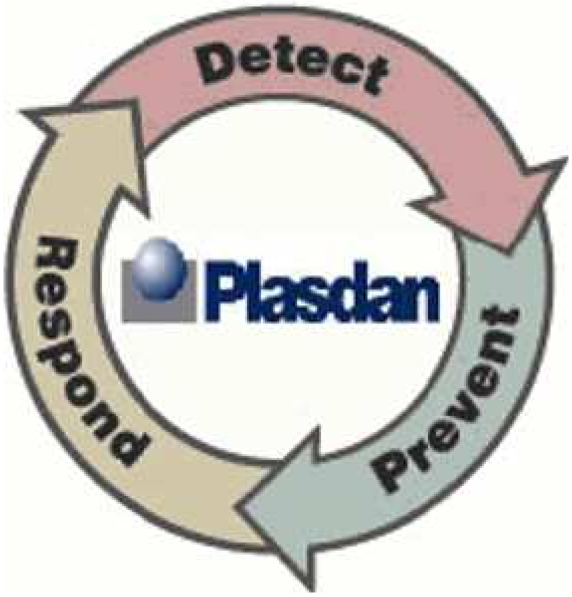
# Internet Security in an international Company




Nikolas Triantafyllidis
(s001077)

MASTER THESIS
Technical University of Denmark
LYNGBY 2002

IMM

## Abstract

Enterprizes around the world have recognized the business potential of leveraging Internet technologies and the Internet itself. Many businesses are becoming increasingly reliant on the Internet for communicating with customers, researching competitors and conducting e-commerce.

This increased use of the Internet, makes business networks become more vulnerable to Internet threats and attacks, emphasizing on the need to address new issues related to the technologies involved, especially in the area of Internet and Network Security. These Internet Security attacks can wreak havoc on any business, leaving valuable data wiped out, confidential information stolen or corrupted, the entire network made inoperable, or access to sites vital to business operations shut down. The 2001 Computer Crime and Security Survey, published by the Computer Security Institute, found that 85% of all companies on-line reported computer security breaches within the last year. [1]

Despite all the security risks and even though there is a considerable corpus of knowledge about tools and techniques to protect networks, detailed information about what the actual vulnerabilities are and how they are exploited, is not generally available. Therefore, only few organizations are taking sufficient measures to protect their networks and applications, leaving the chances of security problems impact every sector of their business life to a maximum and hampering the effectiveness of any kind of security research and practice.

The following master thesis identifies the security vulnerabilities that companies, in particular Plasdan, face if they go on-line without taking the necessary security measures and examines technologies and procedures that can systematically address those vulnerabilities. A detailed description and comparison on various features of the extracted solutions, will give a broad understanding on the detection and prevention possibilities. Finally, a country dependent analysis, in combination with a proposition of multiple product possibilities from a known vendor, as part of an implementation, will make the choice of deployment easier for the company.

## Acknowledgement

I would like to express my sincere gratitude to my academic advisor, Robin Sharp, who helped me, encouraged me and guided me towards my academic, as well as my personal success. I thank him for providing me an opportunity to grow as a student and engineer in the unique research environment he creates.

A special gratitude also goes to the Danish-Portuguese company Plasdan Lda, in particular Paulo Silva and Finn Blom Christensen, for suggesting our corporation, and to all the persons I met during my stay in Portugal, who helped me to gather valuable information about the company and to solve several administrational problems.

Last but not least, I would like to thank my family and my girlfriend for their substantial amount of help and understanding throughout my work. Their encouragement and positive affirmation made it possible to continue the hard work and succeed in completing this master thesis.

# Contents

# List of Tables

# List of Figures

# Chapter 1

# Introduction

With the increased use of the Internet, threats to valuable networks, servers and desktops escalate every day, going beyond viruses to include new and increasingly damaging online threats. At the same time, ever-changing business requirements force corporate networks to grow, and demand that organizations open their systems to partners, customers and their mobile workforce, significantly increasing the value and the vulnerability of their online assets. Business interruption, liability exposure and reduction in brand equity, drive the growing need to protect information resources against attack and misuse.

Considering the above aspects, protecting and extending the network has never been more important than it is today. It is essential and in the interest of companies, that secure Internet communications are simple to install and manage, offering flexibility, continuous availability and significant cost savings, without requiring extensive security expertise at all remote locations.

## 1.1 Problem Statement

This master thesis, which was made in cooperation with the Danish-Portuguese company Plasdan Lda, involves the following problem statement:

- How is the situation today in the area of Internet and Network Security, how does it affect businesses, and what constitutes a secure network from a general point of view?

- Which vulnerabilities and threats is Plasdan exposed to being online with the current configuration of their network?

- Which are the necessary countermeasures in order to address the various threats over the Internet, and which technologies and procedures are involved?

- Which are the country dependent requirements of the different locations the individual branches of Plasdan are situated in, and what the offered solution packages by a known Internet Security vendor?

## 1.2 Assumptions and Limitations

Due to the rather limited time for such an extensive and wide subject for a master thesis, it is rather obvious that a complete analysis of the entire aspects in the area of Internet Security, Plasdan is confronted with, is not possible. Therefore, the project will concentrate only on security aspects involving the company network towards the outside world, in other words, the possible threats and attacks the network is exposed to from the outside perimeter and their possible countermeasures. An analysis of security breaches from employees and "insiders", will not be part of this report.

Furthermore, a source code implementation of particular solutions will, due to time limitations, not be included in this thesis. As part of the mentioned implementation in the project description given by my supervisor, Robin Sharp, will serve solution proposals by one of the known vendors in the area of Internet and Network Security.

Due to the cooperation with Plasdan and the confidentiality issues involved, certain aspects of the company's structure and prizing information will not be revealed in this report.

Moreover, it has been assumed that the proposed requirement document has been accepted by the contact persons of Plasdan, since no further suggestions or changes where made in the period of negotiations.[1]

Concerning the economical analysis of Plasdan's security situation, as part of a risk assessment, it will be done only on a theoretical level. Due to the fact, that such a risk assessment for a medium sized company like Plasdan, would take more than a year to be done by a single person[2], it is rather obvious that a detailed analysis is not possible. Precise calculations for a cost benefit analysis or the Return on Investment (RoI), just to mention some of the important parameters, are not included and serve only the demonstration of the importance of such information to the entire process of a fully professional security analysis.

