Summary

We have chosen to look closer at the area of security for electronic invoices. The purpose of this inquest is to provide our case study with a security analysis of three suggestions and a recommendation of the best solution, according to our test.
This inquiry is targeted towards potential users of electronic invoices, or anyone interested in information about sending invoices electronically.

Our hypothesis is:
To reach an improved security level of the current system, one of the alternatives can be applied.

1. Mail server
2. An ISDN channel via a third party
3. X.25 via Internet bank.

The main problem in the current systems is that the invoice is delivered manually by e-mail. To improve the security level we use Stallings, 2000 security services and X's security policy to test our three alternatives and reach a recommendation. Through literature studies, interviews and the test we have come to the conclusion that the X.25 solution has best fulfilled the security services.

INDEX

Introduction

Trading with goods and services is something that has always existed but in the last years a new trend has come and changed the way of trading. The fact that many companies now use the Internet have led to that new aids have been developed to simplify the trade called electronic commerce. Electronic commerce is defined as “Electronic commerce is any form of business or administrative transaction, or information exchange that is executed using any information and communication technology”(Fredholm, 2000).
An important issue when it comes to electronic commerce is security in other words a company’s possible loss of information and the fact that the customer must feel secure when using systems within the area of electronic commerce.

The rapid development of electronic commerce has made it a competitive tool for businesses. “The fact that many companies now use the Internet has put them in a very favourable position on the market” (Kotler,1998). With the latest information technology businesses’ information can be available to customers and co-operators all over the world at any time. Electronic commerce is not only a competitive advantage but also an effective communication tool, which decreases companies’ expenditure on paper, man craft and stock.

The company in our case study is in this report referred to as X, has a strong market position and a large clientele and therefore we were interested in analysing and improving X’s electronic invoice system. X was in the position of testing an electronic invoicing system towards a selective group of business customers. The major problem with the system was the security issue regarding transferring the file.

Limitation

We include a case study in our investigation of the company X. We have chosen to look at security issues regarding X’s current invoice system targeting its business customers.

We will look at security issues, from the development of the invoice until it reaches the specified customer in other words point-to-point security, and the base protocols that is used and required at X for transmitting files to day. The report will give three suggestions of possible solutions to increase the security level of the system based on X's existing systems in order to make it applicable. The result of the report will contain a final recommendation.

Purpose

Our purpose with this investigation is to provide X with a security analysis of the three suggestions and a recommendation of the best solution, according to our test.

Target group

This report addresses businesses, organisations and institutions that are using electronic invoices. The thesis is also directed to potential users of electronic invoices, or anyone interested in information about sending invoices electronically.

Hypothesis

To reach an improved security level of the current system, one of the alternatives can be applied.

1. Mail server
2. An ISDN channel via a third party
3. X.25 via Internet bank.

Method

Our choice of subject and case study

We started to discuss our mutual interest in the subject electronic commerce and decided to support our thesis with a case study at a company. We took contact with the company X, with a request to accomplish our thesis within the subject of electronic commerce with X as a case study.

X had come to a point where they needed a decision ground for a future manufacturing system. We agreed to focus on the security issue within electronic payment system for X's SME customers (Appendix 15) and provide the company with a proposal of a system with an enhanced security level than the one used today.

To reach a conclusion for the final recommendation, we have chosen to focus on six criteria named security services (see chapter Security Services) which are based on theories from relevant literature. We have chosen these security services as they profound the basic requirement to meet X's security policy, (Appendix 14) and the basic requirements of secure electronic commerce, (Elektroniska Affärer, 2000) which also are included in Stallings, 2000 definition of security services.

The different system solutions will be tested according to the security services in order to find out if our solutions fulfil these requirements. The three solutions shall then be mutually compared and our recommendation is based on the system that provides the best security services. We will draw our conclusion from technical facts gained by literature studies, interviews and knowledge acquired from the courses Local Area Networks, DVC 006, and Network Security, DVC 007 at The Technical Institute of Blekinge 2002.

Choice of Scientific Method

We will use a deductive way in our study since we base our theory on collected information and prove certain variables through scientific literature, interviews and our case study. Our research approach has its anchor in the positivism since we study the reality in a logic and analytic way through a hypothetical-deductive empirical measurement.

Collection of information

This chapter provides the reader with information about how our information was collected.

- Literature studies

- Searching the Web for research reports and scientific articles
- Collecting information from our contact persons at X.
- Interviews with persons from the academic world, users of electronic billing systems and vendors of solutions for electronic systems.
- From studying X's current invoice system and technical documentation

We have studied literature in order to get reliable information from persons with long experience within the subject academically and professionally. The Web was used to find research reports of scientific value for our theories. Articles gave us information about current projects and discussions from the business and research world. Information from X was gathered so we could evaluate the dimension and angle from which we should approach the subject. Vendors and companies in the telecom business gave us their view of electronic invoice systems and security.

We decided to work with our interviews in a qualitative way since they profound a great part of our conclusion. Interviews were made by mail and in some cases we had the opportunity to interview face to face. The questions started in a wide perspective and closed up the subject further on. Some important questions about Internet, ISDN, X.25, human interaction and security served as standards. Related questions followed through the interview according to the person's special knowledge.

After each interview or received mail we analysed the answers and our notes and wrote down a conclusion. This material was constantly used in our discussions.

Reading directions

We recommend this report to be read in the following way. The part called literature provides the reader with the knowledge of the subject and gives a clear picture of the authors view of security within the limited area of this report.

We have chosen to place the literature that commonly treats Internet and security prior to the different suggestions for improved security. The literature that is directly connected to each proposal is placed where we describe the different security solutions.

Literature Study

Accomplishment

Search methods

First of all we have to find all the literature and texts we need to get the overview of the subject we have chosen. The search words we have agreed to use as a beginning are "*electronic commerce*", "*electronic invoicing*", *"information security"* and *"communication network"*, plus a few random other words. From the variation of search words we hope to get a various selection of documents for further selection. We will also borrow books about the subject from the library, and in those books we will mainly look for any chapters or paragraphs containing anything about invoices sent electronically. We shall also interview distributors of electronic invoice systems to get a clear picture of the requirements for secure invoice systems.

Background

Definition of internet security

(Network Security Essentials, 2000)

The expression security exists at many levels when it comes to shared systems and information. In order to compare our three solutions for a secure file transfer we base the comparison upon internet security. We refer to the term internet with a lowercase "i" stated as follows by Stalling, 2000 "to refer to any interconnected collection of network. A corporate intranet is an example of an internet. The Internet with a capital "I" may be one of the facilities used by an organisation to construct its internet".

