Analysis of security issues with respect to Voice over IP technologies

Florian Berthelot

Submitted in partial fulfilment of the
requirements of Napier Edinburgh University
for the Degree of
Computer, Networks and Distributed Systems (HONS)

Work supervised by
Robert Ludwiniak

School of Computing
May 2009

Authorship Declaration

I, Florian Berthelot, confirm that this dissertation and the work presented in it are my own achievement.

Where I have consulted the published work of others this is always clearly attributed;

Where I have quoted from the work of others the source is always given. With the exception of such quotations this dissertation is entirely my own work;

I have acknowledged all main sources of help;

If my research follows on from previous work or is part of a larger collaborative research project I have made clear exactly what was done by others and what I have contributed myself;

I have read and understand the penalties associated with Academic Misconduct.

I also confirm that I have obtained **informed consent** from all people I have involved in the work in this dissertation following the School's ethical guidelines.

Signed:

Date: 6 May 2009

Matriculation no: 07010875

Data Protection Declaration

Under the 1998 Data Protection Act, The University cannot disclose your grade to an unauthorised person. However, other students benefit from studying dissertations that have their grades attached.

Please sign your name below one of the options below to state your preference.

The University may make this dissertation, with indicative grade, available to others.

The University may make this dissertation available to others, but the grade may not be disclosed.

The University may not make this dissertation available to others.

Abstract

After the recent development of Voice over IP technology, this telecommunication implementation type is now in full expansion. The democratisation of private networks tend more and more enterprises to convert to this solution, for cost and flexibility reasons.

However, the security issues involved with VoIP suffer poor description and mitigation at the moment. This is the basis on which this study will focus. The work undertaken has this objective: to develop an understanding of used protocols, to analyse and study security failures. The solutions to mitigate them are also studied.

The first part of the work is a description of VoIP protocols, like SIP and H323. The study is then focused with SIP protocol, which is easier, more flexible and opens up opportunities for future switched networks.

Secondly, a theoretical and detailed study of the risks in using unsecured VoIP is performed. This study will concern deployment of VoIP on existing network infrastructures only. The different attacks like "Denial of Service" and "Phishing", are reviewed, and the risks encountered, are studied, case by case.

For these security issues, the tunnelling technology will be introduced. The ways they can be implemented, and the security that they can provide are a good solution regarding security issues previously seen.

Following this, the third piece of work is the design of the performed study: a simulation of a private switched network set up, with a server running a VoIP server (Asterisk software). Clients are configured to make calls over the network, firstly within the private part of network and secondly from another domain (simulation of a link to another private network, through Internet).

This practical phase is described point to point and the selected choices are justified regarding the cases that the audience could encounter.

After the reading of this dissertation, the targeted audience will be aware of security issues concerned by VoIP, and will have the required knowledge of how to avoid them. The final reflection allows them to have their own distinctive viewpoint on the solution ; depending on the network infrastructure.

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

1 INTRODUCTION

Background

Further to the point made on the development of networked technologies, the use of computing networks is becoming more common place. Most of the companies now have their own private LAN, and extend their performance to new services (Teare, Diane, July 1999). After the explosion of Wireless technology, most successful companies are now interested in Voice over IP (Bill. Trussell, 12 July 2007). This technology allows for transfer of voice channel on a data network, instead of using the classic telephony network.

If the security issues are well known within a classic IP network, the voice over IP has a lack of clarity and definition about the issues associated (Hacking Exposed VoIP: Voice Over IP Security secrets & Solutions, 2006). The fact that the telephony network tend to become more a data network (Voice over IP: security pitfalls, February 2005), is making the VoIP security issues and menace for the data network, already existing and secured. This is why the security issues related to VoIP can interfere with standard data network, and should be seriously considered. This project will focus on these technologies and the security issues associated.

Initial objectives

The main aim of this project is to exemplify security issues encountered in Voice over IP and the mitigation solutions. As this technology emerged few years ago, this study is aimed primarily for a target audience of professionals, who are interested in deploying a VoIP solution in their company.

The outcome of the study will be to present VoIP within its context: in what extend the voice over IP is not a data channel like any other service. An objective will be to show what are the security issues associated to the VoIP service, and how can the main threats exploit them to attack a system or a company.

The second main objective of the study will be to present the solutions which can be deployed to avoid the security issues associated to VoIP. A review and comparison of the main technologies which allow an efficient mitigation will be undertaken.

Finally, the report will carry an analysis of the mitigation solution and their associated issues. The audience will be aware of the solution to mitigate the known security issues, in what extend they can be used and their main cost deployment.

Report layout

This report contains 6 mains chapters. In addition, each part will contain a short introduction which will establish the context, the prerequisites and a summary will act as a link to the following part. This layout has been retained to present a complete study, in a fluid and clear format for the reader.

The **first chapter** will introduce Voice over IP technology. In this part all the main aspects of VoIP will be approached to ensure the basics of the following chapter are understood. The environment of VoIP, the integration and a global description of mains protocols will be described. As the audience will already have some knowledge in Information technology, no deep technical aspect will be researched further in this chapter.

The **second chapter** will be a technical and detailed report about the security issues encountered in VoIP. Details of all will be disclosed and reviewed in detail, permitting the description of vulnerabilities, possible exploits and their consequences.

After this detailed review of the possible threats, the **third chapter** will present and clarify some different solutions to mitigate the presented security issues. This study will perform a global analysis of each issue and will conclude on a chosen solution to apply for the design part.

In the following part of the report, the **forth chapter** is a design of the proceed study: in preparation to the implementation, a theoretical study will present different scenarios, explain why these scenarios and theirs interest in the case of the study.

Then the implementation, as **fifth chapter**, will present the work made in order to stick to the viewed scenarios in the design chapter. A simulation of a network will be represented, some tests will be performed to bring on light the security failures presented in previous parts.

The last part will regroup all the informations and results of the study, to evaluate the securities issues in VoIP and the solution to mitigate them. This part will carry out a complete overview of the study undertaken, and recommendations to mitigate presented issues in the interest of the audience.

Then the **conclusion** will present the global aspects of the project itself.

2 VOICE OVER IP: OVERVIEW

Introduction

The need of telecommunication is vital for everyone, and especially nowadays for business. The telephone was the first direct mode of communication, and has been really popular quickly. It provides a real time mode of communication.

In the beginning of 20th century, the Public Switched Telephone Network (PSTN) was created, to create the network across the countries to allow phone calls. The aim of this infrastructure is to route calls from the caller to the recipient, and so allow the communication to be established. The taxation is based on the time of the communication and the geographical distance.

At the end of 20th century was born Internet: this network infrastructure allows any user to access to data anywhere in the world, at any time and for a fixed price: whatever is the time spent or amount of data transferred. This is a much more interesting solution to communicate regarding prices.

Voice over IP technology was created to use data network (Internet) to carry voice. If is a good alternative from PSTN, the infrastructure is also around the world, and the taxation is cheaper. This solution has been developed for cost reasons. And as now almost everyone has access to Internet, this technology may lead to convergence of PSTN and packet networks.

To implement these functions, VoIP needs to define the way to carry voice as a data on a network. As the voice data should be routed and managed on a data network, there is a need to make the signalisation apart from the voice. The data flux need to be managed by an entity (for example the routers route the packets in function of their IP addresses). Signalisation also help the clients to agree on routes (address destination) and codecs (voice compression and quality).

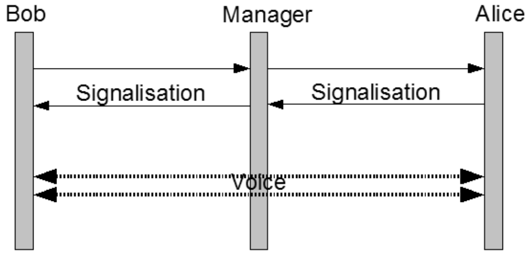


Illustration 1: two channels for the VoIP

The illustration shows how Bob can make a call to Alice: there are two different channels, the signalisation is managed by a central manager, and the voice is carried directly from Bob to Alice.

This has been designed in order to save resources for the call manager, and allow it to be able to deal with more communications simultaneously (bottleneck avoidance).

These definitions will make Voice over IP nothing more than an application on the packet network, with the only difference that this is not only one channel which is open for a transaction, but two.

The study will present the two main signalisation protocols, first H323, which is the first signalling protocol standardised. Then SIP, more recent and considered as the successor of H.323 will be introduced more in details.

2.1 H.323

2.1.a Presentation

H.323 is a recommendation from the ITU Telecommunication Standardization Sector, which defines the interworking of protocols to allow multimedia transmission (voice and video) on a packet-based network. H.323 recommendation is issue from the telephony: it is an adaptation of the H.320 protocol, created for a circuit switched telephony network. It is also the first standardised protocol capable to transmit voice over a local network (IP network).

This protocol defines the coordination of other protocols, in order to manage properly the voice channel. The main protocols managed by H.323 are:

- H.225.0: used for call signalling. This allows to establish/end the communication.
- RAS (Registration Admission Status) Signalling: used to manage the connection: registration, bandwidth registration
- H.245 Call Control: this allows the negotiation of codecs and manages the media flux
- RTP (Real Time Transport Protocol): this is the protocol which transport the voice on the network

H.323 manages these protocols to allow any user to place calls over an IP network, in the same way as if it was using a classic phone line (calls over the PSTN). To manage the above protocols, H.323 defines a series of entities. The understanding of these entities is essential.

2.1.b Elements

Some essentials elements are defined by H.323 recommendation: they are the support for H.323 set of protocols.

H.323 Gatekeeper

A gatekeeper is the equipment what provides an authentication service on a network, and manage if a terminal can or not access to the resource (other terminals) in the zone controlled by the gatekeeper.

H.323 Gateway

The gateway performs the conversion between the controlled zone (local zone, supervised by the gatekeeper) and external networks. Like Internet or the public switched telephone network (PSTN).

H.323 Multipoint Control Unit

The multipoint control unit is the central access point where all the terminals are connected in the case of a conference. All the traffic from the clients go through the MCU, and it retransmitted to the other clients.

The different elements that constitute H.323 structure are usually place within a network topology.

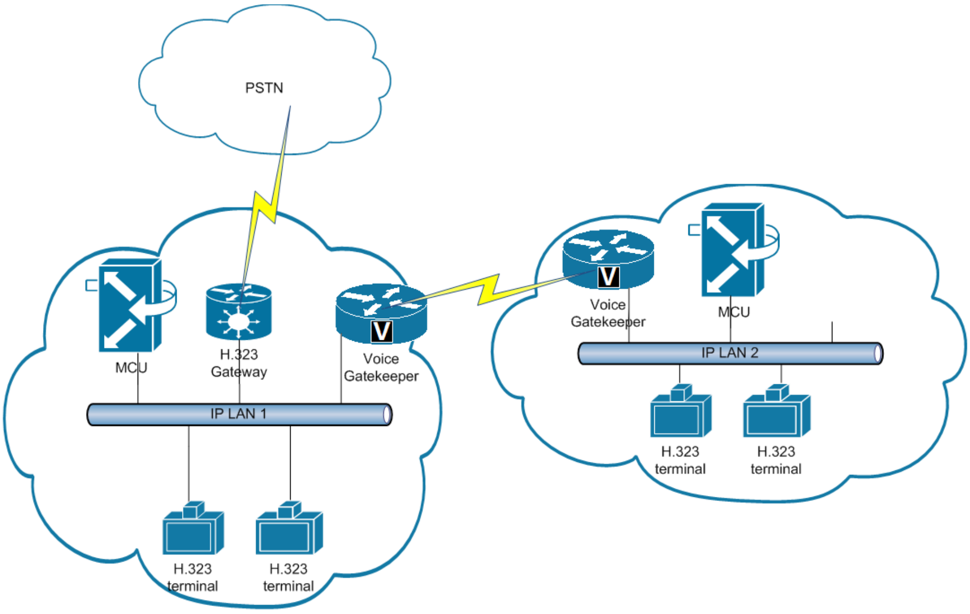


Illustration 2: simple H.323 topology

In the above illustration, the main H.323 elements are present. The gateway allows the communication with the PSTN, and the MCU manages the local multimedia flux, in the case of teleconference (more than two users).

The gateway has different types of interfaces: Ethernet, to be able to connect the IP network and an extension card to be connected within the phone provider.

2.1.c Signalling

The recommendation H.323 set up a voice channel in the below steps (H.323 recommendation, UIT, June 2006).

- **Phase A:** call set-up

This first step allow the gatekeeper to reserve the bandwidth and negotiate the codecs which will be used for the transaction.

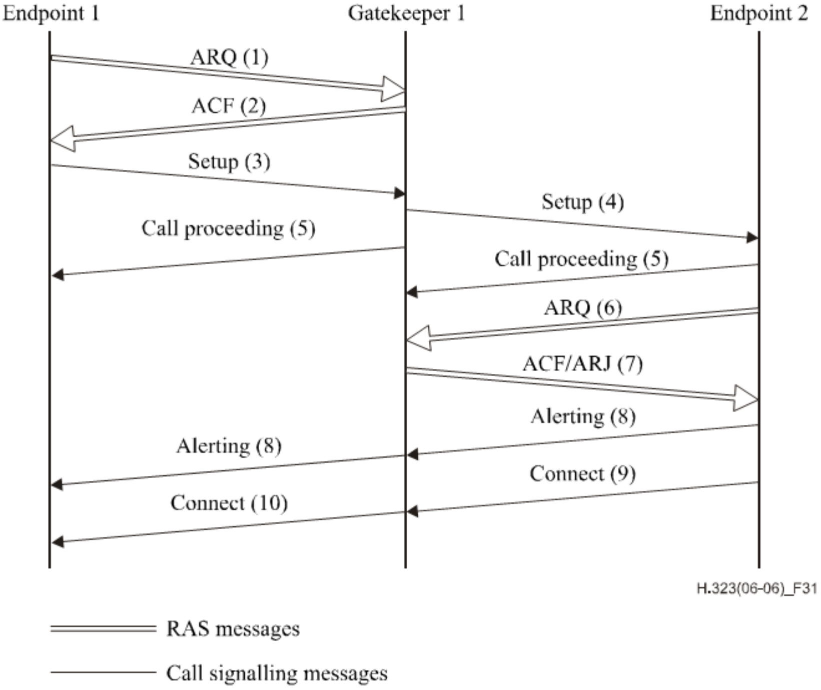


Illustration 3: H.323 simple call (H.323 recommendation, UIT, June 2006)

These messages are sent in accord with the H.225 protocol.

- **Phase B:** Initial communication and capability exchange.

Once the channel is established, the protocol H.245 (call control) make the endpoint exchange their capabilities. This step permits the accord of the used codec and ports used to transmit the data. Depending of the available bandwidth, the codecs and quality of voice are defined. Note that these parameters can be changed during the call (through the signalling channel, phase D).

- **Phase C:** Establishment of audiovisual communication

Following the capability exchange, the end-user are now connected and the voice can transit on the network, in accordance with the specifications (codec and so on) defined during the capabilities exchange (H.245). The voice is transmitted directly from the endpoint to the other, using RTP protocol.

- **Phase D:** Call services

Call services are the signalling messages sent over the established channel, in order to manage the transmission. It will, for example, change the codec used in the case of a network congestion. This service also verifies if both endpoint are on-line (i.e. in case in one of the crashes or network failure). The transmission uses H.245 protocol.

- **Phase E:** Call termination

This last step ends the call. On the H.245 channel "end session" messages are sent, to terminate the logical channel. Then, the connection (allocated bandwidth) is closed by signals on the H.225 protocol.

2.2 SIP

2.2.a Presentation

SIP is the abbreviation of **Session Initialisation Protocol**, a specification of IETF (*RFC 3261, SIP group working, June 2002*). This protocol controls the signalisation of multimedia flux over the packet network: it does not manage the transfer of voice data itself.

As this is a signalisation protocol, SIP manages sessions for the connection. Basically, SIP permits to create, modify and terminate sessions, like classic connection-oriented protocol. Applied to VoIP, sessions are phone calls, multimedia distribution and conferences.

SIP is an IP-based signalisation protocol. It is on the top of the OSI (Open Systems Interconnection) model application layer.

SIP is the equivalent of what HTTP does for Internet: the client ask to the server request, what are sent in clear and human-readable text, and the recipe replies with status codes only (data flux is not transported by SIP). It uses port 5060, on both UDP or TCP connexions.

The basic SIP request are REGISTER, INVITE and BYE. The responses are classified (as HTTP protocol):

#1	1xx	Informational responses
#2	2xx	Successful responses
#3	3xx	Redirection responses
#4	4xx	Client failure responses
#5	5xx	Server failure responses
#6	6xx	Global failure responses

SIP allows signalisation in point-to-point connexion (basic transaction between only 2 computers, see *Illustration 2*), but network topologies are more complex than this.