The information contained in this master thesis about the individual countries Plasdan operates in, as part of the **P**olitical, **E**conomical, **S**ociocultural and **T**echnological (PEST) analysis, represents the current situation in the area of Internet and Network Security. Due to changing technology aspects and conditions and the difficulty of gathering accurate and complete material, this information should not be interpreted to be a commitment and it cannot be guaranteed that any of the information presented will also be valid and accurate in the future.

Though this document contains a large amount of detail on many aspects of the technologies involved with the proposed Internet Security solutions, it is not exhaustive in its discussion. In particular, several aspects that relate to protocol organization and design, are not covered in detail.

## 1.3 Project Objectives

The goal of this project is to identify security vulnerabilities in Plasdan's current network architecture and according to the threats and attacks the company can be exposed to being on-line, extract a number of solutions, which can address the existing security problems. In combination with the proposed solutions, the involved technologies and procedures will be examined. In addition, an extensive comparison of the different countermeasures will be made, by investigating several aspects and features of the involved solutions. Finally, an analysis of the different countries Plasdan operates in, will be extracted and a number of solutions from a known Internet Security vendor will be introduced.

[1] The complete requirement document is included in Appendix A.

[2] Personal experience at my previous education can confirm this statement.

## 1.4 Methodology

Given the complex nature of this thesis research, I hope to offer a multidisciplinary and positional approach on the related aspects.

The methods used in this report, in order to extract information about the suitable solutions for Plasdan, concentrated mainly on interviews with the various users of the system, i.e. Plasdan's network. The interviews pointed out various aspects of usage, needs, problems and ideas by the employees of the company. At a second stage of the proposal of different solutions and as part of a Software Engineering approach to the problem[3], a requirement analysis was made in order to systemize the extracted needs of the company, give the opportunity to the involved persons to gain a first impression of the goals set and enable a healthy extraction of further propositions.

After the requirement document was approved, the gathering of literature and information material, concerning relevant issues, followed the cooperative work with the company's contact persons. A very big part of the research basis and the analysis of the problem was based on my own observations and experiences made while being in Portugal, at the company's headquarters. Those observations, in combination with weekly discussions with my supervisor, made it possible to get an all round vision and understanding of the problem and its perspectives.

The report is build up in such a way, which enables the reader to gain adequate information about the general issues concerning Internet Security, before the individual countermeasures and propositions are listed and analyzed. Due to this fact, the information provided in this master thesis can be applied to almost every structure of a company network and help companies which plan to deploy a security solution.

**Chapter 2** After this short introduction with the problem formulation and methodology of the master thesis, a detailed analysis of today's Internet Security is presented. Security threats, attacks and vulnerabilities of organizations, as well as the various methods and techniques used for attacks, are being described.

**Chapter 3** In this part of the thesis, a general Security Strategy is being analyzed. The methodology and the setup of such a strategy are being presented in details.

**Chapter 4** Security Planning is a crucial part of the individual steps of a Security Strategy. In this chapter the concepts of basic risk assessment and Security Planning are illustrated.

**Chapter 5** This chapter describes the Danish-Portuguese company Plasdan. The organizational aspects, as well as the current network architecture and configuration are being analyzed, in order to determine the weaknesses and the level of provided security.

**Chapter 6** Suitable solutions to Plasdan's network configuration are presented in this part of the report. The related technology aspects provide a scientific character to the thesis.

**Chapter 7** Advantages and disadvantages of the proposed solutions are outlined in this chapter. A comparison on several aspects helps in the choice of deployment.

**Chapter 8** Political and technological factors in the different countries Plasdan operates in, are a very important piece of information, when planning the deployment of an Internet Security solution. These factors are being described in this part of the report. In addition, solution packages from a known vendor are listed.

**Chapter 9** In the conclusion an overview of the thesis is presented, as well as my personal preference of a Security solution. Finally, further general guidelines and future work possibilities conclude this master thesis.

[3] Due to the fact that Plasdan plans to deploy eventually a security solution, a requirement analysis was done by following Ian Sommerville's book on Software Engineering [2]

# Chapter 2

# Internet Security

The Internet offers tremendous opportunities for businesses to change the way they work. Organizations, both large and small, are discovering ways to enhance profitability, improve customer loyalty, reach untapped markets and cut operating costs. To grasp these opportunities, companies need to take the Internet to heart and embed its functionality at the core of their operations.

Joining the Internet is just like joining any other community. If we are sensible, we will ensure that we have adequate protection in place to guard us against accidents and the less desirable elements of the Internet society. If we are not, a company faces a deleterious scenario: Let your guard down just once, or neglect to implement appropriate defense measures and you make your company vulnerable to attack. Lose focus on the process of protecting your online assets just once and you may be attacked. Fail to realize the value of your digital assets on an ongoing basis and you are leaving yourself open to attack and compromise.

Today, some businesses do not fully comprehend why they need a security protection system, or exactly what constitutes a good security policy. These same businesses also do not fully understand that security is about risk management, which must be factored in, when addressing their security requirements.

In the following sections of this chapter, some of the basic elements of Internet Security will be discussed, and a detailed insight to the risks and threats presented by online business operations will be given. Moreover, linking these theoretical approaches to some existing standards and security strategies, will backup this theoretical approach.

## 2.1 Defining Security

There is no such thing as perfect security. Every network or system that connects to the Internet is, to a greater or less extend, vulnerable. To benefit from the Internet, companies have to become a part of it. The question is, how far do they allow this integration to progress.

It is all a question of balance. On the one hand companies need to provide employees and partners with reasonable access to the information they need. On the other hand, they need to prevent unauthorized access to sensitive data. They want to encourage users to take advantage of valuable information on the Web, but they need to ensure that they are using the Internet to benefit the business, and that any sensitive information is protected from prying eyes.

This last statement is a very important aspect of the whole matter, because understanding the details of network attacks is a prerequisite for the design and implementation of secure systems.

Due to this fact the security threats and risks of being on-line will be outlined in the following section, as well as the methods, tools and techniques that intruders use to exploit vulnerabilities in systems, in order to achieve their goals.