Internet security with a lowercase "i" captures both Internet security and security in interconnected networks. According to Stallings, 2000a the boundaries between network

security and internet security is not always clear since a network may consist of different computer equipment inter connected in a network in order to transfer data.

The required level of security

On the basis of the information we have obtained by literature studies and the knowledge acquired through security course we have been able to define security. Borgström and Lindborg states "The level of security is always individual." (Borgström, Lindborg, 1992) By security we intend that the invoice should be transferred from X to the customer without unauthorised people easily taking part of or changing the information in the invoice.

It is not only the information itself that is sensitive; also where the information is forwarded to has to be protected. Another part that is sensitive is how much and how frequent the information is sent. Information has to be secured so that the credibility and quality is intact. The security required by the transfer of the information on the electronic invoice comes within the scope of X's security policy (Appendix 14), which we by security reasons cannot fully publish in our thesis.

Security, definition and reason

(The A to Z, And its role in E-commerce, 1998)
(Firewalls and Internet Security, 1994)

Almost all information today is stored on computers, which has to be protected in the same way as normally, kept in book files and papers. The level of security is set differently regarding to the sensitivity within different areas. This leaves us with the conclusion that security is about not letting anyone perform any form of action not wanted on your computer system, Internet connections or peripheral devices. The purpose of security is "Computer security is not a goal, it is a means toward a goal: information security" (Cheswick, Bellovin, 1994).

It has to be kept in mind that a very high security level can also hurt a company if it interferes with its functionality. It is important to keep good balance between security and possible threats. Security is also an economical matter as it may be very expensive to

fulfil each and every possible security leak. A good security policy is very important where priority is put on different systems and on actions if an incident would occur.

Loss of information can in most companies lead to a great loss of money, and this fact makes most companies put a lot of investment in security. Spreading, modifying or deleting information may be devastating to an organisation or company and may lead to bankruptcy.

Security Services
(Network Security Essentials, 2000)
(Data Kommunikation, 2000)
(Internet and Intranet security, 1998)
(Elektroniska affärer, 2000)
(http://www.ncsa.uiuc.edu/)

A security service provides the functions normally associated with information security in an ordinary communication line like the Post Office. When sending a document by mail, certain security aspects are covered by a time stamp, a senders signature or that an envelope reaches its destination unopened. All these functions in a traditionally information transmission are therefore also important within electronic commerce.

According to Stallings, a security service is "A service that enhances the security of the data processing systems and the information transfers of an organisation." (Stallings, 2000a). Turban et al. 2000 set focus on the importance of security services when it comes to the customer acceptance and implementation of electronic commerce.

Turban et al. continues by explaining that a partnership within electronic commerce is based on security and that it is such an important issue that National Computational Science Alliance (Appendix 17) has made an identification of four cornerstones for secure electronic commerce. These cornerstones are all part of the functions called security services we refer to in the literature.

From several literature studies within the context of security services the following chapter concentrates on six of them because they are all subjects for the intention of

preventing a security attack (see chapter Security assaults). We consider the following security services necessary and adequate since they represent basic requirements for a systems security and according to XX (Department of Security, X) fulfils X's requirements for information security defined in the company's security policy (Appendix 14). XX also explains that all these security services are important especially within the transmission of an invoice over a communication network.

Classification of security services

Confidentiality

Confidentiality protects transmitted data from passive attacks like eavesdropping (see chapter encryption) when data is transmitted in a network. The protection level serves from all transferred data to a single message or a specific field in a message. Encryption stands for the most secure way to protect data and provides different solutions (see chapter encryption).

Equally important as protection of the data, is that the sender and receiver are invisible for someone analysing the traffic. This is a serious problem since companies today send very sensitive and value added information over communication networks. It will be devastating in a competitive perspective if the business' information ends up in the wrong hands.

Integrity

Integrity means that data reaches its destination without unauthorised destruction or modification. Modification includes duplication, reordering, insertion or replays (see replay attack). Integrity may also have a recovery function included, which we will not consider an aspect in our test. Integrity protection is not only needed against active attacks but also against a modification caused by accident.

If a message with important customer or business information is modified or destroyed the consequences may put both parts involved in a very difficult position. Legal aspects

may be involved and without any encryption function it can be very hard to prove if the message has been altered.

Authentication

Authentication ensures that the communication between to parts is authentic, the sender is the actual sender claimed in the message. It is most likely that a potential customer or business partner needs to feel secure enough to enter electronic commerce based on the authentication process. Authentication goes both ways since the sender needs to know the authentication of the destination to transmit data in a secure way.

To protect data from a masquerade or man in the middle attack (see chapter Encryption) a digital signature (see chapter Encryption) can be used. Authentication prerequisite for access control and is therefore of major importance as it serves for access control of a message or the whole system. To prevent modification it is not possible for authentication to stand alone as a service but has to be used in conjunction with a data integrity service.

Access Control

Closely tied to authentication, access control prevents any unauthorised part of using a system's resources. An unauthorised part can gain access to the system from a network device (Glossary), an application or from the network connection. Therefore access control is one of the most basic security services in a network, as Oppliger explains "In general, access control services are the most commonly thought of services in both computer and communication security." (Oppliger, 1998). If a system does not provide a required level of access control it may lead to both active and passive attacks (see chapter Encryption).

Non-repudiation

Non-repudiation is the procedure in which both parties (sender and receiver) acknowledge the transfer of data. The goal of non-repudiation is to prove that a message has been sent and received. In general, non-repudiation is the ability to ensure that a party

cannot deny the authenticity of their signature on a document or the sending of a message that they originated. Non-repudiation becomes particularly important in electronic commerce as it in a twist may serve legal consequences.

Availability

Systems availability is measured in terms of hardware and software problems. If there is an attack on, or an accident causing disruption in the availability it can make both the system and the data unavailable for the user. Some of these attacks are responsible for countermeasures such as authentication and encryption. Other requires more drastic measures where physical actions are enforced like setting up a new communication line if it is cut of.

We have chosen to present three different ways of transferring files electronically, virtual connection, dial-up connection and permanent connection. In the following paragraphs we intend to present background information about the different connections mentioned above. Since the mail server solution is based on transferring the invoice via e-mail over Internet a description of Internet and e-mail is required.