In this basic case, there is no distinction between the signalisation and voice channel: the destination will always be the other node.

The usual topology is within a large network, where many nodes uses the same resources (voice over IP) and need to be in contact with each other (place calls).

The presentation of SIP will more focus on the second aspect: in the case of a company, all the employees have SIP phones (or soft phones) and place call in local (within the company).

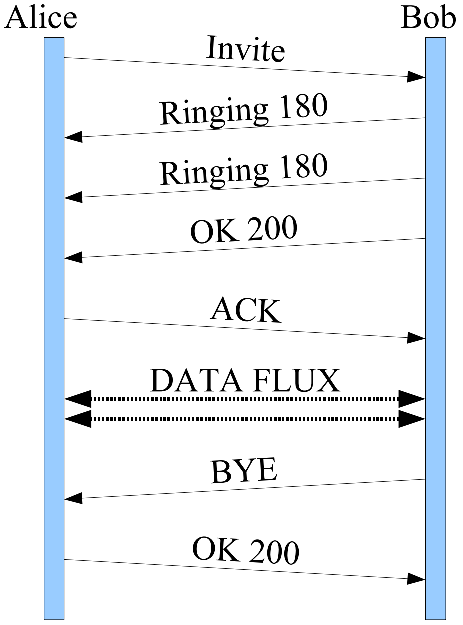


Illustration 4: basic SIP call in point tot point link

In this illustration Alice and Bob are making a call to each other, within the same domain: Alice has Bob's number and establish the call directly to Bob. This case is the simplest one, when both users are in the same LAN. However, in most cases, the Bob and Alice are on different domains (networks).

SIP implement many functions that permit to interconnect different networks, to link them and so place calls. These functions permit to manage the client's mobility, call redirection and domain registration. To implement them, a description of the needed element.

2.2.b Environment

In order to provide the signalling service, the SIP protocol needs to be installed within a networked structure containing some devices. The elements will allow SIP to interconnect the clients within the domain, to connect different domains and manage with calls to / from the PSTN network.

Proxy server

This server allows the resolution of addresses to be able to place a call on the right node, depending of its address. This is one of the most important element, as all the external calls goes through it.

Registrar server

This server contains the list of all SIP user agents of the domain. A user-agent's connection in the domain is the result of a registration on this server.

Redirect server

This server provides an address redirection for the user agents which are not in the domain. It will provide in example an alternative address to the caller, in order to be in communication with the right user-agent, through the proxy server. This service is usually maintained by VoIP providers.

Location database

This server is used by the proxy, and provide a routing service for address resolution in external communications. Location database can be a DNS service, to retrieve IP addresses from domain names (this will be detailed in the following part).

Usually, Proxy, Registrar and Redirect servers are located within the company. Location database is managed by a SIP provider, where companies register to.

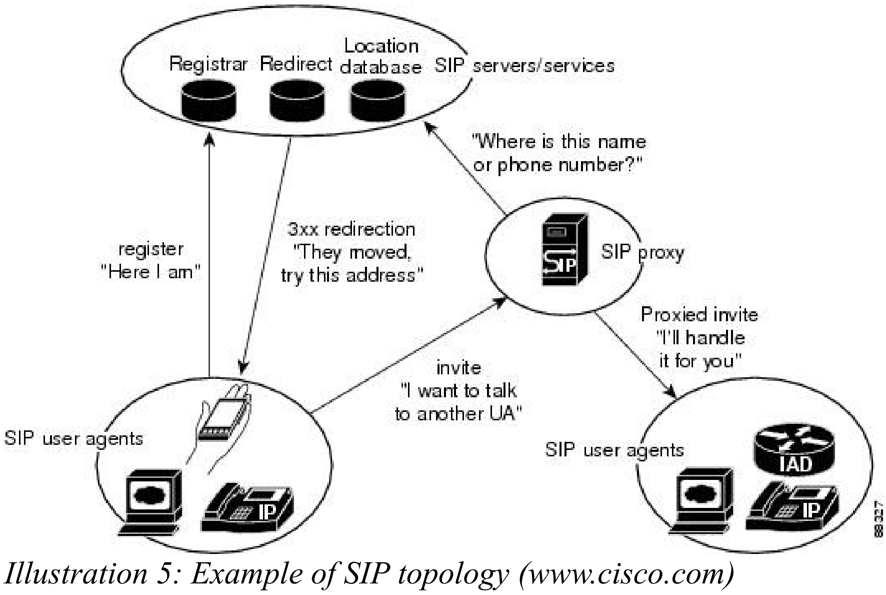

Registrar
Redirect
Location database
SIP servers/services
"Where is this name or phone number?"
register "Here I am"
3xx redirection "They moved, try this address"
SIP proxy
Proxied invite "I'll handle it for you"
invite "I want to talk to another UA"
SIP user agents
SIP user agents
IAD
IP
IP
SIP
88327

Illustration 5: Example of SIP topology (www.cisco.com)

2.2.c Operation

They are different steps which allow SIP to provide the signalling operations.

- **Registration**

The first step to allow making call is to be connected to the network. To do so, the users have to register onto the registrar server, using a user name. Here is a capture packet from a register packet from a client to the registrar server:

```
REGISTER sip:test.com SIP/2.0
Via: SIP/2.0/UDP 192.168.1.1:31782;branch=z9hG4bK-d87543-ac33b5256853a020-1—
d87543-;rport
Max-Forwards: 70
Contact: <sip:1000@192.168.1.1:31782;rinstance=8329073a100d4d9c>
To: "Local"<sip:1000@test.com>
From: "Local"<sip:1000@test.com>;tag=313d8513
Call-ID: Zjg2OTdkNzYzY2M1Mzk2YjBiZTM1YjEwOTQ2MzI0YTY.
CSeq: 1 REGISTER
Expires: 3600
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO
User-Agent: X-Lite release 1011s stamp 41150
Content-Length: 0
```

This packet sent to the server will ask for an authentication, and send some informations.

The most important informations sent in the packets are:

Contact: this is the name of the user, using the registrar server (here the user called “1000” wants to register to the server 192.168.1.1). To “Local” defines a user-friendly URI (Universal Resource Identifier), like DNS for HTTP (IP associated to domain name). This identifier is unique over Internet (like HTTP domains).

Then, Call-ID is the unique identifier, it is unique and created randomly. It permit to identify the call in all the following transactions, within the local loop.

Some other informations are sent, like the allowed messages (INVITE, ACK...) to make sure that the client and servers are using the same version of SIP (e.g. a client could not deal with video).

The registrar server will reply by a similar packet (containing informations about allowed signals and so on) to confirm the user-registration. Now the server will be able to route calls to the user 1000, thanks to its registration (the server knows its IP address).

- **Placing a call**

To allow to place a call, both user must be registered to their own registrar server. The case where Bob wants to call Alice will be presented. First case is when Bob and Alice are within the same domain (registered within the same server).

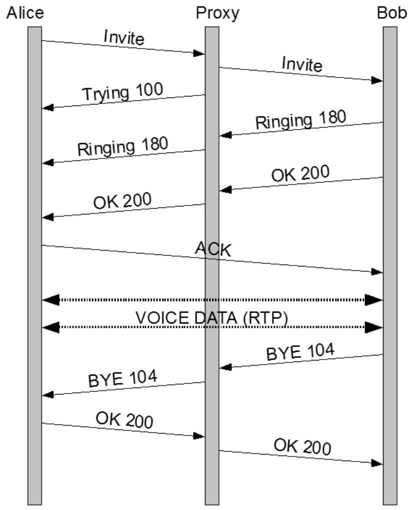


Illustration 6: SIP signalisation for a call

The voice data is independent of SIP. All the signalisation goes through the proxy server, which is aware of all the transactions, and send Alice's IP address to Bob in all the messages.

If Alice and Bob are not within the same domain, the operation is similar, except that Bob will ask its proxy to retrieve Alice's address thanks to her proxy.

This illustration shows the steps to perform a call if Alice wants to call Bob:

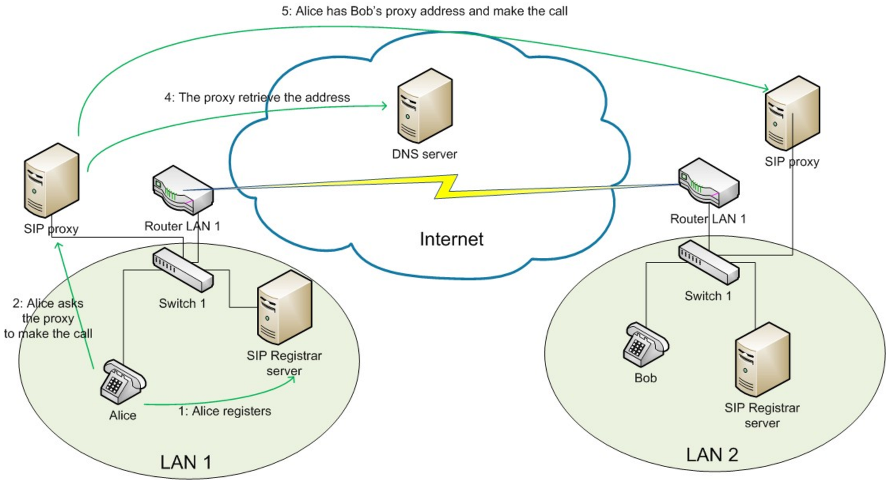


Illustration 7: Alice making a call through proxy server

Like HTML requests, a DNS server is used to retrieve the hosts IP addresses in function of the domain name.

2.3 Evaluation

The presentation of the two main protocols applied to VoIP permitted to bring in light their structure, their needs for deployment and operations. The H.323, which is the root of multimedia transportation on packet network, is more complex to understand and to set up than SIP. Indeed, H.323 uses many protocols and many ports: this is a negative point about security issue (more protocols ta manage, more exceptions for firewalls). Issued from telephony network, this protocol is now out of date to use on IP networks. H.323 allows the reservation of bandwidth, which is nowadays less important, thanks to the democratisation of high-speed connections (DSL connexions for public usage are common and optic connection for professionals is deployed now).

Also, H323 does not include any security protection. Its implementation needs to add another protocol[1] in the H.323 association, which complicate even more the transactions.

In opposition, SIP is easy to use and understand: the handshake to establish the connection is simple and short, only two port used and the elements can be regrouped on the same machine (a server can be the proxy, registration and location server). The signalling type (plain-text over the network) permits easily its extension for new features (i.e. a work-group of IETF are working on an instant messenger implementation[2]). Also, the use of DNS servers is close to HTML protocol, which is widely deployed even on portable devices.

This simplicity, flexibility and ease to understand / set up allows SIP a wide open future, for a long term. It is considered as the future protocol for multimedia transaction on a packet network.

This is why the study will focus now only on SIP protocol.

[1] H.325 implements security in H.323 but is now obsolete: http://www.itu.int/rec/T-REC-H.235/

[2] Instant messenger implementation for SIP can be found at http://www.ietf.org/rfc/rfc3428.txt

Summary

This information carried in this chapter permitted the audience to get a presentation of voice over IP. VoIP cannot be considered as a single data transfer, as it needs some signalisation and voice channel. The presentation of H.323 and SIP showed that both channel cannot be regrouped, because of their type (data for the voice and text for the signalisation), their destination (to the end-user or to a server).

The presentation has shown that none of SIP or H.323 implement any type of security: for both of them the authentication is almost non-existent, and the voice channel is not encrypted. If this is not a problem within the local network (private infrastructure), it can be disturbing to know that your transmission over Internet is not encrypted and clear to be listened from anyone (plain-text for the signalisation or the voice communication).

The delivered evaluation permitted to show the differences between the protocols. SIP has been retained for the rest of this study, for its flexibility and its future in Voice over IP technology.

The main security issues carried by VoIP, and more precisely signalisation, will be shown in the next chapter.

3 SECURITY ISSUES

Introduction

In this chapter the main security issues regarding VoIP will be presented. The context will be introduced and then the different possible attacks and their consequences.

It is in the human nature to envy other's goods. Thieves and dishonest people has always existed, and especially now that our world in controlled by the money. Nowadays essential of business is managed by computing systems. Different type of failure allows pirates to access sensitive information, in order to get directly some money (e.g. bank system attack) or get some informations which will allow them to access money (stealing some commercial data).

All is about money. If a company sudden an attack, if does not directly affect its money state, it will be in an indirect case: a neutralisation of a company's network will avoid the staff to access to the needed resource and work properly. This means a loose of time, reputation and so loosing potential clients.

Privacy is also a major problem in business: if anyone can get important informations from any project, then the concurrency can take advantage of it and anticipate the company's procedures. For example, if a company A is developing a new technology, the company B which keep an eye on company's A records can get those informations to develop the same technology, release it before company A and then get all the profits. This can cost to company A any contract, clients and may lead to bankrupt. This is why privacy should be considered as a non-negligent security issue (M. Benini & S. Sicari,2008).

The stake is so important that nowadays security is a business: many companies are specialised in keep safe other's companies network, data or ensure their privacy (i.e. Secure Works, Symantec). This security and privacy issues are almost non-existent on the PSTN, as it is based on a close and secured network. Also, an attack from the PSTN could not lead to data attack, as the two networks (packet and voice network) are physically distinct. Nevertheless, VoIP has some security failures.

The security issues in Voice over IP has been released in the top 20 security alerts by SANS institute (SysAdmin Audit Network Security, January 2007).

The main known attack will be now described and detailed, in accordance with the aim of the project.

3.1 Discovering the network

The first information which can be retrieved by an attacker is information about the network. These informations themselves are not an attack, but privacy issues. If an attacker can get detailed informations about a network infrastructure (topology, used protocols and servers addresses, location and versions), this may help them to find fails and exploit them to access the resources (Bradbury, D., *Network security*, 2008).

A first and easy information to get is *Banner grabbing (*Endler & Collier, 2006). By generating voluntarily an error, an attacker gets the result of this error. In the case of VoIP, an attacker can call a wrong number to get the error message, which contains (by default) the version of the software used.

Depending of the version used, some security pitfalls can be used to lead to an attack. For example, an old version of a PBX server can have some security issues fixed in the new versions. By getting the version of the used server, an attacker can check on Internet (www.voipsa.org) the known failures and exploit them.

It is strongly recommended to administrators to change default settings (which usually display many informations about versions on the errors displays) to settings which provide less technical informations.

To retrieve these informations, the attacker can make a scan of ports on a IP address. This is illustrated on the following illustration:

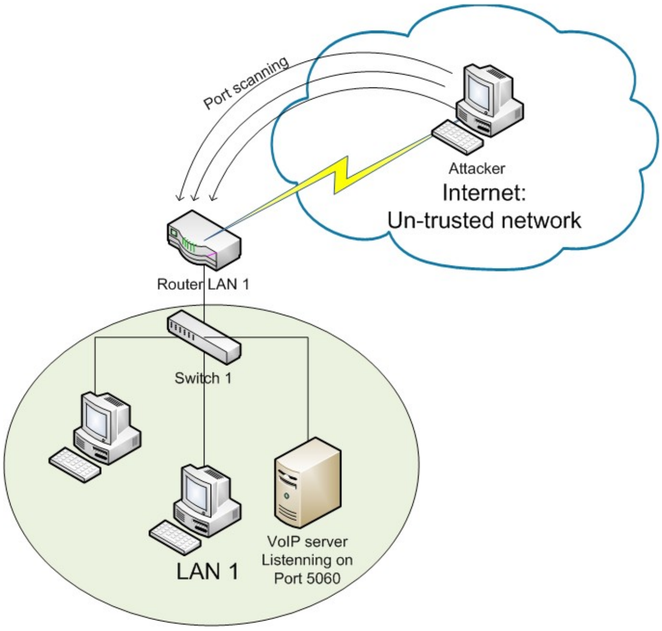


Illustration 8: attacker performing a port scan

This illustration shows the attacker performing a port-scan on the LAN 1 router (which is the gateway between Internet and the local network). To allow VoIP channel over the Internet, the router must allow the VoIP server to be reached from Internet. The attacker, by scanning open ports on the router will retrieve the one open to access VoIP service. By default and for SIP, the port is TCP or UDP 5060.

The attacker can use tools like NetCat (http://netcat.sourceforge.net) to perform the port scanning.

Once the attacker has found the port, it can try to connect on the server. The unsuccessful tries will return error messages which can be interpreted to get information on the LAN.

Note that some tools, like SiVuS (www.voipsecurity.com) allows automatic banner grabbing.

The scan allows the attacker to get the differences between errors: forbidden, unknown user, service unavailable.

3.2 Eavesdropping

Eavesdropping is more considered as an privacy issue than a security issues. However, getting some informations thanks to eavesdropping can help to attack an network / resource (e.g. getting some passwords, user habits and so on).

