Security in VoIP Systems

MASTER'S THESIS
IMM-THESIS-2005-63
Kgs. Lyngby, August 2005

Amit Luthra
(s001702)

Waqas Ashraf
(s001388)

Technical University of Denmark
Informatics and Mathematical Modelling
Building 321, DK-2800 Lyngby, Denmark
Phone +45 45253351, Fax +45 45882673
reception@imm.dtu.dk
www.imm.dtu.dk

Front page images obtained from `www.toneystone.com`.

IMM-THESIS-2005-63

Abstract

The purpose of this thesis has been to analyze the security in VoIP systems as more companies migrate to converged networks consisting of both voice and data.

The security risks and Quality-of-Service issues related to VoIP systems that arise when implementing VoIP have been analyzed in depth. This includes detailed descriptions of attack methods and possible mitigation actions to reduce the risks of the attacks. The mitigation actions provide the motivation and goal of the project - to provide security best practices and general recommendations for securing a VoIP system. Additionally, existing VoIP solutions, offered by vendors today, are examined from a security and functional point of view. The thesis also gives an introduction of a new concept by Voiceline for VoIP systems intended for use in closed networks. To give the thesis a more practical perspective, Elsam A/S, a company considering migrating to a VoIP system, have listed their requirements for such a system. The thesis ends by evaluating whether these requirements can be met by implementing a VoIP system.

Keywords: VoIP, security, risks, QoS, MPLS, SIP, H.323

Preface

VoIP is a becoming a very popular technology. Already millions of people have downloaded and daily use the Internet telephony program Skype. Many papers have also been written and published about the advantages as well as disadvantages of using the Internet for telephony. The papers discuss every aspect of the world of telecommunications including protocols, transport, media and security. However, finding an analytical presentation of the topic with a focus on security as well as including a customer case with specific customer requirements is a difficult challenge. This perspective is exactly where this thesis has its starting point.

This Master Thesis Project has been accomplished in order to obtain the Master of Science degree in Informatics. The project has taken place at the department of Informatics and Mathematical Modelling – Computer Science and Engineering at the Technical University of Denmark with the supervision of Reader Dr. Robin Sharp. The project has been made during the period March 14th to August 29th 2005, and corresponds to 30 ECTS-points.

The project involves a range of interdisciplinary courses which were followed during the Master studies especially Data Security, Network Security, Broadband Networks and Cryptology.

The project is based on a real VoIP security case with Elsam A/S as the cooperating involved party.

This is an edited version of the thesis, released for public use. The version presented here retains the page numbering from the original, but Chapters 10 and 11, and Appendices D, E and F, all of which contained confidential information, have been removed.

Acknowledgements

We would like to take this opportunity to give a special thanks to our supervisor Reader Dr. Robin Sharp for providing many useful inputs during our weekly meetings and helping us taking an idea and see it become a final project.

Additional thanks go to Voiceline for setting up the meetings with the different vendors. Many other companies have contributed with great efforts including Elsam A/S and DK-CERT.

Finally, we would like to thank our families for always supporting and encouraging us with our studies.

Amit Luthra (s001702) and

Waqas Ashraf (s001388)

August 2005

Reading Instructions

This thesis encompasses the results of research completed on VoIP security issues. It provides useful information for students with a special interest in VoIP and security as well as network managers, IT administrators, telephony managers and security managers, all with some basic knowledge of IP networks and who might be considering a VoIP solution for their company. This thesis will help illuminate some of the security struggles, threats and difficulties in a VoIP system that can be very cumbersome to overcome. Other readers with interest in VoIP, security, QoS, MPLS, SIP, H.323 and IP networks in general may benefit from reading this thesis too.

The thesis is divided in chapters with associated sections. Overall the thesis contains two main parts: The first part, that includes chapters 2-9, takes a general approach to VoIP systems with a focus on security. The second part, that includes chapters 10-13, relates to an actual case concerning Elsam A/S along with concluding remarks.

Chapter 1 gives an introduction to the project including the formal project description, scope of the project and a description of the project approach and work process.
Chapter 2 describes VoIP related Quality-of-Service issues. The chapter explains why the voice transportation is dependent of certain QoS parameters.
Chapter 3 examines the difference between the two technologies used for transporting voice, namely circuit switching and packet switching. The chapter explains why the tendency for voice transportation is going towards packet switching and particularly over IP networks.
Chapter 4 specifies the fundamental components that are used in a VoIP system. The chapter is meant to give a basic understanding of the VoIP specific components.
Chapter 5 gives explanations of the security aspects and requirements, the so-called CIA-requirements in relation to VoIP.
Chapter 6 provides a technical description of the processes that take place for voice transmission. The signaling protocols are described as well as encoding/decoding and voice transmission mechanisms.
Chapter 7 describes some of the security risks and problems that VoIP systems are exposed to. Moreover, it is described how these vulnerabilities are exploited in actual attacks. The chapter is also meant as motivation for taking the security problems in connection with VoIP systems seriously.
Chapter 8 presents widely used technologies that can be used to guarantee QoS and security in VoIP systems. These technologies will later be used to prepare a security best practices and recommendation chapter that complies with Elsam's requirements.
Chapter 9 examines existing VoIP solutions that vendors offer for companies wanting to implement a VoIP system. An analysis is made for each VoIP solution to see the security and

functionality extent of the respective solutions.
Chapter 10 specifies the requirements provided by Elsam A/S for a VoIP solution. These include technical, functional, security, economical and user requirements.
Chapter 11 provides best practices when implementing VoIP and possible mitigation actions for reducing VoIP risks. Additionally, Elsam's requirements are evaluated.
Chapter 12 describes the project prospects and further development on how to continue the project both for Elsam A/S and Voiceline.
Chapter 13 points out the main results made in the thesis and provides concluding remarks.

In the thesis, superscript numbers (^{x}) indicate references shown at the bottom of the current page whereas text in squared brackets [xxxyy] are references to the bibliography.
Many technical terms and abbreviations are used throughout the report. Descriptions of technical terms can be found in the Glossary, provided as Appendix. Furthermore the Appendix includes material from Elsam A/S including their requirement specification and IT security policy. Voiceline's concept description is also included. Notice that the material from Elsam A/S and Voiceline is in its original form (Danish language).

Diagram Legend

All figures in this thesis are made in Microsoft Office Visio Professional 2003, if not mentioned otherwise. A few figures are either inspired from or found on the Internet and are provided with the necessary references.

Figure 1 shows the diagram legend for the Visio figures that are included in this thesis.

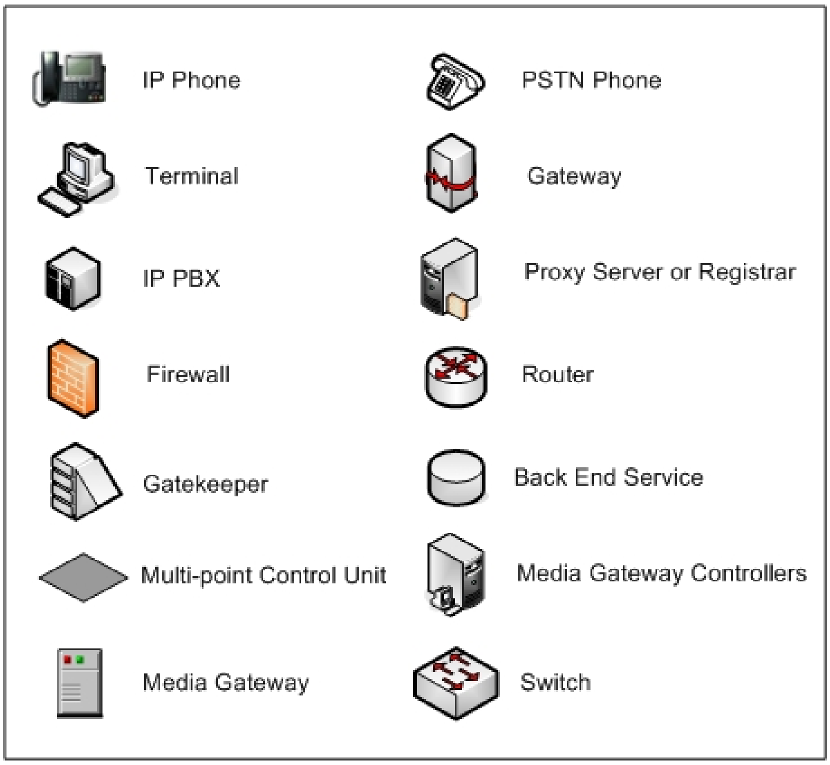


Figure 1: Diagram Legend.

List of Abbreviations

3DES	Triple DES
ADSL	Asynchronous Digital Subscriber Line
AES	Advanced Encryption System
AH	Authentication Header
ALG	Application Level Gateway
ARP	Address Resolution Protocol
ASN.1	Abstract Syntax Notation One
ATM	Asynchronous Transfer Mode
BES	Back End Service
BGB	Border Gateway Protocol
CC	Common Criteria
CIA	Confidentiality, Integrity and Availability
CPU	Central Processing Unit
CR-LDP	Constraint-Based LDP
CTL	Certificate Trust List
DDoS	Distributed Denial-of-Service
DES	Data Encryption Standard
DK-CERT	The Danish Computer Emergency Response Team
DMZ	Demilitarized Zone
DNS	Domain Naming System
DoS	Denial-of-Service
EAP	Extensible Authentication Protocol
ENUM	Electronic Numbering
ESP	Encapsulating Security Payload
FEC	Forward Equivalence Class
FDM	Frequency Division Multiplexing
GRE	General Routing Encapsulation
GSM	Global System for Mobile communication

HMAC	Hashed MAC
HTTP	Hyper Text Transfer Protocol
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPSec	Internet Protocol Security
ISDN	Integrated Services Digital Network
ISO	International Standard Organization
ITU-T	International Telecommunication Union-Telecommunication
L2F	Layer 2 Forwarding
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LDP	Label Distribution Protocol
LSR	Label-Switched Router
MAC	Medium Access Control
MC	Multi-point Controller
MCU	Multi-point Control Unit
MD5	Message-Digest algorithm 5
MEGACO	Media Gateway Control
MG	Media Gateway
MGC	Media Gateway Controller
MGCP	Media Gateway Control Protocol
MIDCOM	Middlebox Communication
MIME	Multipurpose Internet Mail Extension
MPLS	Multi Protocol Label Switching
MPPE	Microsoft Point-to-Point Encryption
MOS	Mean Opinion Score
MS-CHAP	Microsoft Challenge Handshake Authentication Protocol
NAT	Network Address Translation
NAPT	Network Address Port Translation
NIST	National Institute of Standards and Technology
OSI	Open Systems Interconnection
PAP	Password Authentication Protocol
PBX	Private Exchange Branch
PCM	Pulse Code Modulation
PKI	Public Key Infrastructure
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
PSTN	Public Switched Telephone Network

QoS	Quality-of-Service
RADIUS	Remote Authentication Dial In User Service
RAS	Registration, Admission and Status
RC4	Rivest Cipher 4
RSA	Rivest, Shamir and Adleman
RSVP	ReSerVation Protocol
RTCP	RTP Control Protocol
RTP	Real-Time Transport Protocol
S/MIME	Secure MIME
SANS	SysAdmin, Audit, Network, Security
SCCP	Skinny Client Control Protocol
SDP	Session Description Protocol
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SPIT	Spam over Internet Telephony
SRTP	Secure RTP
SS7	Signaling System 7
SSH	Secure SHell
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TE	Traffic Engineering
TFTP	Trivial File Transport Protocol
TLS	Transport Layer Security
UA	User Agent
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
VAD	Voice Activity Detection
VoIP	Voice over Internet Protocol
VoIPoMPLS	Voice over IP over MPLS
VOIPSA	Voice over Internet Protocol Security Alliance
VOMIT	Voice over Misconfigured Internet Telephony
VPN	Virtual Private Network
WAN	Wide Area Network
WLAN	Wireless LAN

Contents

Abstract **iii**

Preface **v**

Acknowledgements **vii**

Reading Instructions **ix**

Diagram Legend **xi**

List of Abbreviations **xiii**

1 Introduction **1**
1.1 Project Description 2
1.2 Scope of the Project 3
1.3 Project Approach 3

2 VoIP Quality of Service Issues **7**
2.1 VoIP Quality 7
2.2 Packet Delay 8
2.3 Jitter 8
2.4 Packet Loss 9
2.5 Summary 9

3 Voice Using Packet Switching **11**
3.1 Circuit Switching versus Packet Switching 11
3.2 Advantages with Voice over Packet-Switched Networks 11
3.3 Underlying Protocols for Voice Services 12
3.3.1 The Reason for Using VoIP 12
3.3.2 Multi Protocol Label Switching 13
3.4 Summary 14

4 Fundamental Components in VoIP Systems **15**
4.1 Terminal 15
4.2 Server 15
4.3 IP Private Branch Exchange 16
4.4 Switch 16
4.5 Router 17

4.6 Gateway 17
4.7 Multi–point Control Unit 17
4.8 Addressing 17
4.9 Firewall 18
4.10 A VoIP System 18
4.11 Summary 18

5 Security Aspects 21
5.1 Confidentiality 21
5.2 Integrity 23
5.3 Availability 23
5.3.1 Quality-of-Service (QoS) 23
5.3.2 Dependability 24
5.3.3 Compatibility 24
5.4 Summary 24

6 VoIP Protocols 25
6.1 Signaling and Gateway Control Protocols 25
6.1.1 H.323 26
6.1.2 Session Initiation Protocol 29
6.1.3 H.323 versus SIP 31
6.1.4 Gateway Control Protocols 31
6.2 Encoding and Decoding 33
6.2.1 Voice Codecs 34
6.3 Voice Transport 35
6.3.1 TCP versus UDP 35
6.3.2 Real-Time Data Transport 35
6.3.3 Secure RTP 36
6.4 Summary 37

7 Risk Analysis 39
7.1 Risk Identification 39
7.1.1 SIP Vulnerabilities 40
7.1.2 H.323 Vulnerabilities 43
7.1.3 Network and Media Vulnerabilities 44
7.1.4 IP Phones and Soft Phones Vulnerabilities 44
7.1.5 IP PBX Vulnerabilities 45
7.1.6 Remote Access 46
7.1.7 Denial of Service Attacks 46
7.1.8 Spam over Internet Telephony 47
7.1.9 Wireless VoIP 48
7.1.10 Scanning Tools 49
7.2 Risk Assessment 50
7.3 Summary 51

8 Technologies 53
8.1 Virtual LAN . . . 53
8.2 Virtual Private Network . . . 55
8.2.1 Point-to-Point Tunneling Protocol . . . 56
8.2.2 Layer 2 Tunneling Protocol . . . 57
8.2.3 IP Security . . . 58
8.3 Multi Protocol Label Switching . . . 59
8.3.1 Forwarding and Routing . . . 60
8.3.2 Label Distribution . . . 60
8.3.3 Multiple MPLS Domains and Label-Stack Operations . . . 62
8.3.4 Traffic Engineering . . . 62
8.4 Firewalls . . . 63
8.4.1 Network Address Translation . . . 64
8.4.2 Firewall and NAT Issues . . . 65
8.4.3 Solutions to Firewall and NAT Issues . . . 67
8.4.4 Intrusion Detection System . . . 68
8.5 User Authentication . . . 69
8.5.1 Static Passwords . . . 70
8.5.2 One-Time Passwords . . . 70
8.5.3 Biometric Authentication . . . 71
8.5.4 Future VoIP Authentication Proposals . . . 71
8.6 Summary . . . 71

9 Existing VoIP Solutions for Enterprises 73
9.1 Alcatel - OmniPCX Enterprise . . . 73
9.1.1 Security Features . . . 73
9.2 Nortel Networks - Succession Communication Server for Enterprise 1000 . . . 74
9.2.1 Security Features . . . 75
9.3 Cisco Systems - Cisco CallManager . . . 75
9.3.1 Security Features . . . 75
9.4 Avaya - Integrated Stackable Telephony Solution . . . 76
9.4.1 Security Features . . . 77
9.5 Comparison of Existing VoIP Package Solutions . . . 77
9.6 Voiceline - IP Matrix . . . 80
9.7 Summary . . . 81

10 Elsam A/S: Requirement Specification 83
10.1 Background of IT and Telecommunication at Elsam A/S . . . 83
10.2 Technical and Functional Requirements . . . 84
10.3 Security Requirements . . . 85
10.4 Economical Requirements . . . 85
10.5 User Requirements . . . 85
10.6 Summary . . . 86

11 Recommendations **87**
11.1 VoIP Security Best Practices . . . 87
11.1.1 VoIP Network Architecture . . . 88
11.1.2 VoIP Phones . . . 90
11.1.3 Security Management . . . 90
11.2 Mitigation Actions . . . 92
11.3 Evaluation of the Elsam A/S Requirements . . . 93
11.4 Summary . . . 96

12 Prospects and Development **97**

13 Conclusion **99**

A Threat Sources **101**
A.1 Hackers and Crackers . . . 101
A.2 Phreakers . . . 102
A.3 Script Kiddies . . . 102
A.4 Terrorists . . . 102
A.5 Industrial Espionage . . . 103
A.6 Insiders . . . 103
A.7 Natural Disasters . . . 103
A.8 Attack Tendency . . . 103

B Risk Assessment **105**

C Voiceline's Concept **111**

D Elsam A/S: Overview of the MPLS-based IP-backbone **127**

E Elsam A/S: Requirement Specification **129**

F Elsam A/S: IT Security Policy **135**

G Contact Persons **209**

H Project Plan **211**

Glossary **213**

Bibliography **228**

List of Figures

1 Diagram Legend. xi

1.1 Approach. 5

2.1 Security versus QoS. 9

3.1 Layers in the IP stack. 13

4.1 Two terminals establishing a connection through an IP PBX. 16
4.2 A set-up of the components in a simple VoIP system. 19

5.1 Security aspects. 22
5.2 Confidentiality, integrity and availability. 22
5.3 Relationship between the security aspects. 24

6.1 The H.323 protocol stack. 26
6.2 The H.323 architecture and direct signaling procedure. 28
6.3 The SIP architecture and signaling procedure. 30
6.4 The MGCP architecture. 33
6.5 RTP can be viewed as a sublayer of the transport layer. 36
6.6 Data and overhead using RTP. 36

7.1 Illustrating a registration hijacking that is used to pull off a Man-In-the-Middle attack. 41
7.2 Exchanged messages between the registrar server and the attacker. 42
7.3 Illustration of proxy impersonation. 43
7.4 Screen dump of a Nessus report. 49

8.1 VLAN infrastructure. 54
8.2 Client-to-LAN VPN. 56
8.3 PPTP packet structure. 57
8.4 L2PT packet structure. 58
8.5 IPSec packet structure for transport mode. 59
8.6 IPSec packet structure for tunnel mode. 59
8.7 The routing and forwarding procedure. 60
8.8 Upstream and downstream LSRs - Label bindings are distributed upstream through label mapping messages. 61
8.9 An illustration of two MPLS domains nested inside each other. In this way tunnels can be created through the network as illustrated by the dotted line. 62

8.10 The NAPT traversal. 64
8.11 A DMZ configuration using two firewalls. 67
8.12 RSA SecurID 700 from RSA Security. 71

9.1 OmniPCX Enterprise. 74
9.2 Succession CSE 1000. 75
9.3 Cisco CallManager can run on an Integrated Communication System 7750. . 76
9.4 Avaya ISTS IP PBX which can be made by a Media Gateway G650 and a Media Server S8700. 77
9.5 Nested customer MPLS domains in the Voiceline MPLS network. 80
9.6 Overview of the customer network for Voiceline. 81

A.1 Attack difficulty versus attacker knowledge. 104

List of Tables

2.1 MOS ratings ranging from score 1.0 - 5.0 8

6.1 Comparison of H.323 and SIP. 32
6.2 Table overview of codecs with bit-rate and expected MOS. 34

7.1 Risk assessment. 50

9.1 Comparison of different IP PBXs. 77

11.1 Mitigation actions for VoIP specific Attacks. 92
11.2 Proposals and comments to Elsams requirements. 94

Chapter 1

Introduction

Voice over Internet Protocol (VoIP) or simply IP telephony is the new hot technology for transmitting speech across data networks like Local Area Networks (LANs). Over the years closed networks, such as LANs, have experienced an almost constant increase of clients and network traffic which sets higher requirements of the existing network infrastructure. New applications and services such as VoIP have emerged. The main three reasons for why VoIP has gained popularity can be listed as following:

- Telecommunications is a business with high revenues and a large customer segment.
- There are fiscal savings related to VoIP such as savings for long distance calls.
- The data network with its flexibility, constant development and openness will generate many new services.

According to IDC[1], 10-15 percent of the Danish companies have already replaced the old telephone system with a VoIP system [ALL05]. Examples of such companies include Novo Nordisk A/S [NNI05] and Danmarks Radio [NET04] who are implementing a VoIP solution hoping the solution will give fiscal savings, more flexibility and easier IT management. Many more companies are considering the same initiative but find themselves in the dilemma of either keeping their existing and well-functional traditional telephone system or implementing a new VoIP solution. This dilemma is in most of the cases well-founded. Although VoIP might be a cheaper and a somewhat clearer alternative to the traditional Public Switched Telephone Network (PSTN) it leads to a plethora of security issues and complications. Since VoIP travels in packets just like other data it has the same threats and attacks that plague data networks. Security incidents and report of incidents occur more often than ever before and the number is still increasing.[2] Therefore security is an essential topic for VoIP systems. To complicate matters even more VoIP is a real-time application so other aspects such as Quality-of-Service (QoS) must also be considered.

Today many organizations in the telecommunications industry are taking the initiative not only to look at the security threats inherent in VoIP but also discuss, exchange experiences

[1] IDC is a subsidiary of the International Data Group (IDG). For more information see `www.idc.com`

[2] Statement from Preben Andersen (UNI-C), see Appendix G.

and come up with new ideas and proposals to prevent exploitation of the security holes in VoIP systems. Examples of these organizations are:

- VoIP Security Alliance (VOIPSA)[3]
- Voice over Packet (VoP) Security Forum[4]
- Defence Information Systems Agency[5]
- Internet Engineering Task Force (IETF)[6]

The authors of this thesis share the same goal as the above mentioned organizations; to enhance the security of VoIP systems.

1.1 Project Description

A new survey [BID05] shows that many companies have a concern about security in VoIP systems where eavesdropping on conversations, interference with audio streams, disconnecting, re-routing or even answering other people's phone calls are the horror scenarios. The security concerns regarding VoIP can be so overwhelming that some enterprise companies discard a VoIP solution despite the possible cost benefits. On the other hand, other companies rush to a hasty VoIP implementation without having completed the necessary security precautions. In this context it is important to emphasize the fact that it isn't necessary to take a strict decision of either having a VoIP solution or a traditional telephony solution. Instead, the decision should be based on choosing the best of the two worlds.

The main purpose of this thesis is to analyze the security of VoIP systems in closed networks. A closed network is meant as the company's corporate network. Scenarios are derived from Elsam A/S, one of the leading power companies in the Danish power industry, who have a need for secure data and voice transmission.
The formal project description is given as follows:

> *"A commercial VoIP system based on MPLS technology and intended for use in closed networks is to be analyzed from the point of view of security. The security requirements are primarily to be derived from scenarios of use within a large company with a need for secure data and voice transmission. If possible, the analysis should illuminate not only the extent to which the large company's specific requirements can be met, but also discuss general aspects of security in VoIP systems of this type."*

[3] VOIPSA's mission is to promote the current state of VoIP security research, VoIP security education and awareness, and free VoIP testing methodologies and tools. VOIPSA is an interesting initiative involving highly recognized research organizations such as the National Institute of Standards and Technology (NIST) and The SysAdmin, Audit, Network, Security Institute (SANS). More information can be found at `www.voipsa.com`.

[4] The VoP Security Forum was formed in 2004 and aims to develop capabilities (e.g. tools, publications, lab facilities) and provide an information exchange forum to address issues related to network convergence (e.g. SS7, VoIP, Voice over Wireless LAN) and security. Further information provided at `www.vopsecurity.org`.

[5] See `www.disa.mil` for more information.

[6] More information can be found at `www.ietf.org`.

Elsam A/S had MPLS implemented in their IP-Backbone network in May 2001 to expand the data communication including voice transmission. MPLS introduces traffic engineering which can make use of the bandwidth more efficiently and thereby increase the value of the network. The introduction of traffic engineering also means that different levels of QoS can be offered.

It is meaningful to analyze a VoIP system seen from a security perspective with real case scenarios. Will a VoIP system comply with Elsam's requirements concerning functionality, infrastructure and most interestingly security? What are the general vulnerabilities today of a VoIP system? Which security countermeasures can be taken to avoid these vulnerabilities? These are only a few of the questions that we will try to give answers to in the thesis.

1.2 Scope of the Project

This thesis is a theoretical study. No testing, actual design or implementation has been carried out. In recognition of VoIP security being a broad topic with many different aspects, the starting point has been to limit the scope of the topic to give a useful report that at the same time is comprehensive and keeps its focus. The focus has been kept on VoIP security for closed networks since open networks introduce many more complexed aspects. Security in the traditional telephone network (PSTN) has only been covered shortly. Even though VoIP systems include voice over wireless, this too, has only been treated to some limited extent. Wireless security for voice media brings many new vulnerabilities to cope with, that fall out of the scope in this project.

When looking at existing VoIP solutions from vendors we have limited ourselves to analyze solutions only from Cisco Systems, Avaya, Nortel Networks and Alcatel. In this way we have reached a number of the leading VoIP providers who offer solutions with varying levels of security.

Lastly, by malicious attacks, we mean attemps launched by a person or people with a motivation for disrupting the voice services. Since VoIP is an application running over the data network, we note, that it may be a victim of any successful attack against a company's data network infrastructure.

1.3 Project Approach

The first phase of the project included studying literature of the VoIP topic obtained from different databases containing technical articles and documentations. The Technical Knowledge Center of Denmark was a frequently used data source. Additionally different security forums and news articles contributed in gaining more knowledge as new topics within VoIP were covered. The literature study was combined with empiric research such as attending The Annual Axcess Conference at Hotel Scandic in Lyngby and having meetings with subject matter experts in the VoIP community. The complete project plan can be found in Appendix H.

The different parties involved in the project includes, besides the department of Informatics and Mathematical Modelling at the Technical University of Denmark, Voiceline which is an entrepreneur company with focus on innovation within VoIP security, NetConcept and Flextronics who are vendors of Avaya and Alcatel equipment respectively, Nortel Networks and finally DK-CERT who have contributed with information regarding attacks on data networks. Contact information of the representatives can be found in Appendix G. Some of the information provided by the vendors may not be reliable due to their commercial interests. In some cases it was time consuming reaching the right people who had the sufficient technical knowledge.

Voiceline played a particular role throughout the project. Voiceline procured contact with Elsam A/S, as well as contributing vendor contacts. It was because of Voiceline this thesis was initialized, first with the intention of designing a secure VoIP solution after physical line-up testing. However, this was not possible due to the time limit given for this project. Instead only a theoretical study was performed.

Elsam's requirement specification was conducted after a meeting with the IT Manager among others held at Elsam's head office in Fredericia. The communication with Elsam has been positive and rewarding in many aspects.

Figure 1.1 gives a visualization of the approach method.

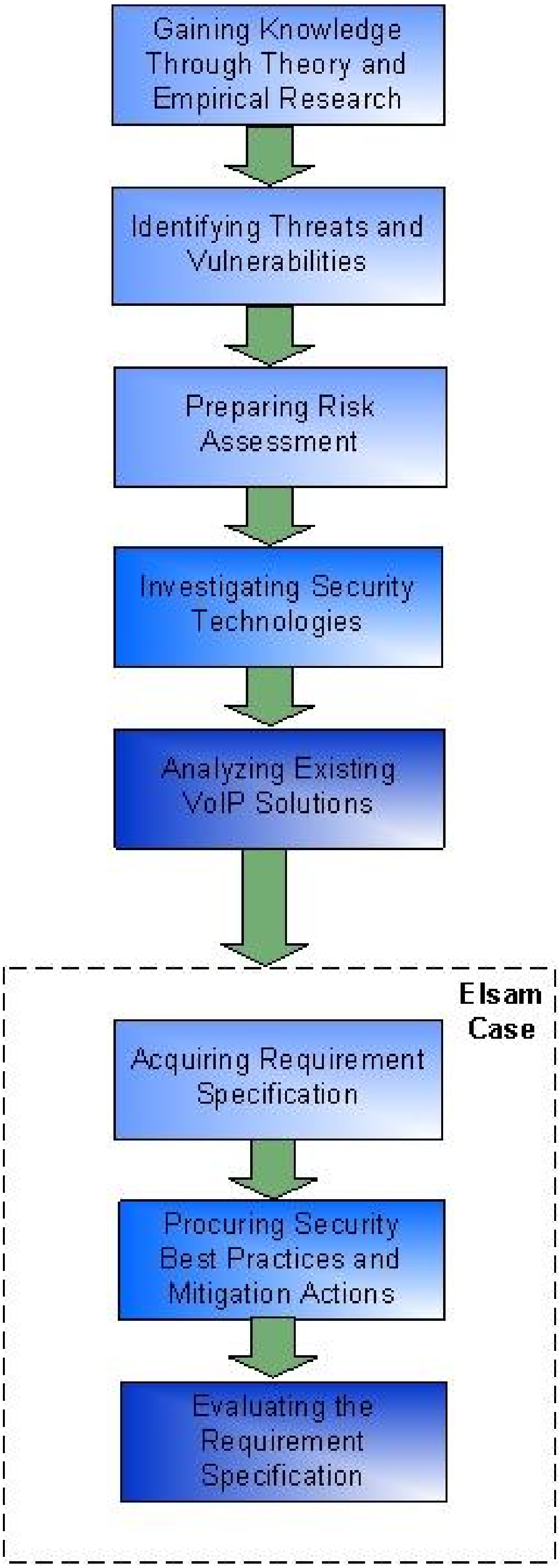

Gaining Knowledge Through Theory and Empirical Research
Identifying Threats and Vulnerabilities
Preparing Risk Assessment
Investigating Security Technologies
Analyzing Existing VoIP Solutions
Elsam Case
Acquiring Requirement Specification
Procuring Security Best Practices and Mitigation Actions
Evaluating the Requirement Specification

Figure 1.1: Approach.

Chapter 2

VoIP Quality of Service Issues

Quality–of–Service (QoS) is an important aspect when implementing VoIP systems. Having high security, such as encryption and filtering, can have a negative influence of the QoS. This chapter describes the necessity of QoS and illuminates different QoS issues associated with VoIP. QoS can be defined as a measure of performance for a transmission system, involving specification of packet delay, jitter, packet loss and availability. It also includes the practice of allocating and prioritizing specific necessary network resources in the form of guaranteed bandwidth.

2.1 VoIP Quality

A VoIP system should provide at least the same quality of the call setup and voice as in the traditional PSTN network. When measuring the quality of voice the Mean Opinion Score (MOS) is applied. MOS is a measurement of the subjective quality of human speech, represented as a rating index ranging from 5.0 as the highest quality and uncompressed speech to 1.0 indicating the lowest rating.[1] MOS is derived by taking the average of numerical scores given by juries to rate quality and using it as a quantitative indicator of system performance. Of course, the perception varies from individual to individual, but usually a large sample of individuals carry out the experiment to obtain a reasonable cross-section of results [STE96]. Table 2.1 gives an overview of the MOS ratings where a MOS value of 4.0 is considered "toll-quality", meaning good quality. The key factor for voice quality in an IP-based network is the broadcasting quality of the underlying IP-infrastructure in relation to certain clearly defined criteria. This is especially significant, when telephony is integrated into the data network, that is, when voice and data traffic with their different demands and characteristics are to be transported over the same IP-network. Furthermore, implementation of security measures can degrade QoS, minimizing the level of performance. This can lead to blocking of call setups by firewalls to encryption-produced latency implying that measures to improve security in traditional data networks are not applicable to VoIP in their current form.

The demands upon voice and data traffic transmission are fundamentally different. While the bandwidth of voice traffic is rather constant, the packets must be transported with the

[1] For more information see `www.voip-info.org`.

Table 2.1: MOS ratings ranging from score 1.0 - 5.0

Rating	Definition	Description
5.0	Excellent	A perfect speech signal.
4.0	Good	Intelligent and natural, like telephone quality (PSTN).
3.0	Fair	Communication quality, but requires some hearing effort.
2.0	Poor	Low quality and hard to understand the speech.
1.0	bad	Unclear speech, breakdown.

least delay possible and with extreme regularity. In contrast data applications like e-mail are carried by unsteady bandwidth demands and are unaffected by normal network delays. To ensure that this unsteadiness has no negative influence on the voice quality, some fundamental rules are wise to follow, when designing such a network. The quality of transporting real-time applications in IP networks is basically defined by packet delay (latency), jitter (delay variations) and packet loss. Therefore, the efforts when designing IP-networks should be concentrated on the improving these three parameters.

2.2 Packet Delay

Packet delay or latency is the overall time for a voice transmission to go from its source to its destination. The greater the latency the more time it will take for the voice transmission to reach its destination. Therefore it would be ideal to have latency as low as possible but every junction in the network, that being a router, a switch or a security checkpoint is a bottleneck and gives rise to more delay. Today, the PSTN network has a one-way upper latency boundary of 150 milli seconds (ms) which was deemed tolerable for domestic calls and 400 ms for international calls [KWF05]. VoIP calls must achieve at least the same boundary leaving very little margin for error in packet delivery. Also VoIP tends to work best with small packets on a logical network keeping latency at a minimum and avoiding bandwidth congestion.

2.3 Jitter

Jitter is variation or a non-uniform packet delay and can cause disorder in processing and arrival of packets. Jitter also causes packets to arrive in clumps analogous to road traffic arriving at a red stop light. When the traffic light turns green (bandwidth opens up) the traffic races through in clumps. One way of avoiding jitter is by traffic engineering. It is the process of dynamically controlling traffic flows, optimizing the availability of resources by moving traffic flows towards less congested paths by choosing routes taking traffic loads and the network state into account.

2.4 Packet Loss

VoIP is not tolerant to packet loss. Lost packets in a VoIP network will appear as noise or gap in the conversation and may require the speaker to repeat the last word or sentence, which is clearly undesirable. Further investigation on packet loss shows that losses of more than 3 percent of the voice packets will give an intolerable quality resulting in dissatisfied users [CHU00]. Since VoIP packets are very small in size a few lost packets will not affect the voice quality noticeably. However, if one packet is lost, the probability that another packet will be lost too is high since packets are usually not lost singly but in parts. When comparing VoIP to e-mail services it is noticeable that it can have great affect if a single bit is lost in the e-mail resulting in a word or number changing meaning considerably. If a few packets are lost in the voice conversation the human brain percepts the missing packets (words).

2.5 Summary

This chapter has focused on QoS issues in VoIP systems. QoS has been clearly defined and the three QoS parameters, packet delay, jitter and packet loss, have been discussed too. Note that not all possible QoS issues have been discussed in the chapter but only the most important parameters that are influenced by security measures. Increasing security in VoIP systems does have a negative affect on QoS. The aim, when implementing a VoIP system, should be to take the best of the two worlds, which is illustrated in Figure 2.1.

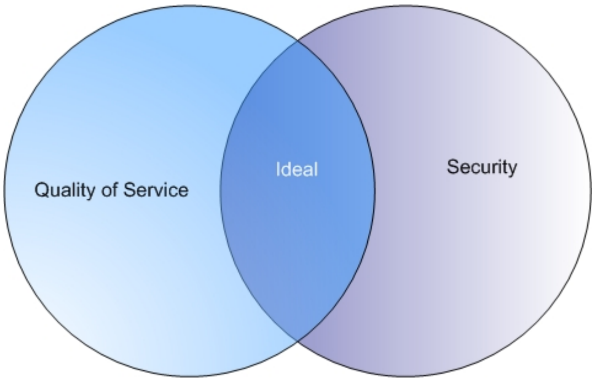


Figure 2.1: Security versus QoS.

Chapter 3

Voice Using Packet Switching

This chapter states the differences between circuit switching and packet switching with the latter having advantages to transmit voice. Additionally, it gives an overview of the supporting protocols for transmitting voice, and discusses various packet switching technologies that can be used to transmit real-time voice.

3.1 Circuit Switching versus Packet Switching

Circuit switching and packet switching are two fundamental approaches for implementing a network. In a circuit-switched network a dedicated connection is created to provide the communication between the end systems, and the data is sent in one continuous stream. A circuit link is implemented with either frequency-division multiplexing (FDM) or time-division multiplexing (TDM). In contrast, the packet-switched network only occupies resources in the form of buffers and bandwidth when needed; data is divided into packets that are transmitted individually and can follow different routes to reach their destination. Once all the packets carrying the data arrive at the destination, they are reassembled to the original data.

Circuit-switched networks are ideal when data must be transmitted quickly and arrive in the same order in which they where sent, which is the case for most real-time data, such as voice and video. Traditional telephone networks are based on circuit-switching, where connections have to be established before data can be transmitted; in modern telephone networks the circuit is implemented by TDM, earlier FDM was used. Packet-switched networks on the other hand are efficient for data that is not sensitive for short delays in transmission, such as e-mail messages and web pages [KUR01].

3.2 Advantages with Voice over Packet-Switched Networks

This section illuminates why more and more companies choose packet-switched networks to carry voice traffic instead of the traditional circuit-switched TDM network. This is because of the fiscal savings that lies from exploiting the existing data network and the increase of voice volume that can be transmitted over available bandwidth. These benefits are not available with circuit-switched TDM networks. Beside the economical benefits, the driving force for the companies to implement a VoIP solution is to have a converged network with IP and voice services [DUR03].