Internet
(Nätverk från grunden, 1998)
(Local and Metropolitan Area Networks, 2000)

Internet is a network of networks, in other word a combination of WANs and LANs. Internet was in the beginning developed by Defense Advanced Research Projects Agency (DARPA). Today the Internet is used all over the world not only by academics but also by individuals and companies to communicate and as market channels.
Services that can be made over the Internet are:

- Send electronic mail to all over the world.
- Transfer documents and files to and from computers connected to the Internet.
- Search and get information from public databases.
- Read and write in newsgroups
- Pay bills.
- Listen to the radio and look at multimedia clips.
- Billing systems.

E-mail
(Nätverk från grunden, 1998)

The purpose of Electronic mail (E-mail) is to transfer messages among individual users over the Internet. Each local authority assigns an address to each authorised user within its domain. An address contains of a string that identify the user, followed by a @, and then a domain name for the machine assigned to handling the domain's e-mail.

There exist persons, who we can call attackers that are interested in information that are not meant form them. The following paragraphs, which are valid for all three connections will thus describe the attackers and their reasons for attacking.

Security assaults
(Informator, 1997)
(Network Security Essentials, 2000)

There exist several reasons for a person to attack computer systems and networks. The reasons are not much different from the reasons for a normal break-in. One reason can be the economical benefit, as the attacker can steal programs, software or other information that can be collected and then sold. Another reason is espionage, this is for example when competitors tries to get access to information about a company's products and future plans. Political motives are also common as the attacker can change and manipulate companies' political preferences and change it into the attackers own believes. Attention is also one reason to crack in to the networks and computer systems. In many circles it is a sport to crack as many machines as possible.

Another important issue is, to attack networks and computer systems, a deep knowledge in TCP/IP and operating systems are required (see also Appendix 6). When attacks are made as a sport it is mostly kids and students who are the attackers, but as companies now are using the Internet in its business and when money is involved it attracts other people and organisations with larger resources and money.

Many types of security risks exist that can occur when handling data and information, the paragraphs to follow describes these risks and the information is found in the literature, Säkerhet I elektronisk post, 1995, Internetsäkerhet – Attacker, brandväggar och kryptering, 1997, Network security Essentials, 2000.

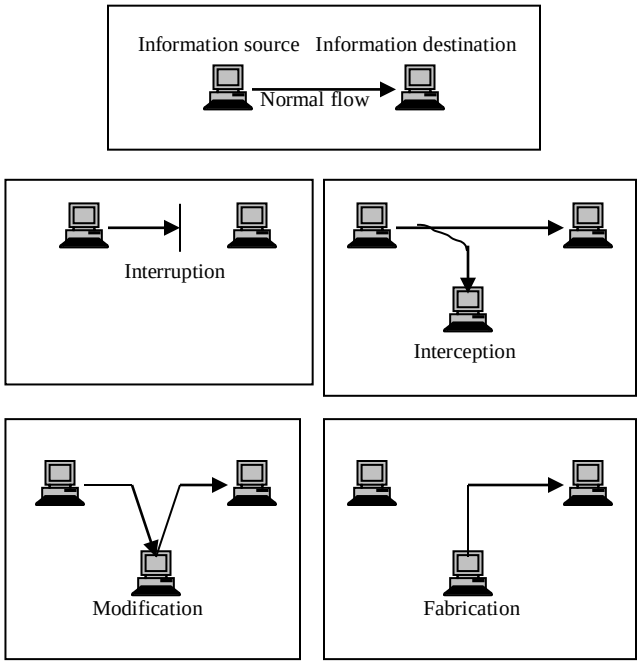
The security risks can be divided in to four main groups:

Interruption: Information can be destroyed from destruction of the system, which is an attack on system or data availability.

Interception: Information can be stolen or copied. This is an attack on system confidentiality.

Modification: Information is gained access to and tampered with, which is an attack on system or data integrity.

Fabrication: An unauthorised party inserts forged objects into the system and this attack is on system authenticity.



Based on Stallings' picture Security Threats (Stallings, 2000a)

Incorrect transmitting is when a message can be transmitted to a reader with the wrong address or a message can be transmitted incorrect because of that the technical equipment is acting incorrectly. This will thus lead to other threats such as the transmitted message can be read by someone unauthorised and the transmitted message will not reach its destination.

Alteration of messages during the way between transmitter and the receiver is a severe threat. If one sends a message by e-mail, the message is stored during its way to the receiver. This can happen without any further delay or that the receiver even notices that the message have been delayed. This is a grand and serious threat, especially if an unprotected EDI (Glossary) message is sent by the use of e-mail.

False sender is when a message is forwarded were the sender of the message pretends to be someone else.

Bugging of information is a risk that can be described as the possibility to overhear the information that is transmitted or spread over the network. There exist several methods and equipment that is physically connected on to the network where data can be collected. In this way the data can also be modified during the transport over the network.

Virus is a grand and serious problem that is spread or distributed over the network. A computer virus is a piece of code that is included and it copies itself into an executable file, program or into e-mail letters with attachments. Virus cannot be spread through text files or e-mail messages that do not contain attachments. A virus might not manifest itself until it is triggered by some kind of event for example a specific date or a name etc. To protect a computer or a company from a virus is it important to constantly upgrade virus programs and minimise the use of floppy disks. One should also only copy files over the network from computers that is administrated in a professional way.

A Worm is very similar to a virus. A worm is an autonomous program that transfers and replicates itself over and over again. It takes up residence in machines until it shuts down the computer system or the network.

A Trojan horse is a piece of code that is hidden inside a login program. When a user logs on to a system where the Trojan horse is hidden, it gets access to the users ID and the users logon becomes compromised. The Trojan horse can use the ID to access the user’s resources. The Trojan horse is hard to discover because after finding the desired information it exits the system and leaves no trace.

To the security assaults mentioned there exists protection and towards the goal of securing information in communication over networks, encryption is the best and most common answer, as stated by Stallings " The most powerful, and most common, approach to countering the threats to network security is encryption" (Stallings, 2000a). The implication of encryption will be pointed out in the following chapter.

Encryption

In this chapter we have chosen to discuss symmetric and asymmetric encryption techniques since they are tools for protecting a message's confidentiality. Of equal importance is authentication of a message and we will therefore focus on digital signatures which are techniques used to provide a message authentication in combination with encryption or by themselves.

Since the secrecy regarding symmetric encryption relays on the secret key and its distribution we will also bring up some issues regarding this subject. To point out the purpose of a message being encrypted while transferred over a communication line, we finally describe the terms passive and active attack and provide some examples of the most common attacks on cryptosystems.

Symmetric encryption

Symmetric encryption also referred to, as secret key, single key or private encryption is according to Stallings, 2000a the most widely used encryption technique. The system involves the following five components.