## 2.2 Security Threats, Attacks and Vulnerabilities

Information is the key asset in most organizations. Companies gain a competitive advantage by knowing how to use that information. The threat comes from others who would like to acquire the information or limit business opportunities by interfering with normal business processes.

The object of security is to protect valuable or sensitive organizational information, while making it readily available. Attackers trying to harm a system or disrupt normal business operations, exploit vulnerabilities by using various techniques, methods and tools. Companies, in particular system administrators and security staff, need to understand the various aspects of security, to develop measures and policies to protect assets and limit their vulnerabilities.

### History

In the 1980s intruders were the system experts, as depicted in the following Figure. They had a high level of expertise and personally constructed methods for breaking into systems. Automated tools and exploit scripts were the exception rather than the rule.

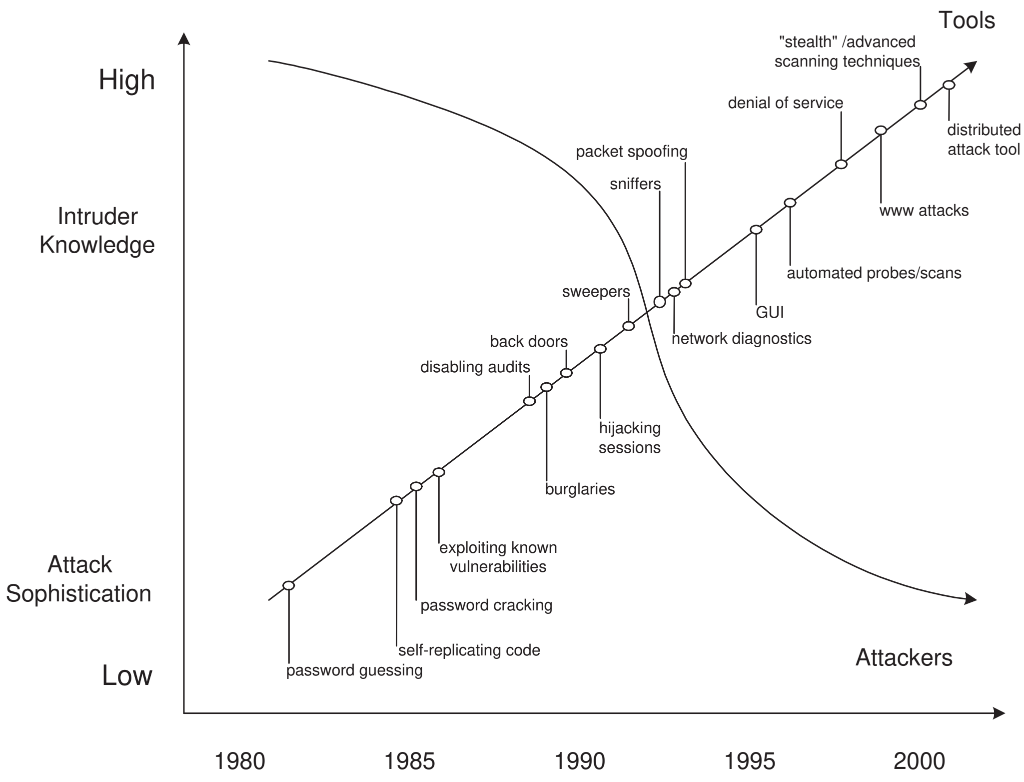



Figure 2.1: Attack Sophistication vs. Intruder Technical Knowledge

Today, absolutely anyone can attack a network due to the widespread and easy availability of intrusion tools and exploit scripts that can easily duplicate known methods of attack. While experienced intruders are getting smarter - as demonstrated by the increased sophistication in the types of attacks - the knowledge required on the part of novice intruders to copy and launch known methods of attack is decreasing. Meanwhile, as evidenced by distributed Denial-of-Service attacks and variants of the Love Letter Worm[1], the severity and scope of attack methods is increasing.

In the early to mid-1980s, intruders manually entering commands on their personal computers could access tens to hundreds of systems. Today, intruders use automated tools to access thousands to tens of thousands of systems. In the 1980s, it was relatively straightforward to determine if an intruder had penetrated your systems, and discover what they did. Today, intruders are able to totally hide their presence, for example, by disabling commonly used services and reinstalling their own versions, then erasing their tracks in audit and log files. In the 1980s and early 1990s, Denial-of-Service (DoS) attacks were infrequent and not considered serious. Today, for organizations such as Internet Service Providers (ISP's), that conduct business electronically, a successful Denial-of-Service attack, can put them out of business. Unfortunately, these types of attacks occur more frequently each year. [4]

Typical risks and attacks in a business environment fall into three categories:

**Confidentiality:** Information should be available only to those with appropriate access. Confidentiality protects therefore sensitive information from unauthorized disclosure or intelligible interception.

**Integrity:** Information should be modified only by people who are authorized to do so. Integrity ensures therefore that information or software is complete, accurate and authentic.

**Availability:** Information should be accessible only to those who need it. Availability ensures therefore that information and services are accessible and functional when needed. [5]

It is obvious that these risks translate into huge financial risks, when the above categories are compromised.[2] In the following section we will look at the individual security threats which can compromise these standard information security services, and examples of how confidentiality, integrity and availability are threatened, will be given.

### 2.2.1 Security Threats Layout

The next Figure introduces a layout that can be used to break up security threats into different areas: [6]

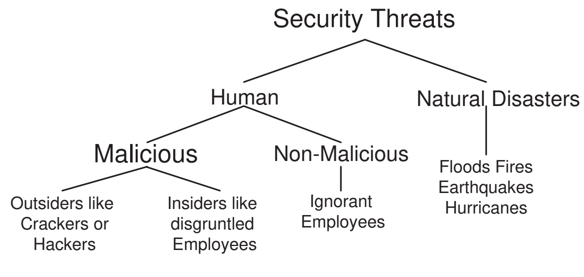



Figure 2.2: Security Threats layout

[1] http://www.cert.org/advisories/CA-2000-04.html [3]

[2] The 2002 Computer Crime and Security Survey reported that 44% of their respondents, who were willing and/or able to quantify their losses, reported $455.848.000 in financial losses. As in previous years, the most serious financial losses occurred through theft of proprietary information ($170,827,000) and financial fraud ($115,753,000). [1]

### Natural Disasters

Nobody can stop nature from taking its course. Earthquakes, hurricanes, floods, lightning, and fire can cause severe damage to computer systems. Information can be lost, downtime or loss of productivity can occur, and damage to hardware can disrupt other essential services. Few safeguards can be implemented against natural disasters. The best approach is to have disaster recovery plans and contingency plans in place.[3] Other threats such as riots, wars, and terrorist attacks could be included here. Although they are human-caused threats, they can be classified as disastrous.