Other benefits include voice compression, silence suppression and statistical gains. The voice conversations in packet-switched networks can be compressed to create additional bandwidth as needed. While removing any silence in the conversation, the packet-switched networks can currently compress up to 1/12 [DUR03] of the required bandwidth used in TDM networks. Since high compression can degrade the quality of the call, considerations of the level of compression have to be made to achieve the desired level of QoS.

Furthermore, packet-switched networks only transmit packets when necessary, also called statistical gains. This is achieved by using a technique called Voice Activity Detection (VAD) which minimizes the use of bandwidth during the silence in a voice conversation. A packet-switched network can for this reason handle a higher number of calls than the circuit-switched TDM network by using the same transmission infrastructure; TDM networks dedicate a specific amount of bandwidth for each conversation during the entire call, including any silence. However, the downside by using VAD is that it contributes to jitter which effects the QoS.

3.3 Underlying Protocols for Voice Services

As with many communication services, the protocols involved in transmitting voice over packet-switched networks use a layered hierarchy which can be compared to the International Standard Organization's (ISO's) Open System Interconnect (OSI) model, also called the OSI seven layer model [RAN05]. Breaking the system into layers can make the system more manageable and flexible. Each layer is considered as a function that takes the input from the overlying layer's output, performs a task and then sends its output to the underlying layer. This means that each layer is independent from the overlying or underlying layer's functionality.

Packet-switched networks use a well-known model called the Internet Protocol Stack. It consists of five layers; physical, data link, network, transport and application layer. Figure 3.1 illustrates the arrangement of these layers including important protocols that run on each layer. As illustrated on the figure, the voice service can run on several underlying protocols. The protocols (TCP, UDP, ATM etc.) in the figure are described more thoroughly in Chapter 6. The question to be answered next is which protocol is the best on each layer and which combination that is actually used to realize voice services.

3.3.1 The Reason for Using VoIP

There has never been the challenge from other network protocols that could threaten the position of IP as the dominant bearer service. In fact, IP has already entered the telecommunications industry for voice services [WRI02]. The purpose of IP is to enable communication between users connected to the network by providing a connectionless service from the network layer to the transport layer. This service can be said to be "a-best-effort-service" meaning that IP tries its best effort to forward packets to the intended destination but that

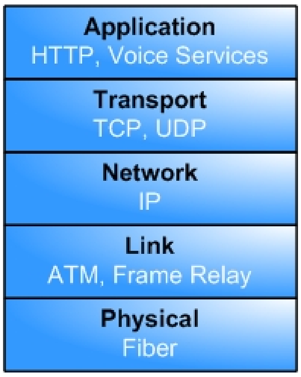


Figure 3.1: Layers in the IP stack.

no guarantees can be made. In other words, IP in itself does not support QoS which is vital for voice services. Instead it relies on underlying protocols, such as Asynchronous Transfer Mode (ATM) to guarantee QoS. Since the IP service is connectionless the transport layer can transmit data without a connection being set up between the end systems, thus decreasing delay in the setup. IP transfers voice packets across the network. The details of the voice packet is discussed in Chapter 6. The use of IP for transporting voice, according to today's principles, causes a lot of overhead as many protocol layers are involved (RTP, UDP and IP) as will be explained in Chapter 6. Therefore, one could be tempted to think that the use of IP for transporting voice is inefficient. This is true in some ways, since large overheads can give rise to increased delays. But so far, the use of IP has proven to be consistent and functional at a satisfactory level [FJE02]. The underlying protocols of the network layer merits some investigation. By which transport arrangement should IP be conveyed by? Should it be Frame Relay (FR), Asynchronous Transfer Mode (ATM) or Point to Point Protocol (PPP)?[1] Since there are different alternatives it all boils down to a few key categories, namely bandwidth utilization, implementation issues and the region of the network (access/backbone) in which the implementation takes place. Surprisingly security is less prominent and does not really impact the transport protocol choice since our study so far does not imply that the security level is dependent of underlying protocols to IP.

3.3.2 Multi Protocol Label Switching

With the introduction of Multi Protocol Label Switching (MPLS) as an efficient transport technology even more new perspectives, opportunities and alternatives arise. MPLS was introduced to overcome the existing problems associated with IP networks especially the destination-based forwarding that IP routers use. As the protocol name indicates MPLS exploits label switching forwarding which is considered more desirable than destination-based forwarding because of its low-cost hardware implementation, scalability to very high speeds and flexibility in the management of traffic flows. The packet forwarding takes place at layer 2 (switching/data link) level rather than at layer 3 (routing/network) making traffic move

[1] The pros and cons of the different packet transport technologies will not be discussed here, since it is beyond the scope of this project. Instead [WRI01] gives an excellent comparison on the efficiency of the different packet voice alternatives.

faster. It is important to stress out that MPLS is more of a concept rather than an actual protocol and works with different protocols such as IP, ATM and FR, thus the name "Multi Protocol". MPLS assists a number of essential capabilities to IP's best effort networks which include:

- Traffic Engineering
- Providing IP based Virtual Private Network (VPN)
- Providing traffic with varying QoS

MPLS is the new trend technology that will be used by many future core networks, including converged data and voice networks. MPLS does not replace the IP routing, but is an adjunct technique that provides high-speed data forwarding between Label-Switched Routers (LSRs) together with reservation of bandwidth for traffic flows with different QoS requirements. The voice service would, of course, have a higher QoS requirement than ordinary data due to its real-time sensitivity. Chapter 8 describes MPLS in more detail.

In the project VoIP refers to Voice over IP over MPLS conveyed by a transport arrangement such as FR, ATM, PPP or Ethernet. Voice can, in fact, also be conveyed directly over MPLS without first encapsulating the voice data in IP. In this case the protocol stack would consist of voice data encapsulated in the MPLS protocol on top of a MPLS transport arrangement. The first arrangement, VoIPoMPLS (VoIP) is largely supported by existing Internet Engineering Task Force (IETF) standards and is currently the most deployed solution while voice directly over MPLS is a relatively new method for efficient transportation. For a thorough evaluation of VoIP compared to VoMPLS the reader is requested to see [FJE02].

3.4 Summary

In this chapter the differences between circuit switching and packet switching have been discussed. Beside the fiscal savings, packet-switched networks provide new business opportunities by integrating data services with voice services. Furthermore, there are benefits in relation to voice compression, silence suppression and statistical gains. A hierarchal overview of the main protocols/technologies in voice over a packet-switched network is also provided. The chapter ends with providing the reasons for the use of IP and lastly introduces the benefits of using MPLS.

Chapter 4

Fundamental Components in VoIP Systems

A VoIP system consists of different type of components and many of these are the same as those in traditional data systems. The chapter introduces the necessary components that are needed to implement a VoIP system. Moreover the communication between the components is described and visualized. The chapter is primarily based on [BRA04, KWF05, TIP04].

4.1 Terminal

A terminal is an endpoint that allows a user to communicate with a computer. It can be a simple Input/Output device such as a keyboard and a monitor or more complex devices where biometric techniques are used to communicate with a computer [PFL03]. In a VoIP system a terminal is mainly used to translate voice to a format suitable for transportation over the network, that is, conversion of human speech to digital voice. This functionality can be fulfilled by either a soft phone, a PC consisting of a headset and associated software, or an IP phone. Each VoIP terminal that is connected to the LAN is located on at least one IP address so other terminals can dial to it.

4.2 Server

The IP address and the port number of the terminal must be used to make a call. To demand the user to remember the IP address is obviously not user–friendly, because these are difficult to remember. The use of dynamic IP addressing makes this requirement even more problematic. This problem is solved by registering the terminals' IP addresses with a server, called registrar server. The server stores these IP addresses along with their associated telephone addresses in a database, whereby the server can map a telephone address to a specific host.

There are basically two kinds of servers: Stateless and stateful servers. The difference between these servers is that stateless servers do not store information regarding packets that have passed while the stateful servers do. This makes the stateful servers capable of retransmitting data in case of timeout and keeping track of earlier connections. The drawback by using stateful servers is that they tend to give delays since additional time has to be used to log the packet information traversing the server.

4.3 IP Private Branch Exchange

The Internet Protocol Private Branch eXchange (IP PBX) is a server that has the same functionalities as the TDM PBX used in the traditional telephone network, such as call control, call signaling, authenticating registrations and authorizing callers. It is a telephone switching component that resides in the private company or organization instead of the telephone company. An IP PBX is an essential component in VoIP systems and is also responsible for delivering services such as dial-tone and telephone conferencing. As shown in Figure 4.1, two terminals have to establish the connection through the IP PBX before they can communicate.

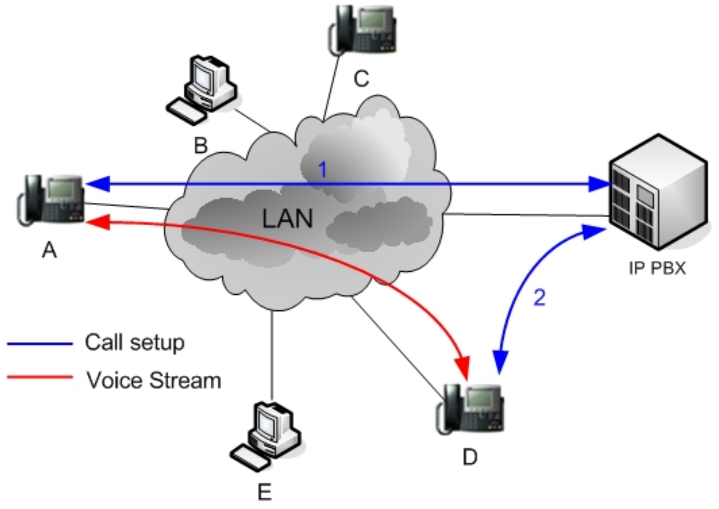


Figure 4.1: Two terminals establishing a connection through an IP PBX.

4.4 Switch

A switch is a network component that channels incoming data from any multiple input ports to the specific output port that will take the data toward its intended destination. The switching takes places at the data link layer of the OSI model where the data is forwarded using Medium Access Control (MAC) addresses.

4.5 Router

A router is a network layer component considered as a special packet switch that connects two networks, such as two LANs or a LAN and a public network. However, it can also be used within a LAN. Routers are responsible for forwarding packets from one network to another that are based on the destination of the packets and the routing decisions in the network layer. The main idea of IP voice packet transmission is that IP routers direct the transfer of voice packets across a data network using routing tables. If the IP address is not the same as the router's own IP address, then the router determines the next-hop router and forwards the voice packet.

4.6 Gateway

A VoIP user and a traditional telephone user cannot communicate directly with each other, since VoIP and PSTN use dissimilar protocols for signaling. PSTN uses Signaling System 7 (SS7) and VoIP can use different protocols such as Session Initiation Protocol (SIP) or H.323. The VoIP system can be connected with PSTN by using a gateway which acts as a highly intelligent switch and works as a translator between two dissimilar protocols.

4.7 Multi–point Control Unit

A Multi–point Control Unit (MCU) is an optional device in a VoIP system that handles voice and video conferencing with multiple users at the same time. This can either be a stand–alone unit or integrated into a terminal or a gateway. It consists of mainly two parts:

- Multi–point Controller (MC) - Handles control and signaling part.
- Multi–point processor (MP) - Receives data from terminals and forwards them to other terminals.

4.8 Addressing

As mentioned earlier, it is not ideal to use terminal IP addresses as the user identifier since these are difficult to remember. Current VoIP systems use two kinds of identifiers:

- Universal Resource Identifier (URI) - Uses a registered naming space to describe a source's location on the network. It is used in a wide range of protocols such as in HTTP, SMTP and VoIP.
- Numbers - The E.164 number system also used in PSTN.

A more adequate description of the identifiers is given in [LEE98, SPR03].

4.9 Firewall

A firewall is a combination of hardware and software that secures the network from intruders. It is considered to be the first point of defence in a network and is usually placed between a company's corporate network and the public network. All traffic traversing from the corporate network to the public (insecure) network, and vice versa, has to pass through the firewall. The firewall is configured with certain security rules to decide whether the traffic should be allowed to pass through or not. The firewall is typically setup as following:

- Allowing traffic from the corporate network to pass through.
- Allowing traffic from the public network that is associated with an inside connection to pass through.
- Blocking traffic that is initiated from the public network.

These firewall rules give problems with VoIP systems since a caller from the public network will not be allowed to initiate calls to the VoIP system. Problems along with solutions related to firewalls are discussed in more detail in Section 8.4.

4.10 A VoIP System

The components mentioned in the chapter are not all strictly necessary to implement a VoIP system. The VoIP system can be simply two terminals connected directly together or can be an advanced system such as those in large enterprises where the PSTN is replaced by a VoIP system. Figure 4.2 shows a set-up of the components where each LAN is connected to the PSTN through a gateway, and to the public IP network through a firewall. While implementing a VoIP system, one has to analyze which components will satisfy the requirements for the telephone system.

4.11 Summary

This chapter described the components that are necessary to implement a VoIP system. These include terminals, servers, IP PBXs, switches, routers, gateways, MCUs and firewalls. Finally an overview of a VoIP system was illustrated and the addressing mechanisms presented.

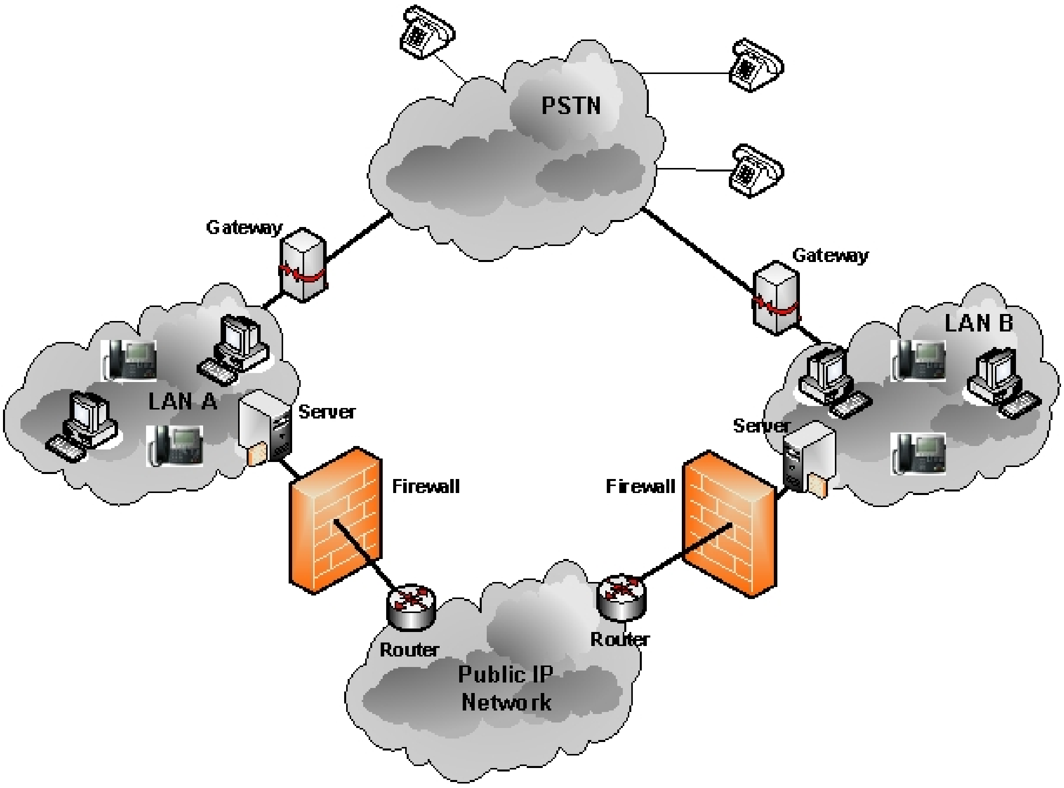


Figure 4.2: A set-up of the components in a simple VoIP system.

Chapter 5

Security Aspects

When using IT systems for storing and exchanging information the need for security arises to protect the data-related assets. The data-related assets can be in many forms, for instance the company's strategy plan, business agreements, confidential telephone conversations, etc.

The definition of security is broadly defined and used in different relations, depending on the situation. However, following definition of security is used throughout the thesis:

- Security is protecting the systems so they work when they are needed.
- Security is preventing unauthorized users to misuse the systems.
- Security is preventing unauthorized users to damage the systems.

The purpose with this chapter is to determine different aspects within computer security with focus on confidentiality, integrity and availability, also called the CIA-requirements [PFL03]. The CIA-requirements are discussed in relation to VoIP systems, Figure 5.1. The security aspects for general data communication are in most cases the same as for VoIP systems.

5.1 Confidentiality

Confidentiality ensures that assets are protected from unauthorized users, illustrated in Figure 5.2[1]. This means that only those who should have access to the assets will actually get access. The classification of confidentiality sounds very straightforward and simple to implement. However, there are some considerations about confidentiality that are immediately difficult to determine in computer related assets. For example, what does "unauthorized users should not have access to assets" mean? Does is mean that they should not have access to eavesdrop parts of the conversation, eavesdrop even a single bit or just not be able to understand the conversation?

A VoIP conversation can contain important assets of information that are being exchanged, such as the company's strategy and economical agreements. If unauthorized users, such as

[1] The figure is inspired from [PFL03].

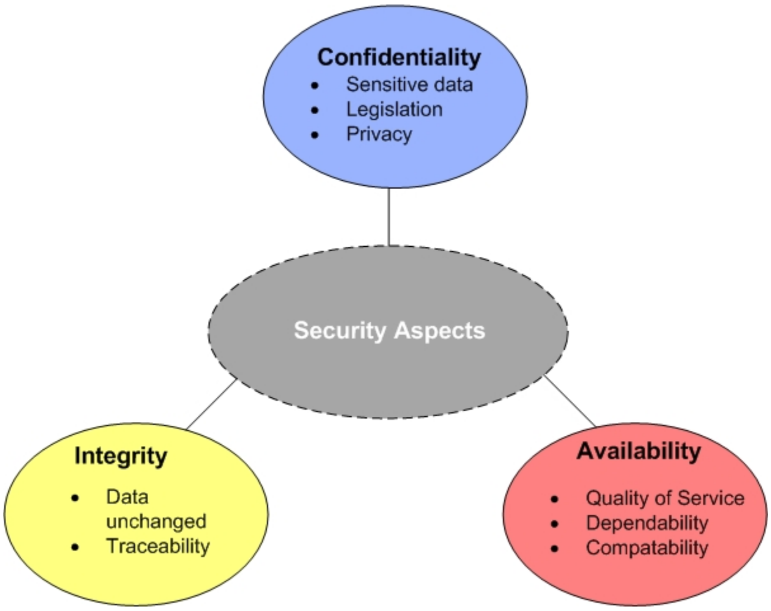


Figure 5.1: Security aspects.

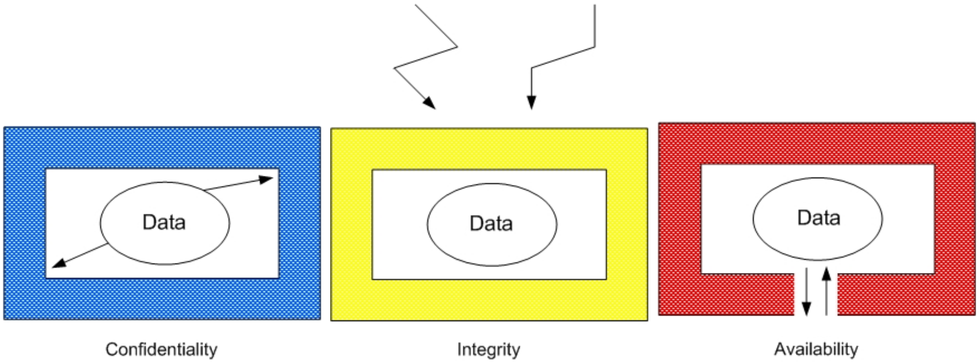


Figure 5.2: Confidentiality, integrity and availability.

competing companies, get access to the voice assets it can have severe consequences and can cause economical damage to the company. It is therefore important that only authorized users get access to the voice data and that strong techniques are used to assure it.

Beside company voice-related assets, VoIP conversations can also be private conversations such as a conversation between an employee and his bank. Classification of personal data has to follow the legislations, for example in Denmark the "Act on Processing of Personal Data" [DAT00] must be followed.

5.2 Integrity

Integrity assures that assets can only be modified by authorized users and processes, illustrated in Figure 5.2. To retain the assets' credibility it is important that the integrity of the assets is preserved.

As mentioned earlier, the VoIP conversations in companies can contain valuable assets of information. It is therefore important that this information reaches its destination without any modification. In most cases the caller knows the callee's voice and can therefore discover if all or some of the voice packets in the conversations are modified by an unauthorized user. However, it is difficult to discover an attack where only few packets are removed by an unauthorized user since the caller and the callee cannot distinguish between the attack and situations where usual packet losses happen.

5.3 Availability

Availability means that assets or services are accessible when requested by authorized users, illustrated in Figure 5.2.

The availability requirement sounds very easy to satisfy, but in relation to IP networks and especially VoIP systems there are some factors which have to be considered:

- Quality-of-Service
- Dependability
- Compatibility

5.3.1 Quality-of-Service (QoS)

The QoS issues were discussed in Chapter 2. Generally the quantitative data flow in a network has to be prioritized such that the speed of different information can be differentiated. This can be compared to the fast lane and the slow lane on the freeway. High priority traffic, such as ambulances, can take the fast lane and thereby reach their destination faster than if they took the slow lane.

Similar situations occur in the data transport, for instance with data that have to be synchronized and VoIP data since these data are highly delay sensitive. This means that some of the traffic gets low priority, such as e-mail, Internet surfing or similar data flows, where short delays will not have an impact on the quality. The data priority is important because the networks do not always have enough capacity to simultaneously transmit all the data. Suitable bandwidth is also a necessary factor to maintain the quality of the data transport.

5.3.2 Dependability

The dependability of a network adds importance to the physical factors. This means that the components should be secured with regards to their physical location, power supply etc. The goal must be to secure a network so its services are always available. The dependability can be implemented by using emergency backup power to power-intensive units and redundancy in the systems, so single failures will not impact the entire network.

5.3.3 Compatibility

For securing the availability in a network it is a condition that there is full compatibility between the network and all the units which are connected to it. Typical use of computer does not give any rise to problems, but special components, such as those used in VoIP systems, can use widely different network configurations. To have a fully functional system that can communicate over the network, it is important that all the components and protocols can communicate with each other.

5.4 Summary

Different security aspects were discussed and should be considered when analyzing a company's data network. Generally it's a description of the processing of information that is known in the usual human working procedures in companies. The system should be effective (available) with minimal risk (integrity) while respecting the company privacy (confidentiality). In other words the assets should be accessed by the right people, at the right time, in the right form and at the right secure place.

As illustrated in Figure 5.3 there are some contrasts between the discussed aspects, but the better technology and design the system is implemented with, the less the contrast will be between various aspects. The succeeding chapters use the security aspects to analyze VoIP security protocols and risks.

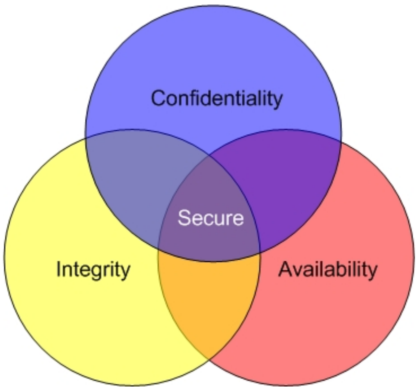


Figure 5.3: Relationship between the security aspects.

Chapter 6

VoIP Protocols

The caller's voice has to traverse a number of processes before it can reach the callee. A process can for instance be to establish a call between the participating parties or translating the human speech to a format suitable for real-time transport over an IP network. Generally the processes can be split into 3 categories:

- Signaling and gateway control
- Encoding and decoding
- Voice transport

The following sections describe these categories together with the protocols that are used to execute tasks defined in the categories. The purpose with this chapter is to give a technical description on how the protocols used in VoIP systems work and which security mechanisms are used to secure the confidentiality and integrity in the VoIP conversations.

6.1 Signaling and Gateway Control Protocols

The purpose of a signaling protocol is to create and manage real-time connections between the terminals, as well as the calls themselves. The signaling protocols also cover how terminals attached to the data network communicate with telephones attached to PSTN. Currently a standard signaling protocol for VoIP systems does not exist. However, the protocols H.323 and Session Initiation Protocol (SIP) are competing strongly to be the new deployed standard for the future.

This section gives an overall description of H.323 and SIP together with two gateway control protocols, Media Gateway Control Protocol (MGCP) and MEdia GAteway COntrol / H.248 (MEGACO/H.248). The security mechanisms in these protocols are also described. The section is based on [BRA04, KWF05, STI02, TIP04].

6.1.1 H.323

H.323 is a set of recommendations approved by the International Telecommunication Union-Telecommunication (ITU-T) in 1996 for transmission of real-time voice, video and data communication over packet-switched networks. The initial version of H.323 has been improved several times leading to version 5, which has new improvements in form of reliability, scalability and flexibility. However, it does not support QoS. It is a binary protocol where the messages are encoded using the Abstract Syntax Notation One (ASN.1) scheme.

H.323 Architecture

A H.323 network consists of terminals, gateways, and optionally gatekeepers, a MCU, and a Back End Service (BES). Descriptions of terminal, gateway and MCU were provided in Chapter 4. Gatekeepers are a wide deployed component in VoIP systems and are responsible for access control, address resolution, bandwidth control and call forwarding. A H.323 network is subdivided into zones where each zone is controlled by one primary gatekeeper and optionally a backup gatekeeper. If a gatekeeper is used, a BES can be placed behind the gatekeeper to store data about the terminals.

H.323 consists of several protocols that each has a specific task to execute, such as call setup, call termination, registration or authentication. The protocol stack used in H.323 is shown in Figure 6.1. Only the call signaling and control of H.323 will be described here while the audio processing and media transport of H.323 are described later in this chapter. Description of the data and video conferencing of H.323 is omitted in this thesis.

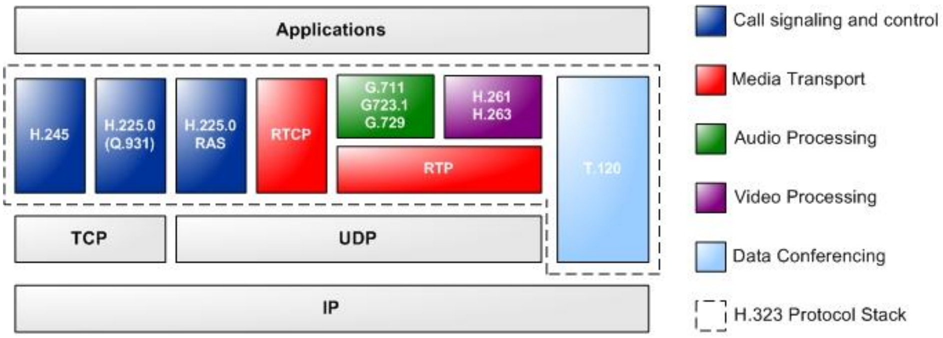


Figure 6.1: The H.323 protocol stack.

Three control protocols are used for call signaling and control in H.323:

- H.225.0 Registration, Admission, and Status (RAS) - The RAS channel is used for registration, admission, address resolution and status messages between the terminals and their gatekeeper (if a gatekeeper is present).
- H.225.0 Call signaling - The call signaling is responsible for negotiating call setup, controlling and terminating H.323 calls. Its messages are based on Q.931 which is the standard used for call signaling in Integrated Services Digital Network (ISDN). The

channel is used end-to-end between the caller and the callee and may run through several gatekeepers.

- H.245 Conference control - The conference control channel is the control protocol for multimedia conferencing within H.323. While the H.225.0 simply negotiates the establishment of a connection, H.245 establish the channel that will be used for media transfer. Furthermore, H.245 negotiates a common voice compression and the logical channels that will be used by all the participating terminals in a session.

As seen in the H.323 protocol stack, H.323 uses both reliable and unreliable communication. H.225.0 RAS requires unreliable transport (UDP) while H.225.0 call signaling and H.245 conference control use reliable transport (TCP).

H.323 Signaling

The H.225.0 and H.245 messages have to be exchanged between the caller and the callee to setup a call. This can either be done by an end-to-end communication between the caller and the callee or through a gatekeeper. Depending on the role of the gatekeeper in H.225.0 and H.245, H323 has three types of signaling procedures:

- Direct signaling - Only H.225.0 RAS messages are routed through the gatekeeper while the other messages are directly exchanged between the terminals.
- Gatekeeper routed call signaling - H.225.0 RAS and H.225.0 messages are routed through the gatekeeper while H.245 messages are directly exchanged between the terminals.
- Gatekeeper routed H.245 control - All signaling and control messages are routed through the gatekeeper while the media stream is directly exchanged between the terminals.

A large number of simultaneous calls can be processed in the direct signaling model since the gatekeepers only participate in the call admission process and have limited knowledge about the connected calls. In the gatekeeper routed call signaling model the gatekeepers are more loaded since they have to handle the Q.931 signaling messages as well. The advantages by using the gatekeeper routed H.245 control model is that the gatekeepers can perform management functions, such as connection and media usage statistics, since only the media stream is sent directly between the endpoints.

An example to illustrate the H.323 signaling is given by the direct signaling procedure in Figure 6.2. The communication here begins with the H.225.0 RAS procedure, the caller sends an `Admission Request` message to the gatekeeper to request access to the H.323 network. The caller can either be a terminal or a gatekeeper since it is possible for a call to route through several gatekeepers. The access will either be granted by the gatekeeper with an `Admission Confirm` message or denied with an `Admission ReJect` message. The call terminates if an `Admission ReJect` message is sent. The caller will receive the destination address within the `Admission Confirm` message and use it in the H.225.0 call signaling procedure to transmit the `Set-up` messages directly to the callee. Next the callee carries out its H.225.0 RAS procedure with the gatekeeper and sends a `Connect` message to the caller to indicate the acceptance of the call. After receiving the `Connect` message, the caller starts the H.245 conference control procedure which establishes the channel used for media transfer.

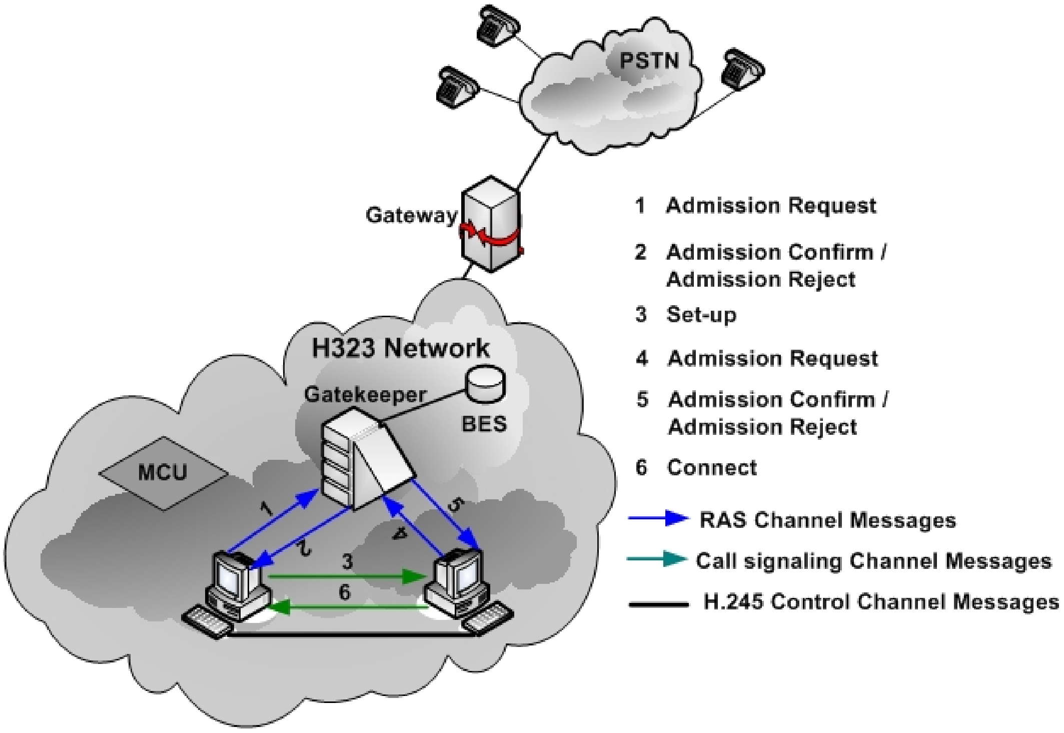

PSTN
Gateway
H323 Network
Gatekeeper
BES
MCU
1
2
3
4
5
6
1 Admission Request
2 Admission Confirm / Admission Reject
3 Set-up
4 Admission Request
5 Admission Confirm / Admission Reject
6 Connect
RAS Channel Messages
Call signaling Channel Messages
H.245 Control Channel Messages

Figure 6.2: The H.323 architecture and direct signaling procedure.

H.235 - Security profiles

Besides the voice media, the call signaling and control process in H.323 also has to be secured to ensure the confidentiality and the integrity of the calls. The H.235 version 2 was approved by ITU-T in November 2000 and defines different security profiles for H.323. It provides enhancements such as support for elliptic curve cryptography and Advanced Encryption Standard (AES) which leads to stronger security mechanisms.[1] The security profiles offer different level of security and are defined in several Annexes to H.235 version 2:

- Annex D: Baseline security profile - This profile relies on symmetric encryption techniques where shared secrets are used to provide authentication and message integrity. Hashed Message Authentication Code (HMAC) Secure Hash Algorithm One (SHA-1) is here used as the cryptographic function. This profile is supported for terminal to gatekeeper, gatekeeper to gatekeeper and terminal to terminal. The profile is not highly scalable since the shared secret has to be predefined.
- Annex E: Signature security profile - This profile relies on asymmetric encryption techniques where certificates and digital signatures are used to provide authentication and message integrity. It uses SHA-1 and/or Message-Digest algorithm 5 (MD5) as the cryptographic function and it is highly scalable since it relies on Public Key Infrastructure (PKI). However, this profile can have a critical impact on the overall performance since digital signature and verification on every message is time consuming.

[1] [STI02] contains further reading about cryptographic algorithms.

- Annex F: Digital signature hybrid security profile - This profile is a combination of the Baseline (Annex D) and Signature (Annex E) security profile. Certificates and digital signatures are used to provide authentication and message integrity for the first negotiation, also called a handshake, between the terminal and the gatekeeper. During this handshake shared secrets are exchanged that will be used further on as described in the baseline security profile. The Diffie-Hellman algorithm is used to assure that the shared secrets are carefully chosen.

The confidentiality of the voice media in all three profiles is offered by the voice encryption option. The algorithm that can be used here are Data Encryption Standard (DES), Triple-DES (3DES) and AES.

H.235 version 3 replaces H.235 version 2 by offering features such as media payload encryption. Moreover it defines a number of new security profiles for RAS key management (Annex H), usage of Secure Real-time Transport Protocol (SRTP)[2] (Annex G) and for better security support for the direct routed model (Annex I) [KWF05].

6.1.2 Session Initiation Protocol

SIP is the Internet Engineering Task Force (IETF) specified signaling protocol used for Internet calls, multimedia conferences and multimedia distribution. Its core protocol specification is defined in RFC 3261 [ROS02]. In contrast to H.323, SIP is specifically designed for voice services.

SIP is an application layer protocol of the OSI communication model that uses text-based messages similar to HTTP. In contrast to H.323, SIP does not require any reliable transport, and can be implemented by using UDP. However, it is recommended that the SIP server supports both UDP and TCP, and that the TCP connection should only be opened if a UDP connection cannot be established.

SIP Architecture and Signaling

The SIP architecture consists of two parts, the SIP User Agent (UA) and the SIP Network Server. The SIP UA is a user's terminal and consists of two main components:

- User Agent Client (UAC) - Responsible for sending requests and receiving responses.
- User Agent Server (UAS) - Responsible for receiving requests and sending responses.

The SIP UA behaves as an UAC when it sends a request to initiate a call and receives a response to the request. On the other hand the callee's UA behaves as an UAS when it receives the request and sends responses.

The function of the SIP Network Server is to provide name resolution and user location. It consists of three main groups:

[2] SRTP is described in section 6.3.3.

- Proxy server - Each LAN has its own proxy server which is used by the UAC to pass the request to the next server. The request can be passed to several proxy servers before reaching its destination. Besides routing decisions, the proxy server also provides functions such as authentication, network access control and security, similar to a firewall.

- Redirect server - Helps terminals to find the desired address by redirecting the user to another server.

- Registrar server - A server that accepts user registration and maps a user's telephone address (such as an e-mail address) with its IP address. It is used because a telephone address is much easier to remember than an IP address.

The SIP call setup is similar to the procedure used in HTTP. It uses a three-way handshake to establish a connection between two terminals, see Figure 6.3. The figure illustrates the setup procedure in a SIP network where a proxy and a registrar server are implemented in a single component. The caller sends an invite request using the Session Description Protocol (SDP) format to the callee through the proxy server. The request is either replied with an `Accept` or a `ReJect` message. If a `ReJect` message is received the call terminates. Otherwise the caller will finish the three-way handshake by sending an `Acknowledgement` message to the callee (through the proxy server) and the media transfer channel will hereafter be created directly between the caller and the callee.