Plaintext:	Consists of the original message.
Encryption algorithm:	Performs the transformation of the text
Cipher text:	The output product consisting of the scrambled message.
Decryption algorithm:	The encryption algorithm runs in reverse as it takes the cipher text and the same secret key and reproduces the plain text.

The technique is based on that the sender and receiver use the same key for encryption and decryption (Appendix 16) This method is fast working but may be complicated since it acquires the parties involved to make up arrangements for their communication. Examples of symmetric encryption are DES, IDEA and RC5 (Glossary)

The distribution of the secret key is very important since the whole encryption process depends on the fact that no one from outside captures the key. As Stallings state it is noticeable that the security issue regarding encryption "depends on the secrecy of the key, not the secrecy of the algorithm."(Stallings, 2000a). If so happens that someone gets access to the secret key all communication using this key is fully readable. Arrangements have to be made up before, by the parties involved so the receiver knows the contents of secret key. The parties can then deliver the key physically (the key is stored on a disk and manually delivered) with the help of a third party. According to Stallings, 2000a it is to prefer that the two parties have an encrypted link to a third party where the key is delivered since it may be awkward for the parties to deliver it manually. Fredholm, 2000 gives another suggestion as he claims that a secure way to deliver the key is by ordinary post.

Asymmetric encryption

This technique builds in two different keys, one private and one public. The sender encrypts the message with the receiver's public key, while the receiver decrypts it with his private key (Appendix 16). The system is based on the encryption key being published in a directory, while its decryption key will be kept secretly stored on a smart card or program.

According to Fredholm, 2000 asymmetric encryption provides a higher security level and is to prefer when it comes to encrypt messages sent by e-mail. Stallings' viewpoint regarding the security level is more technical as he states that the security level depends on "the length of the key and the content of computational work involved in breaking the key." (Stallings, 2000a).

The security level is though depending highly upon how the user stores and protects his/her private key. Examples of asymmetric encryption techniques are Diffie-Hellman key exchange and RSA (Glossary).

Authentication of a message is provided by the use of encryption since only the genuine sender would be able to encrypt the message successfully. Several ways of message authentication without relaying on encryption are though possible to practise which will not be discussed in the report.

Digital signatures

In order to maintain protection against active attacks (explained later in the text) during transmission of data, message authentication verifies the authentication on both the document and the source. These are examples of important security services in order for two parts to exchange information in form of documents or messages in a secure way. If correct time is desirable as a further security level, a timestamp may also be included in the message.

A digital signature stands as an authentication to verify the legitimisation of the sender. This system is of great importance for evaluating the source sending it. The digital signature is created with an algorithm based on the actual document. The RSA algorithm gives a very secure signature because it is impossible to corrupt or falsify the digital signature. The result from the algorithm is named as a hash number and serves as a unique number for that special document. To create the digital signature the hash number is encrypted with the private key from the user. When a receiver gets the message he will decrypt the signature with the sender's public key.

Passive attacks

The passive attack is an attack on the confidentiality on the data transmitted.
Examples of passive attacks are

- Passive eavesdropping when the attacker is simply listening at the traffic.

- Traffic analyses attack is when the observer of two companies communication, trade a large amount of messages and business conclusions are drawn from this.

Active Attacks

Active attacks threaten the integrity or availability of the data. Examples of active attacks are:

Replay:	The message is resent out to the network.
Cut-and-paste:	A new message is produced by combining two given messages, encrypted by the same key.
Masquerade:	This attack occurs when one entity pretends to be a different entity.
Man-in-the-middle:	The attacker is placed in the middle of the communicating parties and impersonates one of them

Current system

Description
(X)

The current system is an invoice sent to the customer through e-mail. The first step is to collect and compile all data into a file. The file is automatically sent forward in seven different invoice periods to another level. At this level the file is formatted in to a common final format of the invoice. Before the invoice is sent to the customer it is copied to another file on the server. X compiles the mail to the customer and attaches the invoice in the mail. The employee is also responsible that the mail is encrypted before it is sent to the customer (Appendix 11)

Problems
The main security problem with the current system today is that there is a human interaction when delivering the invoice. The first problem is that in order to send the invoice the employees have to attach the invoice from their ordinary workstation to a written mail and then remember to encrypt it before sending it to the customer. According to XX at X's security department, the main issue and problem regarding sending the current system by mail is the fact that the sender at X has to start the encryption session by him/her self. The encryption system used is based on symmetrical encryption method, which is a method with lesser security procedure (see chapter Encryption).

The second problem is that the invoice is sent by e-mail. There are several insecure issues concerning sending an invoice with an e-mail. Problems that can occur are that the system can shut down by a virus, someone can analyse, modify, duplicate and delete the information in the message. There is also the possibility of neither authentication by the sender nor by the receiver. If a problem occurs the sender have no proof that it was X who sent the message and no proof that message has not been changed on its way to the customer.

In the interview with Anders Ranefjord at WM-Data (Appendix 5) he expressed his point of view regarding e-mail. " E-mail is the most risky system. Most things go wrong with e-mail. For example: the mail does not arrive, it can be altered, virus can be send and the addresses are not hard to come across. The employee's unawareness results in that they open their mails without concerning the risks and in that way the employee becomes a security risk. Here it is important with well-established security policies. E-mail is the easiest way to sabotage and create huge damage."

Description of the three solutions

We have based our three solutions on the criteria described below. In the chapter called limitation we stated that we should look at point-to-point security as Fredholm discuss "when we talk about security in electronic commerce its about protecting the information from the senders system all the way to the receivers system." (Fredholm, 2000).

Regarding data communication the book electronic commerce by Fredholm, 2000 discuss three types of connections. The first one is a dial up connection, this means that the system makes an up and down connection for every time information is transferred, like an ISDN channel. The second one is a permanent connection by this means that it always exist a connection like a X.25 channel. The third one is a virtual connection this means that the up and down connection is done via an automatic routine as with Internet.

Today the current system is based on an electronic mail delivery with human interaction which main problem is that it is not done automatically. Our solution with a mail server offers automatic routines. We have developed this solution as a possibility for X to use the solution as a product.

The solution with ISDN was chosen because of security advantage it presents according to Stallings "A trusted third party may be needed to achieve secure transmission." (Stallings, 2000a), and since there already exists a co-operation with a third party (Appendix 9).

The solution with X.25 via Internet bank was chosen based upon what the competitors (Appendix 2) were offering their customers. We also chose this solution since the FöreningsSparbanken is directed towards SME customers as Ann-Christin Nilsson at FöreningsSparbanken says " A company that is using the bank over Internet is containing between 0 and 50 employees."(Appendix 3).