### Human Threats

Malicious threats consist of inside attacks by disgruntled or malicious employees and outside attacks by non-employees, just looking to harm and disrupt an organization.

The most dangerous attackers are usually insiders (or former insiders), because they know many of the codes and security measures that are already in place. Insiders are likely to have specific goals and objectives, and have legitimate access to the system. Employees are the people most familiar with the organization's computers and applications, and they are most likely to know what actions might cause the most damage. Insiders can plant viruses, Trojan horses or worms, and they can browse through the file system.

The insider attack can affect all components of computer security. By browsing through a system, confidential information could be revealed. Trojan horses are a threat to both the integrity and confidentiality of information in the system. Insider attacks can affect availability by overloading the system's processing or storage capacity, or by causing the system to crash.

Malicious attackers normally will have a specific goal, objective, or motive for an attack on a system. These goals could be to disrupt services and the continuity of business operations by using Denial-of-Service (DoS) attack tools. They might also want to steal information or even steal hardware such as laptop computers. Hackers can sell information that can be useful to competitors.[4]

Attackers are not the only ones who can harm an organization. The primary threat to data integrity comes from authorized users, who are not aware of the actions they are performing. Errors and omissions can cause valuable data to be lost, damaged or altered. Non-malicious threats usually come from employees who are untrained in computers and are unaware of security threats and vulnerabilities.

Users, system operators and programmers frequently make unintentional errors that contribute to security problems, directly and indirectly. Sometimes the error is the threat, such as a data entry error or a programming error that crashes a system. In other cases, errors create vulnerabilities. Errors can occur in all phases of the system life cycle.[5]The table on the following page summarizes some examples of the various aspects discussed above.

It is important to keep in mind that ignorant employees usually have no motives and goals for causing damage. The damage is accidental. Also, malicious attackers can deceive ignorant employees by using "social engineering" to gain entry. The attacker could masquerade as an administrator and ask for passwords and user names. Employees who are not well trained and are not security aware can fall for this.

[3] A definition of a contingency plan and further information about the planning and implementation of such plans can be found in Chapter 3 Section 3.3

[4] In 1999, a laptop computer was stolen from an employee of Visa International that contained 314.000 credit card accounts. The total cost to Visa for just cancelling the numbers and replacing the cards was $6 million. [4]

[5] The term system life cycle (SLC) can be found in the glossary

| Threats | Motives/Goals | Methods | Security Policies |
|---|---|---|---|
| Employees | Deny services | Social engineering | Vulnerabilities |
| Malicious | Steal information | Viruses, Trojan horses, worms | Assets |
| Ignorant | Alter information | Packet replay | Information and data |
| Non-employees | Damage information | Packet modification | Productivity |
| Outside attackers | Delete information | IP spoofing | Hardware |
| Natural disasters | Make a joke | Mail bombing | Personnel |
| Floods | Show Off | Various hacking tools | |
| Earthquakes | | Password cracking | |
| Hurricanes | | | |
| Riots and wars | | | |

Table 2.1: Overview of Threats, Methods and Security Policies

### 2.2.2 Motives, Goals and Objectives of Malicious Attackers

There is a strong overlap between physical security and data privacy and integrity. Indeed, the goal of some attacks is not the physical destruction of the computer system, but the penetration and removal or copying of sensitive information. Attackers want to achieve these goals either for personal satisfaction or for a reward. [7]

Here are some methods that attackers use:

- Deleting and altering information. Malicious attackers who delete or alter information normally do this to prove a point or take revenge for something that has happened to them. Inside attackers normally do this to spite the organization because they are disgruntled about something. Outside attackers might want to do this to prove that they can get in to the system or for the fun of it.
- Committing information theft and fraud. Information technology is increasingly used to commit fraud and theft. Computer systems are exploited in numerous ways, both by automating traditional methods of fraud and by using new methods. Financial systems are not the only ones subject to fraud. Other targets are systems that control access to any resources, such as time and attendance systems, inventory systems, school grading systems, or long-distance telephone systems.
- Disrupting normal business operations. Attackers may want to disrupt normal business operations. In any circumstance like this, the attacker has a specific goal to achieve. Attackers use various methods for Denial-of-Service attacks; the following section on methods, tools, and techniques will discuss these.

### 2.2.3 Methods, Tools, and Techniques for Attacks

Malicious attackers can gain access or deny services in numerous ways. Here are some of them:

**Viruses.** Attackers can develop harmful code known as viruses. Using hacking techniques, they can break into systems and plant viruses. Viruses in general are a threat to any environment. They come in different forms and although not always malicious, they always take up time. Viruses can also be spread via e-mail and disks.

**Trojan horses.** These are malicious programs or software code hidden inside what looks like a normal program. When a user runs the normal program, the hidden code runs as well. It can then start deleting files and causing other damage to the computer. Trojan horses are normally spread by e-mail attachments. The Melissa virus that caused Denial-of-Service attacks throughout the world in 1999 was a type of Trojan horse.[6]

[6] http://www.cert.org/advisories/CA-1999-04.html

**Worms.** These are programs that run independently and travel from computer to computer across network connections. Worms may have portions of themselves running on many different computers. Worms do not change other programs, although they may carry other code that does.

**Password cracking.** This is a technique attackers use to surreptitiously gain system access through another user's account. This is possible because users often select weak passwords. The two major problems with passwords is when they are easy to guess based on knowledge of the user (for example, wife's maiden name) and when they are susceptible to dictionary attacks (that is, using a dictionary as the source of guesses).