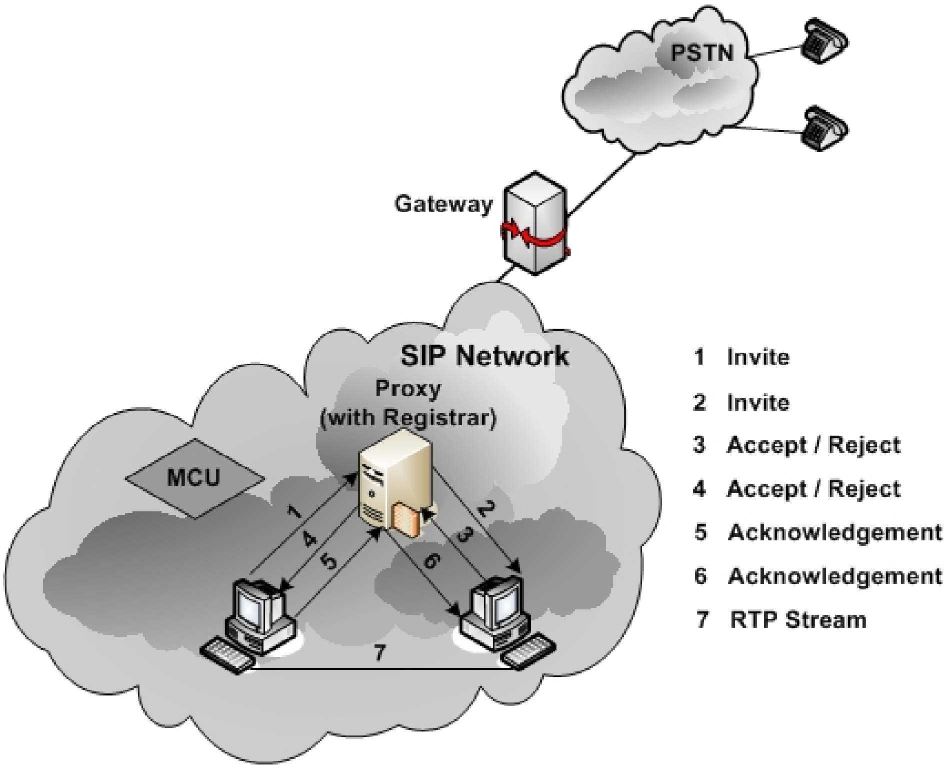


Figure 6.3: The SIP architecture and signaling procedure.

SIP Security

As mentioned earlier, SIP messages and the handshake model are similar to those used in HTTP. This means that all the security features used in HTTP can also be applied within SIP. RFC 3261 [ROS02] describes several security features for SIP, such as HTTP Digest authentication, Secure Multipurpose Internet Mail Extension (S/MIME), confidentiality of the voice media, Transport Layer Security (TLS) and IP Security (IPSec).

The SIP authentication works similar to the HTTP Digest authentication and replies only to user-to-user and user-to-proxy. It is a simple challenge-response procedure where a valid response contains a checksum of the user name, the password, a randomly selected number, the HTTP method and the requested URI. The default algorithm to compute the checksum is MD5.

Since SIP messages carries MIME bodies it can use S/MIME. S/MIME defines security mechanisms such as public key distribution, authentication, integrity and confidentiality of the MIME contents. RFC 3261 [ROS02] recommends using S/MIME as a replacement for Pretty Good Privacy (PGP) for UAs.

SIP does not consider the encryption of the voice media. However, SRTP can be used to provide confidentiality of the voice media. RFC 3261 [ROS02] recommends the use of TLS for UAs, proxy, registrar and redirect servers to protect SIP signaling messages against loss of integrity and confidentiality. TLS works hop-by-hop between UAs/proxies or between proxies, and works only over a reliable communication (TCP). In contrast to TLS, IPSec works on both reliable and unreliable communication and supports hop-by-hop as well as end-to-end security. IPSec can be used to provide security for the SIP signaling at the network layer.

6.1.3 H.323 versus SIP

The architecture and security mechanisms for H.323 and SIP have been described in the preceding sections. In this section H.323 and SIP will be compared against each other by examining the advantages and disadvantages in the protocols. The comparison can be seen in Table 6.1.

SIP is weak from a security point of view since it is still in its early stage of deployment and does not have any integrated security mechanisms.[3] Generally there is a trend that the best features of H.323 and SIP are being implemented in the other. However, SIP is predicted to be the standard protocol in the future since it is less complex, more scalable and has a simplified signaling procedure compared to H.323.

6.1.4 Gateway Control Protocols

VoIP systems and PSTN use dissimilar signaling protocols, and gateways are used to provide communication between these protocols. A decomposed gateway in VoIP systems consists of two parts, Media Gateways (MG) and a Media Gateway Controllers (MGC). MG focuses on the signal translation between VoIP networks (SIP or H.323 signaling) and PSTN (SS7

[3] The vulnerabilities in SIP are discussed in subsection 7.1.1.

Table 6.1: Comparison of H.323 and SIP.

	H.323	**SIP**
Architecture	Covers many services such as capability exchange, conference control, basic signaling and registration.	Covers only basic services such as basic call signaling, user location, and registration.
Message format	Binary in ASN.1 format, gives problems with firewalls.	Text-based, results in more bandwidth overhead and is easy to extend and debug.
Addressing	One address for each physical entity.	E-mail-like identifier for each user.
Complexity	High, due to the large number of protocols in the H.323 protocol stack.	Low.
Scalability	Poor since it was initially designed for LANs.	Good - designed for Wide Area Networks (WANs).
Delay	Possibility of high delay due to the complex signaling procedure.	Low delay, uses a simplified signaling procedure.
Security	Uses the security profiles defined in H.235.	Authenticates via HTTP mechanisms and can use any HTTP security features in the transport layer.

signaling) while the MGC handles the call signaling between the MGs and routing decisions. A single MGC can manage up to several MGs which can lead to cost reduction in larger VoIP systems.

Common examples of protocols that provide the communication between MGCs and MGs are MGCP and MEGACO/H.248 which are described next.

MGCP

MGCP is an IETF standard for providing communication between MGCs and MGs, and is a complementary protocol to H.323 and SIP. It is described in details in RFC 2705 [ARA99] and RFC 3435 [AND03].

The system architecture of MGCP is illustrated in Figure 6.4. MGs are unaware of the calls and conferences and do not maintain calls states. The calls and conferences are instead managed by the MGC that uses MGCP to provide the MGs with the description of the connection parameters such as IP addresses and UDP port. Basically, MGCP works as a master/slave protocol where MGs are expected to execute commands sent by the MGCs.

There are no security mechanisms implemented into MGCP to protect confidentiality and integrity of the MGCP messages. However, RFC 2705 recommends to use the security mechanisms of the underlying layers such as TLS and IPSec. Moreover, MGCP allows the

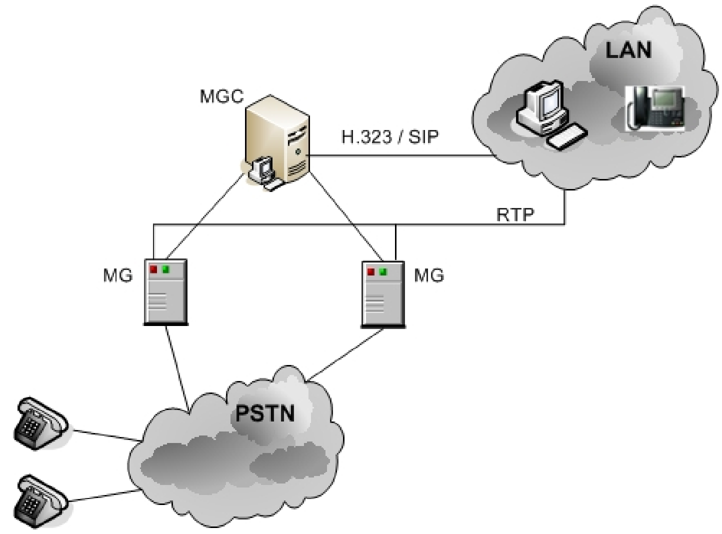


Figure 6.4: The MGCP architecture.

MGC to provide gateways with session keys that can be used to prevent eavesdropping by encrypting the voice messages.

MEGACO/H.248

The MEGACO/H.248 protocol is derived from MGCP, and was in June 1999 accepted by the IETF and ITU-T as a standard.[4] It is expected to win wide industry acceptance as the official standard for decomposed gateway architectures. MEGACO/H.248 inherits all the functionalities of MGCP and in addition, it supports enhanced services for multimedia and multi-point conferencing. The system architecture and commands are similar to MGCP.

Similar to MGCP, MEGACO/H248 recommends using the security mechanisms in the underlying layers, such as IPSec. However, ITU-T goes a step further by demanding to use IPSec if the underlying layers support it.

6.2 Encoding and Decoding

Today PSTN is almost entirely digitalized in technology except for the link between the local telephone office and the telephone users [RAN05]. With time the telephone system will be all digitalized, as more and more analog components will be replaced by more reliable and modern digital circuits. There is no doubt that digital communication systems outperform analog systems in many ways especially in the means of eliminating background noise and encrypting transmission data for security purposes [STI02]. However, there is a trade-off between speech quality, transmission speed and bandwidth capacity when using digital voice. The following section presents different speech coding techniques that attempt to reduce

[4] The protocol is called MEGACO by IETF and H.248 by ITU-T.

Table 6.2: Table overview of codecs with bit-rate and expected MOS.

Codecs	Bandwidth	MOS
G.711 (PCM)	64 kbps	4.10
G.723.1A (ACELP)	5.3 kbps	3.65
G.723.1A (MP-MLQ)	6.4 kbps	3.90
G.726 (ADPCM)	32 kbps	3.85
G.728 (LD-CELP)	16 kbps	3.61
G.729a (CS-CELP)	8 kbps	3.92

network bandwidth while maintaining high-quality speech output during the transmission process.

6.2.1 Voice Codecs

The encoding process takes place at the voice gateway. When using a packet-switched technology it is vital to have an efficient voice encoding and decoding mechanism. The purpose of a voice coder (vocoder) also referred to as ”codec” (**co**ding/**dec**oding) is to use the analog signal, that is the human speech, and transform and compress it into digital data. The continously varying analog voice signal is normally converted to a digital signal by a sampling and quantization process.[5] At the other end, the process is reversed, a process called decoding. This means that the digitized voice data is extracted from the packets and uncompressed and finally processed by a digital-to-analog converter. The quality of voice is considered more important than bandwidth consumption since bandwidth is cheaper than quality.

Waveform coding is the frequently used method for codecs. It attempts to produce a reconstructed signal where the waveform is as close as possible to the original signal without using any knowledge of how the signal to be coded was generated. Different waveform codecs with different bit-rates exist. The lesser the bit-rate the more compression is used thus possibly resulting in poorer quality. Having codecs with high-quality output and a low bit-rate, that is, the lowest data transmission possible, is mutually exclusive since compression degrades the quality. Therefore there are a number of available codecs with different features all specified and approved by the ITU-T. Table 6.2 shows a summary of the popular (all waveform) ITU-T approved codecs.[6] The codecs will not be explained in depth here but for a more thorough and technical reading on codecs see [RAN05].

The simplest form of waveform coding is Pulse Code Modulation (PCM) which involves both sampling and quantization of the input waveform. In other words, the speech signal is transferred from continuous time to discrete time before it can be processed by digital hardware and thereafter segmented into a stream of packets. An example of PCM coder is G.711. which is probably the most applied codec due to its high MOS value. On the downside though is its relatively high bit-rate. The other codecs all have different qualities. For example the G.729A applies an algorithm that only requires few instructions per second

[5] The conversion of analog to digital signal is heavily described in [RAN05].

[6] The MOS values can be found at `http://www.cisco.com/warp/public/788/voip/codec_complexity.pdf`. Note: Login with a Cisco account must be used before getting access to this document.

and can therefore run on slower processors without degrading the quality of the speech. Another codec is the G.723.1 which merely consumes one-twelfth of the bandwidth when comparing it to its predecessor G.711.

6.3 Voice Transport

When the signaling and encoding process have occurred the voice packets need to be transported to the destination (callee) in the VoIP system. The main transport protocols are TCP and UDP but, as will be described, these protocols are not sufficient enough to provide the transport alone. The section is based on [RAN05, KUR01, GAR04, KWF05].

6.3.1 TCP versus UDP

The traditional TCP/IP and UDP/IP protocols model are not very suitable for transporting data of a time sensitive nature. TCP and UDP have different characteristics that various applications can use. If reliability is more important than delay, TCP/IP can be used to guarantee packet delivery. Unlike the TCP/IP protocol UDP/IP does not utilize packet retransmission which makes the reliability of UDP/IP lower. But in most cases a late retransmission is of no use, especially when voice is retransmitted making the speech sound jerky and appear to arrive in bursts. When voice is streamed both delay and jitter is to be avoided. TCP would guarantee the delivery of the voice samples but there would be no guarantee of the time or order the samples would arrive in. Consequently, there is no reason to use TCP with its delivery guarantees, its larger overhead and its high complexity. UDP is more suited for the transportation of the voice packets even though it only delivers by best effort and thereby giving no guarantees to reliable delivery. UDP has a smaller header size and the fact that it does not provide any guarantees to delivery makes it a protocol of low complexity and favorable for voice to be transported via UDP packets. UDP is not ideal though since it does not provide all the facilities to transport VoIP.

6.3.2 Real-Time Data Transport

Two important pieces of information that are missing in both TCP and UDP are sequence information and time stamping. The sequence numbering is needed to enable the receiver to determine the order in which to use the packets, since they are not necessarily received in the correct order. Time stamping information is useful to determine jitter and is used when trying to compensate for it.

This missing information can be provided by Real-time Transport Protocol (RTP), defined in RFC 1889 [SCH89], which is usually run on top of UDP since reliability is not a major concern. This is shown in Figure 6.5.

RTP can be considered as a sublayer of the transport layer and is merely a protocol that implements the functionalities the other transport protocols (TCP and UDP) lack. At the same time it takes advantage of the existing protocols (UDP). The combination RTP/UDP/IP has sufficient information to carry real-time data between terminals as illustrated in Figure 6.6.

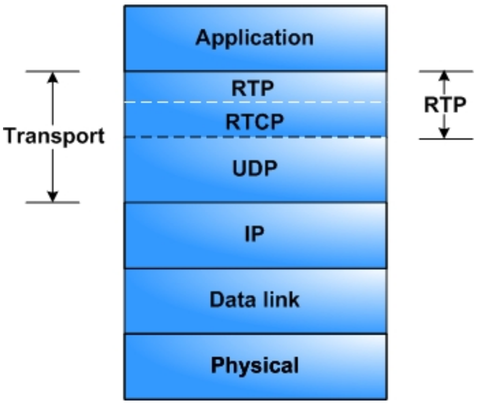


Figure 6.5: RTP can be viewed as a sublayer of the transport layer.

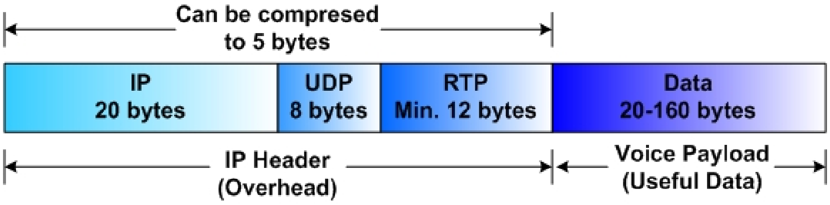


Figure 6.6: Data and overhead using RTP.

RTP consists of two main parts; a data part and a control part, see Figure 6.5. The data part is usually referred to as RTP (a slightly unfortunate naming) and the control part is called RTP Control Protocol or simply RTCP. RTCP allows monitoring of the data delivery of the RTP. Some of the functions that RTCP provides are QoS feedback, session control, user identification and inter-media synchronization, to synchronize between the voice stream. RTCP packets do not encapsulate chunks of voice. Instead, RTCP packets are sent periodically and contain sender and/or receiver information that contain statistics that can be useful to the application. These statistics include number of packets sent, number of packets lost and inter-arrival jitter. Senders can use the feedback information for several purposes, for example to modify their transmission rate or even determine whether problems are local, regional or global.

6.3.3 Secure RTP

RTP and RTCP does not provide security mechanisms which Secure RTP (SRTP), described in RFC 3711 [BAU04], takes in consideration. SRTP can be said to be a profile of RTP which can provide confidentiality, message authentication and replay protection for example by using TLS. SRTP encrypts VoIP packets between the terminals using AES and preserves the opportunity for RTP header compression. On the downside SRTP uses more CPU time and gives rise to more delay. So SRTP is useful for multimedia to secure voice data exchange. It can be used with several session control protocols such as H.323 or SIP.

6.4 Summary

This chapter discussed the 3 main processes of voice traversal. These processes include

- Signaling and gateway control
- Encoding and decoding
- Voice transport

Technical descriptions of the signaling protocols, H.323 and SIP respectively, were provided. Today H.323 is the commonly used of the two protocols but SIP is expected to be the dominant protocol in the future due to its simplicity. When security is a concern SIP still lags behind H.323 since H.323 provides a variety of security profiles while SIP depends on lower layer security protocols. Gateways are used to provide communication between the VoIP system signaling protocols and the PSTN signaling protocols. MGCP or MEGACO/H.248 are typically used at the gateways.

The encoding and decoding processes were also described. It is vital to have efficient voice encoding and decoding mechanisms that provide transformation of analog voice to digital and vice versa. Bandwidth utilization and MOS value is also a concern when choosing a codec for encoding and decoding.

Finally it was described why UDP is the preferred protocol for transporting voice packets compared to TCP. UDP is preferred because of its short delays and low complexity. RTP and RTCP provide sufficient information regarding sequence information and time stamping that UDP lacks. SRTP provides security for the voice media by using AES encryption.

Chapter 7

Risk Analysis

This chapter identifies the different security risks that can possibly damage the VoIP system. A risk can either be considered as a threat or a vulnerability. A threat is a set of circumstances that has the potential to damage a VoIP system while a vulnerability is a weakness in the system, for example in the design or implementation, that might be exposed to cause damage. The succeeding sections describe some of the security risks that are related to VoIP. Even though some of the described security risks are not entirely unique for VoIP, a VoIP implementation will indeed bring new aspects of these risks and therefore should be considered heavily. Please refer to Appendix A for a description of the threat sources.

The risk analysis has been completed for closed networks as opposed to open networks that are considered more insecure. The main difference is that open networks are really open, meaning that basically anyone can access the network any time and anywhere the network is present. No pre-registration is needed. The Internet is considered as an open network. Closed networks are considered more secure as the network limits the access only for users of a certain community or group. For example only the employees of the company have access to the companies internal network, the intranet. This also means that the voice traffic is transported over the private or corporate data network rather than over the Internet.

Three questions will be answered in this chapter for identifying the risks and possible vulnerabilities in closed networks:

- Which threats can companies be exposed to with the introduction of VoIP?
- How vulnerable is the VoIP conversation?
- What are the possible consequences of successful attacks against the VoIP system?

At the end of this chapter a risk assessment is presented for a closed VoIP system and based on confidentiality, integrity and availability criteria.

7.1 Risk Identification

The convergence of the voice and data worlds results in the sum of threats in both the PSTN network and in the IP network. The (American) National Institute of Standards and Technology (NIST) claim that VoIP systems is expected to be more vulnerable than conventional telephony systems [KWF05]. Especially the inheritance of the IP security risks represents heavy concerns when implementing VoIP - now a VoIP implementation also requires measures such as encrypting voice services, building redundancy into the VoIP network, fall back procedures to the PSTN network, locking down VoIP servers, and the importance of regular security audits to maintain a strong and highly secure network. Not all security risks are inherited from IP. Some actually carry over from PSTN such as attacks on modems, denial of service attacks, toll fraud and eavesdropping.

As discussed in Chapter 4, a VoIP system requires more components and software than the traditional circuit-switched network. More components mean greater potential for vulnerabilities. No link in the VoIP system is stronger than the weakest link, as goes for the data network. The next sections identify the different kinds of attacks that are specific to a VoIP system.[1]

To this day, there have been no specific attacks on VoIP systems reported to The Danish Computer Emergency Response Team (DK-CERT)[2]. The risks described next are analyzed as being the most likely scenarios to occur in VoIP systems.

7.1.1 SIP Vulnerabilities

There are a number of problems related to SIP regarding security. Since it is a relative new standard protocol it gives rise to exploitation of implementation flaws. In addition SIP does not have any security mechanisms built into it, but instead recommends the use of lower layer security mechanisms. However, some of these security recommendations are lacking in most implementations. For instance RFC 3261 [ROS02] recommends to use TLS, to protect SIP signaling messages against loss of integrity and confidentiality, which is not implemented in all VoIP systems. Finally SIP messages are text-based which make them easier to analyze and therefore easier targets for attackers. This section focuses on the inherent SIP vulnerabilities that exist in most implementations, such as:

- Registration hijacking
- Proxy impersonation
- Message tampering
- Session tear down
- Denial-of-Service (DoS)

Registration Hijacking

Registration hijacking occurs when an attacker impersonates a valid UA to a registrar server, and then replaces the legitimate registration with its own address. This will cause all incoming and outgoing calls from the legitimate user to be sent to the attacker instead, see Figure 7.1.

[1] Please see [CBR03, PFL03] for general attacks and risks in the data network.

[2] DK-CERT is a department of UNI-C.

As the figure indicates, registration hijacking can be used to pull off a Man-In-the-Middle attack.

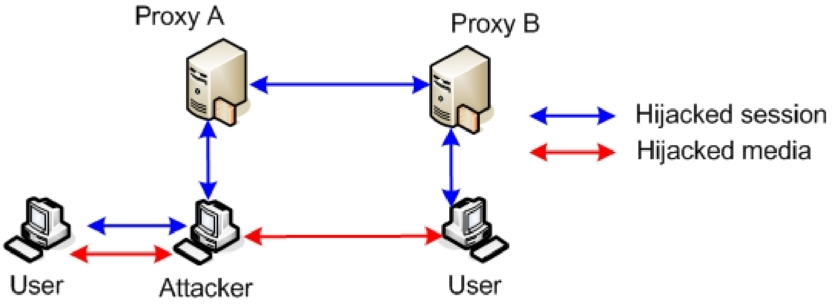


Figure 7.1: Illustrating a registration hijacking that is used to pull off a Man-In-the-Middle attack.

The registration is commonly performed using UDP which is not a secure protocol, since it does not have any security mechanisms implemented, and makes it easier to spoof messages. Furthermore, registration requests are not required to be authenticated by most SIP registrars, and even when authentication is used it is weak such as using MD5 encryption of the user name, password and nonce value. Results from different mathematicians, such as Antoine Joux in April 2004, have shown that there are weaknesses in MD5 [RAN04]. MD5 is known as a hash function which takes an input such as a SIP registration message and generates a unique fingerprint. Changing even a single bit in the input will result in a completely different fingerprint and the nonce value secures that even the same input does not generate the same fingerprint. Antoine Joux proved that it is not hard to find multiple hash collision; finding two messages having the same fingerprint. An attacker can generate a hash collision in a few hours on a standard PC. However, to write a specific message and assign it with a specific fingerprint is more time consuming. RFC 3261 recommends to use MD5 to authenticate registrations and does not allow basic authentication where the user name and password are sent in plaintext. However, this kind of weak authentication was allowed in the previous RFC 2543 [HAN99].

The first step to hijacking a registration is to find a registered IP address [COL05a]. This is easy for internal users who know the structure of the addresses. For external attackers, it is possible to find registered addresses by social engineering or scanning tools. A scanning tool can either generate a single request, or randomly generate a sequence of requests, and thereafter wait for responses to determine if the scanned addresses are valid. If authentication is required during the scanning and hijacking process then the registrar asks for an authentication request. The valid user name and password used to authenticate can be obtained through social engineering or guessing through a dictionary-style attack. In a dictionary-style attack, the attacker tries to log into the system by using different default user names/passwords or by using his knowledge about an employee to guess the user name/password. Dictionary-style attacks can also be pulled off by programs that automatically try to guess passwords. This method is time consuming, and can only be used if the VoIP system does not monitor failed registrations.

Once the target address has been identified, the target's registration can be hijacked. This is done by sending a special register request containing the asterisk character to the target register, which request the register to delete all bindings for the target's SIP address. A second register request containing the attacker's SIP address is hereafter sent and the hijacking is accomplished, see Figure 7.2. Since UAs periodically re-register themselves, the attackers must remove the re-registrations so registration hijacking can continue to function.

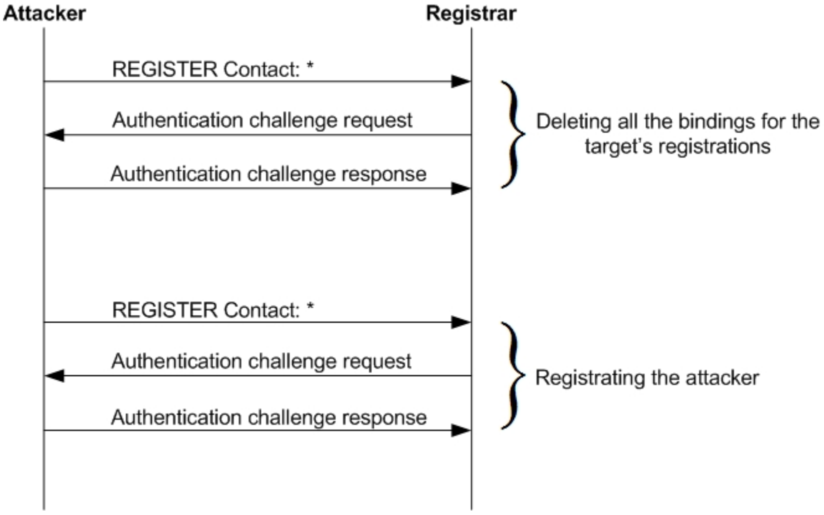

Attacker
Registrar
REGISTER Contact: *
Authentication challenge request
Authentication challenge response
Deleting all the bindings for the target's registrations
REGISTER Contact: *
Authentication challenge request
Authentication challenge response
Registrating the attacker

Figure 7.2: Exchanged messages between the registrar server and the attacker.

Another approach to hijacking a registration is to intercept and modify the register requests that are sent between a UA and a registrar. This attack method is possible with different attack tools but is less common compared to the attack method described above.

Proxy Impersonation

Proxy impersonation describes the situation where an attacker's proxy intercepts the calls that are sent from a UA, either directly or via interleaving proxy/proxies, to a proxy in the callee's domain, see Figure 7.3. Through proxy impersonation an attacker can gain access to all SIP messages, and has complete control of the call. He can trick legitimate UAs and proxy servers to communicate with a rogue proxy server and thereby decide where the calls should be routed.

A proxy impersonation can occur through several means, since UAs and proxies commonly communicate using UDP and do not require strong authentication to communicate with other proxies. The rogue proxy can be inserted into the signaling stream by Domain Naming System (DNS) spoofing, Address Resolution Protocol (ARP) cache spoofing, or simply by changing the proxy address for a SIP phone.

Message Tampering

Message tampering occurs when an attacker intercepts and modifies packets exchanged between SIP components. Message tampering can occur through registration hijacking, proxy

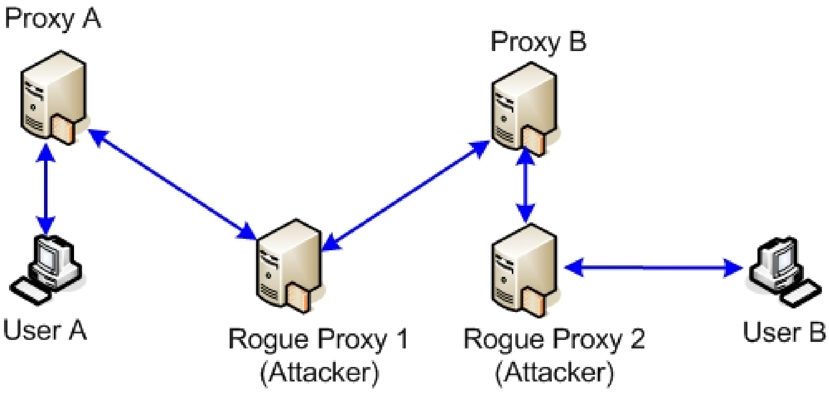


Figure 7.3: Illustration of proxy impersonation.

impersonation, or an attack on any component trusted to process SIP messages, such as proxies, media gateways, or firewalls. S/MIME may used to secure the SIP messages by authenticating and encrypting the text. However, even with S/MIME an attacker can tamper with the routing information since these are sent in plaintext.

Session Tear Down

Session tear down occurs when an attacker observes some parameters of the session, such as the `To` tag and `From` tag indicating the caller and the callee, and then inserts a SIP `BYE` or `re-INVITE` request into the session to either terminate or modify the session. By modifying the session, the attacker has the possibility to redirect the media stream and thereby eavesdrop. Session tear down attacks are difficult to prevent because the necessary fields, such as the destination address, must be sent as plaintext to allow routing.

Denial-of-Service

VoIP systems are more vulnerable to DoS attacks compared to other data systems, due to the QoS requirements. DoS attacks against SIP systems can occur through registration hijacking, proxy impersonation, session tear down or message tampering. Further, flooding attacks on SIP components can be used to achieve DoS by for example flooding the UAs with signaling packets.

7.1.2 H.323 Vulnerabilities

H.323 has been on the market for many years, and is considered as a secure protocol since it has security mechanisms (H.235) built into it. The vulnerabilities mentioned in section 7.1.1 only occur in some extend in H.323, since strong authentication between the H.323 entities is used, and the media stream is also strongly secured.

However, vulnerabilities in H.323 have been found during the past. In January 2004 a number of vulnerabilities in different vendor H.323 implementations (and especially in the sub-protocol H.225.0) were discovered by U.K. National Infrastructure Security Co-ordination Centre (NISCC) [CER04]. The most serious vulnerability was a buffer overflow vulnerability, which could be exploited by an attacker to launch a DoS attack by sending special ASN.1 elements to a vulnerable component.

7.1.3 Network and Media Vulnerabilities

The network itself can be exploited to impact voice services since the voice media traverse over the same physical network as other IP services, consisting of switches, routers and firewalls. One example is DoS on signaling which resembles the classic DoS attack, seeking to overwhelm the signaling element. This can be done by generating a flood of certain signaling requests (e.g., call setup requests) to the IP PBX, the media gateway, or even the IP phone. The targeted device will then be unable to efficiently process legitimate requests. DoS attacks on media are also a serious problem. Since VoIP media is extremely vulnerable to any attack that influences the process of packets in real-time, an attacker will likely feel tempted to congest the network if he wishes to prevent the VoIP service. If the attacker can gain access to a portion of the network where the voice media is present, he can simply inject large number of RTP packets which will contend with the legitimate RTP packets.

Another common vulnerability on the media is the possibility of eavesdropping. Although some VoIP calls are encrypted, most of them are not. Even with encryption it is not a guarantee that eavesdropping cannot take place if there isn't strong authentication. Often eavesdropping is done by a Man-in-the-Middle attack. If the attacker gains access to some unencrypted media he can easily convert it into an audio file by using the attack tool "Voice over Misconfigured Internet Telephones" (VOMIT), see section 7.1.10.

7.1.4 IP Phones and Soft Phones Vulnerabilities

IP phones and soft phones are the least critical part of the VoIP network but at the same time also the most common and least controllable components. The main functionality of IP phones and soft phones is to provide the voice service over the IP network. Attacks on these components are quite frequent since it is easy and cheap for attackers to buy an IP phone and thereby set up and experiment different types of attacks.[3] The main vulnerabilities of IP phones and soft phones which an attacker can exploit are listed below:

DoS: It is seen that several IP phones from Cisco Systems can be forced to restart by using common DoS applications [COL04]. Another possibility to perform DoS attacks is to drown the IP phone with HTTP requests eventually jamming the phone. Both situations will lead to a termination of the active call and thereby a denial of service.

Unauthorized access: This is not a specific type of attack but if access is gained by an attacker to the IP phone it might allow attacks that are beyond DoS. This is especially true if administrative access is gained. The attacker can configure the phone as a Man-In-The-Middle proxy, thus giving the attacker access to all the signaling and media streams.

[3] An IP phone can be bought at eBay at a price from $ 51.00, `http://search.ebay.com/IP-phone_W0QQfkrZ1QQfromZR8`

Protocol implementation attacks: When SIP is used as protocol in the IP phones and the attacker has visibility into the signal he can then send `CANCEL` or `BYE` requests which creates DoS against both or one of the involved phones.

Worms, viruses and other malicious code: They are extremely common on PC's connected to the Internet and an insurmountable problem to defend against. They can be initiated by browsing to a particular web site or through e-mails via attachments, some which do not even require the user to open the attachment. Therefore these vulnerabilities result in an almost unacceptably high risks in the use of soft phones. Although VoIP is a relatively new technology for sending voice communication, the data is still transported over the same network infrastructure that has recently been troubled by Slammer, SoBig and Nimda (worms and virus). The situation with VoIP is therefore not going to be any different since it runs on the same platforms that are currently affected by virus, worms and other malicious code. So the lack of security patching and security fixes that are common in the data world must also be overcome in the VoIP world. Separation of voice and data networks to the greatest extent possible and practical will be described in Chapter 8. The use of a soft phone system conflicts with the purpose of this separation.

Upgrades: Since all IP phones are programmable they can be upgraded with new firmware through for example Trivial File Transport Protocol (TFTP) which is not secure. Using TFTP can allow a Trojan or root kit to be placed in the IP phone resulting in either DoS or unauthorized access.

The above mentioned attacks should not be seen as the complete set of attacks on IP phones or soft phones, but merely a selection of the important and common ones. There are many more attacks that can have influence on the IP phones indirectly, such as general attacks on the data network.

7.1.5 IP PBX Vulnerabilities

The vulnerabilities on IP PBXs are considered as the most critical in VoIP systems due to their role in providing voice services. This makes IP PBX the primary target for the attackers since they can gain control over the entire VoIP network through the IP PBX.

The simplest way to attack an IP PBX is by exploiting the well-known vulnerabilities in the IP PBX software. Usually it runs commercial operating systems including Windows 2000 which has a history of vulnerabilities. Since IP PBX must handle different services, such as multiple calls, it runs extra software programs that also have vulnerabilities.

IP PBXs are managed through a web-based or a network client. In many cases companies allow a third-party to have remote access to the IP PBX to maintain the system. This will make it easier and faster to fix a system in case of failure. Although this practice is flexible and ideal economically it opens up for a large number of critical security risks. For easy management, companies often use well-known standards for setting up the IP PBX for maintenance which can easily be exploited by an attacker. If an attacker acquires the phone number of the modem, he simply has to log in by using an automated script to guess the administrative login and password. In general, default and weak passwords are the most commonly exploited vulnerability on IP PBXs. If the attacker has successfully logged on the IP PBX he can take control of the entire VoIP system.

7.1.6 Remote Access

It's common that some employees work from outside their office, also called a remote office. A remote office can for example be an employee working from a customer's office, from a hotel during business travel or from a home office. To optimize the working procedures from a remote office, it's important that the employee has remote access to the company network. The remote access can be gained by connecting into the office over GSM, PSTN, ISDN or higher speed connections such as Asymmetric Digital Subscribe Line (ADSL). In general, any network that can connect an employee to the Internet may be used.

Companies with a VoIP system have the opportunity to give the remote offices access to the VoIP system and thereby omitting expenses of using traditional and mobile phones at the remote offices. If a remote office already has a remote access to the company network then the remote office can communicate through the VoIP system simply by connecting a soft phone to the computer. The remote access can be implemented by different methods. However, Virtual Private Network (VPN)[4] is the most deployed technology for remote access.

By allowing remote access to the VoIP system the companies open up for new access points to their network. In general, these remote access points are more vulnerable against attacks compared to the access points that are placed inside the company network. First of all, the modem used to connect is physically less secure compared to the component placed within the company. Further, there is the risk that an employee sets up an unauthorized modem or other components that may not be approved, such as wireless routers.

7.1.7 Denial of Service Attacks

As mentioned earlier, VoIP systems are more vulnerable to Denial of Service (DoS) attacks compared to other data systems, due to the QoS requirements. VoIP is a real-time application, and it's therefore important to deliver the voice packets within a short period of time. For instance a delay more than 150 ms [KWF05] between two VoIP terminals will make the VoIP conversation unacceptable for business use.

The goal of a DoS attack is not to gain unauthorized access to a system, but instead to prevent legitimate users to access the system or services. The attacker's motive can be to drive his competitors out of the market by shutting down their system or degrading the QoS so their system does not work as intended.

There are many ways an attacker can pull off a DoS attack. An attacker can for instance send packets to a target VoIP system, causing it to fail or resulting in loss of function for an IP PBX. Another approach to accomplish a DoS attack is to flood the target VoIP system with many packets, which will overwhelm the system and prevent request from legitimate users to be handled. It is hard to distinguish between a DoS that is caused by a flooding attack and a DoS that is caused by legitimate requests. A network has a limited capacity and

[4] See section 8.2 for a description of VPN.

exceeding this capacity with even legitimate requests will cause a DoS. Though the attack is discovered, it is difficult to expose the attacker since they usually send packets with spoofed or useless return addresses. Common types of DoS attacks are discussed below:

Buffer overflow: This is one of the most common kinds of DoS attack. It occurs when a program or process tries to store more data in a buffer than it was intended to hold. The buffer has a finite amount of capacity to store data. The extra data may contain codes designed to trigger specific actions such as sending instructions to the target system that could damage it.