First solution ISDN via a third party

Description
(Data kommunikation, 2000)
(Advances in ISDN and Broadband ISDN, 1992)
(Computer Telephony Integration, 2000)
(Säker Data och Tele Kommunikation 1992)
(Firewalls and Internet Security)

This solution is based upon an already existing communication line to a third party which business concept includes electronic commerce within the context of delivering invoices.

The ISDN-channel establishes a dial- up connection from X to a third party, which in our case study is represented by Strålfors (Appendix 9). The communication line starts from the client X and passes through a router to Strålfors' router and enters a firewall before it enters the client's server.

To establish the connection X calls up Strålfors with a signal containing a key code, which Strålfors identifies with the help of a key, kept in Strålfors's router. The key serves as the "password" to establish an authorised connection and after this procedure the file is copied with RCP (Remote Copy Protocol) to the third party (Appendix 13).

ISDN
ISDN (Integrated Services Digital Network) profound a set of standards for transmission over telephone wires. ISDN is essentially a circuit switched network - there is no

permanent line and a connection is established by dialling up. Disconnecting a line physically when there is no traffic, while maintaining the logical link, simulates a permanent line. When packets need to be sent, the physical line is reconnected. This is transparent to the user as it happens practically instantaneously.

ISDN is an important communication channel over WAN's since it provides a very high transfer rate of data, video, music, graphic etc. ISDN separates bandwidth into different channels and use them dependent on the current data traffic. The channels are separated into B and D channels where D channels transfer data and voice, audio, and video while B channels transfer signalling and control information. Data is transferred at a very high speed and as Stallings states "ISDN employs reliable digital -transmission technology over high-quality, reliable transmission links, many of which are optical fibre."(Stallings, 1992).

Wiretapping the communication line on information cables are not easy targets to passive or active attacks and it takes a lot of work to actually cut of the cable. According to Borgström and Lindblom, 1992 the method for tapping a cable on information is rather complex and involves great knowledge and equipment. A protocol analyser can be looped into the communication circuit gives control to the data and allows manipulation of the data in the D-channel.

Router

A router provides the mechanism of choosing the right path for the packets through the network to reach its final destination. It may act as a device or a software program in a computer. A router is used where any network includes the Internet. The router is connected to two networks and establishes two paths from the source machine to the destination, and reverse. If a router is attacked the data can be re-routed or stolen. The main security issue lies in the authorisation process of the two routers. According to Cheswick et al. 1994 the best way to secure your routers is therefore to disable source routing and configure them so they know if a given path is legal.

RCP Remote Copy Protocol

The protocol is used to copy files between one computer to another in a network. It transports data up to 250 bytes per packet and provides error detection and possibly automatic error retransmission. The protocol does not provide encryption and leaves therefore the data in clear text. The authentication process when RCP connects to a server consists of the server looking for the connection user and host entry in its catalogues. RCP does not involve the exchange of passwords but relay on a connection from an IP-address, which is easy to spoof (Glossary).

Second solution mail server

Description

The X client first formats the file into the final appearance of the invoice, then the client copies the invoice into another file on the client and automatically sends the invoice to the X encryption server and here the invoice is automatically encrypted. The mail server receives the invoice and develops an e-mail, all is done mechanically. The mail server is configured to only forward outgoing SMTP traffic handling the invoice and connected to a database. The customers' addresses and the logs of sent mails are stored in the database. The server is based on UNIX which has sendmail installed. The invoice is automatically sent via SMTP over the Internet to the customers' mail server (Appendix 10).

SMTP

(Maximum Security, 2001; Data communication, 2000)

The simple mail transfer protocol (SMTP) is a mail transfer protocol that traditionally operates over TCP connections on port 25. The SMTP standard for Internet messaging allows electronic mail to forward across a network in "hops" by passing from one computer system to another, repeating this process until the e-mail reaches the recipient.

SMTP is limited as it has difficulties in queuing received messages and is usually used with one of two other protocols, Post Office Protocol 3 (POP3) or Internet Mail Access Protocol (IMAP). Since SMTP has an open design, intruders can attempt to send their e-

mails via someone else's by asking the other computer to route that mail for them. The former issue can also be done by alteration of the message header.

Sendmail
(www.sendmail.net)
(www.linuxplanet.com)

The operating system UNIX comes with the sendmail program as default. Sendmail is a mail transfer agent (MTA) whose purpose is to send and receive e-mail primarily via SMTP. According to Wong sendmail is a well-documented application with comprehensive online tutorial, which is significant for managing the complexity of sendmail. (Wong, 20020516)

One of sendmail's disadvantages is that its configuration file is so complex, if you are not a professional system administrator the complexity will become a security risk. Since SMTP probably is the only open hole in a firewall, sendmail has been scrutinised by attackers trying to break into the system. Wong states "the …issue is that sendmail is often configured with minimal security by default, making it easy to set up but open to attack. If using sendmail then make sure you know what options you have turned on." (Wong, 20020516)

Server
(Nätverk från grunden, 1998)

A server is a computer program that provides services to other computer programs in the same or in other computers. The computer that the server program runs on is also referred to as a server even though it may contain a number of server and client programs.

In the client/server model, a server is a program that awaits and fulfils requests from client programs in the same or in other computers. An application in a computer may function as a client with requests for services from other programs and also as a server of requests from other programs. In a network, the client/server model provides a favourable way to interconnect programs that are distributed efficiently across different locations.

Third solution X.25 via Internet bank
(Elektroniska affärer, 2000)
(Data security in X.25 Networks, 1988)
(Nätverk från grunden, 1998)
(www.privateline.com/Switching/X25.html)
(www.primarykey.co.uk)
(X.25 made easy, 1992)

Description

The X client first formats the file into the final appearance of the invoice. Before transmission the data is segmented into small blocks called packets that do not only contain the data but also control information (flags marketing the beginning and the end, source, destination addresses, sequence number). Packets are routed through the network one at the time and may arrive at their destination by different paths and out of sequence. The receiving server is responsible for bringing together the packets into the correct order before passing them forward. The receiving server is also responsible for creating the invoice into a public format before transmitted to the Internet bank (Appendix 12).

X.25

X.25 is an international protocol for packet switching in network with a high transmission speed. X.25 is used to connect computers via a permanent connection. We consider X.25 as a permanent connection even though the packages are delivered virtually. According to (www.privateline.com) X.25 is an extremely accurate way to pass data but this also limits its speed. X.25 present several advantages both technical and commercial, the most important of which is that it both presents an efficient and cost effective way to send large volumes of data. Many companies have invested in X.25 as the market has increased the use of on-line transaction processing.