**Denial-of-Service (Dos) attacks.** This attack exploits the need to have a service available. It is a growing trend on the Internet, because Web sites in general are open doors ready for abuse. People can easily flood the Web server with communication in order to keep it busy. Therefore, companies connected to the Internet should prepare for DoS attacks. They also are difficult to trace and allow other types of attacks to be subdued.

**E-mail hacking.** Electronic mail is one of the most popular features of the Internet. With access to Internet e-mail, someone can potentially correspond with any one of millions of people worldwide. Some of the threats associated with e-mail are:

- **Impersonation.** The sender address on Internet e-mail cannot be trusted, because the sender can create a false return address. Someone could have modified the header in transit, or the sender could have connected directly to the Simple Mail Transfer Protocol (SMTP) port on the target computer to enter the e-mail.
- **Mail Eavesdropping.** E-mail headers and contents are transmitted in clear text, if no encryption is used. As a result, the contents of a message can be read or altered in transit. The header can be modified to hide or change the sender, or to redirect the message.

**Packet replay.** This refers to the recording and retransmission of message packets in the network. Packet replay is a significant threat for programs that require authentication sequences, because an intruder could replay legitimate authentication sequence messages to gain access to a system. Packet replay is frequently undetectable, but can be prevented by using packet time stamping and packet sequence counting.

**Packet modification.** This involves one system intercepting and modifying a packet destined for another system. Packet information may not only be modified, it could also be destroyed.

**Eavesdropping.** This allows a cracker (hacker)[7]to make a complete copy of network activity. As a result, a cracker can obtain sensitive information such as passwords, data, and procedures for performing functions. It is possible for a cracker to eavesdrop by wiretapping, using radio or using auxiliary ports on terminals. It is also possible to eavesdrop using software that monitors packets sent over the network. In most cases, it is difficult to detect eavesdropping.

**Social engineering.** This is a common form of cracking. It can be used by outsiders and by people within an organization. Social engineering is a hacker term for tricking people into revealing their password or some form of security information.

**Intrusion attacks.** In these attacks, a hacker uses various hacking tools to gain access to systems. These can range from password-cracking tools to protocol hacking and manipulation tools. Intrusion detection tools often can help to detect changes and variants that take place within systems and networks.

**Network spoofing.** In network spoofing, a system presents itself to the network as though it were a different system (computer A impersonates computer B by sending B's address instead of its own). The reason for doing this is that systems tend to operate within a group of other trusted systems. Trust is imparted in a one-to-one fashion; computer A trusts computer B (this does not imply that system B trusts system A). Implied with this trust is that the system administrator of the trusted system is performing the job properly and maintaining

[7] Please refer to the glossary for a correct definition

an appropriate level of security for the system. Network spoofing occurs in the following manner: if computer A trusts computer B and computer C spoofs (impersonates) computer B, then computer C can gain otherwise-denied access to computer A.

### 2.2.4 Security Vulnerabilities

As explained previously, a malicious attacker uses a method to exploit vulnerabilities in order to achieve a goal. Vulnerabilities are weak points or loopholes in security that an attacker exploits in order to gain access to the network or to resources on the network. It is important to keep in mind that the vulnerability is not the attack itself, but rather the weak point that is exploited. Some of these weak points can be:

**Passwords.** Password selection will be a contentious point as long as users have to select one. The problem usually is remembering the correct password from among the multitude of passwords a user needs to remember. Users end up selecting commonly used passwords because they are easy to remember. Anything from birthdays to the names of loved ones. This is a vulnerability because it gives others a good chance to guess the correct password.

**Protocol design.** Communication protocols sometimes have weak points. Attackers use these to gain information and eventually gain access to systems. Some known issues occurred with the TCP/IP protocol stack which has some weak points that allow IP address spoofing and TCP connection request(SYN) attacks.

**Telnet protocol.** Telnet can be used to administer systems running Microsoft©Windows Operating systems and Unix. When using the Telnet client to connect from a Microsoft system to UNIX system and vice versa, user names and passwords are transmitted in clear text.

**File Transfer Protocol (FTP).** As with Telnet, if the FTP service is running and users need to send or retrieve information from a secure location, then user names and passwords are transmitted in clear text.

**Commands revealing user information.** It is not uncommon to find interoperability between Microsoft products and various versions of UNIX. Commands that reveal user and system information pose a threat, because crackers can use that information to break into a system. [8] Here are two ways:

- Finger. The finger client utility on Microsoft Windows NT and Windows 2000 can be used to connect to a finger daemon service running on a UNIX-based computer to display information about users. When the finger program is run with no arguments, information for every user currently logged on to the system is displayed.
- Rexec. The rexec utility is provided as a client on Microsoft Windows NT and Windows 2000. The rexec client utility allows remote execution on UNIX-based systems running the rexecd service. A client transmits a message specifying the user name, the password, and the name of a command to execute. The rexecd program is susceptible to abuse because it can be used to probe a system for the names of valid accounts. In addition, passwords are transmitted unencrypted over the network.

**Asynchronous transfer mode (ATM).** Security can be compromised by what is referred to as "manhole manipulation" - direct access to network cables and connections in underground parking garages and elevator shafts.

**Device administration.** Switches and routers are easily managed by an HTTP interface or through a command line interface. Coupled to the use of weak passwords (for example, public passwords), it allows anybody with some technical knowledge to take control of the device.

**Modems.** Modems have become standard features on many desktop computers. Any unauthorized modem is a serious security concern. People use them not just to connect to the Internet, but also to connect to their office so they can work from home. The problem is that a modem is a means of bypassing the "firewall" that protects a network from outside intruders. A hacker using a "war dialer" tool to identify the modem telephone number and a "password cracker" tool to break a weak password can gain access to the system. Due to the nature of computer networking, once a hacker connects to that one computer, the hacker can often connect to any other computer in the network.

Going into more depth about the different threats and risks of being online and the methods and tools attackers are using in order to access, harm and disrupt companies, will lead at this point too far. Therefore, there has been included some additional information in Appendix B.

