	7.3 - Improper Bypass or Adjustment to Billing	24%	Low	Low	Low
4 - Critical Information	4.5 - Misrepresentation	53%	High	Low	Very High
4 - Critical Information	4.6 - Theft of service	41%	Medium	Low	High
5 - Communication Service	#1 - Personnel Error	53%	Medium	Medium	Very High
5 - Communication Service	#2 - Other human errors	53%	Medium	Medium	Very High
5 - Communication Service	#3 - Acts of Nature	53%	High	Low	Very High
5 - Communication Service	#4 - Hardware Failures	47%	Low	Medium	Very High
5 - Communication Service	#5 - Software failures	47%	Low	Medium	Very High
5 - Communication Service	#6 - Overloads	59%	Very High	Low	Very High
5 - Communication Service	#7 - Denial of Service	35%	Low	Low	High
5 - Communication Service	8.1.4 - Distributed Denial of Service	53%	Very High	Low	High
5 - Communication Service	8.2 - Physical Intrusion	65%	Immense	Low	Very High
5 - Communication Service	9.1 - Loss of Power	35%	Low	Low	High
7 - Welfare	#7 - Denial of Service	18%	Low	Low	Low
7 - Welfare	10.1 - Inability to Locate Emergency Calls	59%	Very High	Low	Immense
7 - Welfare	4.7 - Unwanted Contact	18%	Low	Low	Low
7 - Welfare	8.1.4 - Distributed Denial of Service	35%	Very High	Low	Low
7 - Welfare	9.1 - Loss of Power	29%	Low	Low	High
8 - Reputation	#1 - Personnel Error	59%	Medium	Medium	Very High

8 - Reputation	#4 - Hardware Failures	47%	Low	Medium	High
8 - Reputation	#5 - Software failures	47%	Low	Medium	High
8 - Reputation	#6 - Overloads	65%	Very High	Low	Very High
8 - Reputation	#7 - Denial of Service	35%	Low	Low	Medium
8 - Reputation	8.1.4 - Distributed Denial of Service	53%	Very High	Low	Medium
9 - Revenue	#2 - Other human errors	53%	Medium	Medium	High
9 - Revenue	#3 - Acts of Nature	53%	High	Low	High
9 - Revenue	#4 - Hardware Failures	47%	Low	Medium	High
9 - Revenue	#5 - Software failures	47%	Low	Medium	High
9 - Revenue	#6 - Overloads	59%	Very High	Low	High
9 - Revenue	#7 - Denial of Service	35%	Low	Low	Medium
9 - Revenue	7.2 - Premium Rate Service Fraud	53%	Low	Medium	Very High
9 - Revenue	7.3 - Improper Bypass or Adjustment to Billing	41%	Low	Low	High
9 - Revenue	8.1.4 - Distributed Denial of Service	53%	Very High	Low	Medium
9 - Revenue	9.1 - Loss of Power	41%	Low	Low	High
10 - Databases	4.6 - Theft of service	29%	Medium	Low	Low
11 - Hardware	#1 - Personnel Error	41%	Medium	Medium	High
11 - Hardware	#4 - Hardware Failures	47%	Low	Medium	Immense
11 - Hardware	8.2 - Physical Intrusion	59%	Immense	Low	Very High

Table 16: PSTN Security risk between assets and threats

Reasons behind values

Table 17 shows the reasons behind the values given to the impact of threat for the PSTN analysis. Table 18 depicts corresponding reasons for the probability of each threat.

Threat:	Impact of Threat	Reason
Personnel errors	Medium	The estimates are arrived from a report about PSTN based failures in USA over a two year period (From 1992-1994).
Other human errors	Medium	The estimates are arrived from a report about PSTN based failures in USA over a two year period (From 1992-1994).
Acts of Nature	High	The estimates are arrived from a report about PSTN based failures in USA over a two year period (From 1992-1994).
Hardware failures	Low	The estimates are arrived from a report about PSTN based failures in USA over a two year period (From 1992-1994).
Software failures	Low	The estimates are arrived from a report about PSTN based failures in USA over a two year period (From 1992-1994).
Overloads	Very High	The estimates are arrived from a report about PSTN based failures in USA over a two year period (From 1992-1994).
Denial of Service	Low	Attacker usually has limited phone numbers to call from. If attacks are ongoing the victim can have these numbers blocked by service providers.
Misrepresentation	High	Attacker can gain access to various information that can be harmful to the user. (PIN numbers, company information etc.)
Theft of Service	Medium	This threat has significantly lesser impact for PSTN than for VoIP. Reasons are that attackers can't steal, and resell, millions of phone minutes from a service provider.
Unwanted Contact	Low	This threat is mostly annoying to the user and denies phone activity while the user is being spammed.
Premium Rate Service Fraud	Low	If the attacker abuses this threat to much it will probably get noticed by the SP.
Improper bypass or adjustment to billing	Low	A single user can possibly get away with avoiding bills, which has minimum effect on SP's financial status.
Distributed Denial of Service	Immense	100s/1000s of computers/phones used (often without their owners knowledge) to flood a system and shut it down completely. Especially dangerous if the target is a emergency call centre.
Physical Intrusion	Immense	If an attacker gains access to restricted area he can do great deal of harm.
Loss of Power	Low	PSTN service will, in most cases, remain active during power outage.
Inability to Locate Emergency Calls	Very High	Callers' welfare may be at risk. Inability to locate emergency call can result in serious harm, or even death, of the caller.

Table 17: Reasons behind Impact of Threat values (PSTN)

Threat:	Probability of Threat	Reason
Personnel errors	Medium	The estimates are arrived from a report about PSTN based failures in USA over a two year period (From 1992-1994).
Other human errors	Medium	The estimates are arrived from a report about PSTN based failures in USA over a two year period (From 1992-1994).
Acts of Nature	Low	The estimates are arrived from a report about PSTN based failures in USA over a two year period (From 1992-1994).
Hardware failures	Medium	The estimates are arrived from a report about PSTN based failures in USA over a two year period (From 1992-1994).
Software failures	Medium	The estimates are arrived from a report about PSTN based failures in USA over a two year period (From 1992-1994).
Overloads	Low	The estimates are arrived from a report about PSTN based failures in USA over a two year period (From 1992-1994).
Denial of Service	Low	DoS attacks on more than a single user require lot of time, money and manpower.
Misrepresentation	Low	Not nearly as many means to misrepresent identity in PSTN as it is in VoIP. (In fact the attacker is resorted to lie about his identity and hope that the victim believes him).
Theft of Service	Low	Most PSTN based toll frauds are well known and have already been countered.
Unwanted Contact	Low	The attacker has to consume time and money in order to contact the victim so he has to be sure he gains something from the attack.
Premium Rate Service Fraud	Medium	It's harder to implement PRS scams in Iceland than on International scene. (Due to smaller customer base and fewer international clients)
Improper bypass or adjustment to billing	Low	SPs should keep good records on telephone records and accounting information.
Distributed Denial of Service	Low	The attacker has to possess 100s/1000s of phones in order to implement this attack. (Unlike VoIP he can't use other peoples phones)
Physical Intrusion	Low	SP's usually have a good security system in place. Entrance to important rooms (server rooms etc.) usually requires access key and these rooms are often guarded at all hours.
Loss of Power	Low	Power outages are rare. SP's should have some backup power but single users are likely to lose all service.
Inability to Locate Emergency Calls	Low	PSTN calls can be located in most cases.

Table 18: Reasons behind Probability of Threat values (PSTN)