The data in packet switched networks are separated and transmitted in small units called packets. The packets are only occupying the transmission line for the time of the transmission. Packet switched networks use many switches, this approach allows the traffic load to be distributed to other switches. It also uses at least three lines that are

attached to the switches. This allows the network to route the packets around failed or busy switches and lines, which provides a better availability and reliability in the system.

The use of X.25 permit many channels to share one physical connection, and according to the demand of each channel it can dynamically allocate bandwidth, without denying access to other channels. X.25 is a secure network because of included functions such as control and verification of the data transmitted. X.25 has error checking and error recovery functions on a hop-by-hop basis. It returns an acknowledgement whenever a packet is send, this makes sure that no unfulfilled packets are forwarded. The switch keeps a copy of the packet until the next switch returns an acknowledgement. Other advantages with using X.25 are the possibility to use parallel sessions, the reliability and the international availability of X.25. One other advantage is the function called Closed User Group (CUG) which means that the operator creates a group of the X.25 numbers that the company uses. This will result in difficulties of attacking the net from the outside.

Conclusion

In this paragraph the test is presented. The matrix below explains how the different file transfer systems fulfils the security services. A detailed explanation of the test is presented in order to comprehend the result. We have chosen to include current system in the test to make the problem more clear and to show that our three solutions better meets the security services than the current system.

	Current system	ISDN	X.25	Mail server
Confidentiality	-	+	+	-
Authentication	-	-	+	-
Integrity	-	+	+	-
Nonrepudiation	-	+	+	-
Access control	-	-	+	+
Availability	-	+	-	-

Here follows the evaluation of our test and the different solutions is described in the same order they appear in the matrix above. We will thus below describe the reasons for our decisions.

Current system

Since the current system is distributed over Internet and encrypted with a symmetric encryption technology we consider the confidentiality level to be low (Appendix 8). Though encryption provides a resistance against passive attacks, the distribution of the key in symmetric encryption is inferior to how the distribution functions in asymmetric encryption. Based on our knowledge from the course network security DVC007 we consider that encryption provides security, but since we are aware of that it is possible to

easily be decrypted it cannot provide a fulfilled security level. Another reason for that the confidentiality level is considered to be low is that the encryption is done manually, as we have stated in the chapter about encryption, this is a security risk. It is considered to be a risk to send e-mail over an open network and according to the statement in Spri "Since the message can be stored at many post-offices with different users and system operators, totally outside of the transmitters and receivers control, this threat must be taken seriously."(Spri, 1995).

The authentication level is low based on the lack of confidentiality and the fact that SMTP does not offer any authentication. Another problem is that a mail header can be altered and this makes thus the identification of the sender insecure (see, chapter SMTP).

Integrity is founded on the protection from active attacks. The problem with the message not being protected implies that the data can be modified, which is a security risk.
An example is that the message is not transmitted at a predetermined time and no connection is established before the transmission. We also refer to the quote by Anders Ranefjord in the chapter the current system, problem description.

Non-repudiation is to prove that a message has been sent and received. In the current system digital signatures are lacking, which leads to that it is uncertain to prove that the invoice is sent. And according to Daniel Pettersson, Secode (Appendix 6) digital signatures are necessary for secure transmissions. By the above we consider the non-repudiation level to be low.

Access control is the prevention of any unauthorised part taking use of the system's resources. Since X's security policy permits different communication traffic in their system the possibility of an unauthorised party getting access to the system increases. According to Spri "the problem with data intrusion is thus utmost when computers manages other implementations than used for forwarding electronic mail." (Spri, 1995).

Systems availability is measured in terms of hardware and software problems. Due to that the Internet is an open network the possibility of receiving a virus, worm or trojans increases. The possibility of the system totally or partly crashes or making the data unavailable is enlarged. XX at X states "…though the latest virus will always come through anyway". As a result the reasons above are poorly securing availability.

ISDN via third party

The systems confidentiality level is high while using an ISDN communication line since eavesdropping of a telephone wire requires access to the system and knowledge about the communication line. When the file is copied with RCP the protocol does not provide encryption but we consider the risk to be small that someone catches the right time for the transfer since the ISDN is a dial-up connection providing a high transfer rate. XX at X also explains in his interview (Appendix 4) that he considers ISDN as a communication channel very secure since wiretapping of the telephone lines is most unlikely to happen.

The authentication process between the two routers verifies that X's router is the router supposed to have access to the communication line through the process earlier described to establish connection (see chapter ISDN). The data is though sent by the transfer protocol RCP, which we consider to have a weak authorisation process. The former is based on the fact that the receiver of the copy will manually check if the source is stored in a file.

The root administrator looks for the connection user and host entry in its catalogues and carries manually out the authentication process at the RCP level from the local host at X to Strålfors. As we have stated before, human interaction in a system can lead to weak security services. The system relays on a connection from an IP-address (Glossary), which we consider an insecure system to establish secure authentication.

The possibility of an active attack against system integrity resulting in modification of the data on the file requires someone to gain access to the system from inside tap the wire or hack in the switch placed at Telia. We do not consider either one of these threats to

influence the amount of system integrity. RCP on the other hand provides error detection together with recovery detection preventing the data from reaching its destination in a modified way that ensures data integrity.

ISDN profound a more secure media since it is not as well known as for example TCP/IP, this reduces a certain amount of outside threats. Our conclusion is also based upon XX and Anders Ranefjord earlier statements about ISDN as a secure connection (Appendix 4, 5).

Access control is fully secured at the ISDN communication line as the two routers connection is secured by the password stored in one of them. It is very unlikely that someone gains access to the system from outside according to the facts named earlier based upon the possibility of active attacks. But when it comes to secure access through the user of RCP (ISDN transfer protocol) it is a process performed manually which makes the control unreliable since it is easy to make a mistake while giving the presumed party access to copy the file. Since the communication line consists of telephone wires, which have to be cut of, or bent to make the lines availability weak we refer to Borgström and Lindborg, 1992 where this process is described as rather complicated.

To change the data's availability it is as mentioned before necessary to gain access to the switch and manipulate or reroute the data. We consider this possibility to be low and therefore not affecting the availability of the system.

X.25 via Internet Bank

Regarding X.25 confidentiality, we think that this security service is well fulfilled. As we said in the chapter about X.25 this is based on that the packets do not need to take the same way every time it is transmitted. The IT-consultant Ulf Johansson (Appendix 8) state "…it is very difficult for anyone to know which way an X.25 packet will take as it do not need to take the same way every time. This depends on loading, problems with the wire or nodes and so on."