# Chapter 3

# Security Strategies

## 3.1 Introduction

After the detailed description of the security threats, the different type of attacks and the vulnerabilities affecting on-line businesses and companies, the following section will focus on security strategies to protect the availability, integrity and confidentiality of data in an organization's Information Technology (IT) system.

The methodology that follows, will offer a systematic approach to the important task of establishing security policies. Security administrators need to decide how much time, money and effort needs to be spent in order to develop the appropriate security policies and controls. Each organization should analyze its specific needs and determine its resource and scheduling requirements and constraints. Computer systems, environments and organizational policies are different, making each computer security service and strategy unique. However, the principles of good security remain the same, and the following section about security strategies, focuses on those principles.

## 3.2 How to setup a Security Strategy

Although a security strategy can save the organization valuable time and provide important reminders of what needs to be done, security is not a one-time activity. It is an integral part of the system life cycle. The activities described in this section generally require either periodic updating or appropriate revision. These changes are made when configurations and other conditions and circumstances change significantly or when organizational regulations and policies require changes. This is an iterative process. It is never finished and should be revised and tested periodically. [9]

### Reviewing Current Policies

Establishing an effective set of security policies and controls requires using a strategy to determine the vulnerabilities that exist in computer systems and in the current security policies and controls that guard them. The current status of computer security policies can be determined by reviewing the list of documentation that follows. The review should take notice of areas where policies are lacking as well as examining existing documents:

- Physical computer security policies such as physical access controls.
- Network security policies (for example, e-mail and Internet policies).

- Data security policies (access control and integrity controls).
- Contingency and disaster recovery plans and tests. Computer security awareness and training.
- Computer security management and coordination policies.

Other documents that contain sensitive information such as:

- Computer BIOS passwords.
- Router configuration passwords.
- Access control documents.
- Other device management passwords.

### Identifying Assets and Vulnerabilities to Known Threats as well as likely Attack Methods, Tools and Techniques

Assessing an organization's security needs also includes determining its vulnerabilities to known threats. This assessment entails recognizing the types of assets that an organization has, which will suggest the types of threats it needs to protect itself against.

Listing the threats (and most organizations will have several) helps the security administrator to identify the various methods, tools and techniques that can be used in an attack. Methods can range from viruses and worms to password and e-mail cracking. It is important that administrators update their knowledge of this area on a continual basis, because new methods, tools, and techniques for circumventing security measures are constantly being devised.

### Establishing Proactive and Reactive Strategies

For each method, the security plan should include a proactive strategy as well as a reactive strategy. [9]

The proactive or pre-attack strategy is a set of steps that helps to minimize existing security policy vulnerabilities and develop contingency plans. Determining the damage that an attack will cause on a system and the weaknesses and vulnerabilities exploited during this attack helps in developing the proactive strategy.

The reactive strategy or post-attack strategy helps security personnel to assess the damage caused by the attack, repair the damage or implement the contingency plan developed in the proactive strategy, document and learn from the experience and get business functions running as soon as possible.

### Testing

The last element of a security strategy, testing and reviewing the test outcomes, is carried out after the reactive and proactive strategies have been put into place. Performing simulation attacks on a test or lab system makes it possible to assess where the various vulnerabilities exist and adjust security policies and controls accordingly.

These tests should not be performed on a live production system, because the outcome could be disastrous. Yet, the absence of labs and test computers due to budget restrictions might preclude simulating attacks. In order to secure the necessary funds for testing, it is important to make management aware of the risks and consequences of an attack, as well as the security measures that can be taken to protect the system, including testing procedures. If possible, all attack scenarios should be physically tested and documented to determine the best possible security policies and controls to be implemented.

Certain attacks, such as natural disasters, like floods and lightning cannot be tested, although a simulation will help. For example, a company could simulate a fire in the server room that has resulted in all the servers being damaged and lost. This scenario can be useful for testing the responsiveness of administrators and security personnel and for ascertaining how long it will take to get the organization functional again.

Testing and adjusting security policies and controls based on the test results is an iterative process. It is never finished and should be evaluated and revised periodically so that improvements can be implemented.

## 3.3 Methodology for Defining Security Strategies

The following section discusses a methodology for defining a computer security strategy that can be used to implement security policies and controls to minimize possible attacks and threats. The methods can be used for all types of attacks on computer systems, whether they are malicious, non-malicious or natural disasters, and can thus be re-used repeatedly for different attack scenarios. The methodology is based on the various types of threats, methods of attack and vulnerabilities discussed in the previous section on Security Threats. The following flow chart outlines the methodology. [10]

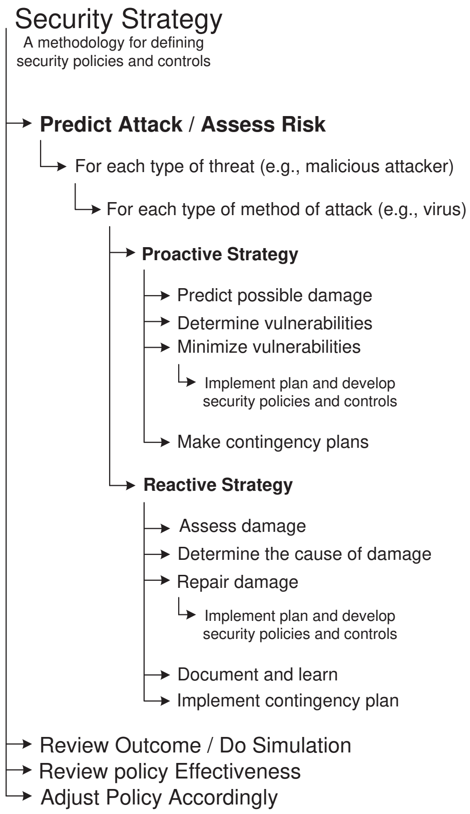



Figure 3.1: Security Strategy Flowchart

1. **Predict Possible Attacks / Analyze Risks**: The first phase of the methodology outlined in the above Flowchart is to determine the attacks that can be expected and ways of defending against these attacks. It is impossible to prepare against all attacks. Therefore, organizations should prepare for the most likely attacks that the organization can expect. It is always better to prevent or minimize attacks, than to repair the damage after an attack has already occurred.
   In order to minimize attacks it is necessary to understand the various threats that cause risks to systems, the corresponding techniques that can be used to compromise security controls, and the vulnerabilities that exist in the security policies. Understanding these three elements of attacks helps us to predict their occurrence, if not their timing or location. Predicting an attack is a matter of predicting its likelihood, which depends upon understanding its various aspects. The various aspects of an attack can be shown in the following equation:

   **Threats + Motives + Tools and Techniques + Vulnerabilities = Attack**

2. **For Each Type of Threat**: Consider all of the possible threats that cause attacks on systems. We saw a detailed description of the type of threats in the previous section. For these different types of threats, security personnel need to implement separate proactive and reactive strategies, following the guidelines in the above Flowchart.
3. **For Each Type of Method of Attack**: In order to launch an attack, a malicious attacker needs a method, tool or technique to exploit various vulnerabilities in systems, security policies and controls. A malicious attacker can use different methods to launch the same attack. Therefore, the defense strategy must be customized for each type of method used in each type of threat. Again, it is important that security professionals keep current on the various methods, tools and techniques used by attackers. A detailed discussion of these can be found in the previous chapter about Security Threats.
4. **Proactive Strategy**: The proactive strategy is a set of predefined steps that should be taken to prevent attacks before they occur. The steps include looking at how an attack could possibly affect or damage the computer system and the vulnerabilities it exploits. We saw this in the above steps 1 and 2. The knowledge gained in these assessments can help in implementing security policies that will control or minimize the attacks. These are the three steps of the proactive strategy:
   (a) Determine the damage that the attack will cause.
   (b) Determine the vulnerabilities and weaknesses that the attack will exploit.
   (c) Minimize the vulnerabilities and weaknesses that are determined to be weak points in the system for that specific type of attack.

   Following these steps to analyze each type of attack has a side benefit; a pattern will begin to emerge, because many factors will overlap for different attacks. This pattern can be helpful in determining the areas of vulnerability that pose the greatest risk to the enterprize. It is also necessary to take note of the cost of losing data versus the cost of implementing security controls. Weighing the risks and the costs are part of a system risk analysis and are discussed in the next chapter about Security Planning.
   Security policies and controls will not, in every case, be completely effective in eliminating attacks. For this reason it is necessary to develop contingency and recovery plans in the event that security controls are penetrated.
5. **Determine Possible Damage Resulting from an Attack**: Possible damages can range from minor computer glitches to catastrophic data loss. The damage caused to the system will depend on the type of attack. Organizations should use a test or lab environment to clarify the damages resulting from different types of attacks, if possible. This will enable security personnel to see the physical damage caused by an experimental attack.
6. **Determine the Vulnerabilities or Weaknesses That an Attack Can Exploit**: If the vulnerabilities that a specific attack exploits can be discovered, current security policies and controls can be altered or new ones implemented to minimize these vulnerabilities. Determin-

ing the type of attack, threat and method makes it easier to discover existing vulnerabilities. This can be proven by an actual test.

7. **Minimize Vulnerabilities and Weaknesses Exploited by a Possible Attack**: Minimizing the security system's vulnerabilities and weaknesses that were determined in the previous assessment is the first step in developing effective security policies and controls. This is the payoff of the proactive strategy. By minimizing vulnerabilities, security personnel can minimize both the likelihood of an attack, and its effectiveness, if one does occur. It is essential not to implement too stringent controls, because the availability of information could then become a problem. There must be a careful balance between security controls and access to information. Information should be as freely available as possible to authorized users.
8. **Make Contingency Plans**: A contingency plan is an alternative plan that should be developed in case an attack penetrates the system and damages data or any other assets with the result of halting normal business operations and hurting productivity. The plan is followed if the system cannot be restored in a timely manner. Its ultimate goal is to maintain the availability, integrity and confidentiality of data. It is the proverbial "Plan B."
   There should be a plan per type of attack and/or per type of threat. Each plan consists of a set of steps to be taken in the event that an attack breaks through the security policies. The contingency plan should:
   - Address who must do what, when and where to keep the organization functional.
   - Be rehearsed periodically to keep staff up-to-date with current contingency steps.
   - Cover restoring from backups.
   - Discuss updating virus software.
   - Cover moving production to another location or site.
9. **Reactive Strategy**: A reactive strategy is implemented when the proactive strategy for the attack has failed. The reactive strategy defines the steps that must be taken after or during an attack. It helps to identify the damage that was caused and the vulnerabilities that were exploited in the attack, determine why it took place, repair the damage that was caused by it, and implement a contingency plan if one exists. Both the reactive and proactive strategies work together to develop security policies and controls to minimize attacks and the damage caused during them.
   The incident response team[1] should be included in the steps taken during or after the attack to help assess it and to document and learn from the event.
10. **Assess the Damage**: Determine the damage that was caused during the attack. This should be done as swiftly as possible so that restore operations can begin. If it is not possible to assess the damage in a timely manner, a contingency plan should be implemented so that normal business operations and productivity can continue.
11. **Determine the Cause of the Damage**: To determine the cause of the damage it is necessary to understand what resources the attack was aimed at and what vulnerabilities were exploited to gain access or disrupt services. Review system logs, audit logs, and audit trails. These reviews often help in discovering where the attack originated in the system and what other resources were affected.
12. **Repair the Damage**: It is very important that the damage is repaired as quickly as possible in order to restore normal business operations and any data lost during the attack. The organization's disaster recovery plans and procedures should cover the restore strategy. The incident response team should also be available to handle the restore and recovery process and to provide guidance on the recovery process.
13. **Document and Learn**: It is important that once the attack has taken place, it is documented. Documentation should cover all aspects of the attack that are known, including: the damage that is caused (hardware, software, data loss, loss in productivity), the vulnerabilities

[1]The incident response team is involved in the proactive efforts of developing incident handling guidelines, identifying software tools for responding to incidents and conducting system attack studies

and weaknesses that were exploited during the attack, the amount of production time lost and the procedures taken to repair the damage. Documentation will help to modify proactive strategies for preventing future attacks or minimizing damages.