SYN flood: As mentioned earlier, a TCP connection is established when a three-way handshake is completed. When a server receives a TCP packet with the synchronization (`SYN`) flag set from the client, it will reserve the memory for the connection and then return a TCP packet with both the `SYN` and `ACK` flag set to the client. The reserved memory will be liberated when the client finishes the three-way handshake by sending an `ACK` packet.

In the SYN flood attack, the attacker floods the target system with several TCP `SYN` packets with a spoofed source IP address. The server will never receive an `ACK` packet from the client, since the client's source address was spoofed. The memory allocated in the server will therefore never be liberated and the server will run out of memory if there are many half-open TCP connections. This will prevent further TCP connections to establish connections to the server.

Distributed DoS (DDoS): As the name indicates, the attacker here uses distributed techniques to pull off the attack. DDoS attacks are DoS attacks, for instance SYN flood attacks, that come simultaneously from many hosts all over the Internet. The attacker uses well known vulnerabilities to install a malicious slave program on as many hosts as he can. The slave program waits for instructions from a master program which is installed somewhere on the Internet. When the attacker sends a message to the master program indicating the IP address of the target, then the master program forwards the target address to each of the slave programs. The slave programs now flood the target system with enough traffic to overwhelm it and thereby causing a DoS.

The message from master program to slave programs usually has spoofed source address which will make it more difficult to identify the master program. However, the attacker does not bother to use spoofed source address for the packets sent from the slave programs to the target, since there are many slave hosts. So innocent users, whose PC's act as slaves or zombies might be exposed.

These attacks along with other types of DoS attacks are discussed in more details in [CBR03, RAN05].

7.1.8 Spam over Internet Telephony

Spam over Internet Telephony (SPIT) occurs when many unsolicited calls are being carried out over the Internet. The reasons for generating SPIT calls are the same as sending e-mail spam. In most cases the purpose is either to sell a commercial product or committing fraud by tricking the callee. VoIP simplifies the task of generating large number of SPIT calls due to the low cost of calling over Internet and the use of automated scripts. The low cost give the opportunity to operate from a foreign country where there are no or limited telesales and telemarketing legislation. Furthermore, it is tempting to use automated scripts to send unsolicited messages to many people in almost no time. Companies can also experience audio equivalent to phishing where attackers leave SPIT voice mails pretending to be someone from the financial institute or e-commerce site to gain personal or financial information. Or it could simply be used as a practical joke sending out a voice message to the employees of the company saying that everyone gets the day off.

The sender of SPIT calls knows that the majority of SPIT call receivers will terminate the call as soon as they discover that they are being spammed. However, the SPIT attackers are satisfied if just a minority of the callees takes the time to listen to the call.

In contrast to e-mail spam, SPIT calls have to be attended when they are received or else they will be redirected to the voice mail. Attending a large number of SPIT calls is time consuming, and can in worst case scenario cause denial of service if all the telephone lines get occupied by SPIT calls. As for e-mails, it is therefore very important to filter the incoming SPIT calls. However, filtering SPIT calls is much harder than filtering e-mail spam since it is difficult to distinguish between SPIT and legitimate calls during the signaling process. The content of a call will first be revealed when the call has been established and the caller starts sending voice messages. Since it is easier for a caller to hide his identity in a VoIP system compared to a PSTN caller, it is expected that SPIT will become more common with the deployment of VoIP systems.

7.1.9 Wireless VoIP

Wireless LAN (WLAN) offer many additional advantages compared with the wired LAN, such as mobility and easier portability. Companies are using more and more wireless equipment since these give their employees better working facilities, such as being able to speak on the phone while they are on their way to a meeting or going outside the office. Typical examples of wireless equipment in the telecommunication business are mobile phones and wireless handsets.

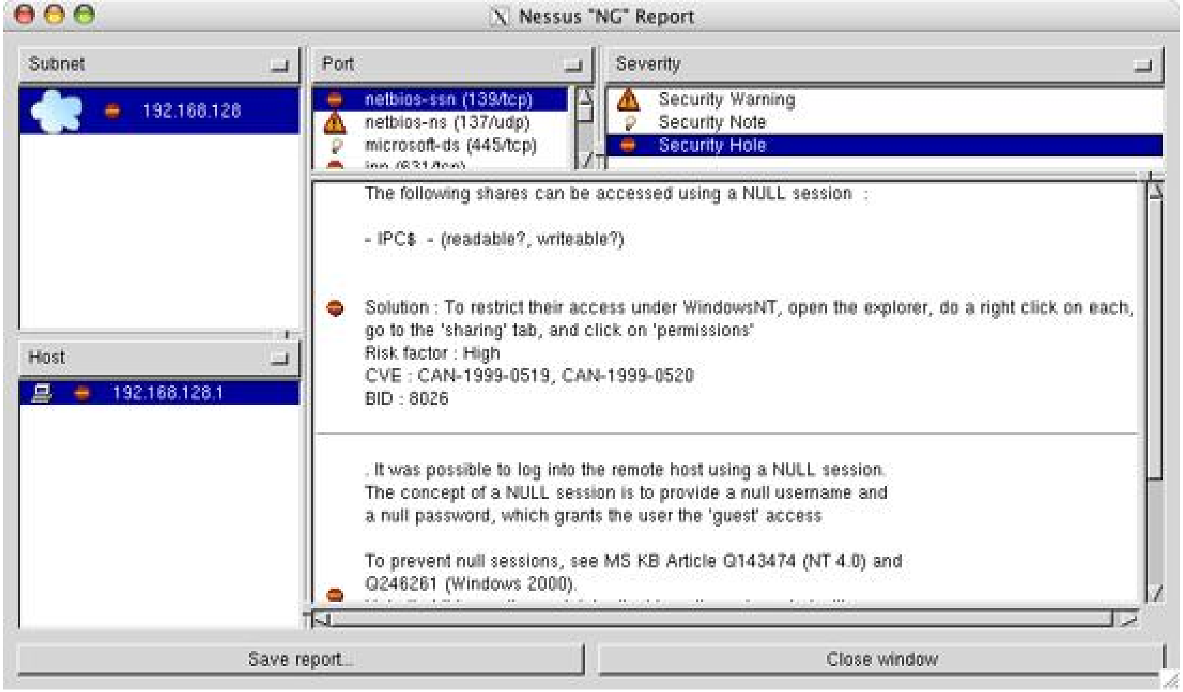
Transmitting voice over WLAN has gained a lot of research attention. As mentioned above there are advantages by using wireless technology but these advantages have to be weighed against the vulnerabilities that are related to them. Wireless VoIP systems inherit all the vulnerabilities that exist in wired VoIP systems and additionally have vulnerabilities such as interference, jamming and easier network access for attackers. Another downside with WLAN is that they are comparatively slow compared to the wired LAN which can give problems with the QoS requirements for VoIP systems.

The integration of wireless equipment with VoIP systems is an interesting topic since it is a new technology and therefore has yet to be adopted by many companies.

7.1.10 Scanning Tools

More websites today give the opportunity to practice ones hacking abilities and the possibility of downloading different scanning tools.[5] Publications of exploitation tools are becoming more common, thus resulting many attacks from less technical individuals, such as script kiddies, who leverage the work of others to achieve their goals. An example of an exploitation tool used for eavesdropping is VOMIT[6] which is a Unix-based software utility that converts voice packets captured by another Unix tool, tcpdump. It then converts the retrieved packets into a wave file that can be used to listen to over the speakers of a computer. The commands used to intercept VoIP traffic are terminal based and quite trivial.[7]

Another tool that can be used for exploitation of a VoIP network is Nessus[8]. This tool is an open source vulnerability scanner that can be used by persons with malicious intent in mind to scan a VoIP component, for example the VoIP proxy server, to locate vulnerabilities. On the other hand, it is also a useful tool for administrators to locate weaknesses in their system. In fact, the program generates a complete vulnerability report identifying all of the common security holes and ports that are open in the network system making it easy for a script kiddie to break in.



```
The following shares can be accessed using a NULL session :

- IPC$ - (readable?, writeable?)


Solution : To restrict their access under WindowsNT, open the explorer, do a right click on each,
go to the 'sharing' tab, and click on 'permissions'
Risk factor : High
CVE : CAN-1999-0519, CAN-1999-0520
BID : 8026

. It was possible to log into the remote host using a NULL session.
The concept of a NULL session is to provide a null username and
a null password, which grants the user the 'guest' access

To prevent null sessions, see MS KB Article Q143474 (NT 4.0) and
Q246261 (Windows 2000).
```

Figure 7.4: Screen dump of a Nessus report.

The last tool that will be described here is ettercap. This tool can be used in a Man-In-

[5] Some examples of hacker-practice sites are `http://academy.dyndns.org/`, `http://www.blind-dice.com/`and `http://www.learntohack.org/`.

[6] VOMIT is freely distributed and can be downloaded from `http://vomit.xtdnet.nl/`.

[7] A complete guideline for using VOMIT is provided at `http://nestonline.com/TrinuxPB/vomit.txt`.

[8] Nessus can be downloaded from its official web site: `http://www.nessus.org/`.

the-Middle attack to reset the ARP information on the phone and on its gateway router. The IP phone sends a `Hello` packet request approximately every 30 seconds to the IP PBX to indicate that it is active on the network. During this procedure the ettercap attack can be initiated.[9]

7.2 Risk Assessment

While the previous sections identified the risks associated with VoIP systems, this section gives an overall assessment of the risks by calculating the risk level for each identified risk. This can be done by using the risk level matrix from [SGF02] where each risk level is based on assessing the likelihood for a threat and assessing the impact of a threat. These assessments are divided into three grades, "Low", "Medium" and "High". The risk level matrix and the definition of the grades are omitted here, since they are described sufficiently in [SGF02] which is enclosed in Appendix B.

It has not been possible to find any statistics on how the identified VoIP risks are distributed and how common they are because of two reasons. First of all DK-CERT have not received any reports on attacks that are specifically aimed against VoIP systems. Secondly, it is difficult to distinguish between an attack that is specifically aimed against a VoIP system and an attack that is aimed against a general IP network. Both of these attacks can be carried out by using the same attack methods, and by attacking the same components.

The authors of this thesis have therefore chosen to let the likelihood of a threat be depended on estimations contrary to statistical calculations. The estimations are based on statements from different parties involved in this project, see Appendix G, and information gained during the project. Table 7.1 shows the evaluated likelihood for each risk together with the corresponding risk impact and calculated risk level. In addition, the table shows whether each risk result in loss of confidentiality, loss of integrity and/or loss of authentication. These are shortened as "C", "I" and "A" respectively in the table.

Table 7.1: Risk assessment.

Attack Description	Likelihood	Attack	Risk Level	C	I	A
SIP Vulnerabilities						
Registration hijacking	Medium	Low	5 (Low)	√		
Proxy impersonation	Low	High	10 (Low)	√	√	√
Session tear down	Low	Medium	5 (Low)	√		√
DoS against SIP components	Low	Medium	5 (Low)			√
H.323 Vulnerabilities						
Registration hijacking	Low	Low	1 (Low)	√		
Gatekeeper impersonation	Low	High	10 (Low)	√	√	√
Session tear down	Low	Medium	5 (Low)	√		√
DoS against H.323 components	Low	Medium	5 (Low)			√
Media Vulnerabilities						
DoS	Medium	Medium	25 (Medium)			√
Man-In-the-Middle	Medium	Medium	25 (Medium)	√	√	

Continued on next page

[9] Visit `http://ettercap.sourceforge.net/` to download ettercap.

Table 7.1 – continued from previous page

Attack Description	Likelihood	Attack Impact	Risk Level	C	I	A
IP Phones and Soft Phones						
Unauthorized access	High	Low	10 (Low)	√	√	√
Worms, viruses and other malicious code	High	Low	10 (Low)			√
Compromising media channel upgrade	Low	Low	1 (Low)	√	√	
DoS	Medium	Low	5 (Low)			√
IP PBX Vulnerabilities						
Compromising software vulnerabilities	Medium	High	50 (Medium)			√
Unauthorized remote access	Low	High	10 (Low)	√	√	√
Remote Access						
Unauthorized access to the remote modem	Low	Medium	5 (Low)			√
Installation of non-approved components (such as router) by an employee	Low	Medium	5 (Low)	√	√	√
Compromising the VPN connection	Low	Medium	5 (Low)	√	√	√
Other						
SPIT	Low	Medium	5 (Low)			√

It is noticeable that nearly all of the VoIP risks mentioned in Table 7.1 results in loss of availability. This is because it is easier to delay the voice packets to reach their destination compared to eavesdropping or modifying the voice packets. Another noticeable aspect is that none of the risks have the grade ”High” as their risk level. Furthermore, only two risks have the grade ”Medium” as their risk level while others all obtain the grade ”Low”. The reason for the lack of high risk levels is that precautions have been taken to secure against risks that can damage the entire VoIP system. Furthermore, the assessment is based on the current situation where there are not many known cases of VoIP attacks. The risk level for each risk is likely to increase in the future as knowledge about VoIP systems become more common and more companies implement them.

7.3 Summary

The main risks in a closed VoIP system have been described as well as how to exploit the risks in actual attacks. SIP and H.323 vulnerabilities include registration hijacking, proxy impersonation, message tampering, session tear down and DoS attacks while other VoIP vulnerabilities on the IP phone and IP PBX were described as well. Different scanning tools were introduced as well as the possible emerging problems of SPIT. The chapter ends by giving a risk assessment of the risks associated with VoIP systems. The risk assessment shows that currently no risks can be characterized as “High” as VoIP is still a new technology that has yet to be a favourable target for attackers. In addition, there are not any statistics indicating a high likelihood of VoIP specific attacks. As VoIP becomes more popular it is expected to be more exposed to attacks.

Chapter 8

Technologies

There exists a number of technologies and methods that can resist the security risks mentioned in Chapter 7. In this chapter, some of the most widespread technologies are described which also provides the basis for the best practices and recommendations for securing a VoIP system. The technologies described here are a result of how security problems can be solved to the greatest extent possible using standard products that are already in use today.

8.1 Virtual LAN

As voice and data traffic traverse over the same physical network in VoIP it can give delay and jitter within the network and thereby affecting the quality of service. Moreover, VoIP systems can be affected by vulnerabilities of other services that traverse on the same physical network as the voice traffic. Using separate physical (packet-switched) networks for the voice and the data traffic can help avoid these problems. However, this solution is not ideal due to the large amount of investment that is required to implement an extra physical network.

A more appropriate approach is to use a technology called Virtual LAN (VLAN) which can be implemented in most switches today [UCD98, MAI03]. This allows administrators to logically segment one or more LANs into VLANs. Users and components will communicate with each other as if they all were physically located on the same LAN. Furthermore, several VLANs can exists on a single switch, giving possibility of creating many VLANs within the same LAN, see Figure 8.1. For instance, it can be advantageous that each department in a company have their own VLAN as the communication within each department can be high. Other advantages by segmenting LANs into VLANs are following:

Performance: VLAN can reduce the need to send broadcast and multicast traffic to unnecessary destinations since this kind of traffic is only sent to the members of the given VLAN. Furthermore, VLANs create broadcast domains using switches instead of routers. This improves the performance since switches require less processing time of incoming traffic compared to routers.

Manageability: VLANs are easy and flexible to manage. They are configured through software rather than hardware, and when a member of a VLAN, for example an IP phone, is physically moved within a LAN, it can stay on the same VLAN without any hardware reconfiguration. Finally, VLAN allows administrators to centralize management of components that are physically located on different networks.

Security: Traffic from one VLAN to another is prevented, unless it is allowed by routers. The access to sensitive data by outsiders can be reduced by placing users and components that has access to this data on their own VLAN.

The main disadvantage by using VLANs is that traffic between two different VLANs has to be routed which might give problems with regards to performance.

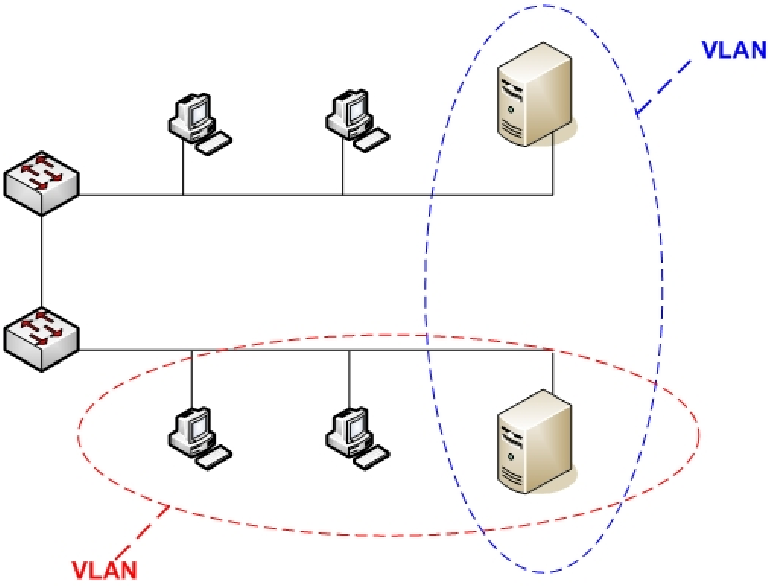


Figure 8.1: VLAN infrastructure.

The traffic from VLANs must be separated from each other to assure that their broadcast do not overlap. This is commonly done by packet filtering and packet identification. The concepts of packet filtering in VLANs are very similar to those used in routers where the routing decisions are based on routing tables (called filtering table in relation to VLAN). The packet identification is a new approach specifically developed for switched networks. In packet identification, a unique identifier is written in each packet header as it is forwarded in the VLAN. The identification headers assure that the packets are only received by those who are members of the given VLAN. Packet identification requires little processing time and gives less overhead, compared to packet filtering, since it functions at layer 2 of the OSI model. The most common ways to implement VLAN is by using the IEEE's specified protocol called 802.1q or Cisco's Inter-Switch Link (ISL).[1]

The membership of a VLAN can be defined by different methods at different layers:

[1] See `http://standards.ieee.org/getieee802/download/802.1Q-2003.pdf` and `http://www.cisco.com/en/US/tech/tk389/tk390/technologies_tech_note09186a0080094665.shtml` for a detailed description of 802.1q and Cisco's ISL.

- At layer 1, the membership can be defined based on the ports that belong to the VLAN. The disadvantage by this classification is that the VLAN has to be reconfigured when a user moves to a different location (unless he stays physically connected to the same bridge).
- At layer 2, the MAC address of the components and the protocol type fields found in the layer 2 headers can be used to define the members of the VLAN. The method of using the MAC address requires that the VLAN members must be defined initially which is difficult in networks containing several hundred users.
- At layer 3, the network IP address can be used. This method allow users to move their terminals without reconfiguring the network address. However, it generally takes longer time to forward packets using layer 3 fields compared to the layer 2 fields (such as using the MAC address).
- At a higher layer, the membership can be defined based on applications.

A LAN containing voice traffic can be logically segmented and classified at different layers. Only layer 1 and layer 2 classifications are supported in 802.1q. The most obvious way to separate the voice and data traffic is by using the protocol type field. For example, a VLAN can be configured to only allow real time traffic which can be identified by the RTP header field.

All voice traffic can be configured into a single VLAN or be divided into several VLANs. For instance, it can be beneficial to isolate IP PBXs, VoIP servers and groups of IP phones on their own VLAN so the traffic does not interact with other servers. Some vendors, such as Avaya, go a step further by placing each IP phone on its own VLAN. This can give scalability and management issues in large VoIP systems.

There are some vulnerabilities with VLANs. These and their attack methods are described in [ROU04]. In general, the primary choice of using VLANs should not be because of security considerations since VLANs only deliver little security improvement compared to ordinary LANs. But VLANs have one great advantage that diminishes the disadvantages; by separating the voice and data network it is possible to make the voice service less vulnerable to attacks directed against the data part of the network. VLANs should also be used to gain advantages in performance, manageability and functionality.

8.2 Virtual Private Network

Virtual Private Network (VPN) is a technology that establishes a private network within a public network, such as the Internet [RAN05, COM, KUR01]. A private network is a network where all the data paths are only visible to a limited group of users. The simplest approach to creating a private network is to isolate it entirely from the public network. It can be implemented using Frame Relay, ATM, or some other form of leased-line solution. Using leased-line solutions can become cost prohibitive and not be practical for companies with remote offices.

There are basically two types of VPN technologies, client-to-LAN and LAN-to-LAN. Client-to-LAN VPN is generally implemented through software running on a user's computer and is the most common type of VPN used by PCs at home offices. Thus, it can be used by remote users to establish a secure connection to the corporate VoIP system. LAN-to-LAN VPN technology often uses hardware VPN routers to establish a virtual network between two or more independent LANs. Figure 8.2 illustrates a client-to-LAN VPN solution. Remote users can connect to the corporate network by using their VPN client to establish a connection to the VPN server managed at the company site. Once the connection has been established, the remote user can communicate with the company network as if he was communicating from the internal LAN itself.

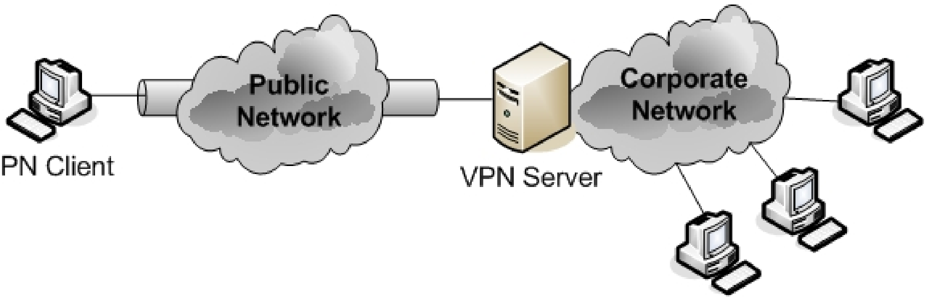


Figure 8.2: Client-to-LAN VPN.

The VPN technology is based on tunneling. Tunneling is a technique that uses a public network to transfer data from one network over another network. The tunneling process consists of payload encapsulation, transmission, decoding and routing. The payload to be transmitted can be sent in packets that are built using another protocol. These packets are built by encapsulating the original packets with new headers so the original header information will only be visible by the tunnel-endpoints. The most widespread tunneling technologies used in VPN are Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP) and IP Security (IPSec).

8.2.1 Point-to-Point Tunneling Protocol

Point-to-Point Tunneling Protocol (PPTP) is a tunneling protocol developed by Microsoft and several other remote access vendors, known as the PPTP Forum [COM, SMI99, SMW99].[2] It works at layer 2 of the OSI model and can be considered as an extension to PPP[3]. PPTP encapsulates PPP frames within IP packets by using a modified version of General Routing Encapsulation (GRE) to get data to and from its final destination, see Figure 8.3.

The security in PPTP can be divided into three areas; authentication, data encryption and PPTP packet filtering. PPTP can use one of several PPP authentication protocols, including Extensible Authentication Protocol (EAP), Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) version 1 and version 2 and the plaintext Password Authentication Protocol (PAP). Of these, MS-CHAPv2 and EAP-TLS are considered the most secure protocols because they provide mutual authentication, in which both the VPN server and the VPN

[2] A RFC draft of the PPTP can be found at http://infodeli.3com.com/infodeli/tools/remote/general/pptp/draft-00.pdf.

[3] PPP is an IETF standard defined in RFC 1661 [SIM04].

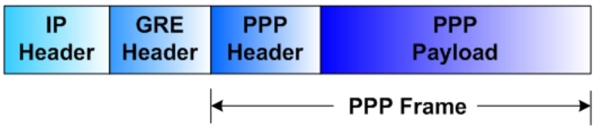


Figure 8.3: PPTP packet structure.

client verify themselves. The payloads inside the PPP frames are encrypted using Microsoft Point-to-Point Encryption (MPPE). MPPE uses the RSA (Rivest, Shamir, and Adleman) Rivest Cipher 4 (RC4) algorithm to provide data confidentiality and can use RC4 session keys up to 128bit. As the name indicates, PPTP packet filtering only allows PPTP traffic to enter the private network.

Microsoft's PPTP is not considered to be secure and several vulnerabilities have been found [SMW99]. There are weaknesses in the most common authentication protocols, MS-CHAPv1 and MS-CHAPv2. MS-CHAPv2 improves the security compared to MS-CHAPv1 by eliminating the LAN Manager hash. In MS-CHAPv1 the LAN Manager hash and Windows NT hash values were sent parallel from the client to the server and was generated based on the same user password. Since the LAN Manager hash is considered weak, password-cracker programs were able to crack the LAN Manager hash and then use that information to crack the Windows NT hash. MS-CHAPv2 is considered to be vulnerable against weak passwords because of the encryption mechanism used. Furthermore, there are weaknesses in the RSA RC4 encryption algorithm since the encryption key is based on the user password and the same encryption key is used by both the server and the client.

Although Microsoft have fixed some of the PPTP's security holes, there are still weaknesses that make PPTP questionable as a secure VPN protocol. All the control operations in the PPTP, such as connection setup and management, are done through a plaintext channel without any authentication. This weakness can be exploited to launch DoS attacks and gain information about the PPTP servers by analyzing the unencrypted and unauthenticated control channel [SMI99].

8.2.2 Layer 2 Tunneling Protocol

Layer 2 Tunneling Protocol (L2TP) is an IETF standard protocol defined in RFC 2661 [TOW99] and provides, like PPTP, tunneling of PPP frames. L2TP tries to merge the best features of Microsoft's PPTP and Cisco System's Layer 2 Forwarding (L2F) protocol.

In contrast to PPTP, L2TP can run over a variety of physical topologies such as X.25, Frame Relay and ATM. However for practical purposes, vendors implement L2TP over UDP for use with Internet tunneling. L2TP encapsulates PPP frames inside L2TP frames which are then sent over the Internet using UDP (GRE encapsulation is not used), see Figure 8.4. By using UDP, L2TP is more appropriate for real time services, such as VoIP systems, compared to PPTP.

L2TP does not deliver security by itself, but instead requires that the underlying transport protocol makes the necessary encryption, integrity and authentication for all the L2TP traffic.

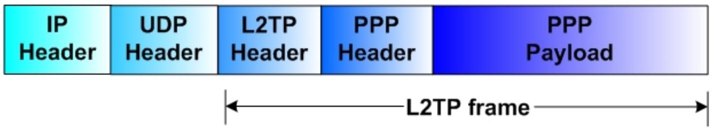


Figure 8.4: L2PT packet structure.

This can either be done by using the security in PPP, which is considered weak, or by using IPSec.

8.2.3 IP Security

IP Security (IPSec) is a set of protocols developed by IETF to provide security at the IP layer. Several documents are written to define the different set of protocols in IPSec. RFC 2411 [THA98] gives an overview of these documents and describes the IPSec architecture. IPSec is widely used in VPN and can either be used as a complete VPN protocol solution or simply as an encryption scheme within PPTP or L2TP.

IPSec uses two protocols to provide security: Authentication Header (AH) and Encapsulating Security Payload (ESP). These protocols are defined in RFC 2402 [KEN98a] and RFC 2406 [KEN98b] respectively and may either be used separately or in combination. AH provides data authentication and protection against replays. The authentication is provided for as much of the IP header as possible as well as the upper layer protocol data. Some IP header fields may be changed as they are transported over routers and other network components and can therefore not be end-to-end encrypted. ESP provides encryption and authentication. In contrast to AH, ESP does not authenticate the IP headers. AH and ESP support two modes, transport mode and tunnel mode.

- In the transport mode, the protocols provide primary protection for the upper-layer protocols. ESP encrypts and authenticates the data in the IP packets, but not the IP header itself. AH authenticates the data and a part of the IP header.
- In the tunnel mode, the entire IP packet including the IP header is tunnelled through the network. A new IP header is added to provide the source and the destination IP address. However, these IP addresses can be different compared to those in the original IP header. ESP encrypts and authenticates the entire original IP packet. AH authenticates the entire original IP packet and some of the IP header fields in the new IP header.

Figure 8.5 and Figure 8.6 illustrates the IPSec packet structure for the transport mode and the tunnel mode.

Even though IPSec is algorithm independent, there are some encryption and hashing algorithms which IPSec must include. These are DES, MD5, SHA and two Diffie-Hellman key sizes. The agreement of which encryption algorithm should be used, has to be decided by the VPN client and the VPN server during the connection setup. This agreement is referred as

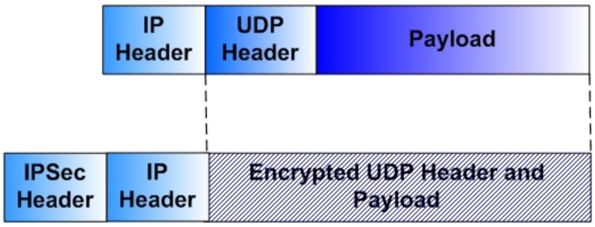


Figure 8.5: IPSec packet structure for transport mode.

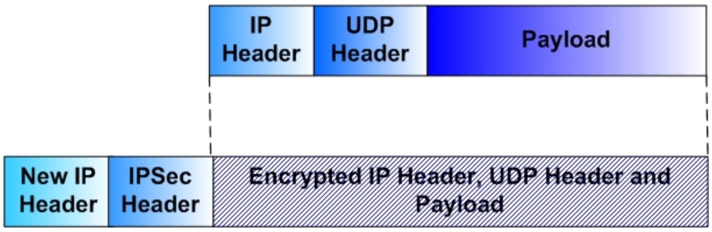


Figure 8.6: IPSec packet structure for tunnel mode.

the Security Association (SA). IPSec allows authentication through shared secrets and certificates. This is considered much more secure compared to PPTP where the authentication is based on user passwords. At this time, IPSec is considered as the most secure tunneling protocol compared to PPTP and L2TP. However, several vulnerabilities and weaknesses in IPSec implementations and protocol have been exploited [CLA02].[4]

The process of IPSec encryption/decryption within the network and the lack of QoS in its crypto engine can cause large amount of latency in the VoIP packet delivery. Tests by NIST have shown that IPSec can be integrated into SIP network with a 3 second addition delay in the call setup, which can be considered as an acceptable delay for many VoIP systems [RAN05].

8.3 Multi Protocol Label Switching

There has been a great motivation to overcome the existing problems associated with IP networks especially the destination-based forwarding that IP routers use. One of the greatest motivations was the increasing need for faster and easier transportation of IP packets as well as the need of traffic engineering. This new procedure is essential for voice traversal which is very dependent on QoS parameters. The IP address lookup in routers where the longest prefix match is required is a complex process and slow for core networks. Multi Protocol Label Switching (MPLS) uses lookup techniques based on a simpler forwarding mechanism and provides many advantages when voice is an integrated service in the data network. However, MPLS does not introduce new security features, but is merely a new technology that makes QoS possible. As the protocol name indicates MPLS exploits label-switching forwarding which is considered more desirable than destination-based forwarding because of its low-cost

[4] Search on `www.cert.org` for information on IPSec vulnerabilities.

hardware implementation, scalability to very high speeds and flexibility in the management of traffic flows. MPLS uses integrated ATM switches and IP routing in the nodes. The following sections describe in more technical detail how MPLS works. This section is based on [GAR04, RAN05, AWD99].

8.3.1 Forwarding and Routing

MPLS has various functionalities and capabilities. One of these is the ability to support all the layer 3 protocols, with the initial focus on IPv4 and IPv6. In addition to this MPLS is able to operate on top of layer 2 technologies such as ATM, frame relay and PPP, thus giving a company the possibility for implementing a VoIP solution on top of their existing infrastructure using MPLS.

The Label-Switching Router (LSR) is a router that supports MPLS by integrating routing and switching functions. The LSR separates the routing and forwarding components as shown in Figure 8.7.

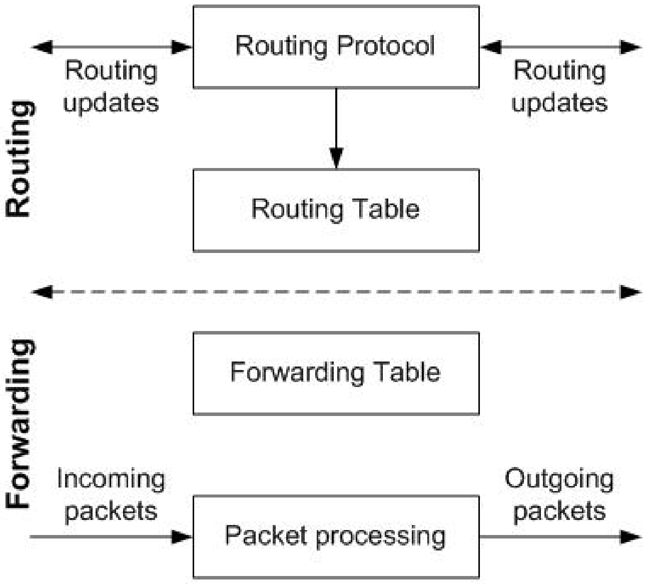


Figure 8.7: The routing and forwarding procedure.

The forwarding components perform the label switching and provide the fast data paths. It can be done by any layer 2 technology. When a LSR interfaces with a traditional router it is called an edge LSR. There are two terms when dealing with traffic to and from an edge LSR. The edge LSR is said to be ingress when it receives traffic from a non-MPLS router while it is said to be an egress LSR when the traffic is sent to a non-MPLS router.

8.3.2 Label Distribution

A way to distribute label bindings is needed in order to create the forwarding tables in the LSRs. The Label Distributing Protocol (LDP) is the main protocol created by the MPLS working group. Other protocols such as the Border Gateway Protocol (BGP) and ReSerVation Protocol (RSVP) can also be used to distribute the labels.

To enable the LSR peers to discover each other `Hello` messages are periodically sent out using UDP. When the Label Swicthed Paths (LSPs), which are tunnels used for the IP transportation, discover each other in this way a TCP connection is established and a LDP session can be initiated. LDP is run over TCP (except the discovery messages) in order to reap the benefits provided by TCP such as reliability and in-order delivery.

Other LDP messages include `initialization` and `keep alive` messages. `Initialization` messages are sent in the beginning of a LDP session so that peer LSR can agree on a number of parameters for the session. The `keep alive` messages are sent periodically to let peer LSRs know that the given LSR is still working if no other messages are sent.

When an upstream LSR needs to establish a LSP it sends a label request message to its downstream peer which in turn is replied to by a label mapping message. The label mapping messages allocate the labels to Forward Equivalence Classes (FECs) which are a group of packets that are forwarded in the same manner. Label bindings are in this way distributed upstream.

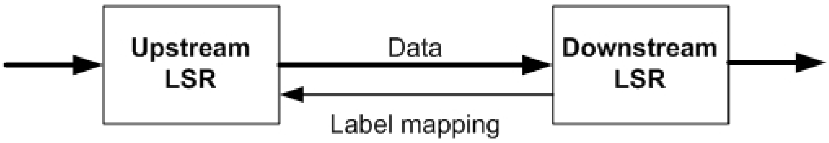


Figure 8.8: Upstream and downstream LSRs - Label bindings are distributed upstream through label mapping messages.

The label bindings associate labels to certain FECs and have to be negotiated between the LSRs. A number of modes for distributing the labels in LDP exist which have to be negotiated between LSRs when LSPs are created.

Two assignment modes exists; "downstream-on-demand" mode and "unsolicited downstream" mode. When an upstream LSR running in "downstream-on-demand" mode has a FEC with a given downstream LSR as its next-hop, it will send a label request downstream. This will, in turn, be answered with a label binding message that tells which label to be associated with the FEC. In unsolicited downstream mode the downstream LSR can distribute label bindings upstream even if they are not requested. Two options are also provided when determining the way the LSPs are set up. In ordered control the label-FEC bindings are initiated at the egress LSR and then they make their way backwards to the ingress LSR. This approach reduces the risk of looping paths being created in the network. It also makes it easier for an administrator to control when MPLS should be used which can be advantageous in a network under migration to MPLS. On the downside it takes more time for the LSP to be created. The alternative is independent control where the individual LSRs can make label bindings to its peers. In this way the advantages of ordered control are lost but waiting time for setup of a LSP is reduced.

The last option is the choice between liberal and conservative label retention. In liberal label retention mode the LSRs keep the allocated label-FEC bindings even if they are not needed at the time of allocation. This can result in faster response to changes in the routing as the labels may already be allocated for the new route. The downside of this method is the greater number of labels needed. In conservative label retention mode only the needed label-FEC bindings are kept.

8.3.3 Multiple MPLS Domains and Label-Stack Operations

When a voice packet enters a MPLS domain at the ingress LSR a MPLS header is attached to the packet using a push operation. At each LSR on the route in the domain the label is swapped according to the routing tables. When the voice packet leaves a domain a pop operation is applied thereby removing the header. It is possible to have more than one MPLS header attached to a voice packet if one MPLS domain is nested inside another as illustrated in Figure 8.9. In this way a tunnel is effectively created through the inner domain thus possibly reducing the required routing of the LSP. An analogy to having more levels in the hierarchy is the classic example of local roads and highways. Going on the highway makes it simpler to find your way and increases your speed.

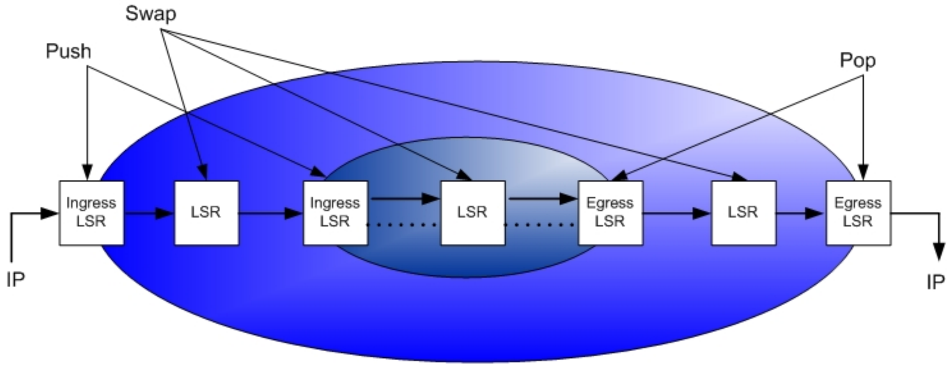


Figure 8.9: An illustration of two MPLS domains nested inside each other. In this way tunnels can be created through the network as illustrated by the dotted line.