As VoIP is a data flux (we consider that only the voice channel is concerned by spying), some bots can be set up to listen and record to voice transmissions. An attacker within Internet network can spoof a device and be allowed to record RTP traffic. Any free and popular packet analyser like Wireshark (or Ethereal) are able to decrypt and merge RTP packets, in order to retrieve the voice flux.

Then the conversation can be recorded as a audio file, and be listened or analysed.

Regarding the signalisation channel, eavesdropping can be used to make, for example, some statistics about which numbers are dialled, how long was the call and so on. It is a less important issue than listening to conversations.

3.3 Flooding

Another important aspect of security failure in VoIP is flooding. This is type of attack does not allow directly to access resources, but can provide a kind of deny of service.

To perform this attacker, the attacker send an important load of VoIP packets to a designed device. For example, sending 200 SIP invites packets to the same device within one minute could lead to crash it.

The main effects are degrading signal quality (for example if the device is in communication) or make it respond poorly (device crash, halt or freeze).

This attack is basically used to make the attacked device confused, and allow to make itself do action which are unusual. For example, flooding a network device can make the security policy crash, so the device will be vulnerable to attacks.

Some tools are freely available on Internet, like Scappy.

3.4 DOS: Deny of Service

Deny of service is an intentional attack on a network, in order to shut down a service (e.g. the telephony service). Applied to VoIP, this attack can end a phone-call, avoid the proper utilisation of this resource (this can result by a degraded quality of sound, inconvenient disconnections or even the impossibility to make or receive calls).

The attacker usually uses flooding to perform this attack: the VoIP server will receive a heavy load of traffic, it will crash, or simply shut down to avoid crash. The attacker sends continually this traffic, so it is almost impossible without any human intervention to restore the service.

If the telephone service is down in a company, the business is down. This attack is well known, and its mitigation is complex.

3.5 Signalling manipulation

Signalling manipulation in VoIP consist in send malicious messages to the VoIP server. Both end-users are not aware of this attack, only the server (gateway) is concern with this threat.

Someone can intentionally send some erroneous signals to the server, in order to just prank people (make a connection between two users without their intervention) or end a call between them.

More serious, an attacker can pretend to be someone else. Sending some signals can inform the change of the user's IP address. Then the attacker can avoid the registration step, and be directly registered to the server, and then use the resources like if this was normal user.

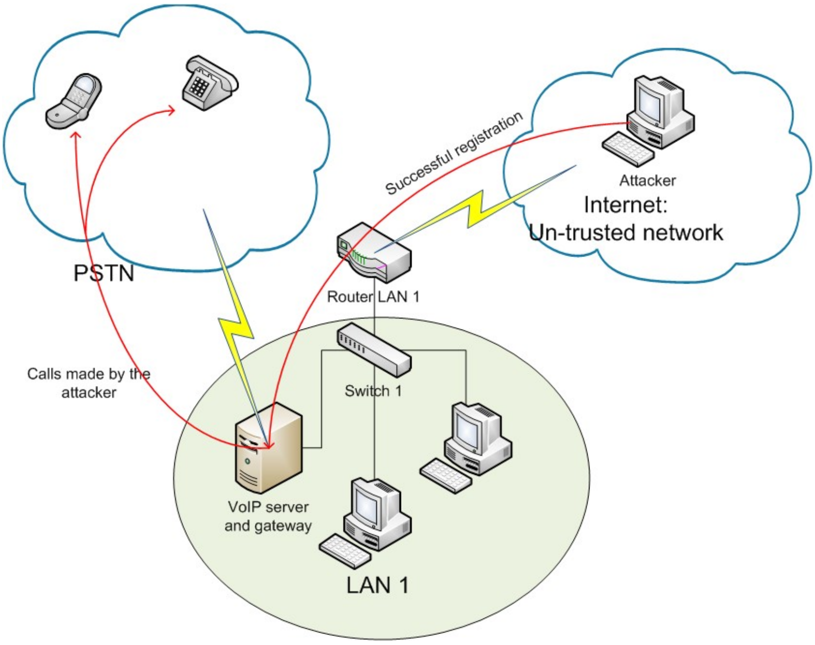


Illustration 9: making free calls with signal manipulation

Another aspect of signalling manipulation consist in changing in the packet the source user (SIP address) and pretend to be another user. Basic configuration (especially for voice mails) have the authentication based on the source user.

The information stored in voice mails are confidential, and must be kept of anybody else than the owner.

3.6 Phishing

Phishing "refers to the sending of bogus emails that pretend to be from reputable sources such as financial institutions so as to persuade people to reveal PIN numbers, passwords, and so on" (on-line Oxford dictionary, *www.askoxford.com*). Usually used for emails, this attack technique applies also to VoIP (Sonja Ryst, July 2006).

The mains goals in using this techniques can be defined by (*www.calleridspoofing.info*):

- Pretending

Making a call pretending to be another company can be useful to retrieve personal informations from the end-user, in order, for example, to retrieve a password. The user who hang up the line sees on the screen that the call is from the IT support service, or other service which could need some personal informations.

- Voice mail hacking

The connexion to the voice mail server could be not secure, and based only with the caller-ID. It the caller-ID is changed, then anyone can access to user's messages, and so private data.

Summary

This part of the study presented the main aspect of security issues of VoIP services. Most of them are related to privacy and authentication issues. Except eavesdropping and deny of service, the attacks can be performed because of the lack security of the signalling protocol (SIP). There is however a use of password for SIP but it can be easily broken (MD5 encryption, subject to dictionary attack) and does not implement any authentication or encryption.

By considering the use of VoIP within a private local network, these issues are minor, because it would be easy to trace any internal attacker thanks to server logs (IP addresses are known, there are statistics about time and user access).

However, using VoIP over Internet as unencrypted traffic will be a threats for the company: this will lead inevitably to attacks. Internet is considered as untrusted network, as anyone has access to it and there is no guarantee about Confidentiality, Integrity and Assurance (CIA model).

The maintain of security at any level is primordial: this is why voice over IP should be protected from external threats. The next part will present the solutions to mitigate.

4 MITIGATION

Introduction

In the previous part, the main security issues has been presented. All of them should be considered seriously. As none of the presented VoIP protocols implement any type of security, the aim of this part will be to present the different solutions available. The presented solutions will be able to implement strong security, data and privacy protection.

To be compliant, the solutions which will be presented will be able to secure the VoIP channels (signalisation and voice data), allow a good authentication and ensure integrity of data.

Instead of suggesting many solutions for each issue (e.g. a solution against Dos, another on against signalling manipulation and so on), the best solution is to use tunnelling for the links considered as non-secured (communication over Internet). Tunnelling is considered as the best solution to communicate between users within an insecure network (Comparing, Designing, and Deploying VPNs, 2006).

Creating a VPN consist in creating a secured tunnel, that can encapsulate different traffic (data, IP packets). All the traffic going through the tunnel will be encrypted by the sender, and only the receiver should be able to decrypt it. Any user which is not part of the VPN will not be able to "see" the traffic.

Any client included in the VPN will use all the applications and resources, as if the user was within a classic LAN (VPN are user-transparency).

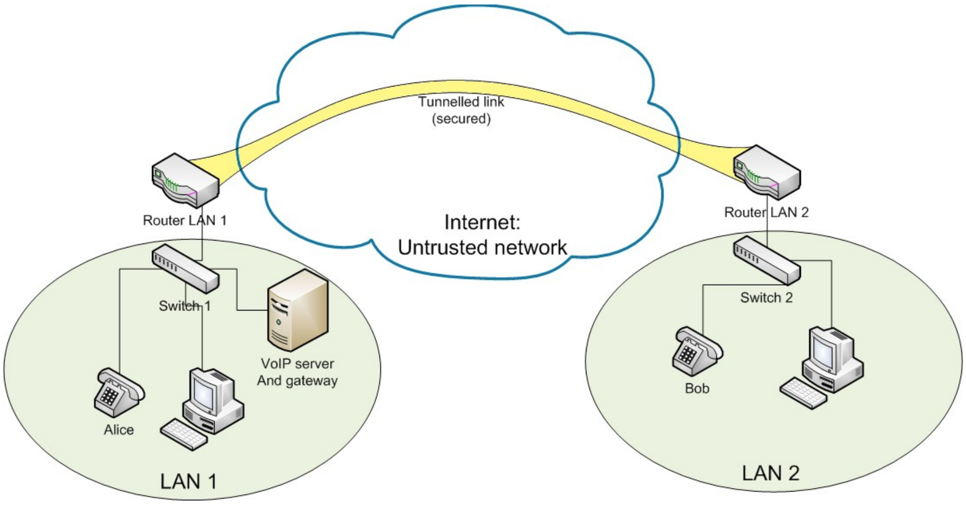


Illustration 10: tunnelling for connecting 2 distant LAN over Internet

As shown on the below illustration, the tunnel will be a virtual link using the Internet infrastructure, to allow the link between two distant sites to be secured. It is also possible to create link between simple node within Internet to the LAN. This part will be developed later.

Using Internet as the infrastructure allows much lower costs than using dedicated hardware, and scalability is better (www.vpn-info.com). The company is not aware of routes which will be used by the traffic: the tunnel will be routed like any other data channel.

As many technologies exist to implement VPN, the study will present the two most-used technologies, widely deployed and using strong encryption and authentication methods.

4.1 IPSEC tunnelling

IPSEC (Internet Protocol SECurity) is a suite of protocols used to secure a connection for packets over a IP network. This framework includes authentication, encryption, which provide a good confidentiality to secure a link over Internet. IPSEC is operating at layer 3 (network layer) of the OSI model. IPSEC is one of the most widely used framework encryption, and well supported, as wall by network devices than end-users (Windows suites includes the framework and it is well deployed on UNIX systems).

IPSEC can be implemented in two different modes:

- **Tunnel mode** allows the secure channel between two network devices, for example to connect two private networks over Internet. The main advantage is that the addresses from the private network are kept secret.
- **Transport mode** is a tunnel between two nodes, as point-to-point link. Only the end-point can decrypt the traffic. Their IP addresses cannot be hidden, because they must be known to allow routing. This implementation is mostly forbidden within corporate network, case the content cannot be checked by the firewalls.

The framework supports a full set of protocols to allow an efficient authentication, encryption and secure packet-transport

This includes:

- **Encryption:** IPSEC can use both symmetric or asymmetric encryption. However it more current to use asymmetric encryption (use of public / private keys). The private key is used to encrypt the data and the public one will be used for authentication. The generation of keys is done using the IKE (Internet Key Exchange protocol, similar to Diffie Hellman method). Keys are regenerated every couple of hour to avoid attacks.
- **Authentication:** both ends are configured with a secret key, which will allow the creation of a public and private key for each device. Theses keys are unique and allows the authentication of the devices. A challenge is sent from a device to the other, and the result is hashed (one-way encryption) with the device private key.
  The remote device will receive the hashed value, and compare with the secret encrypted with its secret key (only key that can decrypt). If the values are the same, then the device will approve the authentication of the remote one.

- **IPSEC framework protocol:** the IPSEC framework can support two encryption methods :
    - **ESP** (Encapsulated Security Payload), which take the IP header off from the packet to encrypt it. Then the original IP header is added to the encrypted data. The packet will be unchanged regarding routing over Internet.
    - **AH** (Authentication Header) encrypt the whole packet (including IP headers). Headers are added to the encrypted packet: this allow an extra authentication, and avoid replay attacks, thanks to a sequence number included within the new header.

Even if ESP does not provide a IP header encryption, the tunnel mode will automatically encapsulate the ESP packet (encrypted and original IP header) in a new IP packet. The local IP addresses are encrypted and so kept secret from Internet.

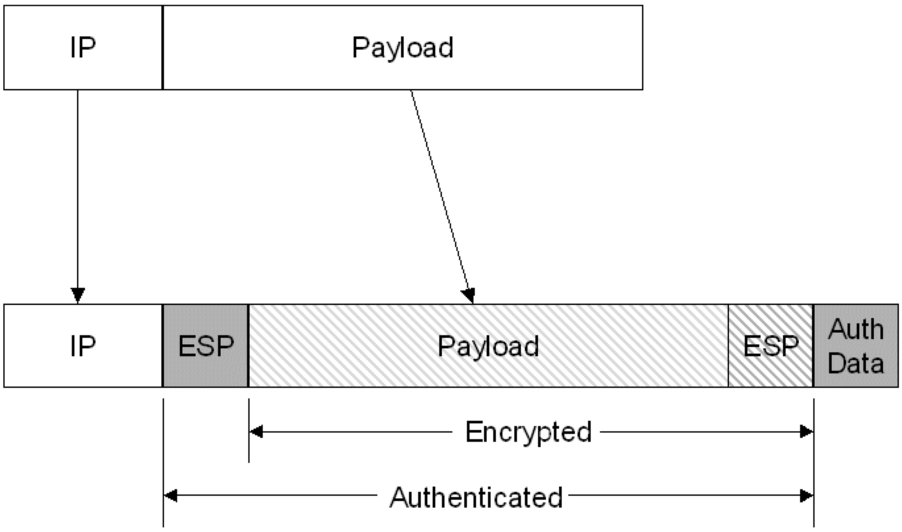


Illustration 11: ESP packet conversion (http://technet.microsoft.com)

4.2 TLS – SSL tunnelling

SSL (Secure Sockets Layer) is an encryption tools which allow the authentication, encryption and integrity on a transport and application layer (OSI model). This protocol is used for different type of usages, like secure web-browsing (HTTP vs. HTTPS), secure emailing, secure file transfer (FTP vs. SFTP), secure remote control (TELNET vs. SSH). The encryption is set-up to end-to-end connexions.

The advantage of this protocol is that it is free, open and non-propriety.

TLS connexions allows one-way identification: the server is identified by a Certificate Authority, but the clients remains anonymous. This is the case for example, on-line transactions like on E bay. The server is identified, but it does not know who is the client (it could be anyone).

However, TLS also allows both-way authentication: this is called mutual authentication. To do so, both the server and client have a certificate, delivered by a Certificate Authority.

Each end-user within the tunnel has a pair of keys: the digital certificate (the public key) and the private key. When an user wants to connect to the other end-point (which could be another client or a server), the public keys are exchanged. Another problem is introduced: how to be sure that the received public key is really from the client ?

There is a need to pass the keys in a secure way. The most reliable solution is to generate some digital certificates from a trusted source (like Verisign, GlobalSign or Microsoft).

These certificates are delivered to the clients, have a validity date and are unique. Then when a client receives the public key from a secure server, the client can verify the signature, thanks to the certificate delivered by the trusted source. These certificates are trusted by both parties.

Once both client and server are authenticated, the client enables a virtual network interface, also called *tun interface*. All the packets send through the VPN will use this interface.

Packets to be send throughout the VPN will be sent to the *tun interface*: they will be then encrypted, authenticated and encapsulate within UDP protocol before being sent to the real network device.

The server will receive the packet on the defined port, decrypt and authenticate them and will be able to use them as normal packet across the network.

Summary

This presentation introduces the two more important VPN solution on the market at the moment. The IPSEC implementation requires more complexity and knowledge to set up, for performances which has been controversial (Attacking the IPSEC Standards in Encryption-only Configuration, 2007). However, IPSEC provides a secure link from network layer: the sender can be authenticated.

The implementation of SSL tunnelling is not only used to encrypt application data stream. Its set up is less complex than IPSEC, but possibilities are limited: a dedicated machine should run the application, instead of using existing routers or networks devices (for IPSEC). SSL tunnelling encrypt only the payload, which allow the IP headers to be visible from external network (node outside the VPN). This also provide the easiest packet routing.

Also, TLS – SSL tunnelling should be used in both-way authentication, as the client should be know to use the resource. The certificate management (creation, copies and installation) is a manipulation that is not needed by using IPSEC.

The following part, Design description, will present how to implement both VPN solutions, to be compliant with VoIP, as security mitigation.

5 DESIGN

Introduction

The study carried until now presented the VoIP, the main security issues and the mitigation solutions. In prevision of the comparison and evaluation of the best solution to mitigate VoIP issues, an implementation will be performed to do test and evaluate results. The design will present the different scenarios possible, the choice of security solutions and their implementation.

We will consider for the rest of the study that a company has a main Network (called HQ, like Headquarters) and some other distant LAN (e.g. distant work-sites across the country). All these private networks are connected thanks to Internet, for cost reasons (a dedicated link is usually really expensive).