We consider that authentication is also very well fulfilled and this is based on that both source and destination address exist in every packet, and the packets are also controlled at every switch. The possibility that the data can be changed is very small because as we said before the packet do not need to take the same way every time and as discussed in the chapter about X.25 were we describe that an acknowledgement is sent back before next packet is sent.
Ewert states “Both X.25 and Frame Relay function so that when a packet is sent a timer is started at the same time. If the station that is receiving the packet do not answer and inform that it has received the packet OK (sent an acknowledgement), before the timer is timed out, will the sending station think that the packet has not been delivered properly.” (Ewert, 2001)

The integrity of the data is very well protected because of functions such as error detection, sequence control and checksums. We think that the possibility of the data being changed is very small based on control-information and the acknowledgement sent at every switch, which control that the data has not been modified before it is transferred forward.

The non-repudiation is also fulfilled as the packet is containing both source and destination address which is controlled at every switch. Based on the former sentence we draw the conclusion that it would be difficult to deny that the data has been sent or has not been received.

As we described in the chapter about X.25 about Closed User Group this will fulfil the access control. Described in the chapter about X.25 this function creates a group of the X.25 numbers that the company uses. This make sure which one that have access to transmitting the data over the X.25 channel and this makes it difficult for others to get in from the outside.

We consider that the availability is fulfilled, because it is very difficult to perform an active attack, which will lead to the system breaking down. The IT-consultant Ulf

Jonsson states that “as I see it the threat must come from the inside. There are too many controls to be able to attack from the outside but today can no one be sure about this either”.

One other possibility to obstruct or destroy the availability is to wire tapping the communication line but it takes a lot of work to actually cut of the cable. According to Borgström and Lindblom, 1992 the method for tapping a cable on information is rather complex and involves great knowledge and equipment. But since in a packet switched network the attacker can reroute the data from the network management centre and modify the data without tampering with any physical connections, we consider that the availability level is unfulfilled.

Mail server

The mail server solution provides a poor confidentiality since it is distributed over the Internet. But since the risk of missing to encrypt the file is eliminated since it is done automatically the confidentiality level is not so sinister. According to Fredholm, 2000 symmetrical encryption conveys a larger security risk than asymmetrical but the problem with passive attacks remains.

The authentication level is poor since confidentiality lacks. The fact that SMTP does not offer authentication without extra RFC extension, also depresses authentication. In the chapter about SMTP we describe that a message header can be altered and this makes thus the identification of the sender insecure.

The integrity service relates to active attacks. The problem with the file not being securely protected means that the data can be modified or a masquerade taking place. The integrity level is therefore unfulfilled and we base this conclusion on the problem discussed with the current system and in the chapter encryption.

As mentioned before non-repudiation is to prove that a message has been sent and received. In the mail server solution digital signatures are lacking, which leads to that it is

uncertain to prove that the invoice is sent and received. But since the logs of sent mails are saved in a database the sender of the mail can at least state that the file has been sent. Since digital signatures are necessary for secure transmissions, we consider the non-repudiation level to be poor.

The access control service implies the ability to control system access. We consider that the access control is fulfilled since the mail server solution only handles outgoing SMTP traffic that occurs when transmitting the invoice, the risks are thus reduced as other SMTP traffic are not allowed. Spri states “There is though a risk that unauthorised users accesses the computer the same way as the messages if the communication software in the computer also allows other types of traffic than electronic mail.”(Spri, 1995).

The availability service implies the loss of accessibility to your system or data. Since the file is forwarded across Internet you cannot predict the path the file takes from X to the customer. The former implies that the file can be infected with virus and Trojans along the way. The file cannot however be infected from X’s mail server since the system does not allow inbound SMTP traffic, on the other hand the file can be caught by virus and Trojans from insiders. By the above we consider that the availability is unfulfilled.

Recommendation

By the help of our test based on Stallings’ Security Services we can verify our hypothesis and make a recommendation.We have come to the conclusion that the X.25 solution has best fulfilled the security services. To provide X with an improved security solution, we consider that X.25 best meets their demands according to their policy.

Discussion

We consider that to be able to make a good recommendation economy and market aspects must also be taken in to consideration. The relation between security and economy shows that it is of great value to have capital to invest in security. The amount of security must also be in relation to the amount of sensitive data the organisation handles. With a look at existing security tools and systems today and with security knowledge it is always possible to get through any system if the information is worth it.

An aspect that has to be taken in to consideration is how the customers are interested in receiving their invoice. The Internet bank can give the customer both the invoice and the possibility to pay on the same interface.

The future is also an important factor, as the use of cellular phones with functions like WAP (wireless application protocol) gives the opportunity to provide a new way for customers to pay bills in a more mobile way.

The solution ISDN and mail server gives the customer the possibility to receive a specified invoice and this is not something that the Internet bank can provide with their present interface.

What competitors offers is also something that should be considered as Tom Michael (Senior Master, the Technical Institute of Blekinge) stated "sometimes it is not the best solution to follow business competitors strategies, it is better to go your own way".

Subject for further investigations

- How mobile phones can alter the procedure of future billing systems

Source criticism

We have mostly based our thesis on acknowledged literature and interviews, but we have also collected information on the Internet. We are well aware of that the information is insecure even if the information is collected from trusted organisations. We still choose to use this information since the content can be confirmed by acknowledged literature.

Glossary

Algorithm: The term algorithm is a procedure or formula for solving a problem

Circuit switched network: Circuit-switched is a type of network in which a physical path is obtained for and dedicated to a single connection between two end-points in the network for the duration of the connection. Ordinary voice phone service is circuit-switched.

client – server: Client/server describes the relationship between two computer programs in which one program, the client, makes a service request from another program, the server, which fulfils the request. Although programs within a single computer can use the client/server idea, it is a more important idea in a network. In a network, the client/server model provides a convenient way to interconnect programs that are distributed efficiently across different locations

Daemon: A daemon is a program that runs continuously and exists for the purpose of handling periodic service requests that a computer system expects to receive.

Default: In computer technology, a default is a pre-designed value or setting that is used by a computer program when a value or setting is not specified by the program user.

Device: In general, a device is a machine designed for a purpose. In a general context, a computer can be considered a device.

Diffie-Hellman key exchange: First developed asymmetric encryption.

Document: A transaction set or message.