8.3.4 Traffic Engineering

Traffic Engineering (TE) is the aspect of network engineering that addresses measurement, modelling, characterization and control of traffic. The achievement of reliable operation and high utilization of resources is also a part of traffic engineering. It is the process of dynamically controlling traffic data flows, optimizing the availability of resources by moving traffic flows towards less congested paths by choosing routes taking into account traffic loads and the network state. With good TE it is possible to increase the value of a network, thus making VoIP quality better.

RSVP is, as mentioned earlier, an alternative to LDP. An extension named RSVP-TE allows traffic engineering to be incorporated in the MPLS network. With this extension it is possible for the ingress LSR to decide the entire route the voice packets have to follow. The list of nodes along the specific route is sent downstream in a path message.

This property is called “explicitly routed” LSP and results in network optimization which would not otherwise be possible. It means that traffic routed over congested connections can be routed through other less loaded channels if such exist. The ingress node has to know about the state of the network in order to compute an efficient way through the network; this knowledge can for example be obtained from a link state database. Another property of RSVP-TE is the possibility to let some LSPs have a higher priority than others which can be a useful property when a certain QoS level is desired.

Another way that MPLS can obtain TE is through the use of an extension to LDP called Constraint-Based LDP (CR-LDP). This expands the label request messages with an explicit route field in order to support explicit routing essential for TE.

Different approaches for calculating the routes exist namely “offline” and “online”. Offline route calculation makes use of statistical models. This works well for predictable traffic but is not suited for voice traffic. Online route calculation is “on demand” and thus better for highly fluctuating traffic but does not scale very well as it can lead to high resource consumption in large systems. A hybrid of these approaches can be desirable as it can use offline procedures to obtain global optimization and online procedures to accommodate actual traffic requests thus allowing prompt reaction to traffic changes.

8.4 Firewalls

As mentioned in section 4.9, firewalls play an important role in securing the network from outside attacks, since all traffic traversing from the corporate network to the public (insecure) network, and vice versa, has to pass through the firewall. Different types of basic firewalls exist that can be used to protect a traditional data network at the different layers in the OSI model. These include:

- Packet filtering firewalls
- Circuit level gateway firewalls
- Personal firewalls

The above mentioned firewalls are not described further in this thesis, since they all are common for traditional data networks. Please read [CBR03, MAI03] for more information about these basic firewalls. In general, basic firewalls are not designed for real-time traffic and especially not for the VoIP protocols. Furthermore, implementing firewalls into a VoIP system complicates several aspects of VoIP, such as dynamic port tracking and call setup procedures.

In addition to the basic firewall functionalities, VoIP aware firewalls usually have the responsibility of handling the data flow between the voice and data segments of the network. For instance, if the functionality is not implemented then all traffic traversing from and to an IP phone has to be allowed into the VoIP system since RTP uses dynamic UDP ports. It is of course possible to leave all UDP ports open, but this is considered lack of security. Thus, all IP phones should be placed behind a stateful firewall so the RTP traffic can be handled properly without opening all the UDP ports. This is just one example of how VoIP aware firewalls can be used to provide a logical segmentation of the voice network, i.e. separation of the voice and data traffic. [KWF05] identifies several other issues where firewalls are necessary to prevent collisions between the voice and data traffic.

This section describes different technologies that can be implemented on the firewall such as Network Address Translation (NAT), Demilitarized Zone (DMZ) and Intrusion Detection System (IDS). Furthermore, VoIP issues and considerations regarding firewalls and NATs are described along with solutions for coping with these problems. The section is primarily based on [KWF05, STU04].

8.4.1 Network Address Translation

Network Address Translation (NAT) is a technique in which the source and/or destination IP packet addresses are changed when they pass through a firewall or a router. It is commonly used to change the hosts' private IP addresses to their corresponding public IP addresses, so they can communicate outside the corporate network. Besides the one–to–one mapping of IP addresses, NAT also has techniques for many–to–one mapping of IP addresses, also called Network Address Port Translation (NAPT)[KWF05]. NAPT is used to enable multiple hosts in a private network to access the Internet by using a common public IP address, see Figure 8.10. For simplicity reasons, NAPT is referred to as NAT throughout the thesis.

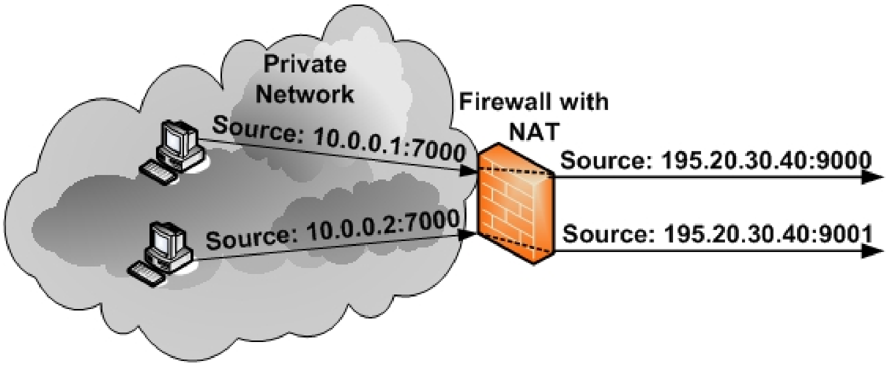


Figure 8.10: The NAPT traversal.

Several types of NAT policies exist which can be categorized into four classes [KWF05]:

Full cone: All requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send packets to the internal host by sending packets to the mapped external IP address.

Restricted cone: Differs from a full cone NAT by only allowing an external host to send a packet with its IP address X to an internal host, if the internal host has previously sent a packet to IP address X.

Port restricted cone: Is like a restricted cone, but the restriction includes port numbers. An external host can send a packet, with its IP address X and IP port P, to an internal host only if the internal host has previously sent a packet to IP address X and port P. It is used to enable sharing of external IP addresses.

Symmetric: All requests from the same internal IP address and port to a specific external destination, are mapped to the same external IP address and port. If the same host sends a packet with the same host IP address and IP port but to a different destination, then a different mapping is used. Furthermore, only the external host that receives a packet can send a UDP packet back to the internal host.

There are two advantages of using NAT. First of all, NAT limits the number of IP addresses by letting the terminals share a single public IP address to communicate with users in other networks. Secondly, if all terminals in a private network share a common public IP address for communicating outside the private network, then all incoming packets have to pass through the NAT before reaching the destination within the private network. This implies that NAT provides a single point of security to the private network since only the firewall or router containing NAT has to be secured from outside attacks. Since the terminals will not be reachable directly from the public network they cannot be attacked by exploiting port vulnerabilities in the terminals. These benefits come at a price since NAT violates the fundamental semantic of the IP addresses, that they should be globally reachable. There are several issues where NAT gives rise to complications for VoIP such as when attempting to make a call into the network and when transmitting the voice media itself.

8.4.2 Firewall and NAT Issues

There are some issues which have to be considered when transmitting voice packets through basic firewalls and NATs. These issues include difficulties for incoming calls to be received by terminals behind the firewall and the NAT. Furthermore, both devices affect QoS and result in problems with the voice stream and the encrypted packets. These issues are not related to any specific VoIP protocol, but instead are of a general character when using firewalls and NATs with VoIP. There are also NAT issues with IPSec.

Effects on QoS

Firewalls and NATs can create performance and reliability issues and thereby degrade the QoS in VoIP systems by introducing latency and jitter. To avoid this, the firewalls must be able to quickly process the packets that are passing through. The processing of the packets do not only depend on how fast the firewalls can interact with the network traffic, but also on how fast their CPU is able to process the packets. There are several aspects which can degrade the behavior of a firewall CPU in relation to VoIP packets. A voice packet header is more complex compared to an ordinary IP data packet header. Thus, it takes longer time for firewalls to investigate the validity of voice packets. If a NAT is used then the issues become more compounded because the packet payload must be modified to correspond to the NAT translated IP addresses and ports.

A second aspect of VoIP that can burden the firewall CPU is the number of RTP packets that make up a VoIP conversation. To limit latency, each RTP packet contains only a small payload. This may results in the firewall's CPU getting overloaded by inspecting a large number of packets.

Incoming Calls

Regardless of the protocol used for signaling, firewalls and NAT present difficulties for incoming calls. Allowing signaling traffic through a firewall from an incoming call will require leaving several ports open that might be vulnerable to attacks. NAT creates even more difficulties for incoming calls. An external caller, or for that matter any IP application, can only make a call to a terminal behind a NAT if the caller knows the callee's external IP address and port. However, this is nearly impossible with the dynamic ports that are assigned by NAT. The terminal behind a NAT will only be able to make outgoing calls.

The Voice Stream

Besides problems with the signaling traffic, firewalls also have problems associated with the voice stream. The RTP voice stream uses dynamically assigned port numbers with only the restriction of using the UDP port range 1024-65534. In addition, the RTCP protocol that is responsible for managing the voice stream will use a randomly assigned port. As pointed out earlier, it is not adviceable to have many open ports. By default, all ports should be closed and only the ones used should be opened. In the past, the default settings were all ports were open, and the ports not used were closed. The latter is not good security practice.

NATs also have major issues associated with the voice stream. It is difficult to keep the association between the RTP and RTCP port numbers, since these are randomly assigned by the NAT. Secondly, the translation of IP addresses and port numbers is also problematic for the packet reception. The problem is aggravated if both the caller and the callee are behind NATs. Furhtermore, the NAT binds a public IP address to a private address only for a finite period of time (t). The binding will be deleted if no traffic is observed by the NAT for t seconds or the connection is turned down explicitly. When TCP is used then the termination of the TCP connection may be used as an indicator for termination of the call. However, when using UDP such an indication is missing since UDP is connectionless. If VAD is used where a silence period of t seconds may occur during a conversation, it can result in some connection information being deleted before the call is actually completed.

Encryption Issues

The end-to-end encryption of the signaling and voice traffic between the terminals can be used to provide strong confidentiality, integrity and authentication and thereby greatly improve the security in the VoIP systems. The enhanced security comes at a price since it results in serious issues with firewalls and NAT. The firewall is only able to intercept the header of an encrypted packet and not the encrypted payload containing the original packet header and payload, to determine the validity of the packet. NAT is not able to intercept the payload of an encrypted packet to convert the source or destination IP address and port.

NAT and IPSec issues

There are incompatibility issues between NAT and IPSec. The NAT traversal hides the internal IP addresses from the outside world, which results in the AH and ESP authentication mechanisms in IPSec to become invalid.

8.4.3 Solutions to Firewall and NAT Issues

As stated in the previous section, there are many issues with firewalls and NATs that have to be taken into consideration when using these devices in VoIP systems. The following sections describe different techniques available to solve the firewall and NAT issues.

Demilitarized Zone

A solution to overcome the problems with firewalls, such as dynamic ports, can be solved by using Demilitarized Zones (DMZs). A DMZ is a subnetwork that is placed between a trusted internal network, such as a private LAN, and an untrusted external network, such as the Internet. It is used to provide additional level of security and usually placed between two firewalls, see Figure 8.11. The dynamic port problem can be solved if a H.323 gatekeeper or a SIP proxy is implemented inside a DMZ, and the firewall is configured to allow communication of terminals with only this gatekeeper or proxy. In this way, the dynamic ports can be managed outside the internal network's firewall, but still inside a secured environment.

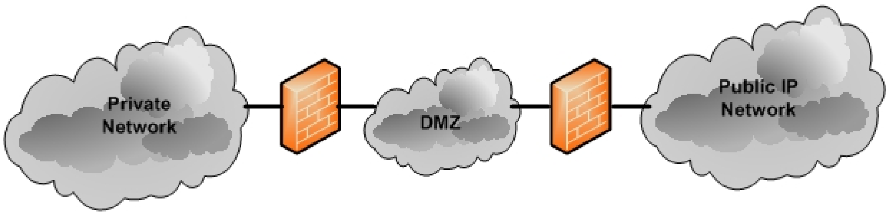


Figure 8.11: A DMZ configuration using two firewalls.

Application Level Gateway

The Application Level Gateway (ALG) requires either software upgrading or replacement of the existing firewall/NAT and is the typical commercial solution to the firewall/NAT traversal problems. It is considered as one of the most advanced form of firewalls since it is able to filter traffic based on knowledge about specific protocols. A VoIP ALG can understand H.323 or/and SIP and thereby is able to dynamically open and close the necessary ports. In addition, the ALG is able to intercept and modify the packet headers so they correspond to the correct source or destination IP address of the private and public network.

The problem with NAT is further reduced when the private IP addresses are replaced with the IP address of the ALG itself. When the RTP traffic is mapped to ports the ALG can read and forward to the correct internal terminal. However, this can cause problems in finding enough ports for the RTP and the RTCP as the number of concurrent calls increase since all the voice traffic is routed through the ALG.

Another drawback with ALGs is that they are implemented in the firewall itself and cause performance issues since the firewall now has additional tasks to perform.

Middlebox Communication

The Middlebox communication (MIDCOM) solution tries to overcome the drawbacks that are related to the ALG by placing many of the ALG functionalities into a device outside the firewall. The device should be placed in a trusted network, such as a DMZ, and can be implemented in a VoIP device such as a H.323 gatekeeper or a SIP proxy. The devices that are controlled by the MIDCOM, is referred to as a middlebox and can be a variety of network devices besides the firewalls and NATs. The ALG functionality is managed by MIDCOM agents through a MIDCOM protocol. Currently, a standard MIDCOM protocol has not been finalized by IETF. The agents are responsible for managing and allowing the signaling and voice stream to pass through the middlebox devices according to certain defined security rules.

Other Solutions to NAT Issues

Beside the above mentioned solutions, there are many other solutions to solve the NAT issues that occur for real-time applications, including VoIP systems. Some of these solutions are described in the following:

Simple Traversal of UDP through NATs (STUN): Allows terminals to determine whether they are located behind a NAT prior to sending registration or call signaling messages. It also allows the terminals to determine what type of NAT they are behind, and the bindings between the public and private IP addresses that are assigned by the NAT. This solution does not work with symmetric NATs, because the IP address and port are here dependent on the destination.

Traversal Using Relay NAT (TURN): Allows terminals behind a NAT, or a firewall, to receive incoming data over TCP and UDP connections, and can be used to solve the limitations of STUN in relation to symmetric NAT. Unlike a STUN server, a TURN server provides ports to terminals that connect to it. Therefore, authorization is needed between the TURN server and its clients. The authentication is performed by using a shared secret in form of a one-time username and password which is shared between the server and the client over TLS.

A technical description on how to solve the NAT and firewall problems can also be found in [STU04].

8.4.4 Intrusion Detection System

A firewall can run an Intrusion Detection System (IDS). An IDS has the purpose to detect intrusions and malicious behaviors on networks and hosts. There are basically two types of

IDSs; signature-based IDS and anomaly-based IDS [CBR03]. A signature-based IDS uses a database containing known attacks to detect malicious behaviors. This technique is easy to implement, since it just requires the IDS to search for strings containing the attack signature in the packets. If the attack signature in the database is too detailed then it is possible for an attacker to unnoticeably pull of an attack by making small modifications to the packet containing the malicious code. If the signature is not detailed then there is the risk that normal traffic will be detected as attacks. The anomaly-based IDS instead detect attacks by looking for unusual system behaviors, such as network traffic patterns. This type of IDS is difficult to implement since it can be troublesome to determine whether an unusual system behavior is a result of an attack or just harmless traffic.

There are several challenges with IDSs when using them in VoIP systems. Some of these are listed below:

- Different protocols are used for signaling and the voice stream.
- The VoIP systems are distributed in nature and employ distributed servers and proxies.
- There are many different types of attacks against VoIP systems.

Proposals for designing VoIP specific IDSs can be found in [DIT04, BAG04].

8.5 User Authentication

Many of the VoIP risks mentioned in Chapter 7 can be prevented by using strong user authentication mechanisms. User authentication is the process of verifying that the user really is the person he claims to be. Thus, it can be used to make sure that only authorized users have access to the VoIP system. Authentication can be based on three factors [CBR03]:

- Something the user knows - This is usually passwords, Personal Identification Numbers (PINs) or any other information that only the user knows.
- Something the user has - This can be a smart card, USB key or any other device that can be used for authentication.
- Something the user is - This refers to biometric techniques, such as fingerprint, eye scanning and DNA.

An authentication solution can involve one or more of the mentioned factors. The more factors that are being used in the authentication process, the more difficult it is for an attacker to get unauthorized access to the system.

There are some issues regarding user authentication in VoIP systems, such as where and when it should be done. One could require that the user should be authenticated each time he wants to use an IP phone. This includes an authentication each time the user wants to make or receive a call. Such a solution is not always practical since it is time consuming and nuisance for users. In general, the user authentication should not reduce the IP phone's functionality when compared to the traditional telephone. For instance, users are used to just picking up the phone when either making or receiving a call. This is most likely also the case for users when migrating to VoIP. This section describes typical methods which can be used to authenticate users in applications including VoIP systems. This includes static passwords, one-time passwords and biometric techniques. Proposals for future VoIP user authentication methods are also provided.

8.5.1 Static Passwords

The most common and simple method to perform user authentication is through a user name and its corresponding password. The user name is commonly sent in plaintext while the password is encrypted based on a given encryption algorithm. The user will only be allowed to access the system, if the system's Remote Authentication Dial In User Service (RADIUS) server accepts the typed user name and password as a valid pair. As mentioned in Chapter 7 there are several weaknesses by using passwords for authentication. Some of these are pointed out here:

- It is common to use simple passwords since these are easy to remember.
- There is the risk that an attacker observes the password while the user is typing it into the application. This can simply be done by looking over the shoulder of a user typing his user name and password or by more technical approaches such as using a keylogger application.
- Many passwords are encrypted with weak encryption algorithms.
- There are several tools available that can be used to crack an encrypted password through dictionary style or brute force attacks.

Attack methods that can be used to compromise different static password authentication procedures are described in [CBR03, KIL04].

8.5.2 One-Time Passwords

One-time password authentication methods increase the security significantly compared to static password methods since one-time passwords can only be used one time, after which they are no longer valid [CBR03]. Even if a one-time password is observed by an attacker while it is being typed, it will not be of any use. Most one-time password authentication methods are two-factored, that is, something the user knows and something the user has. Commonly, it is a password and a device that is synchronized with an authentication server.

One-time passwords can either be challenge/response-based or time-based. In the challenge/response method the authentication server will send a non-repeating challenge to the user, who based on a known algorithm, uses the given challenge and a password to compute a response. The time-based one-time password methods are the preferred solution, and do not require any challenges from the server. Instead, they require typing a password into the application together with a given one-time password. The time-based one-time password is computed based on an algorithm that uses an internal clock. Thus, the password will only be valid for a given time period, typically 15-20 seconds. An example of a well-known time-based one-time password generator is given in Figure 8.12[5].

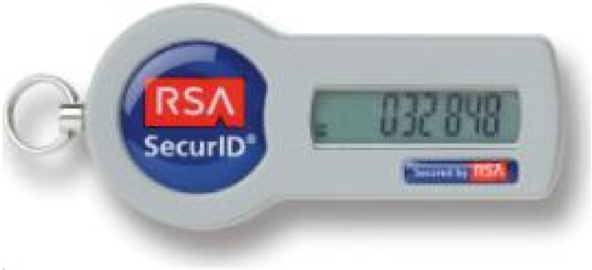


Figure 8.12: RSA SecurID 700 from RSA Security.

8.5.3 Biometric Authentication

Authentications through biometric methods are considered very secure since they are based on something the users are. The most common biometric authentication method is based on fingerprint scanning. Other methods include recognizing voice print, image of the face, shape of the hand and DNA. In contrast to static and one-time passwords, using biometric authentication methods requires installation of special hardware on the PCs.

Currently, VoIP specific components do not use biometric methods for authentication. Hardware components that are not VoIP specific, such as PCs and servers, do make use of biometric authentication.

8.5.4 Future VoIP Authentication Proposals

As VoIP systems become more popular, stronger user authentication on VoIP specific components may become available. Biometric authentication methods on the IP phone is a future solution to a strong user authentication. For instance, an IP phone containing a finger scanner may become available in the future. Risks such as toll fraud can be reduced by using a two-factored authentication on the IP phone. The two-factored authentication may be a method that includes a password combined with a hardware device that can be plugged into the IP phone, such as an USB token or a smart card. These solutions are more expensive compared to the static and one-time password authentication methods. As hardware is becoming cheaper, device and biometric authentication on IP phones will be in more demand.

8.6 Summary

This chapter discussed different technologies that can be used to secure the VoIP systems against attacks. In addition, technologies to guarantee the QoS requirements have also been discussed. The technologies described include:

[5] The figure is taken from http://www.rsasecurity.co.jp/news/images/20050411.jpg.

- VLAN
- VPN
- MPLS
- Firewall and NAT
- User authentication

VLAN can be used to logically segment the network and thereby separate the voice and the data traffic. Besides advantages in performance, manageability and functionality, VLANs provide security in the form of accessibility since data assets are only accessible for the members of the given VLAN. In addition, different types of tunneling techniques used in VPN have been described. These include PPTP, L2TP and IPSec. IPSec is considered the most secure of the three protocols and can either be used as a complete VPN protocol solution or simply as the crypto engine in PPTP and L2TP.

The QoS requirements in VoIP systems can be solved by using MPLS that offers traffic engineering. The label switching technique of MPLS is more desirable compared to the traditional IP destination based routing.

The firewall and NAT issues related to VoIP systems were described together with solutions. Firewalls and NATs result in dynamic ports issues and issues with the voice packet structure. These issues can be resolved by using a VoIP aware firewall that include DMZ, ALG and/or MIDCOM. IDSs detect intrusion and malicious behavior on the network.

Finally different user authentication methods were described. These include static passwords, one-time passwords, biometric techniques and future VoIP authentication proposals. Most of the IP phones use static passwords for user authentication despite being considered weak. It is proposed to use an authentication method that requires more than one factor, such as a password combined with a hardware device.

Chapter 9

Existing VoIP Solutions for Enterprises

Several package solutions exist for enterprises that can be used to implement a VoIP system. These differ from each other in capacity, functionality and security. This chapter examines and compares the VoIP solutions developed by four major vendors; Alcatel, Avaya, Cisco Systems and Nortel Networks. The focus will be on VoIP specific components such as IP PBXs and terminals for enterprises. The chapter is based on dialogues with vendors, white papers and different reviews. The reviews used were completed by Miercom[1] [MIE04, MMT05, STE03].

9.1 Alcatel - OmniPCX Enterprise

OmniPCX Enterprise, see Figure 9.1[2], is Alcatel's solution to an IP PBX for enterprises [ALC03a, KRA03]. It can be implemented as a single system supporting 5.000 terminals, or up to 100 communication server node clusters that can be networked to support long distance locations and 50.000 terminals. It uses Linux/Unix as the operating system. Alcatel was the first major vendor to implement a PBX that could run on a Linux kernel. The architecture of OmniPCX Enterprise is a combination of Alcatel's two VoIP solutions, the OmniPCX Office's hardware and the OmniPCX 4400's software.

9.1.1 Security Features

Currently, Alcatel does not support encryption of the signaling messages. Furthermore, none of the OmniPCX Enterprise IP phones support voice stream encryption. Instead, the voice stream encryption/decryption is carried out in the switches whereas the voice stream is unencrypted between an egress switch and an IP phone. This gives an attacker opportunity to eavesdrop voice packets through wiretapping. The initial registration of IP phones requires

[1] Miercom is a private network company, specialized in networking and communication-related product testing and analysis.

[2] The figure is taken from `http://www.comms4business.com/Images/Vendors/Alcatel/Alcatel2.jpg`.

Figure 9.1: OmniPCX Enterprise.

authentication through a password and the OmniPCX Enterprise Reflexes IP phones can be locked through passwords, thus reducing the chance of toll fraud.

In October 2004, Alcatel and Thales[3] announced a technological partnership to develop a secure VoIP solution based on the OmniPCX Enterprise [ALC04]. This has resulted in Alcatel's forthcoming encryption improvements which can encrypt the voice stream with no notable degradation of voice quality and no added latency.

OmniVista 4760 [ALC03b], Alcatel's network management tool, can be used to provide centralized management for OmniPCX Enterprise through a web browser. The management traffic and sessions are encrypted via secure shell (SSH) and secure FTP (SFTP). These security features are only supported between the OmniVista 4760 from R3.0 and OmniPCX Enterprise from R6.0.

OmniPCX Enterprise can also be combined with CrystalSec to secure the IP communication at different OSI layers. CrystalSec is Alcatel's solution to secure the network infrastructure and supports the security policies of enterprises. It uses a principle called security-by-default where only needed ports are open by default. Furthermore, it forces to change default passwords and activates security features by default. In earlier versions, all security features were turned off by default.

9.2 Nortel Networks - Succession Communication Server for Enterprise 1000

Succession Communication Server for Enterprise 1000 (CSE 1000) is Nortel Networks' solution to an IP PBX for enterprises [NOR02, NOR04a, NOR04b]. It consists of three key components; Call Server, Signaling server and Succession Media Gateway, see Figure 9.2[4]. Each call server is able to support up to either 1000 or 15000 terminals, depending on whether CSE 1000S or CSE 1000E is used. It can be networked to support long distance locations and scale the number of supported terminals. CSE 1000 uses VxWorks 5.4 which is an operating system developed for real-time applications.

[3] Thales is an international company that focus on three key markets; Aerospace, Defense and Information Technology & Services.

[4] This figure is taken from [NOR02].

Figure 9.2: Succession CSE 1000.

9.2.1 Security Features

Nortel Networks is using its proprietary UniStim for signaling between the IP phones and the signaling server. CSE 1000 supports encryption of the signaling messages through Secure UniStim which is a based on AES. Furthermore, the end-to-end encryption between the IP phones is supported by SRTP.

During installation of a Nortel Networks IP phone a password is used to create a cookie, which is stored in the IP phone client. On client registration, the call server looks for the cookie, and if it is not presented the user is prompted for a password. The strength in Nortel Networks IP phones is that there are no open TCP ports and are therefore not vulnerable to attacks that require port numbers. The protection against unauthorized access is done through a SHA-1 password.

Management of the Succession CSE 1000 can be done through a web browser, command line interface and Graphical User Interface (GUI). All of these interfaces are password protected but only the web browser interface is encrypted, using Secure Socket Layer (SSL). Nortel Networks recommends protecting the management system by securing it on its own LAN called Equipment LAN (ELAN) by Nortel Networks. In addition, it is recommended that the Call Server, Signaling Server and Succession Media Gateway communicate with each other across an ELAN.

9.3 Cisco Systems - Cisco CallManager

Cisco Systems offers a range of VoIP solutions based on its IOS software and Cisco Architecture for Voice, Video and Integrated Data (AVVID). The IP PBX in AVVID is called a Cisco CallManager and can for large enterprises run on the Integrated Communication System (ICS) hardware, see Figure 9.3[5].

9.3.1 Security Features

All Cisco IP phones support digitally signed images using Cisco authorized certificates. These images can be used to prevent invalid images being maliciously or mistakenly installed on the IP phones. The Cisco IP phones validate and accept only Cisco images. Each Cisco IP phone

[5] The figure is taken from [STE03].

Figure 9.3: Cisco CallManager can run on an Integrated Communication System 7750.

has a Certificate Trust List (CTL) stored, which contains IP addresses of trusted devices. Only packets from trusted devices are received, while other packets are dropped by the IP phone. Beside component authentication, user authentication is also supported, using a user name and password.

Like Nortel Networks, Cisco is also using its own proprietary protocol, called Skinny Client Control Protocol (SCCP), for signaling between IP phones and the local CallManager. Cisco CallManager 4.0, which was introduced in early 2004, introduces support for encryption of SCCP signaling. However, encryption of the H.323, SIP and MGCP signaling is not supported. The encryption of the voice stream is supported between the newer Cisco 7970 IP phones using AES. The encryption is not supported in the soft phones nor in inexpensive Cisco IP phones.

The management for the Cisco CallManager is web-based and supports multiple levels of administration. Any number of users can be assigned any number of specified sub-groups. The web-based management interface does not support any type of encrypted management session, such as SSL.

A number of vulnerabilities in Cisco CallManager have been reported during the past couple of years. In the last 3 years, DK-CERT have reported 6 vulnerabilities in Cisco CallManager. The latest vulnerability was reported on 12^{th} July 2005 and posed the opportunity to achieve a DoS attack or run any code on the system causing the CallManager to restart or become overloaded.

9.4 Avaya - Integrated Stackable Telephony Solution

Avaya has a range of VoIP solutions, all based on its Enterprise Class IP Solution (Eclips). One of the most popular solutions is IP Office, for companies with up to 180 users. However, this section will look into the Integrated Stackable Telephony Solution (ISTS) which is Avaya's IP PBX solution for enterprises. ISTS is made up by two hardware components, the Avaya Media Gateway G650 and the Avaya Media Server S8700, see Figure 9.4[6].

[6] The figure is taken from [STE03].

Figure 9.4: Avaya ISTS IP PBX which can be made by a Media Gateway G650 and a Media Server S8700.

9.4.1 Security Features

All Avaya's terminals supported by Media Server S8700 use the H.235 protocol for encrypted key exchange and also support password login during installation. Passwords can also be used to place calls over specific trunks, whereby toll fraud can be minimized.

Avaya offers strong encryption mechanisms in its IP PBX solution compared to the other vendors considered in this study as it was governed by the american military to satisfy strict security requirements. The voice stream from any Avaya IP phone, including its soft phones, and from their TDM gateway is strongly encrypted. The encryption is done with either AES or Avaya's own encryption algorithm called Avaya Encryption Algorithm (AEA) which is a modified version of AES. The drawback with Avaya's solution is that the H.323 signaling from the phones is not encrypted. However, the control signaling is encrypted between the media gateway and the media server.

Encryption of the management connections is standard. The web interface for management can be encrypted using SSL.

9.5 Comparison of Existing VoIP Package Solutions

The choice of which of the previous mentioned IP PBXs that should be preferred depends on the requirements the IP PBX has to satisfy. Table 9.1 compares the four examined IP PBXs.

Table 9.1: Comparison of different IP PBXs.

	Alcatel - OmniPCX Enterprise	**Nortel Networks - CSE 1000**	**Cisco Systems - CallManager**	**Avaya - ISTS**
General				
Operating System	Linux/Unix	VxWorks	Windows 2000	Linux (Red Hat)
Maximum number of IP phones	5000 if all IP hard phones, 3000 if all IP soft phones	1000 for CS 1000S(CS 1000M allows up to 15000)	2500	6000

Continued on next page

Table 9.1 – continued from previous page

	Alcatel - OmniPCX Enterprise	**Nortel Networks - CSE 1000**	**Cisco Systems - CallManager**	**Avaya - ISTS**
Maximum system call load (BHCA)[7]	300000	300000	250000	300000
Call control protocol	H.323	H.323, SIP and UniStim for IP phones	SCCP for IP phones and H.323 or MGCP for gateway control	H.323
Other supported VoIP protocols and components	H.323 gatekeeper and gateway, SIP proxy server and gateway	H.323 and SIP for gateway control	H.323 gatekeeper and gateway are integral, SIP requires separate SIP server	H.323 gatekeeper and gateway are integral, SIP requires separate SIP server
Vocoders	G.711, G.723.1, G.729a	G.711, G.723.1 G.729, G.729a	G.711, G.722, G.723.1, G.729.1	G.711, G.722, G.723.1, G.726, G.729.1, G.729a
VAD support	Only for G.723.1 and G.729a	Yes, for all vocoders	Yes, for all vocoders	Only for G.711, G.729 and G.729a
Special Functionality Features				
IP call recording	Yes	Yes	Can be implemented	Yes
System integration using XML	Yes	Yes, needs 3rd party gateway	Yes	Yes
IP Phones				
Soft phones	Yes	Yes	Yes	Yes
Registration	Requires a password	Requires a password	Requires a password	Requires a password
IP phone access	Can be password protected	Can be password protected via SHA-1	Image and device authentication	Can be password protected
3rd party component support	Yes, via H.323 and SIP	Yes, via H.323 and SIP	Yes, via SCCP	Yes, via H.323
Security				
Integrity of signaling messages	None	Secure UniStim (AES 128bit), TLS for terminals	SCCP messages are encrypted between an IP phone and its call manger. However other signaling protocols are not encrypted	Yes, via SRTP
				Continued on next page

[7] Busy Hour Call Attempts; the number of call attempts made during a network's busiest hour of the day.

Table 9.1 – continued from previous page

	Alcatel - OmniPCX Enterprise	**Nortel Networks - CSE 1000**	**Cisco Systems - CallManager**	**Avaya - ISTS**
Integrity of call control messages	Not from the IP phones, encryption is done in the switches	Secure UniStim (AES 128bit), TLS for terminals	N/A	Between the Media servers and Media Gateways
Integrity of voice stream	Not supported by any Alcatel IP phone	SRTP	Yes, done in some IP phones (Cisco 7970 supports 128bit AES)	Avaya IP phones support AES and AEA
Secure Management				
Interface	Web-based	Web-based, command line and GUI	Web-based	Web-based
Security	SSH and SFTP	SSL (only for web-based)	None	SSL
List Price per Station[8]	$586, includes mid-span powering	$637, includes 10/100 switch port for powering	$715, includes 10/100 switch port for powering	$680, includes mid-span powering

In May 2004 Miercom tested the four IP PBXs that have been compared in this chapter, together with a wide range of other vendor IP PBXs. The IP PBXs were exposed to Nessus vulnerability scannings and different types of DoS attacks. The results revealed that all the IP PBXs had open ports with either low or high severity vulnerabilities. All the IP PBXs and IP phones were tested to be vulnerable to different kinds of DoS attacks. However, the DoS attacks against Avaya's and Cisco Systems' IP PBX were considered having the lowest impact.

In late 2004 another review of large IP PBXs was performed by Miercom and published in the January 2005 issue of Business Communications Review (BCR) [MMT05]. Five IP PBX vendors participated in the test, among them Alcatel, Avaya and Cisco Systems. Nortel Networks were invited, but declined due to lack of resources. The Avaya IP PBX gained the overall highest score awarded by Miercom in over five years of testing VoIP systems and was named ”2005 Best-In-Test, Large IP PBX” [MIE05a]. The titles ”Best Performing IP PBX, Large system” [MIE05b] and the ”Most Secure IP PBX, Large System” [MMT05] were awarded to respectively Alcatel and Cisco Systems. The security score defined by Miercom depended on several factors, such as the encryption mechanisms in the IP PBXs and the terminal, the documentation and security alarm/fixes. Both Cisco Systems and Avaya did well in the security test; Cisco Systems gained 9.5 points while Avaya got 9 points out of 10 possible points. Alcatel only obtained a score of 5 points in the security score.

[8] The price list are based on a system supporting 1,500 IP stations, consisting of 1,000 IP hard phones and 500 soft phone licenses, and including voice mail for all, full management, and power to IP phones. The list price for Nortel Networks' CSE 1000 solution is calculated by Ole Villadsen, see Appendix G, while the other prices are taken from [MMT05]. The prices should not be considered as actual prices since companies often receive discounts in the Service Level Agreements (SLA) and the systems compared are not 100 percent identical.

9.6 Voiceline - IP Matrix

Voiceline is an entrepreneur company with focus on innovation within VoIP security. Voiceline has a concept for a VoIP solution intended for use in closed networks and thereby avoiding security problems that arise from open networks, such as the Internet. Voiceline has described the concept in Appendix C.

The Voiceline IP Matrix concept is under development as an ongoing vendor neutral research project, held at the Technical University of Denmark. IP Matrix strives to set the standard for security in closed networks and the customer segment is mainly organizations with a need of high security standards.

The technical solution is built on nested MPLS domains. Each company has its own MPLS domain for the voice communication as illustrated in Figure 9.5[9]. These MPLS domains are connected through a full mesh MPLS network that is controlled by the Voiceline Hosting Centre, see Figure 9.6[10].

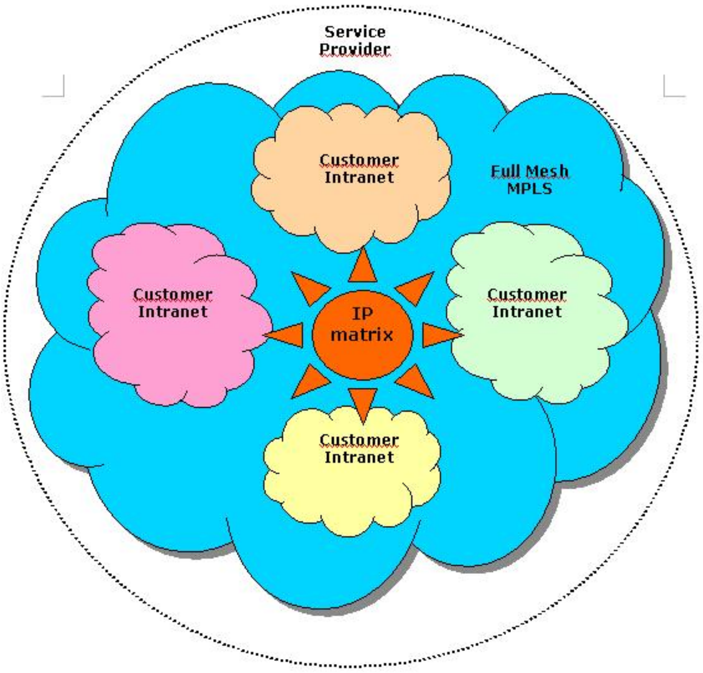


Figure 9.5: Nested customer MPLS domains in the Voiceline MPLS network.