We consider that the main resources (VoIP server in the case of the study) are located within the HQ LAN. Clients, from other LANs, have to register onto the VoIP server, and be able to place and receive calls from any other LAN. The global topology can be resumed by the following illustration:

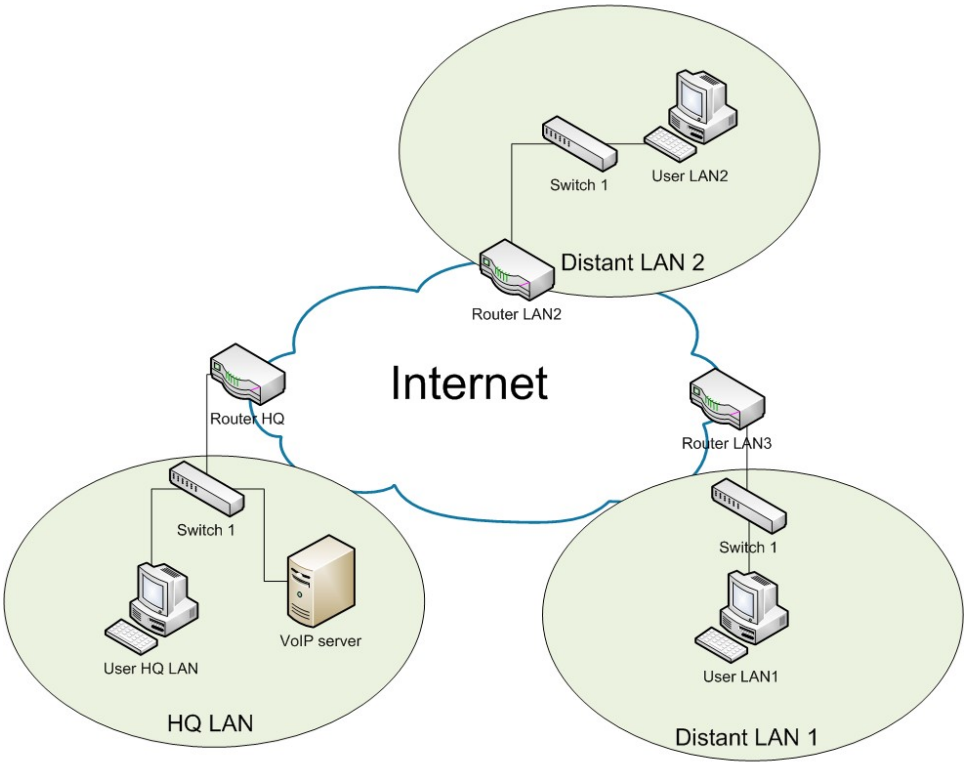


Illustration 12: main scenario with 3 LAN interconnected thanks to Internet

5.1 IPSEC design and possibilities

As presented before, IPSEC allows the transport mode mode (between network devices) or point to point tunnelling. In the case of the presented topology, the transport mode is more appropriated: the tunnels can be set-up between the routers connected to Internet. This would result of these tunnels:

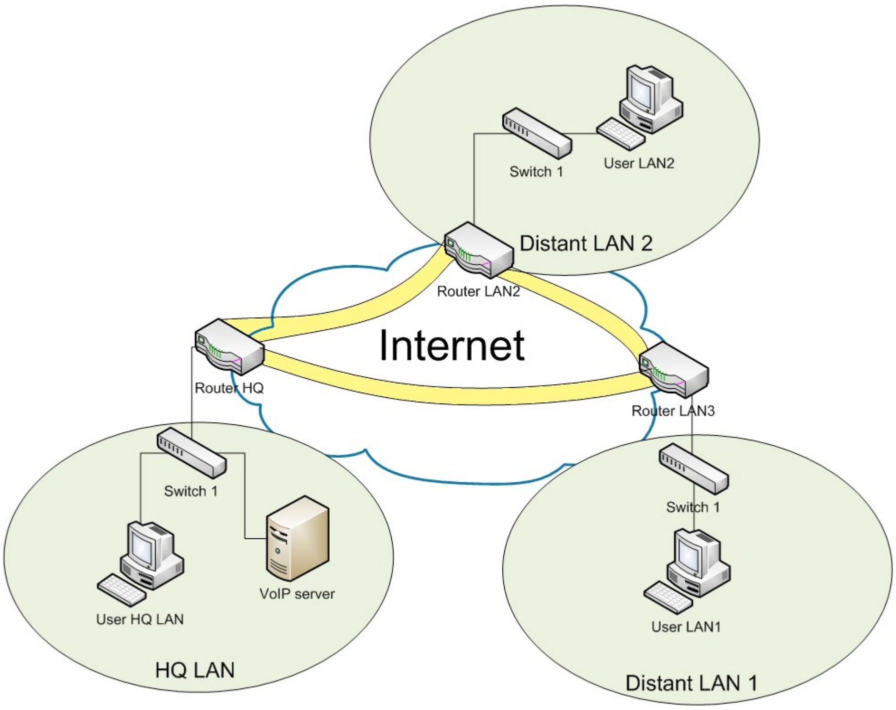


Illustration 13: design of IPSEC tunnelling

The link over Internet will be encrypted thanks to IPSEC in transport mode: it would be like a dedicated link between the LANs. The clients themselves do not have to worry about the tunnel, as the tunnel implementation is made within the routers.

As IPSEC also can manage with end-to-point liaisons, it is possible to create a tunnel from a client within LAN1 or LAN2 to the HQ Router. It is however more interesting in this scenario to link the routers between them.

The tunnels will encrypt any type of data: there will not be any distinction done from the voice / signalisation channels than the other type of traffic (e. g. HTTP, FTP and so on).

5.2 SSL – TLS design

SSL – TLS tunnels can also be used within the designed topology. As the SSL tunnels can be made only by point-to-point transport, the only solution is to create tunnels from each clients to the server. A server have to be set-up within the HQ LAN to enable the remote connection from the clients.

This server will receive the packets from the VPN clients, and route them within the HQ LAN.

The topology will be so:

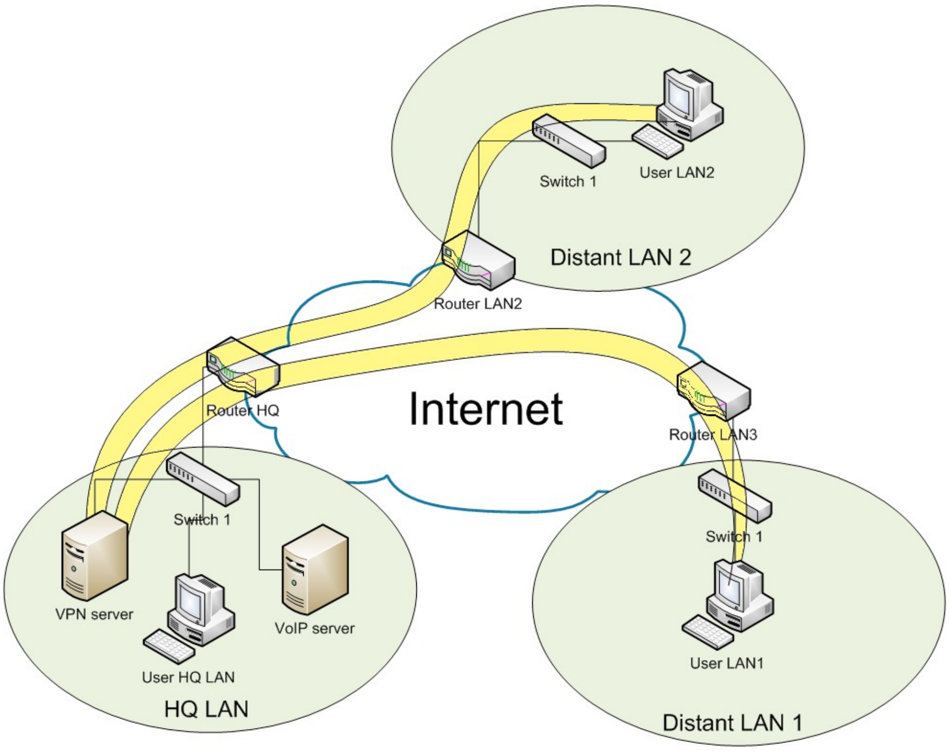


Illustration 14: design of SSL tunnelling

The tunnels (in yellow) are set-up from the clients to the VPN server, situated within the HQ LAN. Each client will have to be connected to the VPN server to be able to use the resources in the HQ LAN.

Once the clients are connected to the server, they get a virtual IP address associated to their virtual network adapter. The VPN server will act like a router, to route packets from the virtual pool to the physical network.

5.3 Configuration

The configuration of the equipments is also an essential point: this will present the scenario as close as possible as a real company has. The operating systems, tunnelling solution and software used for the study should be some that can be used for a commercial use (within a company).

5.3.a VoIP server

One of the main feature of the network will be the VoIP server: it must be a reliable, flexible and secure resource. This is why the choice of Asterisk software is a good solution: it is free, open source and really popular. One of Asterisk's most powerful features is its ability to connect different technologies within the same feature-rich environment (Asterisk open-source PBX system, 2004). Its wide range of plugins and regular patches and updates are maintained thanks to the active community (http://www.asterisk.org/community), this solution is well deployed.

The use of a UNIX-based system allows a more stable and secure platform for running the server. In the case of the study an Ubuntu distribution will be used to host the software.

5.3.b IPSEC VPN

The IPSEC VPN will be set-up from routers to routers: the devices should implement the set of protocols which define IPSEC. The devices used will be some CISCO routers and switches, for their wide deployment in most of the companies. Update IOS can manage with IPSEC, as the framework (IPSEC) is popular. As a client can also directly be connected on the router, the use of a IPSEC client like EasyVPN (from CISCO) will be used.

5.3.c SSL VPN

The easiest and one of the more popular solution to create a SSL VPN is to use OpenVPN. Widely deployed, free and open source, OpenVPN is an up-to-date and reliable solution to create SSL VPN. Also, OpenVPN can be used both on UNIX and Windows systems.

As a server must be set-up within the Headquarters LAN, the use of a single computer is enough to manage the tunnel connexions. OpenVPN in server mode should be running on a UNIX machine (for security reason, but it could also work on a Windows computer).

For some computer limitations, the implementation of the VPN server will be made onto the same machine of the VoIP server. If the server was distinct from the machine, it would have been exactly the same, except that there is one machine less on the HQ LAN.

Summary

The design description allowed the presentation of the scenario that will be set up for the implementation. This theoretical part is essential for the understanding of the rest of the study. The presentation was global, but allowed to show which equipments will be used and in what context they will be running.

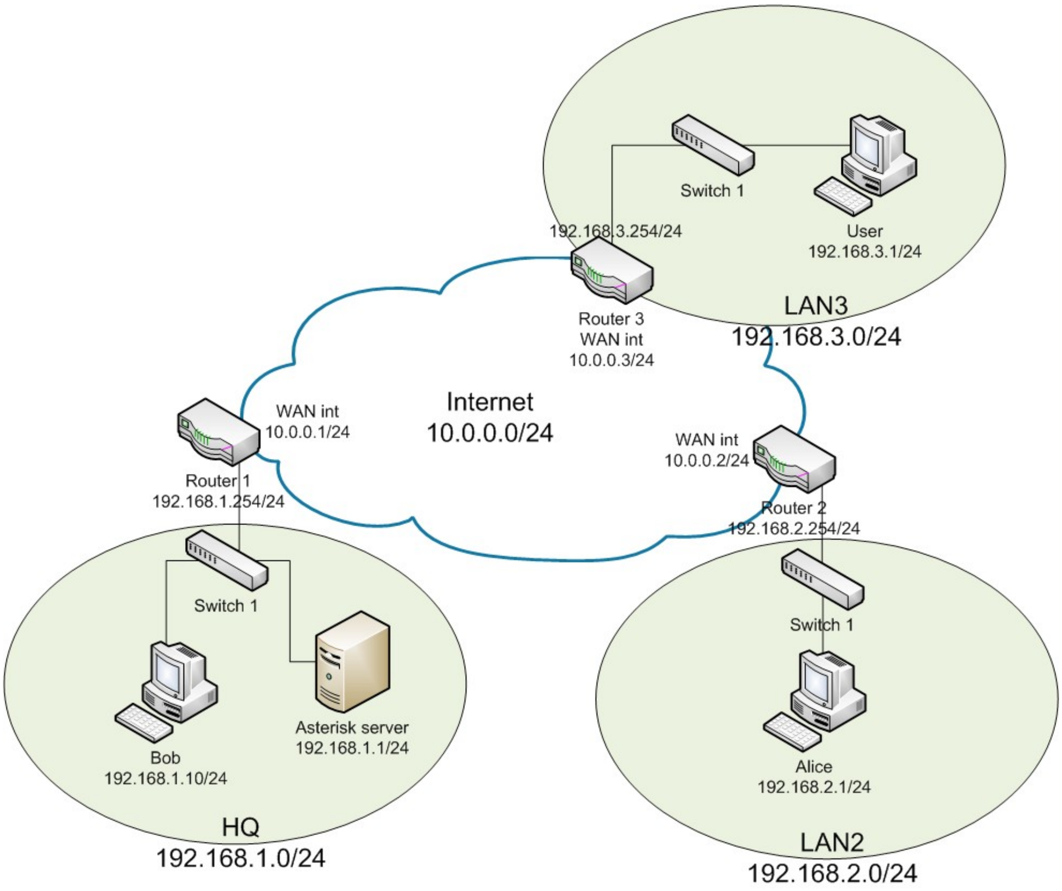
The configuration in details will be presented in the Implementation chapter. This will detail how the equipments are set-up to meet the requirement of the study, and be able to make the tests.

6 IMPLEMENTATION

Introduction

Thanks to design description presented before, the scenario, all the equipments and software are defined and justified. The implementation will now show how the scenario will be set up, in details, to meet the requirement of the study. The results will be presented as well, and discussed later.

The global structure of the scenario presented in the design is realised, using the following IP addresses:



The IP addresses used are all private networks (for tests) and the IP range for each LAN is different (to allow routing).

6.1 Internet link simulation

As defined within the design part, the network equipments are all from the manufacturer CISCO. As a leader in networking equipments market, most of the companies in the world, are using their equipments.

To implement the link over Internet, a switch is placed between the routers, and the port where the attacker is connected is configured to be able to listen to all traffic (like a HUB).

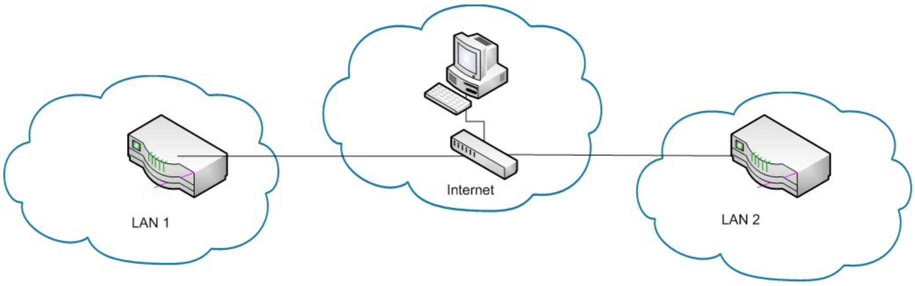


Illustration 16: implementation of the Internet link

Internet itself is a very complex topology, using routing protocols, making the packet to use different possible routes. In the case of the study, the routing is not evaluated so not important regarding the tests. This simple topology can act like Internet: both end point can communicate, but the network is not secured (anyone can list to the traffic).

To implement this “lack of security”, where anyone can listen to the traffic, a node is placed onto a privileged port, which will copy all the traffic from the switch on it.

The configuration of the switch is using SPAN, which allow to redirect all traffic from a port / range of ports to a specified port. Here is the part of the configuration that allow the redirection:

```
monitor session 1 source vlan 1 rx
monitor session 1 destination interface Fa0/24
```

These lines allow all the traffic from VLAN1 to be relayed on the port 24. As no VLAN are configured on the switch, all the ports belongs to VLAN1. The rx allows the attacker to listen only. It cannot transmit any packet on the switch (this is to simplify the capture). A computer running a network analyser (like Wireshark) will be connected to the port 24, so will be able to listen to all the traffic.

6.1.a VoIP server: Asterisk

The VoIP server is represented by a dedicated computer, running a UNIX (Ubuntu 2.10, www.ubuntu.com). The chosen software to implement the server is Asterisk (www.asterisk.org). The installation steps and configurations can be performed thanks to the manual or the book Asterisk ™: The Future of Telephony, they do not consist an interesting piece of work for the study.

Once installed, the SIP clients have to be defined in the */etc/asterisk/sip.conf* file. For the needs of the tests, only 3 clients are defined (users 1000, 2000 and 3000). The very basic (but working) configuration of a client is:

```
[1000]
type=friend
context=phones
host=dynamic
```

The *type* line allows to define the right of the client: *friends* give any possibilities (send and receive calls). The context will define if the associated client is a standard user (phone), or another device (e.g. devices dealing with video, voice mail...). The *host* parameter allows to place the user within the network: it is usually defined by an IP address but still for the tests and more flexibility, *dynamic* setting is used (the client can have any IP address).