DoS:	Denial of service. It is a condition that results when a user maliciously renders an Internet information server inoperable, thereby denying computer service to legitimate users.
EDI:	EDI (Electronic Data Interchange) is a standard format for exchanging business data
Hash number:	A hash function produces a “fingerprint” on the data, which ensures authentication. The hash function takes an input in form of a variable- size message and produces a fixed size message as an output
IDEA	International Data Encryption Algorithm, is another system similar to DES despite that it uses 128 bits to decrypt 64 bits of blocks.
IMAP	Internet Mail Access Protocol is an electronic mail server for Internet.
IP:	In a network it is necessary that packets of data can be transferred over multiple networks and for this purpose IP is used. Therefore, IP is the protocol, which makes it possible for data to be sent to another host through one or more routers.
LPC:	The Link Control Protocol (LCP) establishes, configures, and tests data-link Internet connections.
MTS:	The Microsoft Transaction Server (MTS) is a program that runs on an Internet or other network server with a Windows NT system and manages application and database transaction requests on behalf of a client computer user, servers, and transaction integrity.

Mutex:	In computer programming, a mutex (mutual exclusion object) is a program object that is created so that multiple program thread can take turns sharing the same resource, such as access to a file.
Netmon:	Network monitor
NTFS:	NTFS (NT file system; sometimes New Technology File System) is the file system that the Windows NT operating system uses for storing and retrieving files on a hard disk.
Parser:	In computer technology, a parser is a program, usually part of a compiler, that receives input in the form of sequential source program instructions, interactive online commands, markup tags, or some other defined interface and breaks them up into parts (for example, the nouns (objects), verbs (methods), and their attributes or options) that can then be managed by other programming (for example, other components in a compiler). A parser may also check to see that all input has been provided that is necessary.
POP	Post Office Protocol is an electronic mail server for Internet. The difference between POP and IMAP is that POP get all mail to a user directly when the user is connecting to the server.
RC5	Previously RC2 and RC4, captures different lengths of the encryption keys

RSA.	RSA is an Internet encryption and authentication system that uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman
SNMP:	Simple Network Management Protocol is the protocol governing network management and the monitoring of network devices and their functions.
SPOOF:	To deceive for the purpose of gaining access to someone else's resources (for example, to fake an Internet address so that one looks like a certain kind of Internet user). To simulate a communications protocol by a program that is interjected into a normal sequence of processes for the purpose of adding some useful function or to playfully satirise a Web site.
TCP:	TCP is the protocol that keeps track of the data transferred to ensure that the data reaches the right application. In order to check the reliability of the data delivered, TCP breaks the data blocks in small segments and then adds control information to every piece. In contrast to IP, TCP only has to be implemented in the end system.
TCP/IP:	Transmission and Control Protocol/Internet Protocol (TCP/IP) is a combination of communication protocol that is used over the Internet. TCP is handling the transmission of messages between two computers by connecting a virtual link in other words a communication link between the two computers without any physical connection. IP is a network layer

protocol and is taking care of data packages and is responsible that the packages are reaching the right Internet address.

Works cited

Books

Abrams Marshall D et al, 1995, *Information Security An introduction of essays,* IEEE Computer Society Press, Los Alamitos California.

Anonymous et al, 2001, *Maximum security,* SAMS, Indianapolis.

Black Uyless, 2000, *Internet Secure Protocols, Protecting IP traffic,* Prentice Hall Inc. Upper Saddle River New Jersey.

Borgström Håkan, Lindborg Lennart, 1992, *Säker Data och Tele kommunikation,* Affärsinformation AB, Stockholm.

Casad Joe, Newland Dan, 1997, *MCSE training guide Network Essentials,* New Riders Publishing, Indiapolis.

Cheswick William R., Bellovin Steven M, 1994, *Firewalls and Internet Security, Repelling the Wily Hacker,* 5th edition, Addison-Wesley publishing company, Massachusetts.

Ewert Magnus, 2001, *Datakommunikation Nu och I framtiden*, Third edition, Sweden, Studentlitteratur, Lund

Fredholm Peter, 2000, *Elektroniska affärer,* Studentlitteratur, Lund.

Freese Jan, Holmberg Sten et al, 1993, *Data säkerhet,* Affärsinformation AB, Lidingö.

Gärdenfors Per, 1996, *Fängslande information,* Natur och Kultur, Stockholm.

Hedemalm, Gunvald, 1998, *Nätverk från grunden*, second edition, Pagina AB, Upplands-Väsby.
Informator, 1997, *Internetsäkerhet – Attacker, brandväggar och kryptering*, Informator Utbildning Svenska AB, Stockholm.

Jilovec Nahid, 1998, *The A to Z, And its role in E-commerce*, second edition, Duke Communications International, Canada

Lax Stephen, 2001, *Access denied in the information age,* Palgrave, NewYork.

Oppliger Rolf, 1998, *Internet and Intranet security,* Artech House, Norwood

Patel Runa, Tebelius Ulla, 1987,*Grundbok I forskningsmetodik*, Studentlitteratur Lund.

Spri,1995, *Säkerhet I elektronisk post* ,Spris förlag, Stockholm.

Stallings William, 2000a, *Network security essentials,* Prentice Hall, New Jersey.

Stallings William, 2000b, *Local & Metropolitan Area Networks,* Prentice Hall, New Jersey

Stallings William, 1992, *Advances in ISDN and Broadband ISDN*, IEEE Computer comity Press, Los Alamitos.

Thorpe Nicholas M, Ross Derek, 1992, *X.25 Made easy,* Prentice Hall International, The United States of America.

Turban Efraim, Lee Jae, King David, Chung H. Michael, 2000, *Electronic Commerce a Managerial Perspective,* Prentice-Hall, New Jersey.

Yarberry William, 2000, *Computer Telephony Integration*, CRC Press LLC, Florida

World Wide Web

www.whatis.com

http://searchwebmanagement.techtarget.com/sDefinition/0,,sid27_gci212399,00.html

http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci213821,00.html

http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci214314,00.html

http://www.e-faktura.org

http://searchwindowsmanageability.techtarget.com/originalContent/0,289142,sid33_gci817464,00.html

http://www.sharecenter.net/network/Computer_Networking/05.10.htm

http://www.sendmail.net/smfaq09.shtml

http://www.linuxplanet.com/linuxplanet/reviews/1640/1/

http://www.privateline.com/Switching/X25.html

http://www.swrtec.de/rcp/

http://www.ncl.ac.uk(ucs/unix/rcp.html

http://www.feynman.physics.lsa.umich.edu/

http://secinf.net/info/misc/gshb/t/t5063.htm

http://www.primarykey.co.uk/Andy/Papers/x25paper.pdf

http://www.tekes.fi/eng/information/sme.html

Appendix