The principle and goal for the IP Matrix is to deliver unique VoIP and data security. All the users, that is the customers, are registered in the IP Matrix and given a unique ID, so only registered users in the IP Matrix can communicate with each other in the MPLS network. This means the authorization process takes place centrally in the IP Matrix. Once the user has gained acknowledgement as a registered user in the IP Matrix, a second authorization process is initiated. The independent Electronic Numbering (ENUM) service, which is a

[9] The figure is taken from the Voiceline description of the concept, Appendix C.

[10] The figure is taken from the Voiceline description of the concept, Appendix C.

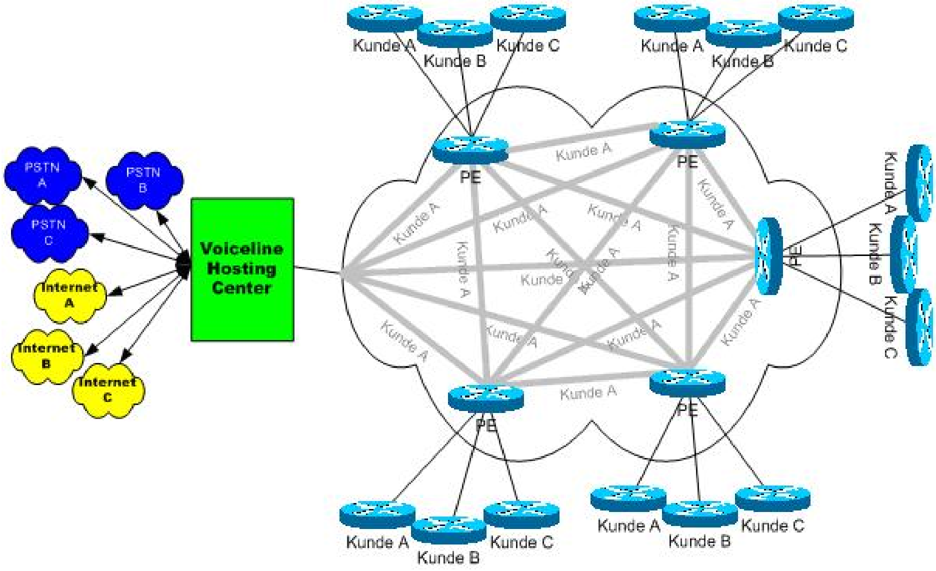


Figure 9.6: Overview of the customer network for Voiceline.

protocol for telephone number mapping, also holds the specific end-user information. This data must match the end-user information for that specific user in the IP Matrix. If the user is not acknowledged as a valid registered user in the Matrix's hosting centre, the user will not be allowed access to the Matrix and can thereby not compromise security. Unregistered users can only communicate with members in the MPLS network via the PSTN.

Only by physical line-up testing can an optimal solution be found, which might consist of, for example, Avaya routers, Cisco IP phones, and Alcatal's OmniPCX Enterprise. However, our theoretical research has shown that it might lead to compatibility and management problems. Even if a mixture of vendor components proves to give higher security it might result in problems with upgrades and installation of patches. With the current state of the art, it is very unclear and not without a comprehensive program to investigate the issue, will it be clear whether a combination of products will lead to a higher level of security.

9.7 Summary

Four existing VoIP solutions for enterprises developed by major vendors have been described and compared in this chapter. These include:

- Alcatel - OmniPCX Enterprise
- Nortel Networks - CSE 1000
- Cisco Systems - Cisco CallManager
- Avaya - ISTS

The focus has been on the security features of the IP PBXs and terminals. Avaya and Cisco are considered to have the most secure solution due to the support of AES encryption of the voice stream in the IP phones.

Finally, the Voiceline IP Matrix concept was introduced. The technical solution is based on nested MPLS domains that are controlled by a hosting centre. Furthermore, the aim is to use ENUM for user authentication.

Chapter 12

Prospects and Development

It is a reasonable assumption that the thesis will be used by Elsam A/S to gain technical information concerning the risks and technologies that are associated with VoIP systems. In addition, it may be used as a guideline if they decide to implement VoIP to the end-users. The first step will be to make a design proposal based on the given recommendations. The design proposal should take Elsam's existing network infrastructure into consideration. Next, the design proposal should be tested by physically setting up the components based on the design proposal and testing for component compatibility and security. If the test results do not give any concerns, then Elsam can implement the design proposal to their own network infrastructure. The implementation should be split into discreet project phases and always have a back up service in case of complications.

The project results can also, to a great extent, be used by other companies who are considering designing a VoIP system for their corporate network with similar security requirements as Elsam. Companies with severe security requirements can use the thesis as a basic guideline. Since the thesis contains confidential information, it must be reviewed before it can be seen by a third party. An article summarizing the VoIP issues and recommendations could be prepared and published instead.

Voiceline can use the project results to achieve a technical foundation for the IP Matrix concept. Moreover, it can be used to identify which areas of the IP Matrix concept that should be illuminated further. Voiceline have already initiated a co-operation with COM, an institute at the Technical University of Denmark, with the intention of starting new VoIP projects. The results from this thesis can to some extent be used in some of the new projects at COM. It will certainly be of interest to see whether Voiceline will realize the idea of IP Matrix to a final product and thereby set new security standards for VoIP.

The project was limited to only review VoIP systems in wired networks. It could be interesting to analyze the security in wireless VoIP as well. The security and QoS requirements for wireless communications are more difficult to guarantee compared to the communications over wired networks. Several vendors are making significant technology improvements to gain market shares. One of these technologies is to combine wireless VoIP and GSM access. With this combination the mobile phone can use the wireless VoIP connection to communicate and switch over to the GSM when the wireless network is out of range. This may give large economical savings since communication through GSM is expensive compared to using PSTN.

Besides wireless VoIP, there are several other topics that would provide a natural extension to this project, for example, design and implementation of a VoIP aware firewall combined with IDS that detects the risks that have been pointed out in the thesis. Especially, designing an IDS that is able to detect SPIT calls is difficult.

Looking into similar services, such as video over IP, could be another extension to the project. Actually, there already exits a large number of video conference services that are freely available on the Internet such as MSN Messenger, Yahoo Messenger and the very popular Skype. However, these Internet services do not provide the security and the QoS that are needed for business use. Especially the QoS requirements for video conferences are difficult to guarantee due to the synchronization between the audio and the video, and the bandwidth capacity that is needed. All in all, there are many reasons and prospects for a continuation of the project.

Chapter 13

Conclusion

This thesis presents security in closed VoIP systems through a theoretical study. Evaluations of VoIP risk assessment, VoIP technologies and existing VoIP enterprise solutions have resulted in security best practices and recommendations on how to secure a VoIP system. These describe in detail the possible mitigation actions that can reduce the risks in VoIP systems. Our risk assessment shows that at present there are no VoIP specific risks that can be classified as high level risks mainly because of two reasons. Firstly, VoIP is still in an early stage of deployment that has yet to be a tempting target for potential attackers. Secondly, no VoIP specific incidents have been reported by DK-CERT meaning that the likelihood of an actual attack is still not at a serious level.

Although implementing a VoIP system might seem harmless from a security point of view after having read the risk assessment and after having taken the necessary security precautions, there is no doubt that the risk levels will increase as VoIP becomes more popular. The most likely attack scenarios that can occur in VoIP systems are analyzed to be DoS attacks on VoIP components such the IP PBX and IP phones. Attacks on the IP PBX will have serious impact on the overall VoIP system as it is the main component managing the telephone calls. In addition, SPIT attacks are likely to be prevalent in the future since they are difficult to detect.

Many technologies that are used to guarantee the QoS and the security in traditional data networks can also be implemented in VoIP systems. Thus VLAN, VPN and MPLS technologies are recommended to be used in VoIP systems. There are issues related to firewalls and NATs due to the dynamic ports and the complex packet structures used in VoIP systems. VoIP aware firewalls and NAT traversal solutions can be used to avoid these problems. Many of the security risks with VoIP can be avoided to some extent by using strong user authentication methods based on two-factored authentication.

The VoIP system can be more secure by following the VoIP best practices and recommendations provided in the thesis. The best practices and recommendations should be considered as guidelines and not strict requirements.

Generally, companies are primarily concerned about voice quality, latency and interoperability which are all fundamental QoS considerations. Companies need to address these before they begin to justify the move to VoIP. Security in VoIP systems merits more attention as it is expected that deployment of VoIP systems and VoIP specific attacks will become far more common in the future than today.

Appendix A

Threat Sources

Threats can come from different sources. Threats can for example come from attackers who intentionally exploit the vulnerabilities in a system or from employees that by mistake damage the system. The driving force for the threat sources depend on their motives. Some are motivated by obtaining free long-distance calls, others by disrupting the key business services by delaying the phone calls or obtaining insider information by capturing the voice data. The most common threat sources for VoIP systems will be described in detail together with their method and motivation for the attacks.[1]

Generally a malicious attacker must have three properties to pull off an attack on a computer system [PFL03]:

- Method – The skills, knowledge and tools to pull off the attack.
- Opportunity – The time and access to accomplish the attack.
- Motive – The reason for wanting to perform the attack.

If one of the three properties is not present then the attack will not be initiated. However, it is difficult for an administrator to take measures that will prevent any of the properties. Instead the administrator should aim to protect his system so the cost for the attacker is higher than the value gained after a successful attack. Unfortunately, companies have difficulty in determining the cost versus the benefit for protecting against threat sources. In addition, companies worry more about QoS and functionality features than securing against threat sources.

A.1 Hackers and Crackers

Originally the term hacker describes someone who makes furniture with an axe.[2] However, a hacker in the computer world can have different definitions. In the beginning the term

[1] Note that the threat sources listed for the VoIP systems are similar to the threat sources existing for general computer systems.

[2] `http://dictionary.reference.com/search?q=hacker`.

hacker was used to describe any computer programmer who discovered ways to make software run more efficiently. It could be anyone who writes computer programs, modifies computer hardware, or just someone who has a lot of knowledge about how computer and network systems work.

The public and especially the media nowadays constantly use the term hacker to describe a person who tries to get unauthorized access to a computer system for malicious purposes. The legitimate hackers resent the association of the term hacker with criminal activity and use the term cracker to describe the illegitimate hackers. The crackers can exploit the vulnerabilities in a system using cracking tools, malicious scripts programmed by themselves or go to more aggressive activity to pull off an attack. They can have many motives, for example the motive can be the challenge of trying to log into secured systems and collect information without being revealed. Others are motivated by damaging the system and thereby getting attention. Another motivation is just simply to obtain respect in the cracker environment.

In this thesis the term hacker will be used to describe a cracker, since it is often done in the public.

A.2 Phreakers

A phreaker refers to someone who has the knowledge and the techniques of cracking the telephone network, for example to make free long-distance calls. An example of a "phreaking attack" has recently been brought by the Danish media, where a blind autist besides overloading the telephone network succeeded in making 72 hours of free long distance phone calls [THO05]. This was done by using a backdoor in one of Tele Danmark Communication's (TDC's) PBX.

A.3 Script Kiddies

Script kiddies are considered as amateurs who think they are hackers or want to be like them. They use scripts developed by others to pull off attacks. They do not have the technical skills to make their own programs or even understand the consequences of executing the malicious script. The malicious script can simply be downloaded from the Internet and thereafter executed. The script can either be executed on a specific target or it can scan for vulnerable systems and attack them.

A.4 Terrorists

Since computer systems are essential for companies, organisations and governments they have become a possible target for terrorists. Attacks on computer systems can cause the same economical damage as by traditional terrorist attacks with bombs. Just imagine the consequences if the computer systems controlling supply installations get paralyzed or exploited by cyber terrorists.

A.5 Industrial Espionage

Industrial espionage is espionage conducted for commercial purposes. It can be competing companies or foreign governments who are motivated by getting competitive advantages. This group consists of professional hackers who have the technical skills and resources needed to execute attacks. A successful attack could result in high economical gains for the attacker.

An example of industrial espionage was revealed in November 2002 where three persons were arrested and two Russian diplomats were expelled from Sweden because they were involved in severe industrial espionage against the Swedish teleconcern Ericsson in favor for the Russian Intelligence Services [BER02].

A.6 Insiders

Recent computer crime statistics show that companies are more likely to be attacked by their own employees (insiders) than by outsiders [GOR04]. Attacks by insiders are easier to pull off since they have easier access and more information regarding the system they are attacking.

An insider can be a disgruntled or former employee who wants revenge against the company, steal sensitive information and sell them to a competing company. The three persons arrested because of industrial espionage against Ericsson were actually one current employee and two former employees.

A threat source can also be an employee that unintentionally or inadvertently damages the system. It can be because of poor training or deliberately violating the company's security policy for example by checking private mails or connecting unauthorized hardware to the network. In general, systems that are controlled by humans will be vulnerable to human errors.

A.7 Natural Disasters

VoIP systems are also subject to threats from natural disasters. They can be flooded, burnt, hit by falling objects or destroyed by earthquakes, storms or tornados. Too much heat or inadequate power is also a threat since computers are sensitive to their operating environments.

A.8 Attack Tendency

An interesting aspect is to see which kind of attacks these threat sources, mainly hackers and script kiddies, perform. Figure A.1[3] shows the sequence of attacks that have taken place the last 25 years. It is concerning to see that the need of technical knowledge and understanding in order to perform a sophisticated attack has decreased for an attacker thus resulting in a large number of attacks accomplished by script kiddies. From the figure it can also be seen that tools used for the attacks are becoming highly advanced.

[3] The figure is taken from the Annual Axcess Conference held at Hotel Scandic in Lyngby, Denmark.

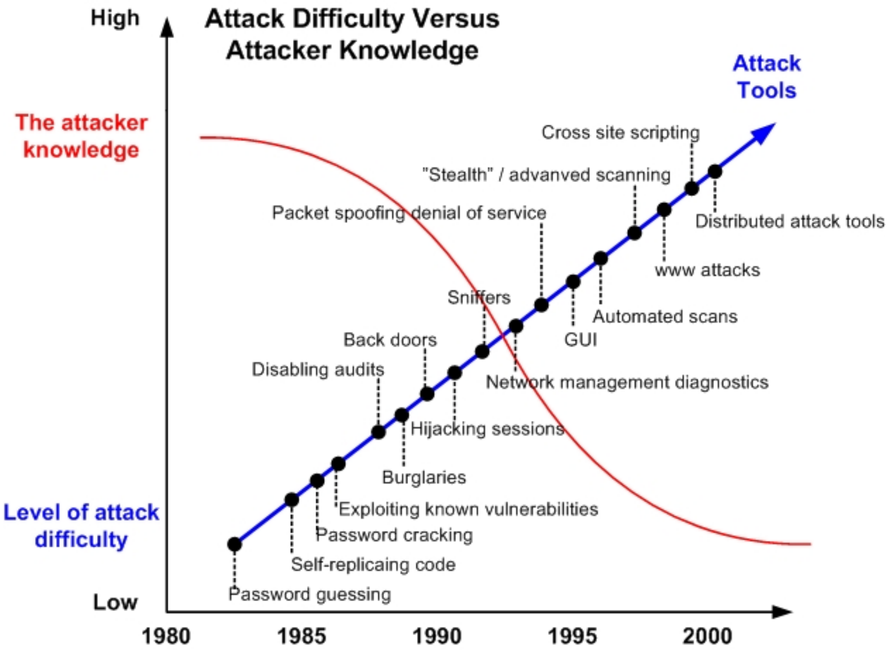


Figure A.1: Attack difficulty versus attacker knowledge.

Appendix B

Risk Assessment

This Appendix provides pages 21-25 in [SGF02] describing how to calculate the risk levels.

3.5 STEP 5: LIKELIHOOD DETERMINATION

To derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment, the following governing factors must be considered:

- Threat-source motivation and capability
- Nature of the vulnerability
- Existence and effectiveness of current controls.

The likelihood that a potential vulnerability could be exercised by a given threat-source can be described as high, medium, or low. Table 3-4 below describes these three likelihood levels.

Table 3-4. Likelihood Definitions

Likelihood Level	Likelihood Definition
High	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Medium	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

Output from Step 5—Likelihood rating (High, Medium, Low)

3.6 STEP 6: IMPACT ANALYSIS

The next major step in measuring level of risk is to determine the adverse impact resulting from a successful threat exercise of a vulnerability. Before beginning the impact analysis, it is necessary to obtain the following necessary information as discussed in Section 3.1.1:

- System mission (e.g., the processes performed by the IT system)
- System and data criticality (e.g., the system’s value or importance to an organization)
- System and data sensitivity.

This information can be obtained from existing organizational documentation, such as the mission impact analysis report or asset criticality assessment report. A mission impact analysis (also known as business impact analysis [BIA] for some organizations) prioritizes the impact levels associated with the compromise of an organization’s information assets based on a qualitative or quantitative assessment of the sensitivity and criticality of those assets. An asset criticality assessment identifies and prioritizes the sensitive and critical organization information assets (e.g., hardware, software, systems, services, and related technology assets) that support the organization’s critical missions.

If this documentation does not exist or such assessments for the organization's IT assets have not been performed, the system and data sensitivity can be determined based on the level of protection required to maintain the system and data's availability, integrity, and confidentiality. Regardless of the method used to determine how sensitive an IT system and its data are, the system and information owners are the ones responsible for determining the impact level for their own system and information. Consequently, in analyzing impact, the appropriate approach is to interview the system and information owner(s).

Therefore, the adverse impact of a security event can be described in terms of loss or degradation of any, or a combination of any, of the following three security goals: integrity, availability, and confidentiality. The following list provides a brief description of each security goal and the consequence (or impact) of its not being met:

- **Loss of Integrity.** System and data integrity refers to the requirement that information be protected from improper modification. Integrity is lost if unauthorized changes are made to the data or IT system by either intentional or accidental acts. If the loss of system or data integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud, or erroneous decisions. Also, violation of integrity may be the first step in a successful attack against system availability or confidentiality. For all these reasons, loss of integrity reduces the assurance of an IT system.
- **Loss of Availability.** If a mission-critical IT system is unavailable to its end users, the organization's mission may be affected. Loss of system functionality and operational effectiveness, for example, may result in loss of productive time, thus impeding the end users' performance of their functions in supporting the organization's mission.
- **Loss of Confidentiality.** System and data confidentiality refers to the protection of information from unauthorized disclosure. The impact of unauthorized disclosure of confidential information can range from the jeopardizing of national security to the disclosure of Privacy Act data. Unauthorized, unanticipated, or unintentional disclosure could result in loss of public confidence, embarrassment, or legal action against the organization.

Some tangible impacts can be measured quantitatively in lost revenue, the cost of repairing the system, or the level of effort required to correct problems caused by a successful threat action. Other impacts (e.g., loss of public confidence, loss of credibility, damage to an organization's interest) cannot be measured in specific units but can be qualified or described in terms of high, medium, and low impacts. Because of the generic nature of this discussion, this guide designates and describes only the qualitative categories—high, medium, and low impact (see Table 3.5).

Table 3-5. Magnitude of Impact Definitions

Magnitude of Impact	Impact Definition
High	Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human death or serious injury.
Medium	Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human injury.
Low	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest.

Quantitative versus Qualitative Assessment

In conducting the impact analysis, consideration should be given to the advantages and disadvantages of quantitative versus qualitative assessments. The main advantage of the qualitative impact analysis is that it prioritizes the risks and identifies areas for immediate improvement in addressing the vulnerabilities. The disadvantage of the qualitative analysis is that it does not provide specific quantifiable measurements of the magnitude of the impacts, therefore making a cost-benefit analysis of any recommended controls difficult.

The major advantage of a quantitative impact analysis is that it provides a measurement of the impacts' magnitude, which can be used in the cost-benefit analysis of recommended controls. The disadvantage is that, depending on the numerical ranges used to express the measurement, the meaning of the quantitative impact analysis may be unclear, requiring the result to be interpreted in a qualitative manner. Additional factors often must be considered to determine the magnitude of impact. These may include, but are not limited to—

- An estimation of the frequency of the threat-source's exercise of the vulnerability over a specified time period (e.g., 1 year)
- An approximate cost for each occurrence of the threat-source's exercise of the vulnerability
- A weighted factor based on a subjective analysis of the relative impact of a specific threat's exercising a specific vulnerability.

Output from Step 6—Magnitude of impact (High, Medium, or Low)

3.7 STEP 7: RISK DETERMINATION

The purpose of this step is to assess the level of risk to the IT system. The determination of risk for a particular threat/vulnerability pair can be expressed as a function of—

- The likelihood of a given threat-source's attempting to exercise a given vulnerability
- The magnitude of the impact should a threat-source successfully exercise the vulnerability
- The adequacy of planned or existing security controls for reducing or eliminating risk.

To measure risk, a risk scale and a risk-level matrix must be developed. Section 3.7.1 presents a standard risk-level matrix; Section 3.7.2 describes the resulting risk levels.

3.7.1 Risk-Level Matrix

The final determination of mission risk is derived by multiplying the ratings assigned for threat likelihood (e.g., probability) and threat impact. Table 3.6 below shows how the overall risk ratings might be determined based on inputs from the threat likelihood and threat impact categories. The matrix below is a 3 x 3 matrix of threat likelihood (High, Medium, and Low) and threat impact (High, Medium, and Low). Depending on the site's requirements and the granularity of risk assessment desired, some sites may use a 4 x 4 or a 5 x 5 matrix. The latter can include a Very Low /Very High threat likelihood and a Very Low/Very High threat impact to generate a Very Low/Very High risk level. A "Very High" risk level may require possible system shutdown or stopping of all IT system integration and testing efforts.

The sample matrix in Table 3-6 shows how the overall risk levels of High, Medium, and Low are derived. The determination of these risk levels or ratings may be subjective. The rationale for this justification can be explained in terms of the probability assigned for each threat likelihood level and a value assigned for each impact level. For example,

- The probability assigned for each threat likelihood level is 1.0 for High, 0.5 for Medium, 0.1 for Low
- The value assigned for each impact level is 100 for High, 50 for Medium, and 10 for Low.

Table 3-6. Risk-Level Matrix

Threat Likelihood	**Impact**		
	Low (10)	***Medium*** (50)	***High*** (100)
High (1.0)	**Low** 10 X 1.0 = 10	**Medium** 50 X 1.0 = 50	**High** 100 X 1.0 = 100
Medium (0.5)	**Low** 10 X 0.5 = 5	**Medium** 50 X 0.5 = 25	**Medium** 100 X 0.5 = 50
Low (0.1)	**Low** 10 X 0.1 = 1	**Low** 50 X 0.1 = 5	**Low** 100 X 0.1 = 10

Risk Scale: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)[8]

3.7.2 Description of Risk Level

Table 3-7 describes the risk levels shown in the above matrix. This risk scale, with its ratings of High, Medium, and Low, represents the degree or level of risk to which an IT system, facility, or procedure might be exposed if a given vulnerability were exercised. The risk scale also presents actions that senior management, the mission owners, must take for each risk level.

Table 3-7. Risk Scale and Necessary Actions

Risk Level	**Risk Description and Necessary Actions**
High	If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
Medium	If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
Low	If an observation is described as low risk, the system's DAA must determine whether corrective actions are still required or decide to accept the risk.

Output from Step 7—Risk level (High, Medium, Low)

[8] If the level indicated on certain items is so low as to be deemed to be "negligible" or non significant (value is <1 on risk scale of 1 to 100), one may wish to hold these aside in a separate bucket in lieu of forwarding for management action. This will make sure that they are not overlooked when conducting the next periodic risk assessment. It also establishes a complete record of all risks identified in the analysis. These risks may move to a new risk level on a reassessment due to a change in threat likelihood and/or impact and that is why it is critical that their identification not be lost in the exercise.

Appendix C

Voiceline's Concept

The successive pages provice the Danish description of Voiceline's concept.

Voiceline 19. juni 2005

Konceptbeskrivelse.

IP matrix - et VOIP projekt.

Indhold

1. Projektbeskrivelse…………………………………………………………………… 1

2. Løsninger på markedet……………………………………………………………… 2

2.1 Model 1. Punkt til Punkt IP/VPN……………………………………………… 3

2.2 Model 2. peer to peer…………………………………………………… ….. 4

2.3 Model 3. Boligforeninger………………………………………………………. 5

3. Voiceline´s løsning……………………………………….…….……………….. 6

3.1 Model 4. IP matrix…………………………….……………………….…….. 7

3.2 IP matrix (Oversigt)……………………………………………….………..... 8

3.3 IP matrix (kundenet)……….……………………………………………….… 9

3.4 IP matrix (Full Mesh)…………………………………….…..….…………… 10

3.5 IP matrix (Hosting Center)……….….……………………………….…….... 11

3.6 IP matrix (Telefoni)………………………………………….…………………. 12

3.7 Model 5. IP matrix med ENUM…………………….……..….………….… 13

Projektbeskrivelse

Dette oplæg beskriver et koncept som Voiceline har valgt at kalde IP matrix. Denne matrix knytter principielt alle kendte VOIP udbydere sammen, i et virtuelt MPLS miljø. ENUM håndtere persondata og danner bro imellem PSTN og Internet.

konceptbeskrivelse skal danne grundlag for et projekt, som identificerer, opdeler og beskriver de forskellige elementer, som nødvendigvis må indgå i en sammensat løsning jf. figur 10 på side 13. De forskellige elementer bør efterfølgende analyseres i separate projekter.

Formålet med konceptbeskrivelsen er at danne grundlag for en række løsningsorienterede forskningsprojekter, som samlet set skal bidrage til viden omkring ”IP telefoni” i forhold til sikkerhed, redundans (tilgængelighed) og tale kvalitet. Projekterne tager udgangspunkt i Voiceline´s løsningsmodel, som beskrevet i denne konceptbeskrivelse, men projekterne skal være 100 % uvildige.

Løsninger på markedet

Der skelnes grundlæggende imellem to typer af løsninger på markedet, åbne Internetbaserede løsninger, som anses for at være de ”usikre” løsninger med stor funktionalitet og de lukkede løsninger som anses for at være de ”sikre” løsninger, med lav funktionalitet.

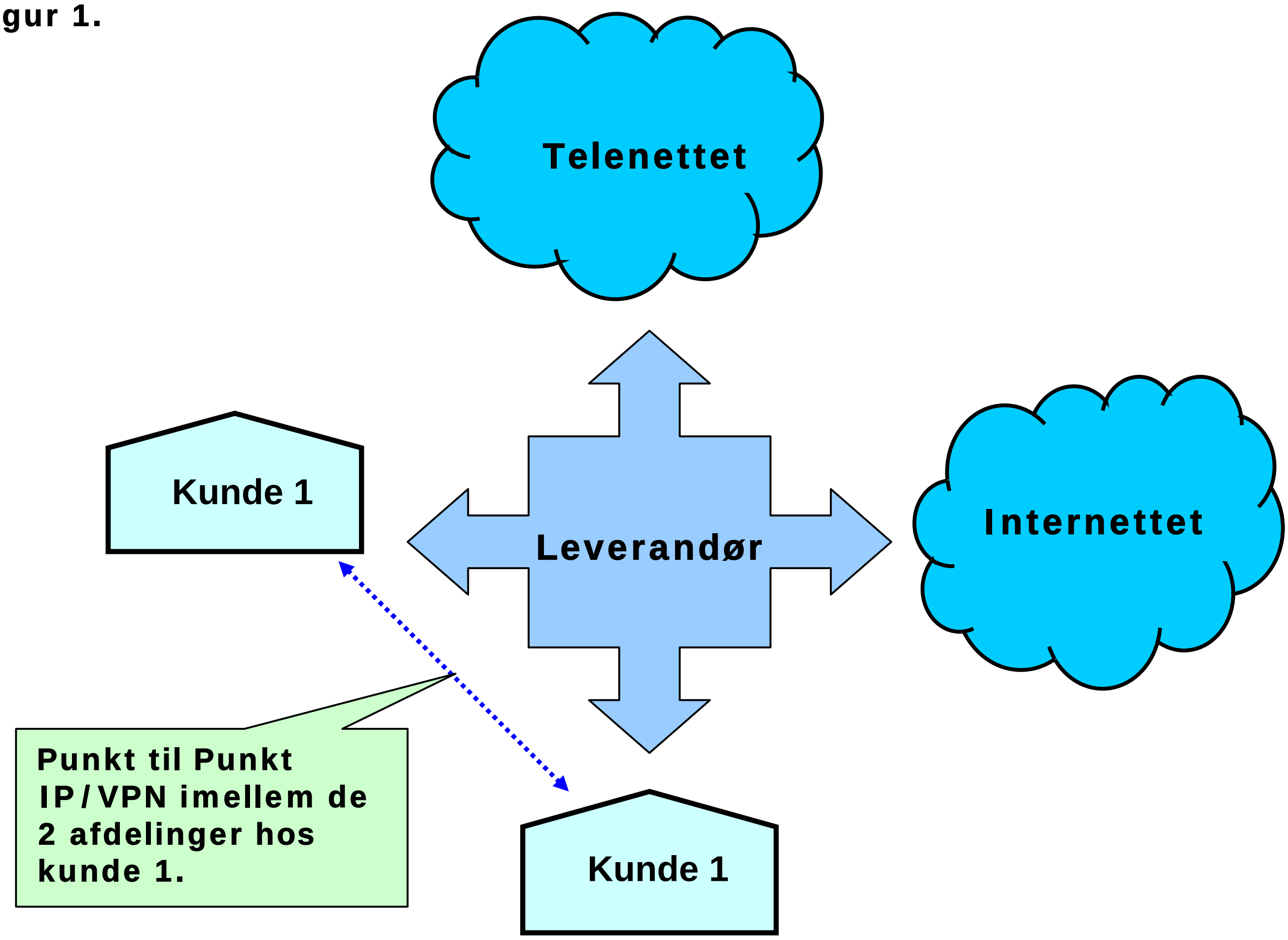
Model 1. Punkt til Punkt IP/VPN

Denne (lukkede) løsning startede med IP backbones og Punkt til Punkt (leased line) forbindelser imellem to adresser. Løsningen er typisk en XDSL forbindelse med IP/VPN på MPLS eller ATM. Denne løsning er det eneste "sikre" alternativ til traditionel telefoni via ISDN.

Fungerer via virtuelle LAN på udbyderens eget, eller en kombination af forskellige udbyderes kobber eller fiber net. Sikkerheden er som udgangspunkt god, og kvaliteten kan sidestilles med traditionel telefoni.

Telefoni og data køres over samme linie og giver derfor virksomheden besparelser. Virksomheden kan dog kun kommunikere frit imellem egne afdelinger og betaler for opkald uden for egen organisation.

Figur 1.

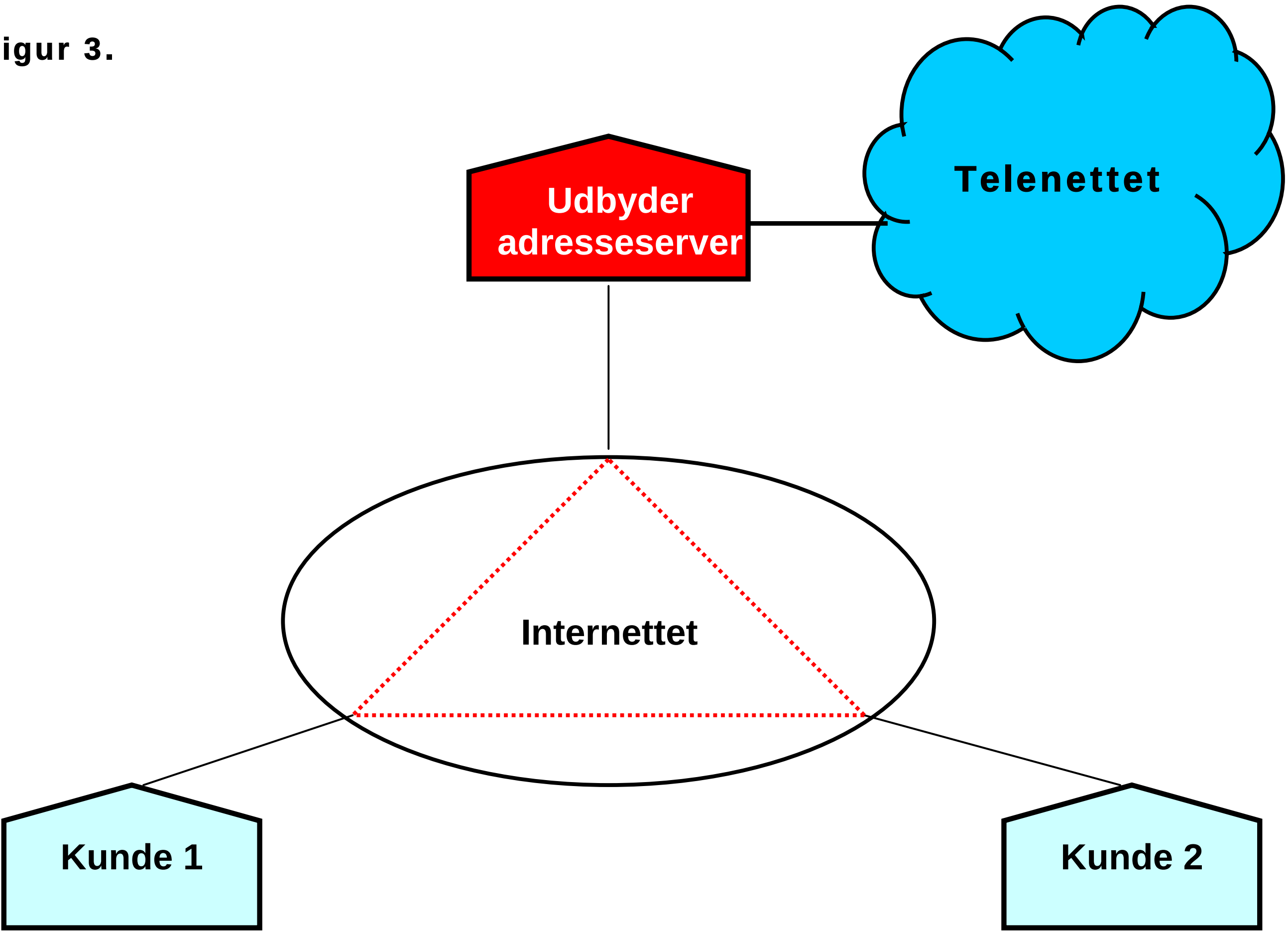


Model 2. Peer to peer

Denne (åbne) løsning levers af mange VOIP udbydere på marked i dag. Nogle vælger at sælge en omformerboks kaldet en ATA adapter med i løsningen. Det betyder så at kunden kan tilslutte sin normale telefon til adapteren, i stedet for at bruge en PC soft phone.

Denne peer to peer løsning er foruden XDSL abonnementet, i princippet ”gratis” - når vi taler ren IP trafik. Mangel på QoS, (Quality of Service), i denne løsning kan potentielt skabe så meget delay (jitter), at talen bliver uforståelig. Sikkerheden kan også nemmere kompromitteres.

Figur 3.



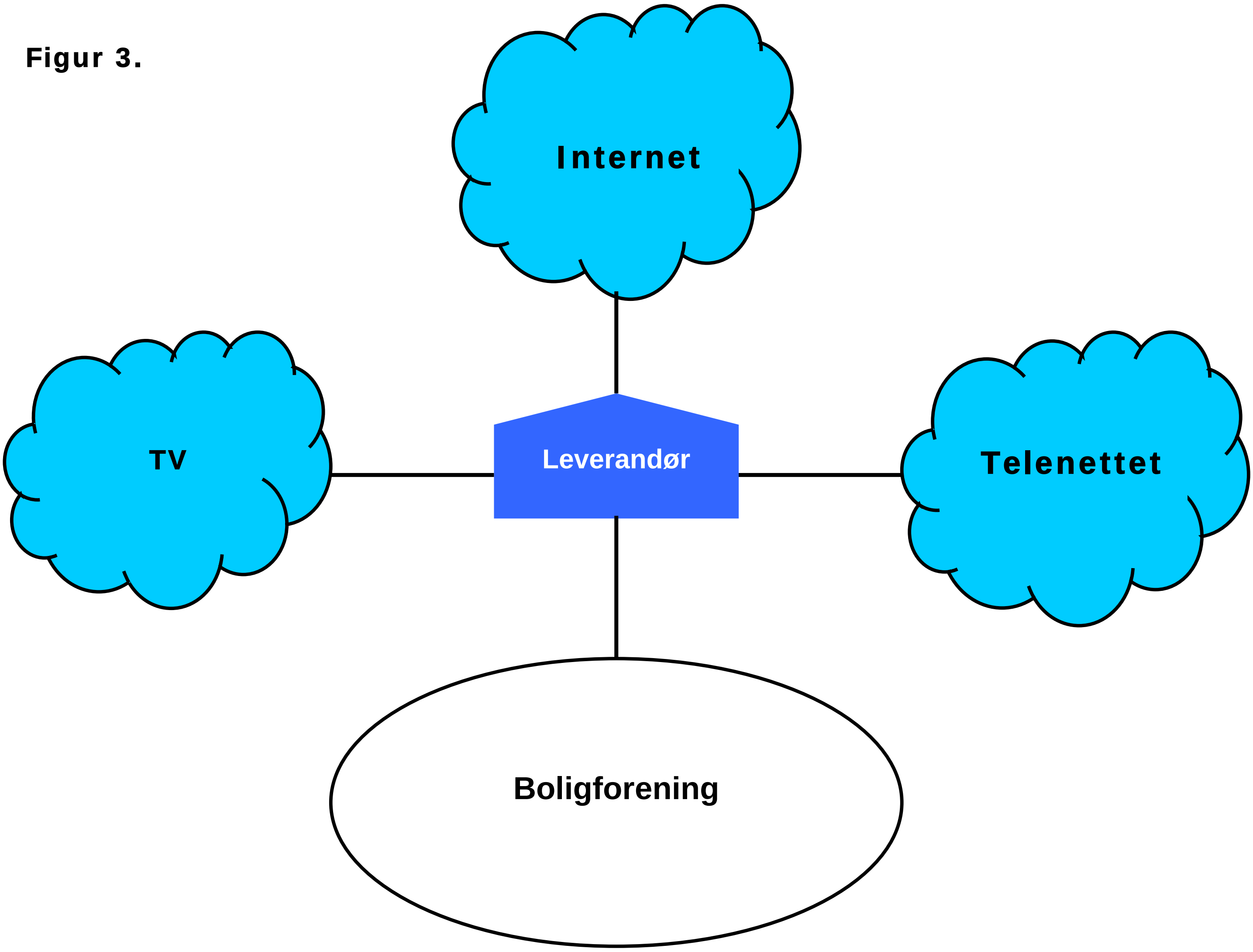
Model 3. Boligforeninger.