Anyway, when the client will send the REGISTER packet, it will send its IP address, allowing the server to locate the client.

Now that the clients are configured, the dial plan should be configured as well: this plan will define what to do when the server receive signals. This can allow, for example, to put a waiting sound if the line is busy, to make interactive menus (e.g. answer phone) or redirect some calls.

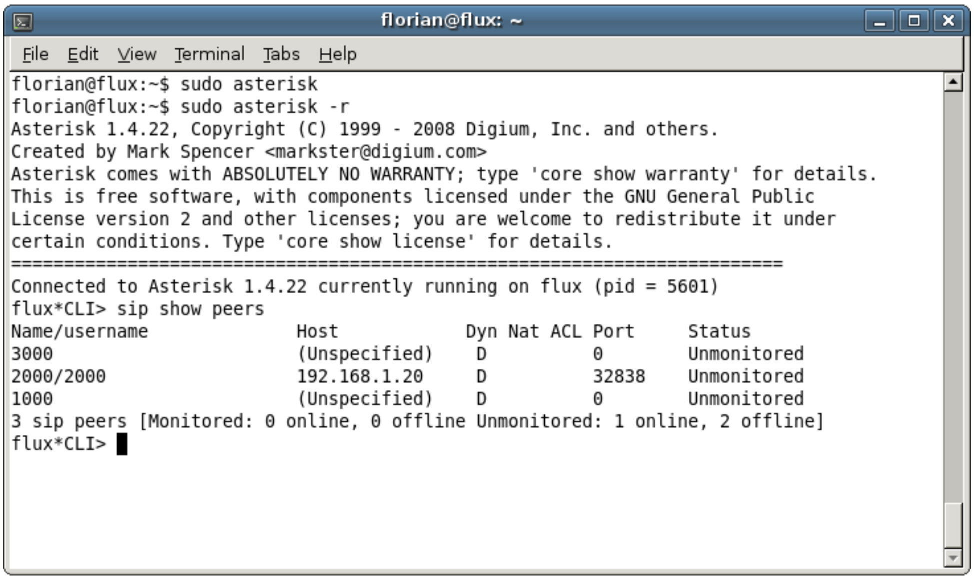
To configure the dial plan, the file */etc/asterisk/extensions.conf* contains all the plans. It is important to define which user will be called, in function of the dialled number.

```
[internal]
exten => 1000,1,Dial(SIP/1000)
exten => 2000,1,Dial(SIP/2000)
exten => 3000,1,Dial(SIP/3000)
```

A new rule called *internal* will call the SIP user XXX when XXX is dialled on the soft phone. This is not flexible, not fully-featured, very basic but it works for tests. This can be improved thanks to regular expressions and programming syntaxes (detailed in the documentation).

The full configuration files can be retrieved in the annexes part.

Then Asterisk should be started as root thanks to the command *sudo asterisk*. The process is launched in background is no errors are displayed. Then to access to the console, the command *asterisk -r* can be used:



```
florian@flux:~$ sudo asterisk
florian@flux:~$ sudo asterisk -r
Asterisk 1.4.22, Copyright (C) 1999 - 2008 Digium, Inc. and others.
Created by Mark Spencer <markster@digium.com>
Asterisk comes with ABSOLUTELY NO WARRANTY; type 'core show warranty' for details.
This is free software, with components licensed under the GNU General Public
License version 2 and other licenses; you are welcome to redistribute it under
certain conditions. Type 'core show license' for details.
=========================================================================
Connected to Asterisk 1.4.22 currently running on flux (pid = 5601)
flux*CLI> sip show peers
Name/username              Host            Dyn Nat ACL Port     Status
3000                       (Unspecified)    D          0        Unmonitored
2000/2000                  192.168.1.20     D          32838    Unmonitored
1000                       (Unspecified)    D          0        Unmonitored
3 sip peers [Monitored: 0 online, 0 offline Unmonitored: 1 online, 2 offline]
flux*CLI> 
```

The illustration shows a fully functional Asterisk server running (no warnings or errors). The three clients defined are displayed, but only one of them is connected (the network was not up when the capture was made).

Now that Asterisk is running properly (user are defined in the conf file and call procedures are defined), the clients must be configured to be allowed connecting to the server.

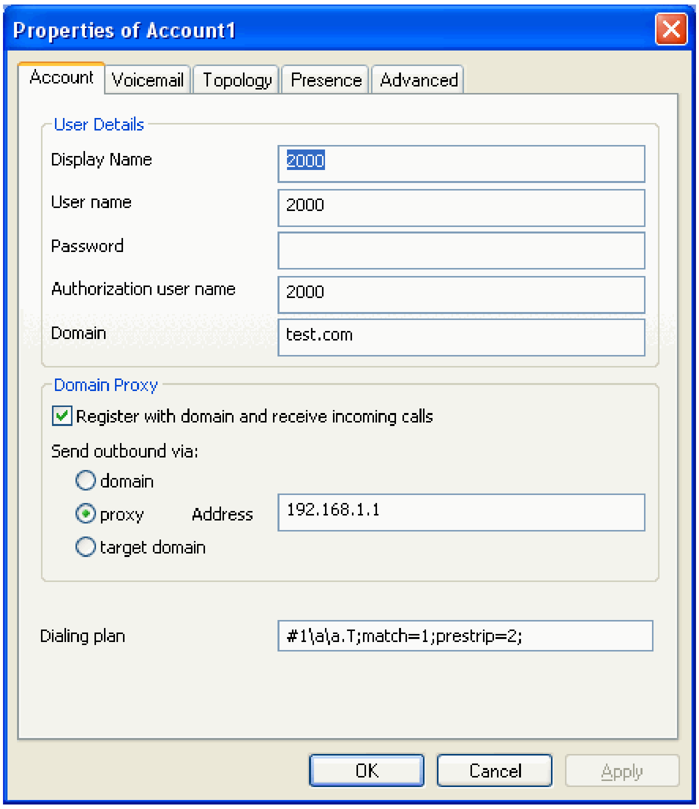
6.1.b Software and OS

The clients (work stations within the LANs) will run Windows XP SP3, the most used up to date version of Windows.

The nodes are running X-LITE as a SIP client (free soft-phone, downloadable at www.counterpath.com). The configuration of SIP soft phones must allow a registration to the server, previously configured. The clients will register to Asterisk PBX, using a valid user name, and then will be able to make / receive calls.

To do so, they register using a proxy (the PBX), thanks to its IP address or host name. The user must provide the user name and specify that the client must register first.

The illustration above shows the SIP configuration for a client (using X-Lite):



Display Name: 2000

User name: 2000

Password:

Authorization user name: 2000

Domain: test.com

☑ Register with domain and receive incoming calls

Send outbound via:

○ domain

● proxy Address: 192.168.1.1

○ target domain

Dialing plan: #1\a\a.T;match=1;prestrip=2;

Illustration 18: SIP configuration

The configuration should define the Proxy server to connect to (Asterisk server). The user name / authorisation name are defined in the *sip.conf* onto the VoIP server. The domain should be defined to facilitate the registration within the Proxy.

6.1.c Security implementation

In order to meet the requirements for the study, the test should implement some security. Both IPSEC and SSL-TLS VPN will be tested. The detailed configuration and set-up is described in the two next parts, describing each scenarios.

However the network topology does not implement any type of firewall. Its integration is not necessary for the tests, as the study has for aim to present the security issues and how to mitigate them. In the case of this study, firewall application will allow the VoIP channels, as this application represent an allowed traffic across the network.

6.2 Scenario 1 VPN SSL

6.2.a Installation and configuration

As justified in the design part, OpenVPN is the software which is used to create the tunnel. The first step is to retrieve it on www.openvpn.org and install it (see the manual).

Once installed, the next step is the creation of keys and certificates, to define which machines can be connected into the tunnel. Note that for companies, the certificates should be delivered by a Certification Authority.

For the tests, the certificates are created and self signed.

By entering in the OpenVPN folder (after extracting the files from the archive set-up), the tools needed to create the keys are located in the open-plan*/examples/easy-RSA/2.0* directory.

The instructions in the *ready-made* explain step to step how to create the different keys, for the server and the clients. Also, Diffie Hellman parameters must be defined to allow the server to pass public key to the clients.

Once the key are created, the server must have the following files:

File name	Description	Who	Privacy
ca.crt	Certification Authority certificate	Server and all clients	Public
ca.key key	Certificate Authority signature	Server	Private
dh{n}.pem	Diffie Hellman parameters	Server	Public
server.crt	Server public certificate	Server	Public
server.key	Server secret key	Server	Private
client{x}.crt	Public client certificate	Client{x}	Public
client{x}.key	Private client key	Client{x}	Private

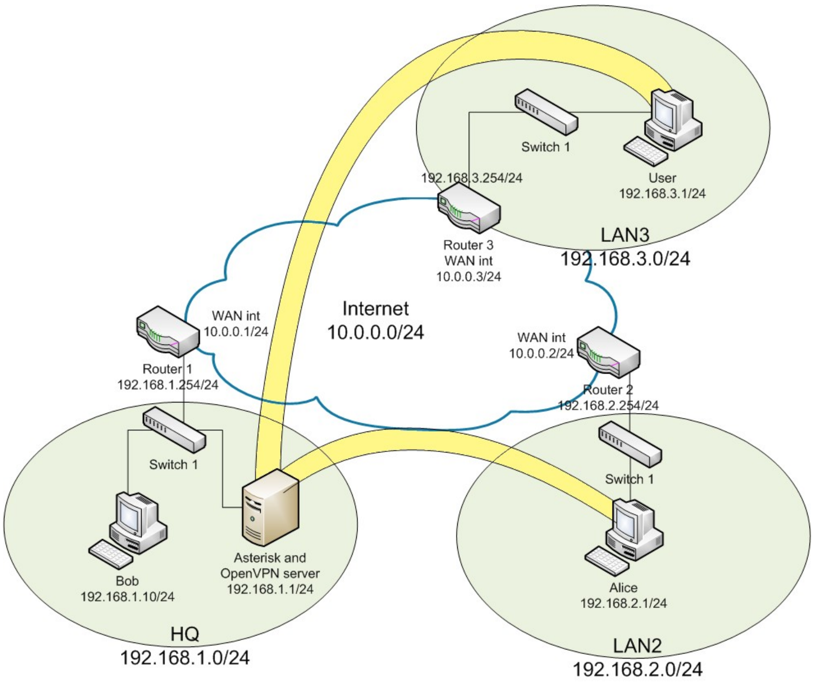
Now that all the clients have their needed files, the server needs to be configured to accept only associated certificates. The client configuration file defines the path to the certificates to use, the IP address to reach the server and the virtual network adapter to use (Windows user needs to create one using the tool installed with OpenVPN).

The server configuration file define what type of VPN will be created (routed or bridged), the port to listen on, the IP addresses pool for the clients. The use of routed VPN is more interesting if the machine is not a gateway (have only one network adapter).

The configuration files are in Annexes.

6.2.b Topology and tests

As defined in the Design part, the following topology has been set-up:



This design present a single user connecting onto the VPN server, which is in the HQ LAN. The OpenVPN server works as a bridge: it receives the client-connection request, check the validity of the certificates, and then grant the connection to the client.

The client retrieve thought the VPN its configuration: IP address, mask and routes. When successfully connected, the client has a virtual network connection, where all traffic going through will be encrypted and sent to the VPN server. The client pull its configuration from the server (defined in *server.conf* file on the server).

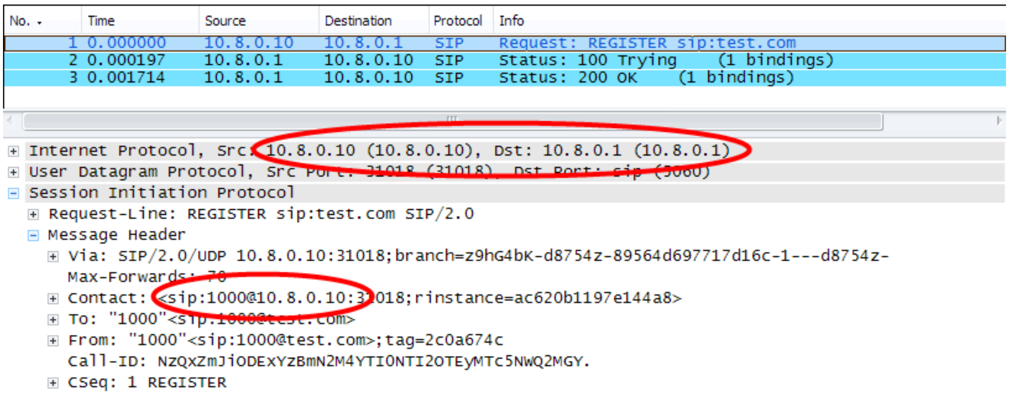
In this implementation, Bob's VPN network adapter configuration is:

```
IP address:    10.8.0.6/24
Gateway:       10.8.0.1
Route:         10.8.0.0 /24 ; 192.168.2.0/24 ; 192.168.3.0/24
```

Routes allows the traffic from the client to networks 192.168.2.0/24 and 192.168.3.0/24 to be redirected through the VPN.

Now that User (LAN3) and Alice (LAN2) are connected to the VPN server, they both are on the same virtual network (10.8.0.0/24). They are able to see each other like if they were in local, thanks to the virtual adapter.

The connection to Asterisk must be done thanks to the VPN server IP address, or the traffic will not go through the VPN. The server IP address is 192.168.1.1 (physical address) AND 10.8.0.1 (VPN address). The SIP clients should so connect the the VPN adapter IP:

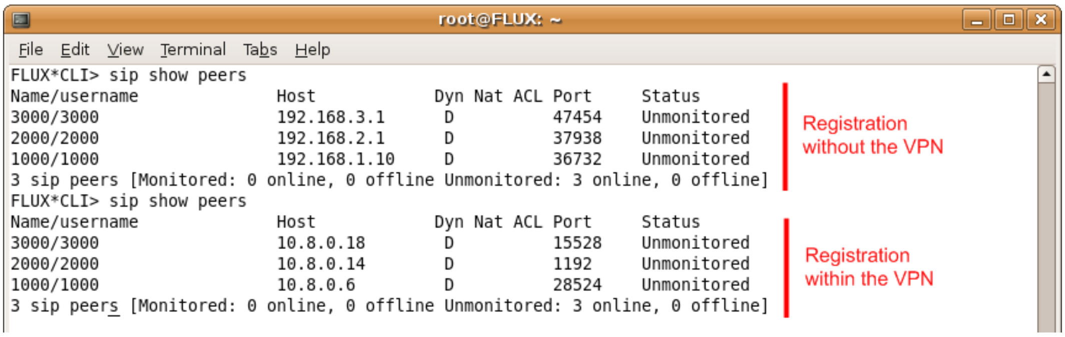


```
No.   Time        Source       Destination  Protocol  Info
    1 0.000000    10.8.0.10    10.8.0.1     SIP       Request: REGISTER sip:test.com
    2 0.000197    10.8.0.1     10.8.0.10    SIP       Status: 100 Trying     (1 bindings)
    3 0.001714    10.8.0.1     10.8.0.10    SIP       Status: 200 OK     (1 bindings)

⊞ Internet Protocol, Src: 10.8.0.10 (10.8.0.10), Dst: 10.8.0.1 (10.8.0.1)
⊞ User Datagram Protocol, Src Port: 31018 (31018), Dst Port: sip (5060)
⊟ Session Initiation Protocol
  ⊞ Request-Line: REGISTER sip:test.com SIP/2.0
  ⊟ Message Header
    ⊞ Via: SIP/2.0/UDP 10.8.0.10:31018;branch=z9hG4bK-d8754z-89564d697717d16c-1---d8754z-
      Max-Forwards: 70
    ⊞ Contact: <sip:1000@10.8.0.10:31018;rinstance=ac620b1197e144a8>
    ⊞ To: "1000"<sip:1000@test.com>
    ⊞ From: "1000"<sip:1000@test.com>;tag=2c0a674c
      Call-ID: NzQxZmJiODExYzBmN2M4YTI0NTI2OTEyMTc5NWQ2MGY.
    ⊞ CSeq: 1 REGISTER
```

Illustration 20: SIP registration through the SSL VPN

The above capture has been made on the virtual interface of the server: the packets are not encrypted yet. The registered client is from the VPN IP pool, which allow the traffic to be redirected in the virtual adapter (and be encrypted).

Once registered, the command *sip show peers* onto Asterisk allows to see the connected peers:



```
FLUX*CLI> sip show peers
Name/username              Host            Dyn Nat ACL Port     Status
3000/3000                  192.168.3.1      D          47454    Unmonitored
2000/2000                  192.168.2.1      D          37938    Unmonitored
1000/1000                  192.168.1.10     D          36732    Unmonitored
3 sip peers [Monitored: 0 online, 0 offline Unmonitored: 3 online, 0 offline]
FLUX*CLI> sip show peers
Name/username              Host            Dyn Nat ACL Port     Status
3000/3000                  10.8.0.18        D          15528    Unmonitored
2000/2000                  10.8.0.14        D          1192     Unmonitored
1000/1000                  10.8.0.6         D          28524    Unmonitored
3 sip peers [Monitored: 0 online, 0 offline Unmonitored: 3 online, 0 offline]
```

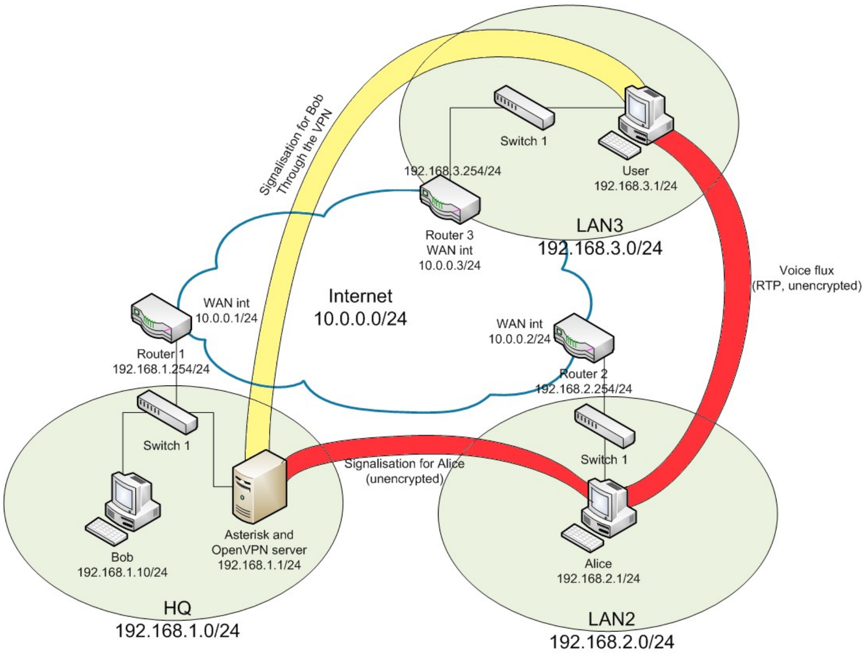
Registration without the VPN

Registration within the VPN

The first bloc shows the clients which are registered using their physical IP address (the traffic does not through the VPN). The second bloc shows that the clients are registered with their virtual IP addresses, that mean that Asterisk will route the packets through the VPN, and so encrypt the traffic.

Now that the clients are within the VPN, all the traffic goes through the VPN server (it is the gateway for the VPN). All traffic seen from Internet and LANs is encrypted, only the clients can see unencrypted traffic onto their virtual adapter.

However, if User (LAN3) wants to call Alice (LAN2), and Alice is not registered to Asterisk through the VPN, User will retrieve the physical IP address from Alice (192.168.2.1) to place the call. All the signalisation will go to Asterisk through the VPN, but the voice channel will directly go to Alice's IP address



The solution is to push another route into the User's VPN configuration. The configuration should include a route to reach Distant LAN through the VPN. This can be easily done by adding a line in *server.conf*, on the VPN server :

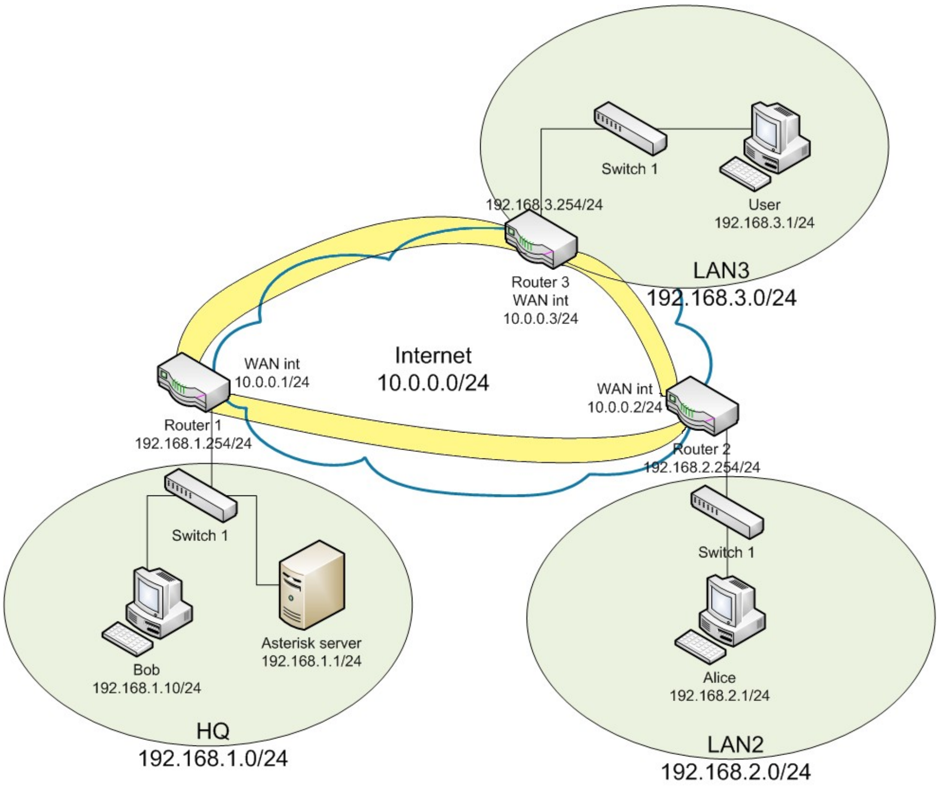
```
push "route 192.168.2.0  255.255.255.0"
```

Once User has its routing table up to date (disconnect and reconnect to the VPN server), all the traffic (signalisation and voice data) will come from User to the VPN server, and then to Alice.

However, note this modification dos not allow the encryption of the traffic between Asterisk server and Alice.

6.3 Scenario 2 VPN IPSEC

The implementation of the IPSEC tunnels consist in creating a tunnel from routers to routers. In the presented network topology, there is three routers, so any of them will have two tunnels to the others routers:



The tunnels are created only from the routers: the clients are not aware about the encryption. As IPSEC is a framework, there are two central elements to configure:

- The Internet Key Exchange (IKE) parameters
- IPSEC parameters

The IKE parameters allows the routers to pass and validate the IKE policies to each other. IKE parameters are configured thanks to a Internet Security Association and Key Management Protocol (ISAKMP) policy. This policy defines the authentication, encryption and hashes methods.

```
!
crypto isakmp policy 10
        encr aes 256
        authentication pre-share
        group 5
        lifetime 3600
!
```

The policy defined allows a encryption using AES 256, using SHA hashing and the lifetime (for the keys) is 3600 seconds (one hour). Changing regularly the key allow a good security against brute force or dictionary attack as hashing is one-way *encryption*.

The next step defines the pre-sharing keys. These keys will be used to authenticate the routers within the VPN. In this example, the keys are *cisco*, they should be more complex for a production network.

```
crypto isakmp key cisco address 10.0.0.2
crypto isakmp key cisco address 10.0.0.3
```

Note that both of the end-point should have the same keys, and IP addresses can be replaced by host names.

The IPSEC parameters are defined, to allow tunnel encryption:

```
crypto ipsec transform-set 50 ah-sha-hmac esp-aes 256 esp-sha-hmac
crypto ipsec security-association lifetime seconds 1800
```

Then the interested traffic should be defined: the access lists will define which traffic to encrypt. In our case the traffic which should be encrypted is between Router HQ and the two others, so:

```
access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
access-list 102 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
```

With some versions of CISCO IOS, it is possible to encrypt only the traffic defined by the source or destination port. This can be interesting if we do not want all the traffic to be encrypted from the LANs.

The last step consist in creating the crypto maps: they allow to regroup all the configurations made before to encrypt the right traffic (thanks to the ACL) to the right peer (thanks to the keys defined before) and using the encryption.

```
!
crypto map SITETOSITE 10 ipsec-isakmp
        set peer 10.0.0.2
        set security-association lifetime seconds 900
        set transform-set 50
        set pfs group5
        match address 101
!
```

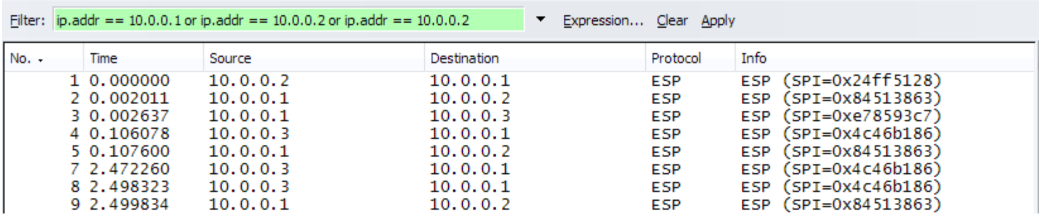
For each tunnel a policy should be defined: in our case, they are two tunnels so it should be another policy named:

```
crypto map SITETOSITE 20 ipsec-isakmp
```

Now that the crypto map is defined, it should be applied to the external interface (the one connected to Internet):

```
!
interface FastEthernet0/0
        ip address 10.0.0.1 255.255.255.0
        crypto map SITETOSITE
!
```

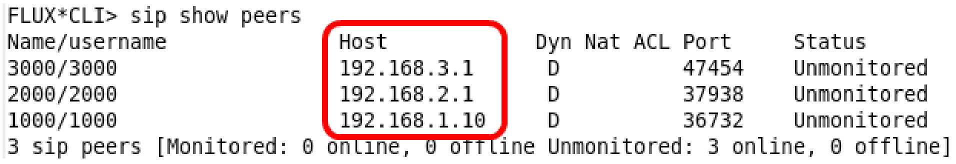
Once all the routers are configured, the tunnels should be created automatically at the first traffic between the LANs. To do so, a ping is enough. Capturing packets from Internet network shows that all the packets are encrypted using ESP encryption:



Filter: ip.addr == 10.0.0.1 or ip.addr == 10.0.0.2 or ip.addr == 10.0.0.2

```
No.  Time      Source      Destination  Protocol  Info
  1 0.000000  10.0.0.2    10.0.0.1     ESP       ESP (SPI=0x24ff5128)
  2 0.002011  10.0.0.1    10.0.0.2     ESP       ESP (SPI=0x84513863)
  3 0.002637  10.0.0.1    10.0.0.3     ESP       ESP (SPI=0xe78593c7)
  4 0.106078  10.0.0.3    10.0.0.1     ESP       ESP (SPI=0x4c46b186)
  5 0.107600  10.0.0.1    10.0.0.2     ESP       ESP (SPI=0x84513863)
  7 2.472260  10.0.0.3    10.0.0.1     ESP       ESP (SPI=0x4c46b186)
  8 2.498323  10.0.0.3    10.0.0.1     ESP       ESP (SPI=0x4c46b186)
  9 2.499834  10.0.0.1    10.0.0.2     ESP       ESP (SPI=0x84513863)
```

From Asterisk console, the users are registered with their physical IP address:



```
FLUX*CLI> sip show peers
Name/username             Host            Dyn Nat ACL Port     Status
3000/3000                 192.168.3.1      D          47454    Unmonitored
2000/2000                 192.168.2.1      D          37938    Unmonitored
1000/1000                 192.168.1.10     D          36732    Unmonitored
3 sip peers [Monitored: 0 online, 0 offline Unmonitored: 3 online, 0 offline]
```

Illustration 24: SIP users registered

From the VoIP server, it is the same configuration as if there was no tunnel: the clients can be access from Asterisk using their global IP. The connectivity is working, as the server sees the clients as *active.*

There is also a possibility for the clients which are not connected within the LANs (mobile node within Internet) to be connected to one of the routers, using an IPSEC client, like CISCO EasyVPN.

To do so, the router should implement another piece of configuration:

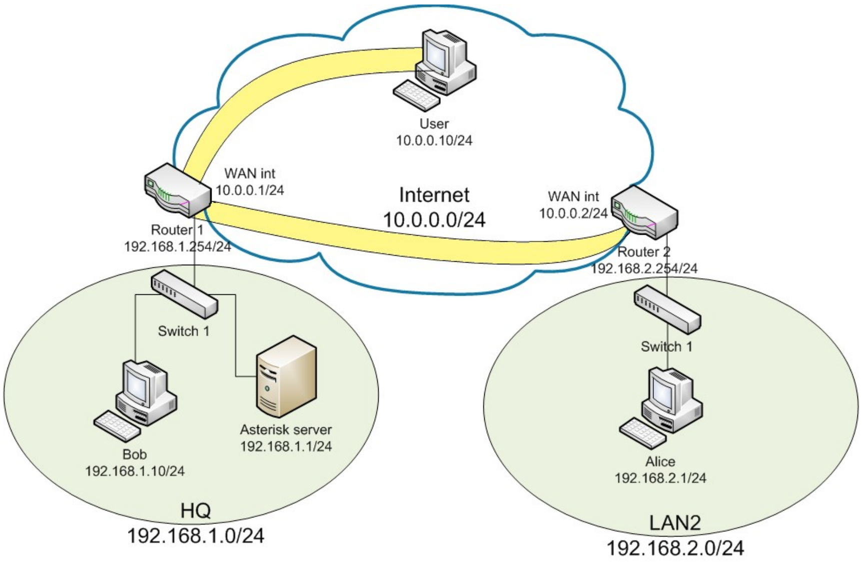
```
aaa new-model
aaa authentication login default local none
aaa authentication login VPNAUTH local
aaa authorization network VPNAUTH local
ip local pool VPNCLIENTS 192.168.5.10 192.168.5.20
crypto isakmp client configuration group ciscogroup
        key ciscogroup
        pool VPNCLIENTS
        acl 110
        netmask 255.255.255.0
!
crypto ipsec transform-set CLIENTTRANS esp-3des esp-sha-hmac
crypto dynamic-map TUNNELS 20
        set transform-set CLIENTTRANS
        reverse-route
!
crypto map TUNNELS client authentication list VPNAUTH
crypto map TUNNELS isakmp authorization list VPNAUTH
crypto map TUNNELS client configuration address respond
crypto map TUNNELS 20 ipsec-isakmp dynamic EASYVPN
interface Loopback0
        ip address 192.168.5.254 255.255.255.0
!
```

The part of configuration above allow the connexion from remote users, using ESP encryption. The clients will get a dynamic IP address (like DHCP server) from 192.168.5.10 to 192.168.5.20. the key (password) to allow the connexion is “ciscogroup”. The interface Loopback0 is the gateway of the VPN clients.

An ACL (here defined as number 110) will define which traffic will be encrypted by this tunnel.

```
access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.5.0 0.0.0.255
```

Once established, the topology can be resumed with this illustration:



User has a IPSEC client running on its computer, and will connect to Router1. All the signalisation to Asterisk server will be encrypted, as the default route to HQ LAN goes through the tunnel.

However, the voice and data from User to Alice will use an insecure channel (Internet) to reach LAN2. The tunnel configuration should specify some routes to allow the traffic from User to LAN2, through the tunnel.

Then the traffic will be encrypted from User to Router 1, and the Router 1 will decrypt, analyse (route) the packet and encapsulate it within the tunnel to LAN2.

None of the packets will be unencrypted within Internet network.

Summary

The implementation presented has been realised in accordance to the design, introduced in the previous part. The set-up and explanation of the tests allowed to bring in light some differences, advantages or inconveniences of the mitigation solutions.

The use of tunnels should have avoid any unencrypted traffic within Internet network. However the Evaluation part will present the results of captures and tests, and explain if the solutions meet or not the system requirement.

7 EVALUATION

Introduction

Following the implementation of the mitigation solutions, an evaluation will allow to the audience to be aware of the main aspects and differences of the tests realised before. As the Mitigation chapter presented the tunnelling technologies within a global context, the evaluation will now present in what extend these solutions are adapted or not to VoIP.

The part will take point by point the different aspects for each implementation made in the previous chapter. These points will explain how the solution has been efficient or not, why it is adapted to VoIP, and in what extend.

Some of the encountered problems have been speedily presented during the implementation, they will be more detailed and explained. Also, some other major problems will be presented, problems which were not evident during the tests, because tests has been made in a local network, on a simple topology.

7.1 SSL tunnelling evaluation

The implementation of SSL tunnelling applied to the topology posed some problems. Even if all the traffic was encrypted and secure, some points should be discussed.

7.1.a End-to end tunnelling

As the SSL is an end-to-end tunnel, the clients must be aware of it and change their configuration, in order to allow the traffic to go through the tunnels. If the client configuration define the server to register to as its physical IP address, the traffic will not go through the tunnel. It will go directly by the Internet network, so the link will be insecure.