Denne (lukkede) løsning kendes fra virksomheder som typisk leverer til boligforeninger.

Leverandøren bygger et fiber eller kobber LAN hos boligforeningen, derved opnår man principielt den samme sikkerhed som man kunne opnå på et privat LAN.

Telefoni, data og TV - køres over samme linie og giver derfor kunden besparelser. Kunden kan kommunikere frit i eget net og betaler kun for almindelige opkald.

Figur 3.



Voiceline´s løsning

Løsningen bygges primært på eksisterende komponenter og teknologi. Løsning giver i princippet peer to peer funktion, i et lukket MPLS miljø. Derfor kan man sige at denne løsning tager de bedste egenskaber fra de foregående løsninger. Voiceline´s koncept ”IP matrix” tilsigter at sætte standarten for sikkerhed i lukkede miljøer.

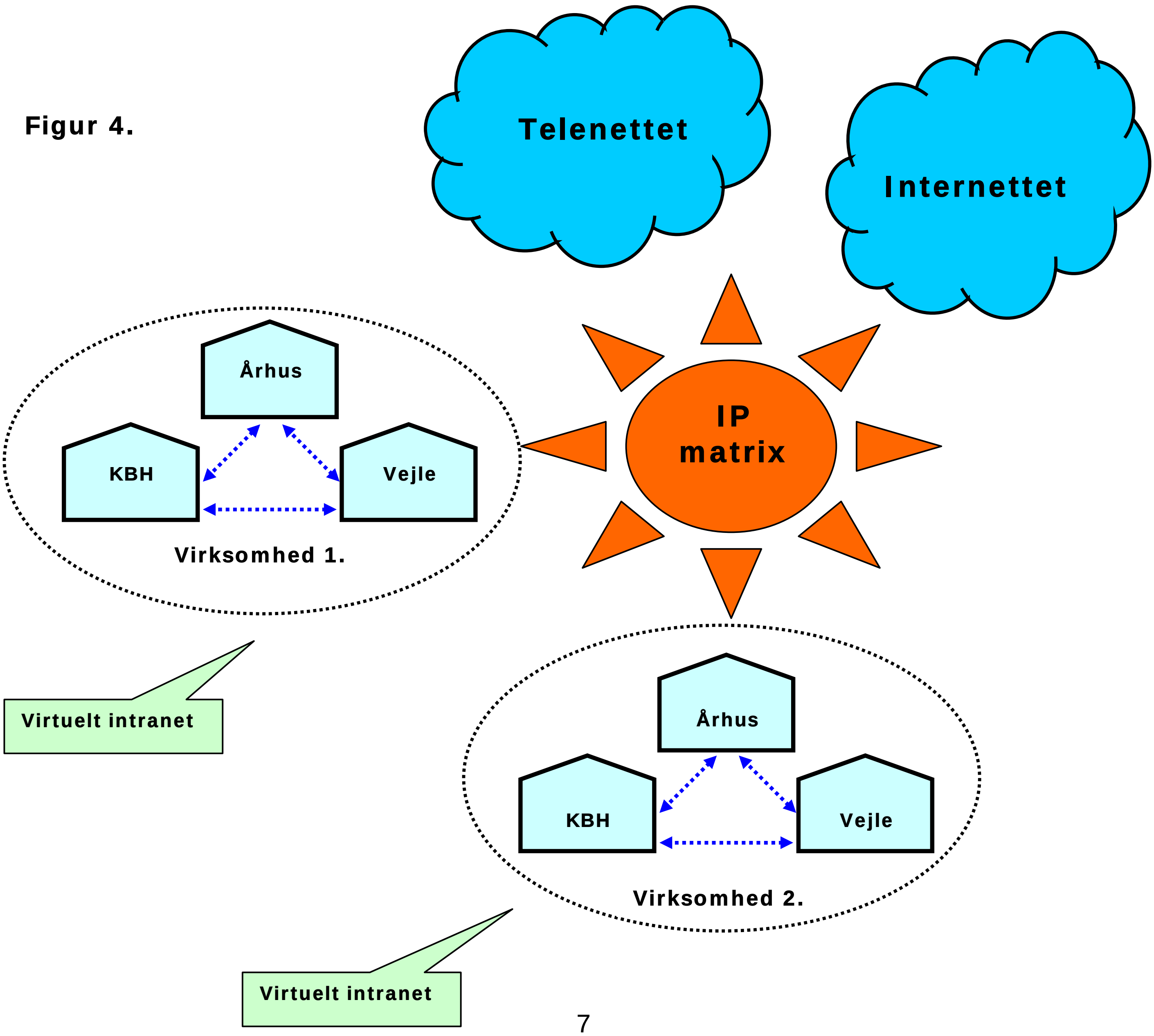
Model 4. IP matrix

I denne (lukkede) løsningen kan alle brugere af matrixen kommunikere frit IP til IP. Sikkerheden i denne løsning er i teorien - optimal.

Tesen er, at bruger ID er den eneste måde at løse de sikkerhedsmæssige udfordringer som truer Internettet. Hvis man ikke bliver godkendt som registreret bruger I matrixens host center, så kan man ikke få adgang til matrixen og derfor kan man heller ikke kompromitterer sikkerheden.

Denne løsning skal analyseres i forhold til sikkerhed, redundans (tilgængelighed) og tale kvalitet, derfor har Voiceline indgået samarbejde med DTU.

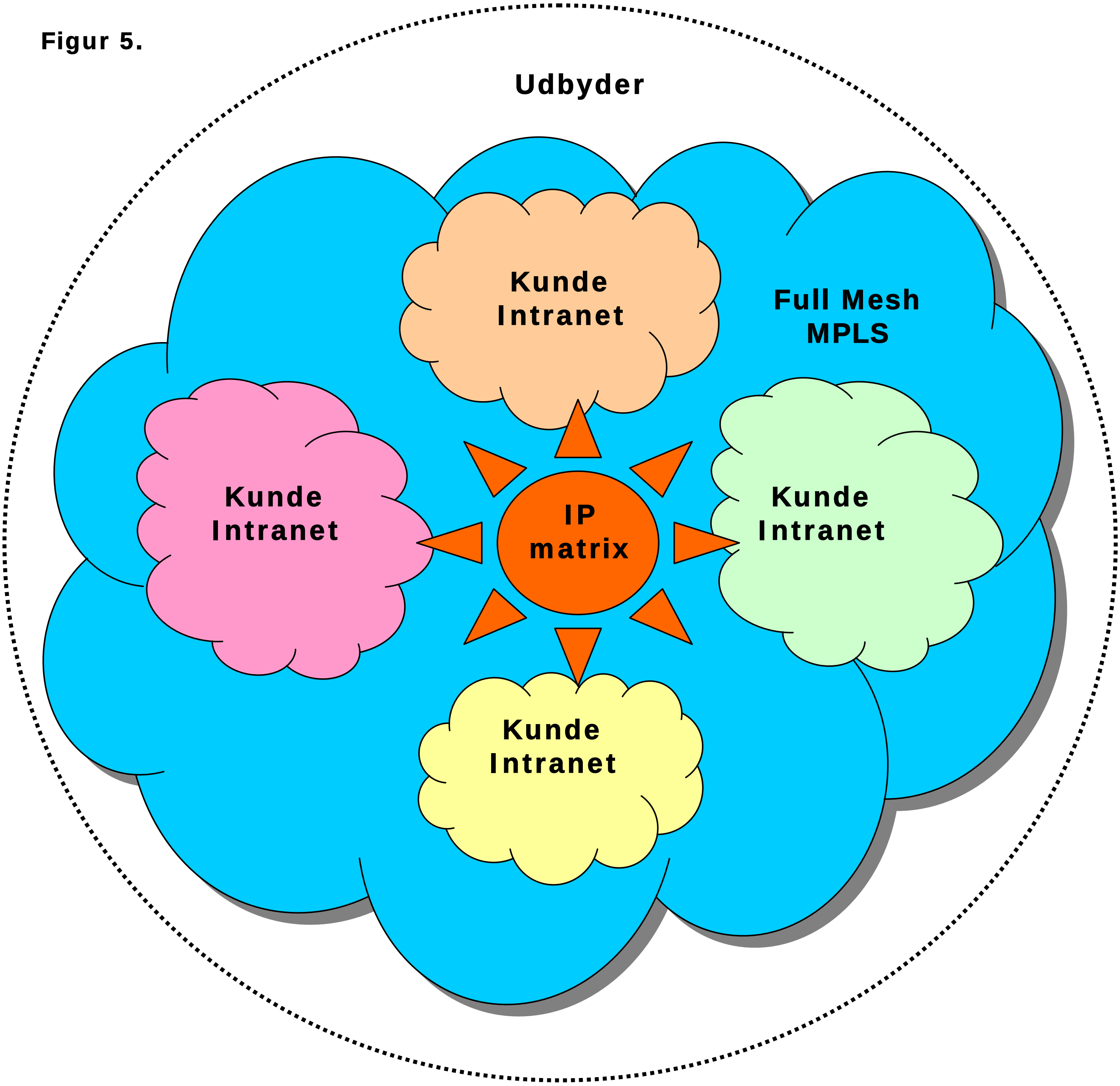
Figur 4.



IP matrix (Oversigt)

Den tekniske løsning skal bæres af MPLS (Multi Protocol Label Switching). Begrundelsen for at benytte denne teknologi er sikkerhed, samt det faktum, at de enkelte intranet kan opdeles på en hensigtsmæssig måde, som samtidig giver mulighed for integration af hosted services til den enkelte kunde.

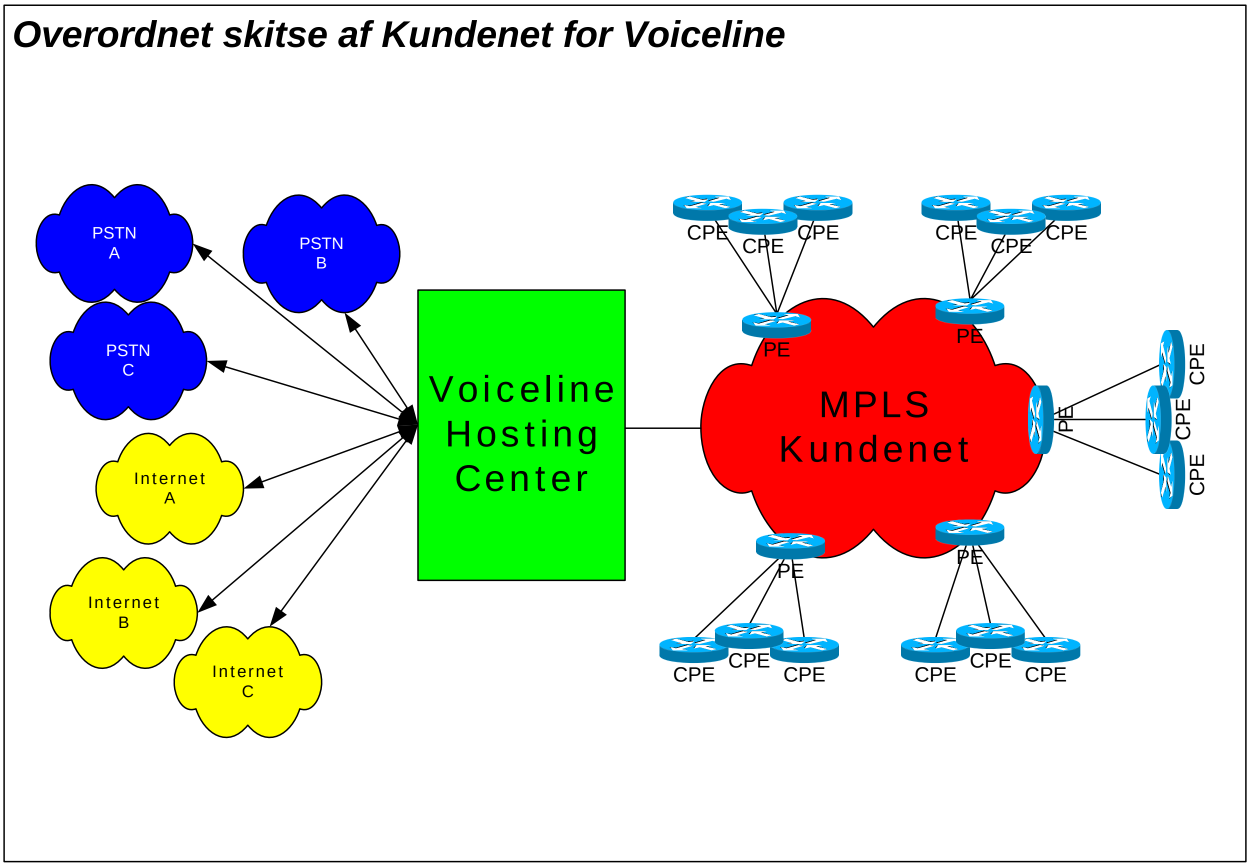
Figur 5.



IP matrix (kundenet)

Som det fremgår af figur 6. består nettet af et MPLS net. Nettet giver mulighed for end-to-end QOS (Quality Of Service). Fordelene ved MPLS og label switchede netværk, frem for destinationsbaseret IP routing er mange. En nærmere uddybning af dette kan findes i Voiceline´s og IMM´s projekt ”Security in VOIP Systems”.

Figur 6.



Overordnet skitse af Kundenet for Voiceline

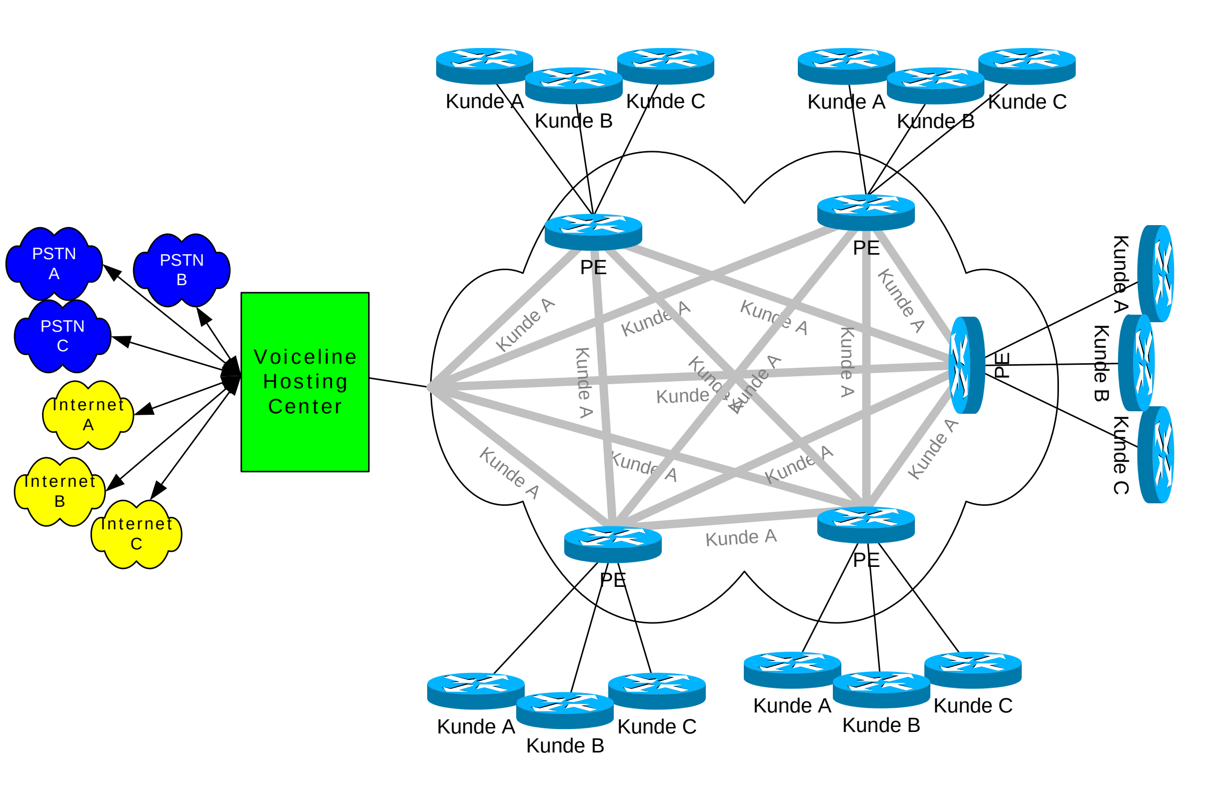
IP matrix (Full Mesh)

Dette setup gør det muligt at give virksomhederne et Full Meshed netværk. Et Full Meshed net betyder at virksomhederne altid benytter den korteste vej imellem de forskellige afdelinger og at løsningen er redundant, da der altid er alternative ruter.

En anden fordel, ved et sådan system, er at virksomheder tilsluttet dette netværk, kan ringe til hinanden gennem dette netværk.

Figur 7.

Overordnet skitse af Kundenet for Voiceline



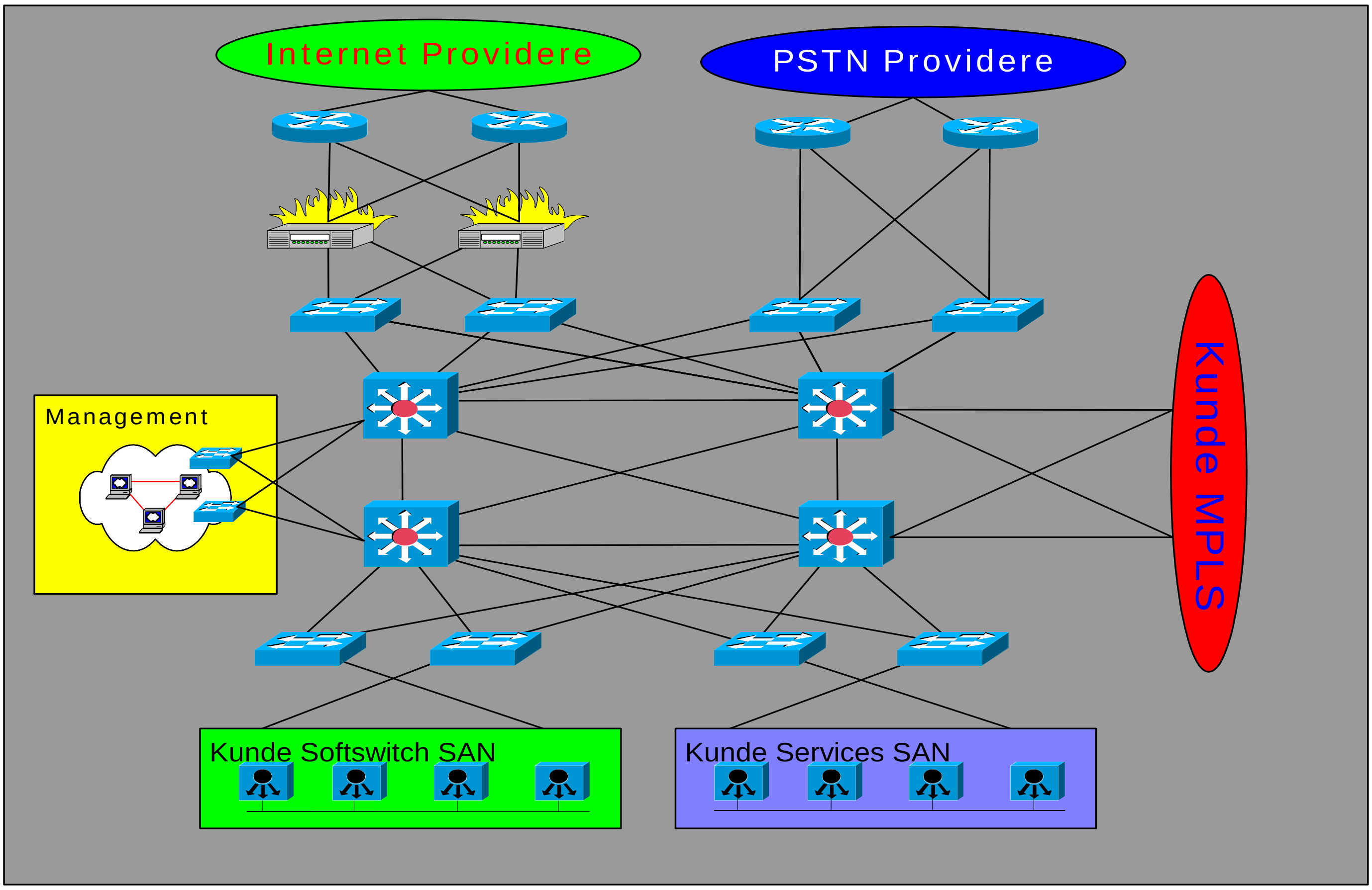
IP matrix (Hosting Center)

Centeret er selve hjertet i hele netværket. En af de ting som er vigtig i dette Center, er at sikre den enkelte virksomhed, total adskillelse fra de andre kunder på nettet. Derfor må det sikres at der ikke er forbindelse mellem de enkelte netværk. I figur 10 vises den principielle opbygning af selve centeret. Centeret terminerer alle MPLS forbindelser. For at sikre den maksimale oppe tid, er der indført fire store lag 3 switche.

To switche har til formål at leverer forbindelse til PSTN nettet og Internettet. Virksomhederne terminerer direkte på switche i hosting centeret. Dette betyder at udstyret i selve hosting centeret skal være i stand til at håndterer mange VRF'er (VPN Routing and Forwarding).

Figur 8 viser bare det overordnede billede. De enkelte gateways placeres evt. i forskellige lande.

Figur 8.



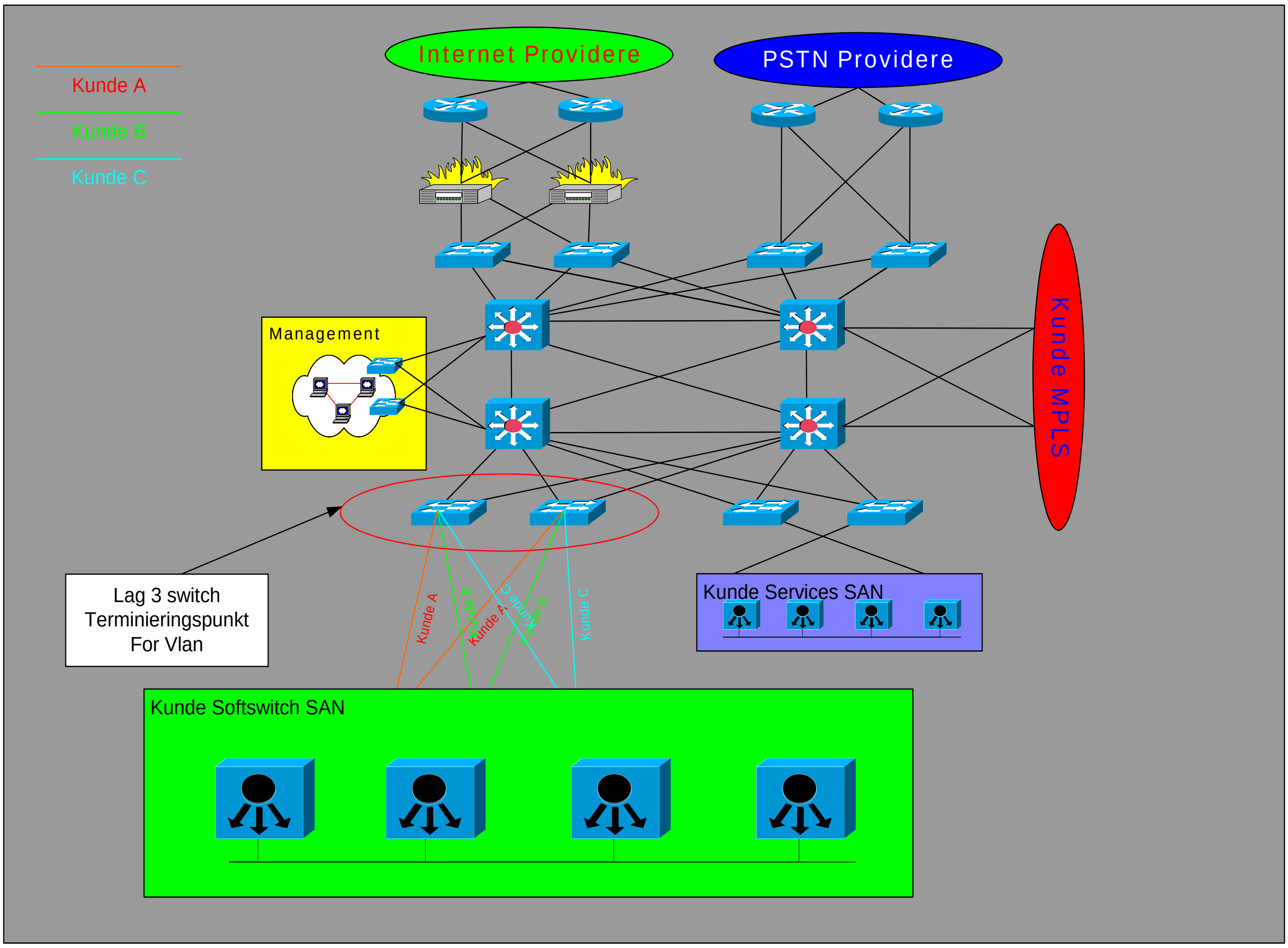
IP matrix (Telefoni)

Et af de vigtigste hensyn er sikkerheden. For at sikre virksomhederne, terminers de enkelte virksomheder direkte på en PE router, hvorfra den enkelte kunde bliver tildelt et VLAN.

VLAN's er i princippet logiske adskilte LAN, som en Lag 3 switch kan route imellem. Ser vi på figur 9 kan vi se hver kunde er opdelt i deres eget VLAN.

Således kan virksomhederne i dette netværk ikke se hinanden. Kunden oplever at have sin egen switch som kan route kald imellem andre kunder i matrixen, såvel som til modtagere i telenettet (PSTN).

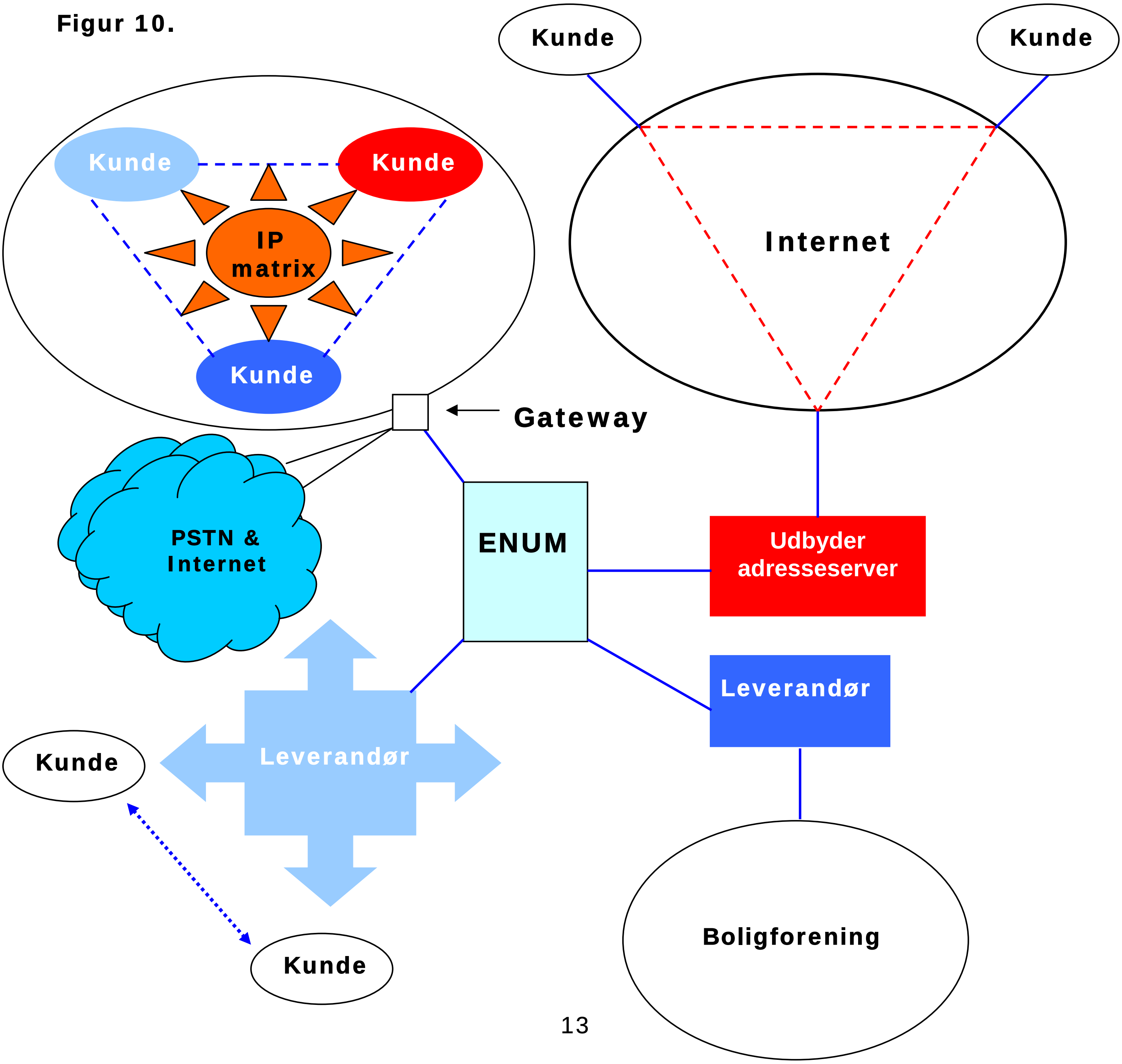
Figur 9.



Model 4. IP matrix med ENUM

Denne løsning er ment som et reelt bud på fremtidens løsning. Den binder eksisterende løsninger på markedet sammen via ENUM. IP matrixen hoster de eksisterende udbyderes løsning. Med brugeridentifikation og adgangskontrol er det tesen, at man kan forhindre uautoriseret adgang til matrixen. Med Intrusion detection (IDS), skal matrixen via neurale netværk, være i stand til at indlede realtidsmodangreb på uautoriserede forsøg på at skaffe sig adgang til matrixen.

Figur 10.



Appendix G

Contact Persons

Name	**Title**	**Company**	**Contact Information**
Anders Pedersen	Product Manager, Voice	Flextronics Network Services A/S, supplier of Alcatel components	anders.pedersen@dk.flextronics.com
Claus Flygenring	Product Manager, Data	Flextronics Network Services A/S, supplier of Alcatel components	claus.flygenring@dk.flextronics.com
Jytte Noerulf	Responsible for the telephony network	Elsam A/S	jyn@Elsam.com
Kjeld T. Petersen	Responsible for the data network	Elsam A/S	ktp@Elsam.com
Michael Stamm	Specialized Consultant	UNI-C	michael.stamm@uni-c.dk
Ole Villadsen	Salesperson	Nortel Networks A/S	olev@nortel.com
Patrick W. Ireland	Entrepreneur	Voiceline	patrick@voiceline.dk
Preben Andersen	Manager Consultant and Superintendent of DK-CERT	UNI-C	preben.andersen@uni-c.dk
Preben Jensen	Technician	NetConcept A/S, supplier of Avaya components	pje@netkoncept.dk
Sten Buus	IT Manager	Elsam A/S	sbj@Elsam.com

Appendix H

Project Plan

The successive pages provide an overview of the project plan made in Microsoft Project Professional 2003.

ID	ℹ	Task Name	Start	Finish
1		**Project start**	**Thu 17-03-05**	**Mon 11-04-05**
2	📅 📝	Main search for litterature	Thu 17-03-05	Fri 01-04-05
3	📅	Acquire general information on notions and components	Thu 17-03-05	Mon 11-04-05
4				
5		**Elsam requirement specification**	**Wed 16-03-05**	**Fri 06-05-05**
6	📅 📝	Contact Elsam	Wed 16-03-05	Thu 14-04-05
7	📅	Analyse the received requirement specification	Thu 14-04-05	Mon 18-04-05
8	📅	Dialogue with Elsam	Tue 19-04-05	Fri 06-05-05
9				
10		**Component analysis**	**Mon 27-06-05**	**Fri 12-08-05**
11	📅	Contact Cisco Systems	Mon 27-06-05	Fri 22-07-05
12	📅	Contact Flextronics (Supplier of Alcatel components)	Mon 27-06-05	Fri 22-07-05
13	📅	Contact Netconcept (Supplier of Avaya components)	Mon 27-06-05	Fri 22-07-05
14	📅	Contact Nortel Networks	Mon 27-06-05	Fri 22-07-05
15	📅	Component analysis	Mon 11-07-05	Fri 29-07-05
16	📅	Compare components	Mon 01-08-05	Fri 12-08-05
17				
18		**Report development**	**Mon 21-03-05**	**Mon 29-08-05**
19	📅	Make Master Document	Mon 21-03-05	Mon 21-03-05
20	📅	Write keywords in Master Document	Mon 21-03-05	Mon 25-07-05
21	📅	Write requirement specification	Thu 07-04-05	Fri 15-04-05
22	📅	Main focus on the report	Thu 30-06-05	Fri 12-08-05
23	📅	Delivery of the report	Mon 29-08-05	Mon 29-08-05
24		**Project Close**	**Wed 31-08-05**	**Fri 30-09-05**
25	📅	Prepare presentation slides	Wed 31-08-05	Fri 09-09-05
26	📅	Practice presentation	Thu 15-09-05	Tue 20-09-05
27	📅	Presentation Day	Mon 26-09-05	Fri 30-09-05

Glossary

A

Abstract Syntax Notation One (ASN.1) A formal language for abstractly describing messages to be exchanged among an extensive range of applications including VoIP.

Address Resolution Protocol (ARP) A TCP/IP protocol used to map an IP address to a physical hardware (MAC) address.

Address spoofing A type of attack in which the attacker steals a legitimate network address of a system and uses it to impersonate the system that owns the address.

Addressing A method for identifying the components, such as the terminals, on a network by assigning them a unique address.

Advanced Encryption Standard (AES) A symmetric block cipher encryption algorithm that is used to protect sensitive data. AES uses keys of 128-, 192-, or 256- bit lengths and is helping to phase out and replace the Data Encryption Standard (DES) and Triple DES (3DES) which are based on less secure and easier breakable, cryptography algorithms.

Application Level Gateway (ALG) It is considered as one of the most advanced form of firewalls since it is able to filter traffic based on knowledge about specific protocols. ALG can be implemented as a VOIP aware firewall.

Assets Averything a company owns, such as money, equipments, buildings and computer related data.

Asymmetric encryption A method where different keys are used for encryption and decryption.

Asynchronous Digital Subscriber Line (ADSL) A technology that allows more data to be sent over existing copper telephone lines.

Asynchronous Transfer Mode (ATM) A connection-oriented packet switching technology that combines some of the advantages from packet and circuit switching networks. It is based on a fixed-length 53-byte cell and all broadband transmissions (whether audio, data, imaging or video) are divided into series of cells and routed across an ATM network consisting of links connected by ATM switches.

Authentication A secure process by which a call controller, IP phone, media gateway, or other component verifies the authenticity of a user or call before access is permitted to a resource or device. A username and password exchange is the most common form of authentication, although considered increasingly limited as far as security effectiveness.

Authentication Header (AH) A protocol used in IPSec for data authentication and protection against replays. The authentication is provided for as much of the IP header as possible as well as the for upper layer protocol data.

Authorization The process of assigning privileges, or allowing access to resources, based on identity.

Availability Assets, information and services are accessible when it is requested by authorized users.

B

Backbone The part of a network that acts as the primary path for traffic moving between networks.

Biometrics A method for generating unique, replicable authentication data by digitizing measurements based on physical characteristic that can be used to communicate with a system. Often a fingerprint, facial characteristic such as retinal pattern, voiceprint or handwriting is used to determine the correct identity.

Border Gateway Protocol (BGB) A dynamic routing protocol used between inter-domains to exchange routing information.

Brute force attack An attack method where the attacker tries all the combinations available to guess a secret (such as a password).