The is also another important issue by using end-to-end encryption: the traffic cannot be checked by the firewalls. It is important within a company to check the incoming / outgoing traffic to prevent security issues (e. g. viruses, worms propagation). As the traffic can be decrypted only by the end-points, the administrator cannot be aware of the traffic between the nodes. If a client is infected by a virus, it could infect the whole network as the VPN server is within the infrastructure.

7.1.b Certificate management

The use of SSL authentication needs to retrieve some certificates, in order to authenticate the server / client. The use of certificates, as explained in the mitigation chapter, is provided by some Certificate Authorities. A certificate is needed for the server, but also for each clients. These certificates are not free, they need to be bought directly from the CA provider. The prices should not be neglected, it can be around $400 a year, each (www.verisign.com).

If the solution is software-free (e.g. use of OpenVPN, which is an open-source program), the certificates are the price to pay to provide a good security.

During the tests, the certificates created were self-signed, this mean that no CA has checked them. Although they are free, they should never be trusted.

Also, the management of the certificates is not easy: the administrators should make sure that none of the certificate are copied onto another machine. Another example is that if a computer is stolen, the administrator have to cancel the validity of the certificate within the stolen machine. This will result by cancellation costs or buying a new certificate.

7.1.c Efficiency and scalability

Implementing a SSL VPN, using point-to-point connections, has another inconvenient: all the clients are attached to the server. The VPN server acts like a gateway: all the clients must authenticate on it before been able to access to the resources.

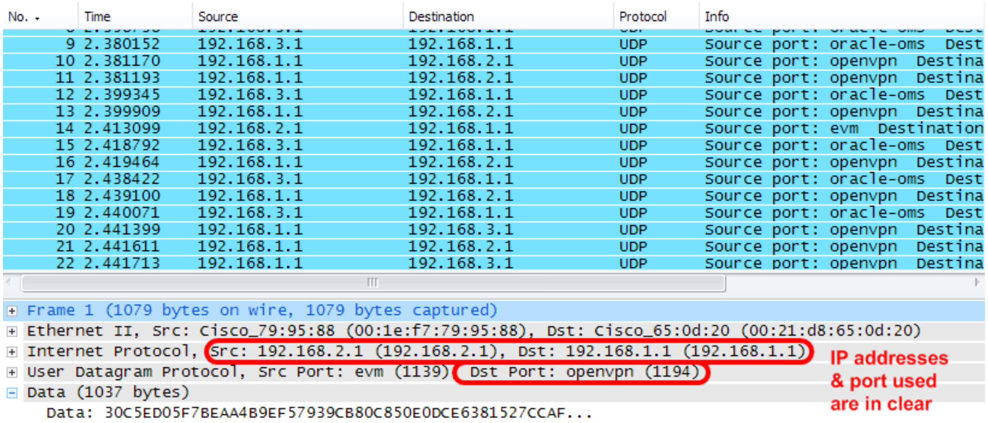
This mean that the server is a centralised resource. The can be a weakness, in the case where the server is attacked or crashes. This can be avoided by using many servers (location transparency thanks to a proxy or DNS) but this is another complex implementation to add to the network.

However, there is a possibility to create direct clients-to-clients tunnels: each client should be also a server. This means more certificates, more complex configurations of the computers.

This cannot be a solution as any modification extension of the network topology will result to a re-configuration of all the nodes. This is problem of scalability transparency.

7.1.d Transparency

As the SSL tunnel encrypts only the payload, the IP addresses from the end-users are not encapsulate within the encryption. A capture realised from Internet network prove that it is possible to see the end-users IP addresses:



```
No. -   Time        Source          Destination     Protocol  Info
   9 2.380152    192.168.3.1     192.168.1.1     UDP       Source port: oracle-oms  Dest
  10 2.381170    192.168.1.1     192.168.2.1     UDP       Source port: openvpn  Destina
  11 2.381193    192.168.1.1     192.168.2.1     UDP       Source port: openvpn  Destina
  12 2.399345    192.168.3.1     192.168.1.1     UDP       Source port: oracle-oms  Dest
  13 2.399909    192.168.1.1     192.168.2.1     UDP       Source port: openvpn  Destina
  14 2.413099    192.168.2.1     192.168.1.1     UDP       Source port: evm  Destination
  15 2.418792    192.168.3.1     192.168.1.1     UDP       Source port: oracle-oms  Dest
  16 2.419464    192.168.1.1     192.168.2.1     UDP       Source port: openvpn  Destina
  17 2.438422    192.168.3.1     192.168.1.1     UDP       Source port: oracle-oms  Dest
  18 2.439100    192.168.1.1     192.168.2.1     UDP       Source port: openvpn  Destina
  19 2.440071    192.168.3.1     192.168.1.1     UDP       Source port: oracle-oms  Dest
  20 2.441399    192.168.1.1     192.168.3.1     UDP       Source port: openvpn  Destina
  21 2.441611    192.168.1.1     192.168.2.1     UDP       Source port: openvpn  Destina
  22 2.441713    192.168.1.1     192.168.3.1     UDP       Source port: openvpn  Destina

+ Frame 1 (1079 bytes on wire, 1079 bytes captured)
+ Ethernet II, Src: Cisco_79:95:88 (00:1e:f7:79:95:88), Dst: Cisco_65:0d:20 (00:21:d8:65:0d:20)
+ Internet Protocol, Src: 192.168.2.1 (192.168.2.1), Dst: 192.168.1.1 (192.168.1.1)
+ User Datagram Protocol, Src Port: evm (1139), Dst Port: openvpn (1194)
- Data (1037 bytes)
    Data: 30C5ED05F7BEAA4B9EF57939CB80C850E0DCE6381527CCAF...
```

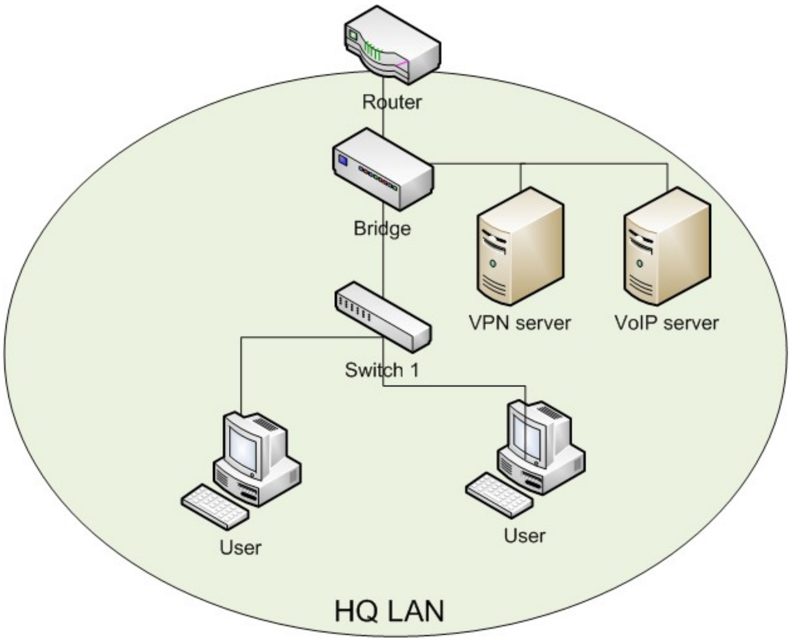
IP addresses & port used are in clear

This can be a lack of security: if an attacker knows where is located a server (thanks to its IP address) then the server can be subject to Deny of Service attack, or signalling manipulation (if the VPN server is the same machine as the VoIP server).

7.1.e Topology

The location of the server within the network is an essential point: all the traffic from the clients will go through the server (even client-to-client traffic). The server can be overloaded (voice over IP takes a lot of resources on the bandwidth) and the traffic generated by the client connection within the VPN server can affect the other traffic. This can result of a bottleneck for the whole network traffic within the LAN where the VPN server is located.

This is why the server should be placed or on a dedicated port or the router, or within a separate LAN:



To avoid bandwidth overload within the HQ LAN, the servers are in a separate network segment. This can be made physically (different interface, different IP pool) or by using VLAN (Virtual Local Area Network). In both case the collision domain are different, so the traffic should not affect the one in other segments.

7.2 IPSEC tunnelling evaluation

The implementation of IPSEC tunnels has been realised more easily than the SSL one: the only devices that had to be configured were the routers, and in a more complex network topology, it would have been only the router directly connected to Internet.

The simplicity of setting up the tunnels is an advantage, but it could be more complex in the case of lot of different distant LANs.

7.2.a Devices configuration

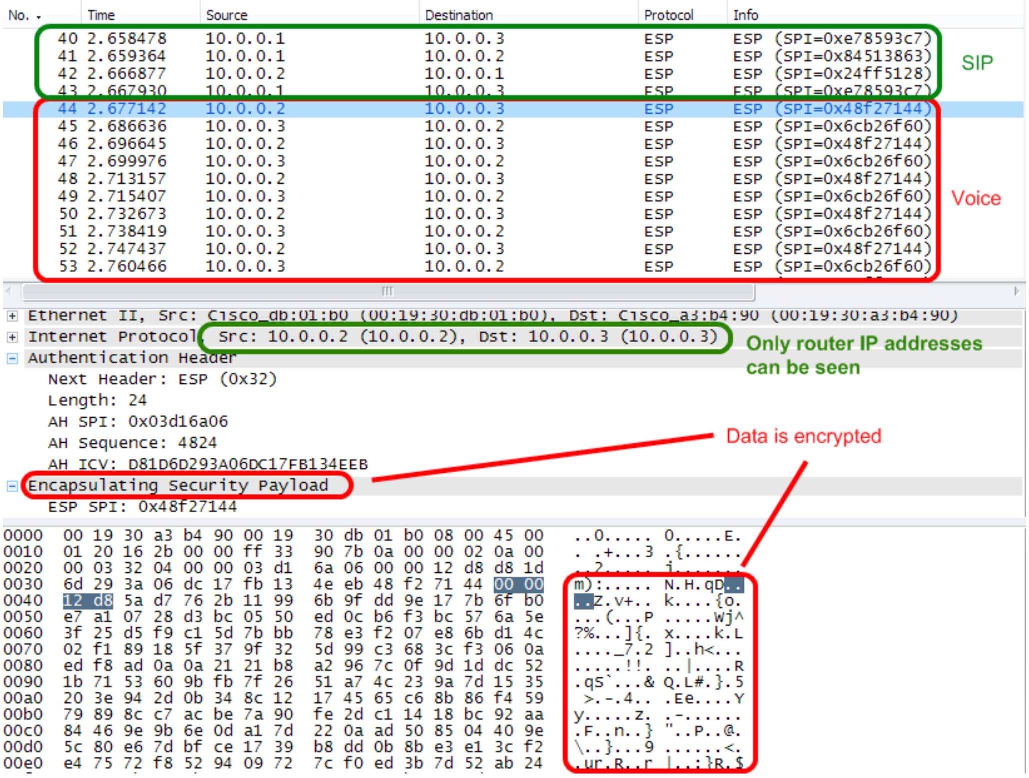
Not all the network devices can deal with IPSEC framework: however, CISCO devices (up to date) manage this well, and no upgrade is needed as the protocols used to create the tunnels are well standardised. However, if the devices are from different constructor (e.g. 3COM, NETGEAR...) the administrator should make sure that the protocols used are compatibles (both end implement them).

7.2.b Transparency

As presented in the implementation chapter, the clients are not aware of the tunnel: they can register to the VoIP server without any change about the configuration (the proxy address is still the VoIP server physical IP address).

This present an important advantage, as the clients can be contacted by they physical IP address (which usually is defined by a static configuration). In the case of calls made from or to another network that the company one, the client will be reachable.

Also, the encrypted packets between the routers encapsulate the IP addresses: the nodes within the LANs are not visible from Internet, as only router IP addresses are used for the transmission.



```
No.   Time       Source        Destination    Protocol  Info
   40 2.658478   10.0.0.1      10.0.0.3       ESP       ESP (SPI=0xe78593c7)
   41 2.659364   10.0.0.1      10.0.0.2       ESP       ESP (SPI=0x84513863)
   42 2.666877   10.0.0.2      10.0.0.1       ESP       ESP (SPI=0x24ff5128)
   43 2.667930   10.0.0.1      10.0.0.3       ESP       ESP (SPI=0xe78593c7)
   44 2.677142   10.0.0.2      10.0.0.3       ESP       ESP (SPI=0x48f27144)
   45 2.686636   10.0.0.3      10.0.0.2       ESP       ESP (SPI=0x6cb26f60)
   46 2.696645   10.0.0.2      10.0.0.3       ESP       ESP (SPI=0x48f27144)
   47 2.699976   10.0.0.3      10.0.0.2       ESP       ESP (SPI=0x6cb26f60)
   48 2.713157   10.0.0.2      10.0.0.3       ESP       ESP (SPI=0x48f27144)
   49 2.715407   10.0.0.3      10.0.0.2       ESP       ESP (SPI=0x6cb26f60)
   50 2.732673   10.0.0.2      10.0.0.3       ESP       ESP (SPI=0x48f27144)
   51 2.738419   10.0.0.3      10.0.0.2       ESP       ESP (SPI=0x6cb26f60)
   52 2.747437   10.0.0.2      10.0.0.3       ESP       ESP (SPI=0x48f27144)
   53 2.760466   10.0.0.3      10.0.0.2       ESP       ESP (SPI=0x6cb26f60)

+ Ethernet II, Src: Cisco_db:01:b0 (00:19:30:db:01:b0), Dst: Cisco_a3:b4:90 (00:19:30:a3:b4:90)
+ Internet Protocol, Src: 10.0.0.2 (10.0.0.2), Dst: 10.0.0.3 (10.0.0.3)
- Authentication Header
    Next Header: ESP (0x32)
    Length: 24
    AH SPI: 0x03d16a06
    AH Sequence: 4824
    AH ICV: D81D6D293A06DC17FB134EEB
- Encapsulating Security Payload
    ESP SPI: 0x48f27144

0000  00 19 30 a3 b4 90 00 19  30 db 01 b0 08 00 45 00   ..0..... 0.....E.
0010  01 20 16 2b 00 00 ff 33  90 7b 0a 00 00 02 0a 00   . .+...3 .{......
0020  00 03 32 04 00 00 03 d1  6a 06 00 00 12 d8 d8 1d   ..2..... j.......
0030  6d 29 3a 06 dc 17 fb 13  4e eb 48 f2 71 44 00 00   m):..... N.H.qD..
0040  12 d8 5a d7 76 2b 11 99  6b 9f dd 9e 17 7b 6f b0   ..Z.v+.. k....{o.
0050  e7 a1 07 28 d3 bc 05 50  ed 0c b6 f3 bc 57 6a 5e   ...(...P .....Wj^
0060  3f 25 d5 f9 c1 5d 7b bb  78 e3 f2 07 e8 6b d1 4c   ?%...]{. x....k.L
0070  02 f1 89 18 5f 37 9f 32  5d 99 c3 68 3c f3 06 0a   ...._7.2 ]..h<...
0080  ed f8 ad 0a 0a 21 21 b8  a2 96 7c 0f 9d 1d dc 52   .....!!. ..|....R
0090  1b 71 53 60 9b fb 7f 26  51 a7 4c 23 9a 7d 15 35   .qS`...& Q.L#.}.5
00a0  20 3e 94 2d 0b 34 8c 12  17 45 65 c6 8b 86 f4 59    >.-.4.. .Ee....Y
00b0  79 89 8c c7 ac be 7a 90  fe 2d c1 14 18 bc 92 aa   y.....z. .-......
00c0  84 46 9e 9b 6e 0d a1 7d  22 0a ad 50 85 04 40 9e   .F..n..} "..P..@.
00d0  5c 80 e6 7d bf ce 17 39  b8 dd 0b 8b e3 e1 3c f2   \..}...9 ......<.
00e0  e4 75 72 f8 52 94 09 72  7c f0 ed 3b 7d 52 ab 24   .ur.R..r |..;}R.$
```

The illustration presents a capture realised within the Internet network, in promiscuous mode: all the traffic is captured. The capture has been realised during a call establishing: the user from LAN 1 (behind 10.0.0.2 router) called User from LAN2 (behind 10.0.0.3 router).

They are two distinct traffic: the signalisation (first part, underlined in green), which goes from the VoIP server LAN (10.0.0.1) to the clients LAN (10.0.0.1 and 10.0.0.3 routers) and the voice channel (once the called user picked up).

Both of the channels are encrypted with IPSEC tunnel. And none of the clients IP addresses are visible from Internet.

The fact that local IP addresses are not visible is an advantage, this allow to “hide” the network, any user onto Internet cannot see where are the servers.

7.2.c Scalability

The use of IPSEC tunnels in transport mode (between routers) is used the secured links between known networks. If the links between all routers which belong to the company implement secure tunnels, then the defaults routes will carry the channels, using encryption:

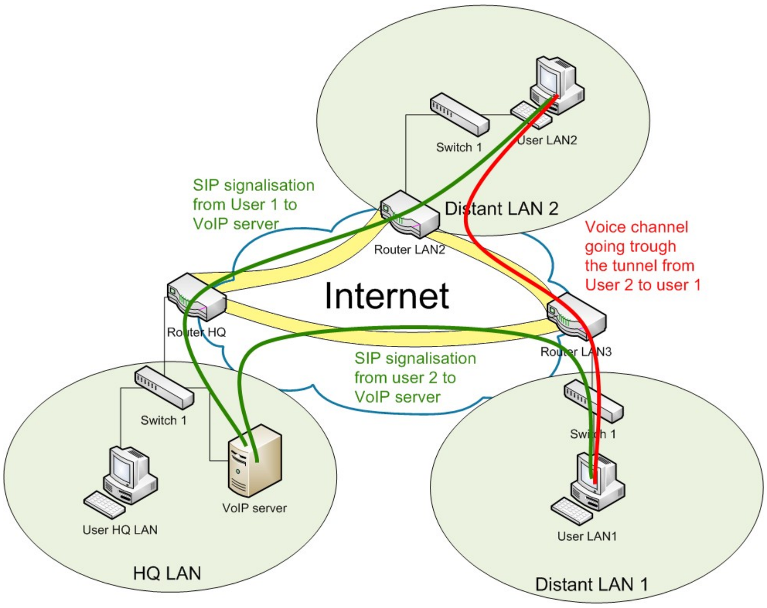

Switch 1
User LAN2
SIP signalisation from User 1 to VoIP server
Distant LAN 2
Router LAN2
Voice channel going trough the tunnel from User 2 to user 1
Internet
Router HQ
Router LAN3
SIP signalisation from user 2 to VoIP server
Switch 1
Switch 1
VoIP server
User HQ LAN
HQ LAN
User LAN1
Distant LAN 1

Illustration 29: IPSEC routes for signalisation and voice

The illustration shows that both signalisation and voice channels are encrypted, using different tunnels: this is the same topology as if there were no tunnels.

With more LANs, the routers should implement N-1 tunnels (where N is the number of LANs).

For any modification of the global topology (addition or removal of a LAN), all the routers should be reconfigured (add or remove a tunnel). This can be a lack of scalability, but it is usually rare that a whole distant LAN is added or removed (e.g. expansion of the company on another campus).

The configurations of the routers can be easily managed remotely (e.g. SSH remote access) as the administrators usually use CLI (Command Line Interface). CISCO propose also some solutions to manage configuration (edition, backup...) using a more user-friendly software (like CISCO Network Assistant).

We can consider that the scalability of the solution is good.

Summary

The evaluation allowed to bring in light the main technical issues encountered in the implementation. The application of different tunnels technologies applied to the same scenario has proven the differences between a SSL implementation and IPSEC.

The use of two different channels by VoIP make the implementation of tunnelling more complex, especially within an scalability and optimisation.

The scalability is limited in the case of the need of a centralised resource, like VPN server. All the traffic should go through the server, creating a bottleneck. The use of IPSEC site-to-site tunnelling allowed to mitigate a part of this issue, but not in the extend of a single node. Also, the costs in bandwidth should be considerer by using a centralised resource.

Regarding the security issues, the captures of traffic allowed to show that there is not any unencrypted channel across Internet structure. Both channel are fully secured thanks to the encryption. The solutions presented allowed the mitigation of the main VoIP security issues presented in the literature review.

One issue has not been presented: Quality of Service and delays for encryption. As VoIP is a real-time application, it can suffer about time-delays, in example, if a link is overloaded. QoS is a complex mechanism which should be presented in a dedicated study.

Also, the time taken to encrypt and decrypt the packets can act on time-delay. An detailed analyse could perform the tests about the time taken to elaborate the tunnel, encrypt the data and the bandwidth impact.

To finish this study, a conclusion will present in what extend the study has met the requirements.

8 CONCLUSION

The carried work in respect of the study has been presented in this report. The aspects of security issue and their mitigation has been introduced, detailed and tested.

VoIP architectures are vulnerable to attacks against the signalisation, while voice suffers of poor privacy. Both of the channels security pitfalls show the necessity of security guidelines.

It has been demonstrated that tunnelling provide efficient security, thanks to the use of encrypted tunnels. Both technologies have been tested in the scope of the study: evaluate the mitigation solution in respect with voice over IP. The main points have been underlined: despite of an efficient security, the scalability is the main issue. It has been shown that SSL is more concerned about this problem.

However IPSEC allow a better scalability, easier configuration and reduced price. It seems to be more adapted to the reassurance of VoIP structure, in the limit where mobiles clients are a few.

In a global scope, the lack of scalability and flexibility of tunnels is a problem with the use of signalling protocols, foe example SIP, which is in opposition to tunnels: simple and flexible. Tunnels can be deployed within a SIP architecture in a easier way than H.323, as a single server can act as all the elements (Asterisk acted as gateway, gatekeeper and registrar server).

Indeed SIP needs a much simpler topology and range of devices.

Moreover, an aspect has not been aborted within the study. As VoIP is a real-time application, it need to use Quality of Service to allow reliable liaisons. However, QoS cannot be implemented by using tunnels. This can be an important issue, and some further work can be done in order to create tunnel dedicated to voice channel. This tunnel could be specified within the QoS configuration.

To conclude the study, the implementation of tunnels to secure voice over IP structure can be adapted, but present problems. This solution is reliable and low-cost, in the extend where there is no need to create new protocols and end-points hardware do not have to implement any authentication and encryption algorithms. However tunnels can be difficult to implement within complex structures. As a long-term solution, the constraints engendered tunnels should motivate the industry to create new solutions, more adapted to voice over IP.

The report meet the initial objectives, by informing the audience about the security issues with respect of voice over IP, the mitigation solution and their majors problems. A description of a possible further work will be detailed to inform the audience how these problems can be resolved.

Personal statement

The research performed for the requirements of the study allowed to author acquire some knowledge about technologies which has never been aborted before. Voice over IP technologies and encryption tunnelling were some notions very global, and the study presented allowed the author to bring an important piece of work.

The progress of the project, during eight months, was in accordance with the plan (see the gant chart in appendices) defined during the first weeks. The documentation about Security issues was difficult to retrieve as they are not well documented yet. The design has been validated by the project supervisor, and the implementation performed in time.

The management of such a project allowed the author to get more confidence about making a research, writing a report in a formal way.

Further work

To finish the conclusion, the study can be expanded to further work to counter in problems raised by the presented work. The main issues encountered by using tunnels (lack of scalability, non support of Quality of service) should motivate the signalisation and voice protocol to evolute to some security implementation. SIP should implement an stronger authentication procedure, and voice should be encrypted from point to points.

To adapt SIP to SSL VPN, some modifications within SIP headers could be modified, to allow the routing of voice outside the tunnel. This would solve the problem of performance, as all the traffic goes through the VPN server in SSL implementation.

9 APPENDICES

9.1 References

Teare, D.(2006). *Designing Cisco Networks*. Indianapolis: Cisco Press, July 1999

Edelson, E.(2005). Voice over IP: security pitfalls. *Network security*. Retrieved November 2008 from Science-Direct database.

Trussell B. (2007, February 25). *How Popular Can Wireless Networking Really Get?*. Retrieved November 12, 2008 from http://www.pewinternet.org/PPF/r/203/report_display.asp

Telecommunication Standardization Sector of ITU (June 2006). *H.323 recommendation*. Retrieved October 29, 2008 from http://www.itu.int/rec/T-REC-H.323-200606-I/en

IETF, The Internet Engineering Task Force (June 200).*SIP reference.* Retrieved October 2008, from http://www.ietf.org/rfc/rfc3261.txt

VOIP and VPN, December 2008, Retrieved February 2009, from http://www.voip-info.org/wiki/view/VOIP+and+VPN

Meggelen J.V., Madsen L. & Smith J. (2007). *Asterisk ™: The Future of Telephony (2nd edition)*. USA: O'Reilly (available on-line from http://my.safaribooksonline.com/9780596510480).

SysAdmin Audit Network Security, January 2007, *Top-20 2007 Security Risks*. Retrieved November 12, 2008 from www.sans.com/top20

Geneiatakis, C. Lambrinoudakis & G. Kambourakis, A. (2008). An ontology-based policy for deploying security SIP-based VoIP services. *Computers & security*, 27(1), 285–297. Retrieved December 22, 2008 from Science-Direct database.

M. Benini & S. Sicari (2008). Assessing the risk of intercepting VoIP calls. Retrieved November 2008 from Science-Direct database.

Bradbury, D. (2008). Network security. *Network reconnaissance*, 2008. Retrieved November 12, 2008 from Science-Direct database.

Endler & Collier (2006) Hacking Exposed VoIP: Voice Over IP Security Secrets & Solutions. *Chapter 3: enumerating a VoIP network.* Retrieved November, 2008, from http://www.hackingexposedvoip.com

Sonja Ryst, July 2006 http://www.businessweek.com/technology/content/jul2006/tc20060710_811021.htm

Lewis, 2006. Comparing, Designing, and Deploying VPNs (Networking Technology) CISCO Press

W. Bou Diab, S. Tohme & C. Bassil (2007). Critical VPN Security Analysis and New Approach for Securing VoIP Communications over VPN Networks. Retrieved February 2009, from ACM Portal database.

B. Swardz, 2004, Asterisk open-source PBX system, *Linux Journal*, Volume 2004 Issue 118. Specialized Systems Consultants, Inc.

9.2 Configuration files

This part contains the main configuration files used for the implementation of the work.

Asterisk SIP configuration (*sip.conf*):

```
[general]
context=default          ; Default context for incoming calls
allowoverlap=no          ; Disable overlap dialing support. (Default is yes)
bindport=5060            ; UDP Port to bind to (SIP standard port is 5060)
                         ; bindport is the local UDP port that Asterisk will
                         ; listen on
bindaddr=0.0.0.0         ; IP address to bind to (0.0.0.0 binds to all)
srvlookup=yes            ; Enable DNS SRV lookups on outbound calls
                         ; Note: Asterisk only uses the first host in SRV records
                         ; Disabling DNS SRV lookups disables the
                         ; ability to place SIP calls based on domain
                         ; names to some other SIP users on the Internet
domain=test.com

[1000]
type=friend
context=phones
host=dynamic

[2000]
type=friend
context=phones
host=dynamic

[2000]
type=friend
context=phones
host=dynamic
```

Asterisk dial plan (*extensions.conf*):

```
[default]
exten => s,1,Verbose(1|Unrouted call handler)
exten => s,n,Answer()
exten => s,n,Wait(1)
exten => s,n,Playback(tt-weasels)
exten => s,n,Hangup()

[internal]
exten => 1000,1,Dial(SIP/1000)
exten => 2000,1,Dial(SIP/2000)

[phones]
include => internal
```

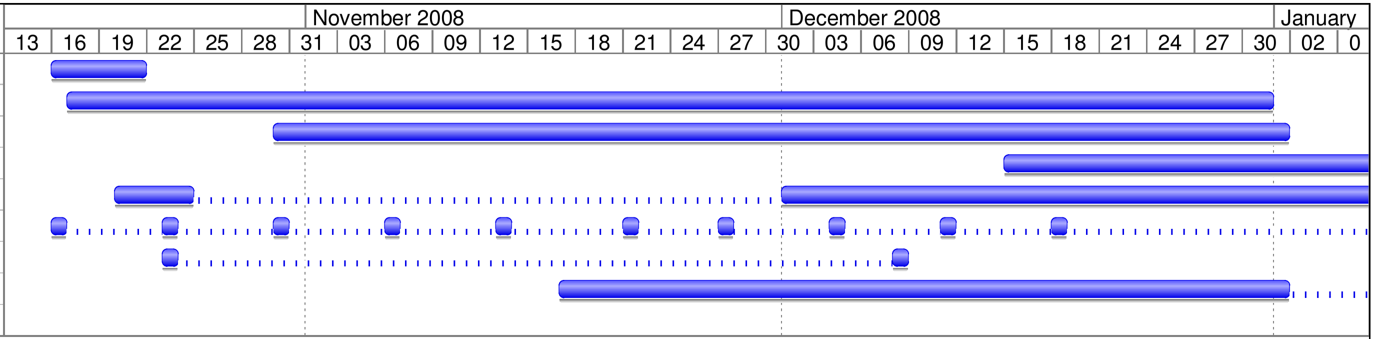
OpenVPN server configuration file (*server.conf*):

```
# Which local IP address should OpenVPN
# listen on? (optional)
local 192.168.1.1

# Which TCP/UDP port should OpenVPN listen on?
port 1194

# TCP or UDP server?
proto udp

#Device : tunnel
dev tun

# SSL/TLS root certificate (ca), certificate
# (cert), and private key (key).
ca ca.crt
cert Asterisk.crt
key Asterisk.key

# This file should be kept secret
# Diffie hellman parameters.
dh dh1024.pem

# Configure server mode and supply a VPN subnet for OpenVPN to draw client addresses from.
server 10.8.0.0 255.255.0.0

# Push routes to the client to allow it to reach other private subnets behind the server.
push "route 192.168.2.0 255.255.255.0"
push "route 192.168.3.0 255.255.255.0"

# Uncomment this directive to allow different
# clients to be able to "see" each other.
client-to-client

# Uncomment this directive if multiple clients might connect with the same certificate/key
# files or common names.  This is recommended only for testing purposes.  For production use,
# each client should have its own certificate/key pair.
duplicate-cn

keepalive 100 200

# Enable compression on the VPN link.
;comp-lzo
# The persist options will try to avoid accessing certain resources on restart
# that may no longer be accessible because of the privilege downgrade.
Persist-key
persist-tun

# Output a short status file
status openvpn-status.log

# Set the appropriate level of log file verbosity.
Verb 3
```

9.3 Gantt chart

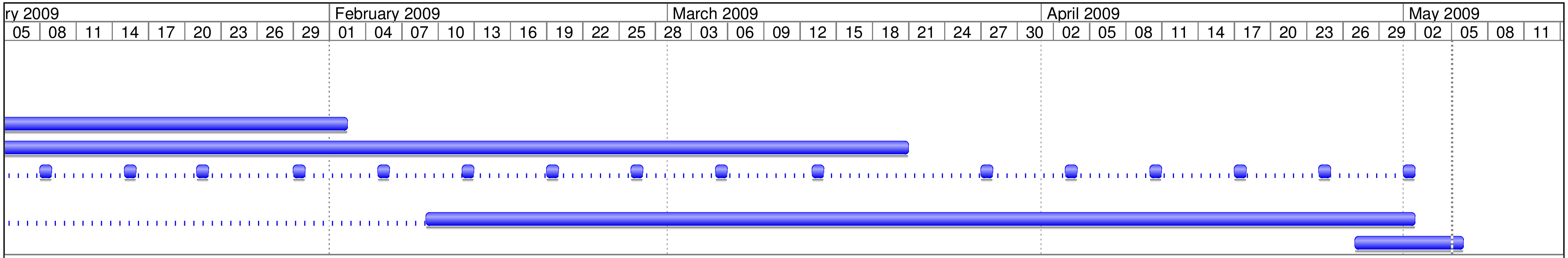
The Gantt Chart has been established at the beginning of the study: it allowed the author to manage their time to finish the project in time.

ID	Task Name	Duration	Start	Finish
1	Project planning	4 days	Thu 16/10/08	Tue 21/10/08
2	Research	54 days	Fri 17/10/08	Wed 31/12/08
3	Analysis	46 days	Thu 30/10/08	Thu 01/01/09
4	Design	36,5 days	Mon 15/12/08	Mon 02/02/09
5	Implementation	86 days	Mon 20/10/08	Fri 20/03/09
6	Meetings with supe	26 days	Thu 16/10/08	Fri 01/05/09
7	Meetings second r	2 days?	Thu 23/10/08	Mon 08/12/08
8	Report writing	94 days	Mon 17/11/08	Fri 01/05/09
9	Poster	7 days?	Mon 27/04/09	Tue 05/05/09



Project: HONOURS
Date: Tue 05/05/09

Task	▬	Milestone	◆	External Tasks	▬
Split	┄	Summary	▬	External Milestone	◇
Progress	▬	Project Summary	▬	Deadline	⇩



Project: HONOURS
Date: Tue 05/05/09

Task		Milestone	◆	External Tasks	
Split		Summary		External Milestone	◇
Progress		Project Summary		Deadline	⇩

9.4 Project diary

The following pages content the weekly sheets completed both by the student and the supervisor.