Buffer overflow The effect of placing more information than can be stored in a temporary data storage area or buffer. The data that does not fit within the allocated buffer space can overflow into the preceding buffers, thus overwriting or corrupting data. The overflow portion of the data can, in some attacks, then provide instructions to execute commands not intended by the application that originally allocated the buffers. This condition also results in system crashes, the creation of a back door leading to system access or a denial of service. The buffer overflow attack is usually aimed at servers or controllers.

C

Cache Memory that holds copies of recently accessed data.

Call control Is used to monitor and maintain connections once they have been established.

Certificate A set of data issued by a trusted Certificate Authority (CA) to an individual, device or other entity (an IP phone, or application), after the authority has verified the authenticity of the entity, for use by that entity in proving proper identification and credentials to a third party. A digital certificate is tamper-proof and cannot be forged, and is signed by the private key of the Certification Authority which issued it.

CIA-requirements Confidentiality, integrity and availability (CIA) requirements. The three different security aspects regarding computer systems. These requirements are typically listed when preparing a requirement specification regarding security. See the glossary for Confidentiality, Integrity and Availability respectively.

Circuit switching A method for establishing dedicated connection between the end systems through one or more switching nodes. The data is sent in one continuous stream after establishment of the connection. Unlike other methods of transmission, such as packet switching, it requires the link to be established before any communication can take place. Circuit switching is characteristic of telephone connections.

Closed networks Closed networks are considered secure as the network limits the access only for users of a certain community or group.

Codec Short for COding/DECoding.

Common Criteria (CC) An international standard (ISO 15408) for computer security. Its purpose is to allow users to specify their security requirements, to allow developers to specify the security attributes of their products, and to allow evaluators to determine if products actually meet their claims.

Confidentiality Has been defined by the International Standards Organization (ISO) as "ensuring that information is accessible only to those authorized to have access". Confidentiality is one of the design goals for many cryptosystems, made possible in practice by the techniques of modern cryptography.

Connection-oriented A network where the connections have to be established before data can be transmitted.

Connectionless A type of protocol that sends the data across the network to its destination without guaranteeing data delivery.

Cracker A person who engages in one or more of the following: 1) breaks into a computer system; 2) figures out ways to bypass security or license protection in software; 3) intentionally breaches computer security. Contrary to popular belief, a cracker is not synonymous with hacker.

D

Data Encryption Standard (DES) The most common encryption algorithm with symmetric keys. Like other private key cryptographic methods, both the sender and the receiver must know and use the same private key. DES applies a 56-bit key to each 64-bit block of data. The process can run in several modes and involves 16 rounds or operations. Although this is considered ”strong” encryption, many companies use ”triple DES”, which applies three keys in succession.

Decoding Converting compressed data to their original form.

Demilitarized Zone (DMZ) A network area that is placed between an organization’s internal (corporate) network and an external network, usually the Internet. The DMZ allows connected hosts to provide services to the external network, while protecting the internal network from possible intrusions.

Denial-of-Service (DoS) A form of malicious network attack that deprives users or devices of access to a service that is normally available, such as network connectivity, VoIP call processing, email, and so on. DoS attacks are considered extremely difficult to defend against due to their many permutations and evolving nature. Buffer overflows and floods are typical methods that are used to induce a denial of service.

Dictionary style attack An attack method where the attacker uses a large set of likely combinations to guess a secret (such as a password).

Diffie Hellman A public key algorithm which allows two parties to agree on a secret key over an insecure communication.

Digital signature A piece of code that is used to authenticate the identity of the sender. A private key is used to create the digital signature, and a corresponding public key is used to verify that the signature is really generated by the holder of the private key.

Digital voice Analog voice that has been digitized, converted to bits.

Distributed Denial of Service (DDoS) An attack against a site or server launched from multiple sources. This is sometimes carried out by concealed exploiting servers to function as agents for transmitting the attacks. In many cases, the attacker will place client software on a number of unsuspecting remote computers and then use these computers to launch the attack. A Distributed Denial of Service attack is more effective than a simple Denial of Service attack, as the volume of traffic is considerably higher, and is more difficult to prevent. Examples of DDoS attacks are Syn flood, Smurf attack and Targa attack.

DK-Computer Emergency Response Team (DK-CERT) The Danish research and development center who focus on Internet security vulnerabilities, provide incident-response services to sites that have been victims of attack, publish security alerts, research security and survivability in WAN computing, and develop site security information.

Domain Naming System (DNS) An Internet service that translates domain names into IP addresses. Since domain names are alphabetic, they’re easier to remember. The Internet however, is based on IP addresses. Every time one uses a domain name, a DNS service must translate the name into the corresponding IP address. The DNS server is the server that performs the translation.

E

Eavesdropping Unauthorized intercepting and reading of messages.

Electronic Numbering (ENUM) A IETF standard that uses DNS to map telephone numbers to Web addresses or URL.

Elliptic curve cryptography An encryption method that uses public-key cryptography based on the mathematics of elliptic curves .

Encapsulating Security payload (ESP) A protocol used in IPSec for data confidentiality, protection against replays, and authentication. In contrast to AH, ESP does not authenticate the IP headers.

Encapsulation A technique used by layered protocols in which a layer adds header information to the protocol data from the layer above.

Encoding The conversion of analog voice to digital voice.

End-to-end Used to indicate the communication between two nodes in a network.

Extensible Authentication Protocol (EAP) A PPP authentication protocol which supports multiple authentication mechanisms. EAP typically runs directly over the link layer without requiring IP and therefore includes its own support for in-order delivery and retransmission.

F

Fiber A telecommunications medium made of thin glass fibers bundled inside an insulated cable. It is used for high-speed voice, video, and data transmission.

Fingerprint A one way hash value calculated over a digital certificate which serves as a unique identifier.

Firewall A firewall is a combination of hardware and software that secures the network from intruders. It is considered to be the first point of defense in a network and is usually placed between a company's corporate network and the public network.

Flooding An attack method used to pull of a DoS attack. Flooding occurs when an attacker overwhelm a server or a client with large amount of packets.

Forward Equivalence Class (FEC) A term in MPLS networks used for a group of packets that are forwarded in the same manner.

Frame The packets into which data is placed by the Data Link Layer.

Frame relay A high-speed packet switching protocol for connecting devices on a WAN.

Frequency Division Multiplexing (FDM) A technology for data transmission where multiple signals share a single transmission path, such as a cable or wireless system, each occupying a different frequency.

G

Gatekeeper A H.323 component in VoIP systems and are responsible for access control, address resolution, bandwidth control and call forwarding.

Gateway A highly intelligent switch that works as a translator between two dissimilar protocols, such as H.323 and SS7.

Global System for Mobile communication (GSM) The most widely used technology for mobile telephony.

GRE A method used to encapsulate IP packets.

H

H.225.0 call signaling A signaling protocol used in H.323 for negotiating call setup, controlling and terminating H.323 calls.

H.225.0 Registration, Admission and Status (H.225.0 RAS) A control protocol in H.323 that is used for registration, admission, address resolution and giving status messages between the terminals and their gatekeeper.

H.235 Defines different security profiles for H.323.

H.245 A H.323 protocol that establishes the channel that will be used for media transfer. Furthermore, H.245 negotiates a common voice compression and the logical channels that will be used by all the participating terminals in a session.

H.323 H.323 is a set of recommendations approved by ITU-T in 1996 for transmission of real-time voice, video and data communication over packet-switched networks. In VoIP systems H.323 is used for the signaling process.

Hacker Is used in the public to describe a malicious attacker, cracker. However, a hacker is actually any computer programmer who discover ways to make software run more efficiently.

Hashed MAC (HMAC) A unique value that is calculated by using a mathematical hash function on the MAC address.

Hop-by-hop A special case of end-to-end, where the endpoints are not terminal but other network components such as servers and gateways.

Hyper Text Transfer Protocol (HTTP) A communication protocol used to connect to servers on the World Wide Web (WWW). The primary function of HTTP is to establish a connection with a Web server and transmit HTML pages to the user's browser.

I

Integrated Services Digital Network (ISDN) A telecommunication technology used for transmitting digital voice and data over telephone lines at speeds up to 128Kbps.

Integrity Assures that assets can only be modified by authorized users and processes.

International Standard Organization (ISO) An non-governed organization that promotes the development of standards for computers. Developers of the OSI model.

International Telecommunication Union-Telecommunication (ITU-T) An organizations that develop standard for telecommunication technologies. Developers of H.323.

Internet Engineering Task Force (IETF) A large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual. Developers of SIP.

Internet Protocol (IP) A layer 3 protocol in the OSI model that allows for the transmission of data across networks.

Intrusion Detection System (IDS) A system that has the purpose to detect intrusions and malicious behaviours on networks and hosts.

IP Address An identifier for a computer or device on a IP network.

IP header Information, such as the source and destination address, protocol type and identifier, that are attached to each IP packet.

IP PBX Has the same functionalities as the TDM PBX used in the traditional telephone network, such as call control, call signaling, authenticating registrations and authorizing callers.

IP Security (IPSec) IPSec is a set of protocols developed by IETF to provide security at the IP layer. It can either be used as an encryption engine or as a tunneling protocol in VPN.

IP Stack A well known model used to describe the network communication. It consists of five layers; physical, data link, network, transport and application layer.

IP telephony Also called VoIP, a technology where voice calls are converted into data packets and transmitted over an IP network.

J

Jitter A variation or a non-uniform packet delay and can cause disorder in processing and arrival of packets. Jitter also causes packets to arrive in clumps very analogous to road traffic arriving at a red stop light.

K

Key logger application A program that logs a user's key tokens.

L

Label Distribution Protocol (LDP) Considered as the main protocol created by the MPLS working group. It defines a way to distribute label bindings in order to create the forwarding tables in the LSRs.

Label-Switched Router (LSR) A router that supports MPLS by integrating routing and switching functions.

Label switching Techniques used to forwarding IP packets using labels instead of IP addresses.

LAN Manager hash A Microsoft hash function that is based on the DES encryption algorithm. It is used in many Windows NT authentication protocols.

Latency Also called packet delay, is the overall time for a IP packet to go from its source to its destination.

Layer 2 Tunneling Protocol (L2TP) An IETF standard protocol for tunneling of PPP frames.

Local Area Network (LAN) A local computer network for communication between computers that is limited to an organization, such as a company network.

M

Man-In-the-Middle attack An attack method where an attacker not only listens to the packets that are sent between two parties but also can modify, delete, and replay the packets.

Mean Opinion Score (MOS) A measurement of the subjective quality of human speech, represented as a rating index ranging from 5.0 as the highest quality and uncompressed speech to 1.0 indicating the lowest rating.

Media Gateway Control / H.248 (MEGACO/H.248) A gateway control protocol accepted by the IETF and ITU-T as a standard.

Media Gateway Control Protocol (MGCP) An IETF gateway control protocol used to provide the signaling between to dissimilar protocols.

Medium Access Control (MAC) address A hardware address that uniquely identifies each device on a network.

Message-Digest algorithm 5 (MD5) A message digest algorithm (one-way hash function) that digits a message of arbitrary size to 128 bits.

Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) The Microsoft version of CHAP and used for PPP authentication. The authentication occurs between a PC using Microsoft Windows and a network access server.

Multi-point Control Unit (MCU) An optional device in a VoIP system that handles voice and video conferencing with multiple users at the same time.

Multi Protocol Label Switching (MPLS) A technology used to increase the speed of network traffic flow by inserting information (called labels) about a specific path the packet is taking to route to its destination.

Multipurpose Internet Mail Extension (MIME) A standard that allows Internet users to exchange e-mail messages enhanced with graphics, video and voice.

N

National Institute of Standards and Technology (NIST) NIST is a branch of the United States Department of Commerce that ensures standardization within government agencies.

Network Address Port Translation (NAPT) A technique used to enable multiple hosts in a private network to access the Internet by using a common public IP address.

Network Address Translation (NAT) A technique in which the source and/or destination IP packet addresses are changed when they pass through a firewall or a router.

Network Infrastructure The network architecture, the components and connections that make up the network.

Nonce value A randomly chosen value used to protect against replays.

O

One-time password An authentication method where the passwords are only used once within a short period of time, after which they are no longer valid.

Open networks Open networks are considered as really open, meaning that basically anyone can access the network any time and anywhere the network is present. No pre-registration is needed. The Internet is considered as an open network.

Open Systems Interconnection (OSI) model The OSI model is standard used to describe the network communication architecture. It consist of 7 layers; physical layer, link layer, network, transport layer, session layer, presentation layer and application layer.

P

Packet A packet is an aggregation of bytes sent over the network.

Packet delay Also called latency, is the overall time for a IP packet to go from its source to its destination.

Packet filtering The process of limiting data flow based on present rules for processing the data, such as source, destination or type of service being provided on the network.

Packet loss A term used when packets do not reach their destination. This can for instance happen if the network is overloaded.

Packet switching A packet-switched network only occupies resources in form of buffers and bandwidth when needed; data is divided into packets that are transmitted individually and can follow different routes to reach their destination. Once all the packets performing the data arrive at the destination, they are reassembled to the original data.

Plaintext Unencrypted data also referred to as clear text. It is the opposite of cipher text and often used to describe transmissions, between devices on a network that can be captured using a sniffing tool and easily read. Telnet is for example considered a plaintext protocol.

Point-to-point Tunneling Protocol (PPTP) A tunneling protocol developed by Microsoft and several other remote access vendors, known as the PPTP Forum. It works at layer 2 of the OSI model and can be considered as an extension to PPP.

Port An interface in network devices used to communicate at layer 2 in the OSI model.

Private Exchange Branch (PBX) A telephone switch located in an end-user organization's premises which provides connection between terminals connected to it, including dial service, and may provide connections to other communications network, including the PSTN.

Private network A network where all the data paths are only visible to a limited group of users.

Proxy server Provides functionalities such as routing decisions, authentication, network access control and security.

Public Key Infrastructure (PKI) A system consisting of digital certificates, certificate authorities, and other registration authorities that verify and authenticate the validity of each party involved in an Internet transaction. It uses public and private keys for encryption and decryption.

Public Network A network designed for open access such as the Internet.

Public Switched Telephone Network (PSTN) An international telephone system that is almost entirely digital in technology except for the final link from the local telephone office to the user. It uses SS7 for signaling.

Q

Q.931 The standard used for signaling in ISDN.

Quality-of-Service (QoS) QoS can be defined as a measure of performance for a transmission system, involving specification of packet delay, jitter, packet loss and availability. It also includes the practice of allocating and prioritizing specific necessary network resources in form of a guaranteed bandwidth.

R

Real-Time Transport Protocol (RTP) An IP protocol for transmitting real-time data such as audio and video. It can be considered as a sublayer of the transport layer and is merely a protocol that implements the functionalities the other transport protocols (TCP and UDP) lack.

Redirect Server A server that help users to find desired addresses by redirecting to another server.

Registrar server A server that accepts user registration and maps a user's telephone address (such as an e-mail address) with its IP address.

Remote Access Access to a network from a distant location, usually by dialing in with a modem.

Remote Authentication Dial In User Service (RADIUS) An authentication server that identifies remote users.

Remote Shell (SSH) A command line interface used to securely access a remote computer.

Remote user A user that is connected to a network from a distant location.

ReSerVation Protocol (RSVP) A signaling protocol that allows the sender and the receiver in a communication to set up a reserved route for data transmission with a specified quality of service.

Rivest Cipher 4 (RC4) A symmetric encryption algorithm developed by Ron Rivest (the R in RSA).

Rivest, Shamir and Adleman (RSA) A public key encryption algorithm developed by Rivest, Shamir, and Adelman. The public and priavte keys are here based on prime numbers.

Router A router is a network layer component that connects two networks, such as two LANs or a LAN and a public network. Routers are responsible for forwarding packets from one network to another that are based on the destination of the packets and the routing decisions in the network layer.

RTP Control Protocol (RTCP) Allows monitoring of the data delivery of the RTP. Some of the functions that RTCP provide include QoS feedback, session control, user identification and inter-media synchronization, to synchronize between the voice streams.

S

Scalability The ability to expand the number of users or increase the capabilities of a computing solution without making major changes to the systems.

Secure File Transfer Protocol (SFTP) Similar to FTP, but performs all operations over an encrypted SSH transport.

Secure Hash Algorithm (SHA) A message digest algorithm (one-way hash function) that digits a message of arbitrary size to 160 bits.

Secure MIME (S/MIME) A standard for end-to-end encryption of e-mail messages.

Secure RTP (SRTP) A profile of RTP which can provide confidentiality, message authentication and replay protection for example by using TLS.

Secure Socket Layer (SSL) A standard for establishing a secure communication link using a public key system.

Server A computer that handles client requests and answers with responses.

Session Description Protocol (SDP) An IETF specified protocol used for session description. It is a structured textual description of the name and purpose of the session, and the media, protocols, codec formats and transport information.

Session Initiation Protocol (SIP) SIP is the IETF specified signaling protocol used for Internet calls, multimedia conferences and multimedia distribution.

Signaling Responsible for creating and managing real-time connections between the terminals. The signaling also covers how terminals attached to the data network communicate with telephones attached to the PSTN. At this moment SIP and H.323 are the dominant signaling protocols used in VoIP systems.

Signaling System 7 (SS7) The international signaling standard that is used in telecommunication networks, such as the PSTN. It has many of the same functionalities as VoIP signaling protocols, such as to provide signaling to establish and terminate connections.

Silence suppression Removing any silence that occurs in the conversation.

Simple Mail Transfer Protocol (SMTP) SMTP is an IETF defined protocol used for sending e-mail messages between servers. Most e-mail systems that send mail over the Internet use SMTP to send messages from one server to another. In addition, SMTP is generally used to send messages from a mail client to a mail server.

Skinny Client Control Protocol (SCCP) Cisco Systems' proprietary protocol used for signaling between the IP phones and the signaling server.

Social Engineering An attack based on deceiving users at the target site, typically carried out by telephoning users and pretending to be to an authorized user to attempt to gain illegal access to systems.

Spam over Internet Telephone (SPIT) An attack that occurs when many unsolicited calls are being carried out over the Internet. It is similar to e-mail spam.

Spoofing A method an attacker can use to pretend to be someone else, for instance by changing the sender address in IP packets (called IP spoofing). Spoofing is commonly used in the Man-In-The-Middle and DoS attacks, since attackers do not want to reveal themselves.

Stateful server A server that stores information regarding packets that it has served.

Stateless server A server that does not store information regarding packets that it has served.

Statistical gains Only transmitting packets when necessary. This is achieved by used a technique called VAD.

Switch A network component that channels incoming data from any multiple input ports to the specific output port that will take the data toward its intended destination.

Symmetric encryption A cryptographic method where the same key is used for both the encryption and decryption.

T

Terminal A terminal is an endpoint that allows a user to communicate with a computer or IP phone. In VoIP systems a terminal is typically an IP phone or a soft phone.

Time Division Multiplexing (TDM) A method of putting multiple data streams into a single signal. Each signal is separated into many segments and get bandwidth periodically during brief time intervals.

Traffic Engineering (TE) The aspect of network engineering that addresses measurement, modelling, characterization and control of traffic. The achievement of reliable operation and high utilization of resources is also a part of traffic engineering.

Transmission Control Protocol (TCP) A connection-oriented transport protocol. In contrast to UDP, TCP guarantees delivery of data packets and that packets are received in the same order in which they are sent.

Transport Layer Security (TLS) An IETF specified protocol that is based on Secure Socket Layer (SSL). TLS provides security on the transport protocol by using digital certificates for authentication and digital signatures to ensure message integrity, and can use public key cryptography to ensure data privacy.

Transport mode In this mode the AH and AES protocols provide primary protection for the upper-layer protocols.

Triple DES (3DES) A more secure version of the DES. 3DES uses 168-bit key.

Trivial File Transport Protocol (TFTP) A simplified version of FTP that transfer files but does not provide password protection.

Tunnel mode In this mode the AH and AES protocols tunnel the entire IP packet including the IP header through the network.

Tunneling The process of encapsulation data from one protocol to another.

U

Unistim Nortel Networks proprietary protocol used for signaling between the IP phones and the signaling server.

User Agent (UA) The SIP UA is a user's terminal and consists of two main components, User Agent Client (UAC) and User Agent Server (UAS). The UAC is responsible for sending requests and receiving responses while the UAS is responsible for receiving requests and sending responses.

User authentication The process of verifying that the user really is the person he claims to be.

User Datagram Protocol (UDP) UDP is a connectionless protocol that is used for data transport. UDP has a smaller header size and the fact that it does not provide any guarantees to delivery makes it a protocol of low complexity and favorable for voice to be transported via UDP packets.

V

Virtual Private Network(VPN) VPN is a technology that is used to connect components over different networks. It is typically used in companies to allow their employees to securely connect to the company's LAN from an external network. The media stream is often encrypted to prevent eavesdropping.

Voice Activity Detection (VAD) VAD is used to only transmit audible speech over the network; silence is not transmitted. When VAD is used, the sound quality is slightly degraded but the connection uses considerable less bandwidth.

Voice compression The conversion of an analog voice signal into a digital signal using minimum bandwidth.

Voice media The physical material where the voice packets are transmitted.

Voice over Internet Protocol Security Alliance (VoIPSA) VoIPSA was established February 2005 and includes Verizon Communications, Nortel Networks, VeriSign, PricewaterhouseCoopers, and about 50 other vendors and service providers. Its mission is to promote the current state of VoIP security research, VoIP security education and awareness, and free VoIP testing methodologies and tools.

Voice over Internet Protocol (VoIP) A technology where voice calls are converted into data packets and transmitted over an IP network, such as a private network or the Internet.

Voice Stream A logical path between two network devices that can send and receive voice messages.

W

Wide Area Network (WAN) A communication network that covers a large geographical area, such as cities, countries and the world. A WAN can also be a number of LANs connected to each other, and are in most cases connected through a public network, such as a telephone system.

Windows NT hash A Microsoft hash function that is based on the MD5 one way hash function. It is used in many Windows NT authentication protocols.

Wireless LAN (WLAN) A LAN that uses high radio frequency to communicate instead of wires.

Wiretapping A term used for monitoring telephone conversations.

X

X.25 A network access standard for connecting computers and other network devices to a packet-switched network.

Bibliography

[ALC03a] Alcatel, *"Alcatel OmniPCX Enterprise - Summeary Specification"*, Alcatel, 2003, http://www.alcatel.com/enterprise/en/products/ip_telephony/omnipcxenterprise/pdf/omnipcx_enterprise_summary.pdf.

[ALC03b] Alcatel, *"OmniVista 4760 - The Open Management Platform"*, Alcatel, 2003, http://www.alcatel.com/enterprise/en/products/ip_networking/network_management/pdf/omnivista_4760_brief.pdf.

[ALC04] Alcatel, *"Thales and Alcatel partner to secure IP communications for enterprises"*, Oct. 14, 2004, http://www.home.alcatel.com/vpr/vpr.nsf/0/8497eb5ffd170fadc1256f960035440c?OpenDocument.

[ALL05] Mads Allingstrup, *"Firmaer optager telefonsamtaler ulovligt"*, Computerworld Jun. 24, 2005, http://www.computerworld.dk/default.asp?Mode=2&ArticleID=28750.

[AND03] F. Andreasen and et. al., *"Media gateway Control Protocol (MGCP)"*, RFC 3435, Jan. 2003, http://www.ietf.org/rfc/rfc3435.txt.

[ARA99] M. Arango and et. al., *"Media gateway Control Protocol (MGCP)"*, RFC 2705, Oct. 1999, http://www.ietf.org/rfc/rfc2705.txt.

[AWD99] Daniel O. Awduche, *"MPLS and Traffic Engineering in IP networks"*, IEEE Communications Magazine, December 1999 http://www-net.cs.umass.edu/cs653/documents/mpls-te-awduche.pdf.

[BAG04] Saburah Bagchi et. al, *"SCICIVE: A Stateful and Cross Protocol Intrusion Detection Architecture for Voice-over-IP Enviroments"*, Proceeding of the 2004 International Conference on Dependable Systems and Networks, IEEE Computer Society, 2004.

[BAU04] M. Baugher and et. al., *"The Secure Real-time Transport Protocol (SRTP) "*, RFC 3711, Mar. 2004, http://www.ietf.org/rfc/rfc3711.txt.

[BID05] Elizabeth Biddlecombe, *"Hold the Phone, VoIP Isn't Safe"*, Wired News Feb. 07, 2005, http://www.wired.com/news/technology/0,1282,66512,00.html.

[BRA04] Margit Brandl et al., *"Ip Telephony Cookbook"*, TERENA March 2004, ISBN: ISBN 90-7759-08-6.

[BER02] Jen Bertelsen, *"Sverige udviser to Ericsson-spioner"*, Computerworld Nov. 11, 2002, http://www.computerworld.dk/default.asp?Mode=2&ArticleID=16912.

[CBR03] William R. Cheswick, Steven M. Bellovin and Aviel D. Rubin, *"Firewalls and Internet Security, Second Edition"*, Addison Wesley 2003, ISBN: 0-201-63466.

[CER04] CERT, *"CERT Advisory CA-2004-01 Multiple H.323 Message Vulnerabilities"*, CERT Jan. 13, 2004, http://www.cert.org/advisories/CA-2004-01.html.

[CHU00] C-N. Chuah, *"Providing End-to-End QoS for IP based Latency sensitive Applications"*,Dept. of Electrical Engineering an Computer Science, University of Califonia at Berkeley, 2000.

[CLA02] Daniel Clark, *"Vulnerability's of IPSEC: A discussion of possible weaknesses in IPSEC implementation and protocols"*, SANS Institute, Mar. 14 2002.

[COL04] Mark D. Collier, *"Enterprise Telecom Security Threats"*, SecureLogix Coporation, 2004, http://download.securelogix.com/library/Enterprise_Telecom_Security_Threats_Draft_10-12-04.pdf.

[COL05a] Mark D. Collier, *"VoIP Vulnerabilities - Registration Hijacking"*, SecureLogix Coporation, 2005, http://download.securelogix.com/library/Registration_hijacking_060105.pdf.

[COL05b] Mark D. Collier, *"Voice Over IP and Firewalls"*, SecureLogix Coporation, Feb. 25, 2005, http://download.securelogix.com/library/voice_over_ip_firewalls_050105.pdf.

[COM99] Common Criteria, *"Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model"* version 2.1, Common Criteria Aug. 1999, CCIMB-99-031.

[COM] Compnetworking, *"VPN Tutorial"*, http://compnetworking.about.com/od/vpn/l/aa010701a.htm.

[DAT00] Datatilsynet, Act No. 429 of 31 May 2000, http://www.datatilsynet.dk/include/show.article.asp?art_id=443&sub_url=/lovgivning/indhold.asp&nodate=1.

[DIT04] Saburah Bagchi et. al, *"Network based Intrusion Detection to Detect Steganographic Communication Channels"*,2004 IEEE 6th Workshop on Multimedia Signal Processing, 2004.

[DUR03] James F. Durkin, *"Voice-Enabling the Data Network: H.323, MGCP, SIP, QoS, SLAs, and Security"*, Cisco Press 2003, ISBN:1-58705-014-5.

[EDE05] Eve Edelson, *"Voice over IP: security pitfalls"*, In *Network Security*, volume 2005, issue 2, pages 4-7, Elsevier Feb. 2005, ISSN:13534858.

[FJE02] Edward Bjarte Fjelleskål and Stig Solberg, *"Evaluation of Voice over MPLS (VoMPLS) compared to Voice over IP (VoIP)*, Faculty of Engineering and Science, Agder University College, May 2002.

[FLY03] Claus Flygenring and Anders Pedersen, *"Klassiske problemstillinger med Voice over IP"*, In *Installations nyt*, volume 27, nr.3, pages 4-12, 2003.

[GAR04] Alberto Leon-Garcia and Indra Widjaja, *"Communication networks: fundamental concepts and key architecture"* 2. edition, McGraw-Hill Education - Europe 2004, ISBN:0071198482.

[GOR04] L. Gorden et al., *"Computer Crime and Security Survey"*, CSI/FBI 2004, `http://www.i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf`.

[HAN99] M. Handley and et. al., *"SIP: Session Initiation Protocol"*, RFC 2543, Mar. 1999, `http://www.ietf.org/rfc/rfc2543.txt`.

[HOL00] Jon Hollandsworth, *"Overview of IPSEC Manageability and Security"*, Jul. 25 2000, `http://madchat.org/reseau/ipsec.htm`.

[HOW97] John D. Howard, *"An Analysis of Security Incidents on the Internet"*, PhD thesis, Carnegie Mellon University, Apr. 1997, `http://www.cert.org/research/JHThesis/Start.html`.

[JEN05a] Dan Jensen, *"Analytikere spår boom for internet-telefoni"*, Computerworld Apr. 5, 2005, `http://www.computerworld.dk/default.asp?Mode=2&ArticleID=27687`.

[JEN05b] Dan Jensen, *"USA advarer mod IP-telefoni"*, Computerworld Feb. 3, 2005, `http://www.computerworld.dk/default.asp?Mode=2&ArticleID=26919`.

[KEN98a] S. Kent and et. al., *"IP Authentication Header"*, RFC 2402, Nov. 1998, `http://www.ietf.org/rfc/rfc2402.txt`.

[KEN98b] S. Kent and et. al., *"IP Encapsulating Security Payload (ESP)"*, RFC 2406, Nov. 1998, `http://www.ietf.org/rfc/rfc2406.txt`.

[KIL04] Frederik Kilemark, *"Secure Working from Home in an Industrial Context"*, Informatics and Mathematical Modelling, Technical University of Denmark 2004, IMM-Thesis-2004-06.

[KRA03] Eric Krapf, *"Alcatel, Eads Raise Stakes For IP-PBX"*, In *Business Communications Review*, pages 62-64, Apr. 2003, `http://www.bcr.com/bcrmag/2003/04/p62.php`.

[KRA05a] Klaus Krabbe, *"Virus og hackere truer IP-telefoni"*, Computerworld Feb. 9, 2005, `http://www.computerworld.dk/default.asp?Mode=2&ArticleID=26985`.

[KRA05b] Klaus Krabbe, *"EU kæmper mod trusler fra cyberspace"*, Computerworld Apr. 19, 2005, `http://www.computerworld.dk/default.asp?Mode=2&ArticleID=26985`.

[KWF05] D. Richard Kuhn, Thomas J. Walsh And Steffen Fries, *"Security Considerations for Voice Over IP Systems, Recommendations of the National Institute of Standards amd Technolology"*, National Institute of Standards an Technology Jan. 2005, NIST SP 800-58.

[KUR01] James F. Kurose and Keith W. Ross, *"Computer Networking, A Top-Down Approach Featuring the Internet"*, Addison Wesley Longman, Inc. 2001, ISBN:0-201-47711-4.

[LEE98] T. Berners-Lee and et. al., *"Uniform Resource Identifiers (URI): Generic Syntax "*, RFC 2396, Aug. 1998, `http://www.ietf.org/rfc/rfc2396.txt`.

[NOR02] Nortel Networks, *"Succession Communication Server for Enterprise 1000"*, Nortel Networks, 2002.

[NOR04a] Nortel Networks, *"Communication Server 1000 Portfolio"*, Nortel Networks, 2004.

[NOR04b] Nortel Networks, *"Features in Communication Server 1000 Release 4.0"*, Nortel Networks, 2004.

[MAI03] Soeren Maigaard, *"Undersoegelse af datasikkerhed i forbindelse med hjemmearbejdspladser i Danmark"*, Informatics and Mathematical Modelling, Technical University of Denmark 2003, IMM-Thesis-2003-41.

[MEH01] Princy Mehta and Sanjay Udani, *"Voice over IP, Sounding good on the Internet"*, In *IEEE Potentials*, volume 4, issue 4, pages 36-40, 2001, ISSN:02786648.

[MIE04] Mier Communications Inc., *"2004: A VoIP Security Assessment"*,Mier Communications Inc., May. 2004.

[MIE05a] Mier Communications Inc., *"Lab Testing Summary Report"*,Mier Communications Inc., Report number 050131, Jan. 2005.

[MIE05b] Mier Communications Inc., *"Lab Testing Summary Report"*,Mier Communications Inc., Report number 050128, Jan. 2005.

[MMT05] Edwin E. Mier, David C. Mier and Robert B. Tarpley, *"Which Large IP-PBX Rules?"*, In *Business Communications Review*, pages 24-37, Jan. 2005.

[NET04] Netdesign, *"Presseklip august 2004"*, Aug. 2004, http://www.netdesign.dk/Presse/presseklip/august04.htm.

[NNI05] NNIT, *"IP-telefoni til Novo Nordisk"*, Apr. 19, 2005, http://www.nnit.com/DK/Secondary/Presse/Pressemeddelelser/Iptelefoni.htm.

[PAU02] Victor Paulsamy and Samir Chatterjee, *"Network Convergence and the NAT/Firewall Problems"*, IEEE Computer Society, 2002.

[PFL03] Charles P. Pfleeger and Shari Lawrence Pfleeger, *"Security in Computing"* 3. edition, Prentice Hall 2003, ISBN: 0-13-035548-8.

[RAN04] James Randall and Michael Szydlo, *"Collisions for SHA0, MD5, HAVAL, MD4, and RIPEMD, but SHA1 Still Secure"*, RSA Security Aug. 31, 2004, http://www.rsasecurity.com/rsalabs/node.asp?id=2738.

[RAN05] James F. Ransome and John W. Rittinghouse, *"VoIP Security"*, Elsevier Digital Press 2005, ISBN: 1-55558-332-6.

[ROS02] J. Rosenberg and et. al., *"SIP: Session Initiation Protocol"*, RFC 3261, Jun. 2002, http://www.ietf.org/rfc/rfc3261.txt.

[ROU04] Steve A. Rouiller, *"Virtual LAN Security: weakness and countermeasures"*, SANS, 2004, http://www.sans.org/rr/whitepapers/networkdevs/1090.php.

[SAN05] Jesper Stein Sandal, *"Sammenslutning vil gøre IP-telefoni sikkert"*, Computerworld Mar. 30, 2005, `http://www.computerworld.dk/default.asp?Mode=2&ArticleID=27624`.

[SCH89] H. Schulzrinne and et. al., *"RTP: A Transport Protocol for Real-Time Applications"*, RFC 1889, Jan. , `http://www.ietf.org/rfc/rfc1889.txt`.

[SGF02] Gary Stoneburner, Alice Goguen and Alexis Feringa, *"Risk Management for Information Technology Systems"*, National Institute of Standards an Technology Jul. 2002, NIST SP 800-30.

[SIC04] Duglas C. Sicker and Tom Lookabaugh, *"Security: Not an Afterthought"*,In *ACM Queue Magazine*, volume 2, no. 6, Baseline Sep. 2004.

[SIM04] W. Simpson and et. al., *"The Point-to-Point Protocol (PPP)"*, RFC 1661, Jul. 2004, `http://www.ietf.org/rfc/rfc1661.txt`.

[SMI99] Randy Franklin Smith, *"Is PPTP Safe?"*, CERT May.1999,WindowsITPro, `http://www.windowsitpro.com/Articles/Print.cfm?ArticleID=5188`.

[SMW99] Bruce Schneier, Mudge, David Wagner , *"Cryptanalysis of Microsoft PPTP - Authentication Extensions (MS-CHAPv2)"*, CERT Oct. 19, 1999, `http://www.schneier.com/paper-pptpv2.pdf`.

[SPR03] SpraakMaker Telecom, *"Numbering plans guide"*, SpraakMaker Telecom 2003, `http://www.numberingplans.com/index.php?goto=guide&topic=E164`.

[STE96] Ralf Steinmetz, *"Human Perception of Jitter and Media Synchronization"*,In *IEEE journal on selected areas in communications*, volume 14, no. 1, IEEE Jan. 1996.

[STE03] Allan Stevens, *"IP telephony Solutions"*,In *Personal Computer World*, VNU Business Publications LTD, May 2003.

[STI02] Douglas R. Stinson, *"Cryptography, Theory and Practice"*, Chapman & Hall 2002, ISBN: 1-58488-206-9.

[STU04] Michael Stukes and Douglas C. Sicker, *"An Evaluation of VoIP Traversal of Firewalls and NATs within an Enterprise Enviroment"*, In *Information Systems Frontiers*, volume 6, issue 3, pages 219-228, Kluwer Acadimic Publishers, 2004.

[THA98] R. Thayer and et. al., *"IP Security - Document Roadmap"*, RFC 2411, Nov. 1998, `http://www.ietf.org/rfc/rfc2411.txt`.

[THO05] Casper Thomsen, *"Blind irakisk autist hackede TDC"*, Computerworld Nov. 25, 2004, `http://www.computerworld.dk/default.asp?Mode=2&ArticleID=26985`.

[TIP04] TippingPoint, *"Intrusion Prevention: The Future of VoIP Security"*, TippingPoint Technologies, Inc. 2004, `http://www.tippingpoint.com/resources_whitepapers.html`.

[TOW99] W. Townsley and et. al., *"Layer Two Tunneling Protocol (L2TP)"*, RFC 2661, Aug. 1999, `http://www.ietf.org/rfc/rfc2661.txt`.

[UCD98] UCDAVIS, *"VLAN Information"*, UCDAIS, University of Califonia, 1998, `http://net21.ucdavis.edu/newvlan.htm`.

[VOI05] Voiceline, *"Konceptbeskrivelse. IP matrix - et VOIP projekt"*, 19. juni 2005, The document can be found on the enclosed CD.

[WRI01] David J. Wright, *"Voice over Packet Networks"*, John Wiley & Sons 2001, ISBN: 0-471-49516-6.

[WRI02] David J. Wright, *"Voice over MPLS Compared to Voice over Other Packet Transport Technologies"*, IEEE Communications Magazine November 2002.