14. **Implement Contingency Plan**: If a contingency plan already exists, it can be implemented to save time and to keep business operations functioning correctly. If no contingency plan exists, organizations should develop an appropriate plan based on the documentation from the previous step.
15. **Review Outcome / Do Simulations**: The second major step in the security strategy is to review the findings established in the first step (Predicting the Attack). After the attack or after defending against it, organizations should review the attack's outcome with respect to the system. The review should include: loss in productivity, data or hardware loss and time taken to recover. Also, the attack should be documented and, if possible, tracked where it originated from, what methods were used to launch the attack and what vulnerabilities were exploited. Simulations in a test environment should be done to gain the best results.
16. **Review Policy Effectiveness**: If policies exist for defending against an attack that has taken place, they should be reviewed and checked for their effectiveness. If no policies exist, new ones must be drawn up to minimize or prevent future attacks.
17. **Adjust Policy Accordingly**: If the policy's effectiveness is not up to standard, the policy should be adjusted accordingly. Updates to policies must be coordinated by the relevant managerial personnel, security officer, administrators and the incident response team. All policies should comply with the organization's general rules and guidelines. For example working times might be from 8am to 6pm. A security policy could exist or be created that allows users to logon to the system only during these times.

In Chapter 5 the above methodology for establishing a security policy, will be partly implemented for the current network architecture and configuration at Plasdan. Certain parts of the Security Strategy Flowchart[2] will be visualized for a example scenario, in order to point out the importance of defining a Security Strategy.

[2] See Figure 3.1

# Chapter 4

# Security Planning

In the previous chapter we looked into detail on the development of strategies to protect availability, integrity and confidentiality of data in an Information Technology system. Before any of these strategies are able to be deployed, it is crucial to plan carefully the individual steps of the company's strategy. It is not possible to plan for security however, until a full risk assessment has been performed. Security Planning involves developing security policies and implementing controls to prevent computer risks from becoming reality.

## 4.1 Basic Risk Assessment

### Overview

Risk assessment is a very important part of computer security planning. No plan of action can be put into place before a risk assessment has been performed. The risk assessment provides a baseline for implementing security plans to protect assets against various threats. There are three basic questions one needs to ask in order to improve the security of a system: [11]

- What assets within the organization need protection?
- What are the risks to each of these assets?
- How much time, effort and money is the organization willing to spend to upgrade or obtain new adequate protection against these threats?

A company cannot protect its assets, if it doesn't know what to protect against. Computers need protection against risks, but what are risks? In simple terms, a risk is realized when a threat takes advantage of a vulnerability to cause harm to your system. After you know your risks, you can then create policies and plans to reduce those risks.

There are many ways to identify all the risks to a company's assets. One way is to gather personnel from within the organization and have a brainstorming session where everybody list the various assets and the risks to those assets. This will also help to increase security awareness within the organization.

Risks can come from three sources, like we saw in previous chapters: natural disaster risks, intentional risks, and unintentional risks. The following Figure illustrates these sources, by binding also the notion of assets to them:

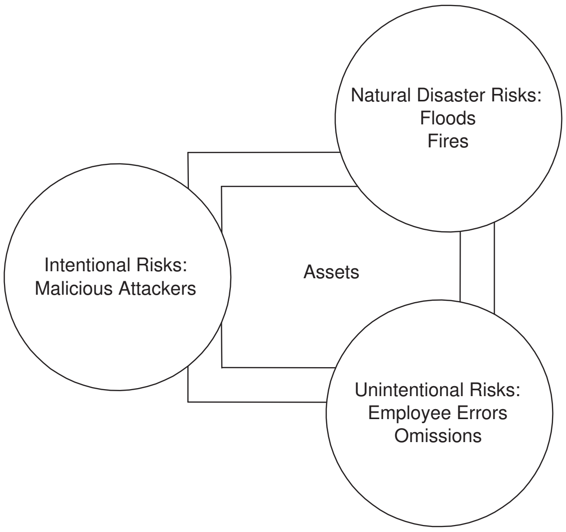



Figure 4.1: Risk Sources

We saw in the previous chapter a methodology to define security strategies. In the following section we will take a closer look at the first step of the security strategy, namely the risk assessment, which can be divided into further steps:

1. Identify the assets a you want to protect and the value of these assets.
2. Identify the risks to each asset.
3. Determine the category of the cause of the risk (natural disaster risk, intentional risk, or unintentional risk).
4. Identify the methods, tools or techniques the threats use.

Once these steps have been completed, it is possible to plan security policies and controls to minimize the realization of risks.

Companies are dynamic, and their security plan must be too. The risk assessment must be updated periodically. In addition, the risk assessment must be redone, whenever there has been a significant change in operation or structure. Thus, if the company reorganizes, moves to a new building, switches vendors, or undergoes other major changes, it should reassess the risks and potential losses.

## Identifying the Assets

One important step toward determining the risks to assets is performing an information asset inventory by identifying the various items that need to be protected within the organization. The inventory should be based on a business plan and the sensitivity of those items. Organizations should store the inventory online and categorize each item by its importance. The inventory should include everything that the organization would consider to be valuable. To determine if something is valuable, it has to be considered, what the loss or damage of the item might be in terms of lost revenue, lost time or the cost of repair or replacement. Some of the items that should be on the item inventory are:

- Physical items
  - Sensitive data and other information
  - Computers, laptops, palmtops, etc.
  - Backups and archives

  - Manuals, books, and guides
  - Communications equipment and wiring
  - Personnel records
  - Audit records
  - Commercial software distribution media
- Non-physical items
  - Personnel passwords
  - Public image and reputation
  - Processing availability and continuity of operations
  - Configuration information.
  - Data integrity
  - Confidentiality of information

For each asset, the following information should be defined:

- Type: hardware, software, data
- General support system or a critical application system
- Designated owner of the information
- Physical or logical location
- Inventory item number where applicable
- Service levels, warranties, key contacts, where it fits in to supplying availability and/or security and replacement process

### Identifying Risks to the Assets

After identifying the assets, it is necessary to determine all the risks that can affect each asset. One way of doing this is by identifying all the different ways an asset can be damaged, altered, stolen or destroyed.

In order to develop an effective information security policy, the information produced or processed during the risk analysis should be categorized according to its sensitivity to loss or disclosure. Most organizations use some set of information categories, such as Proprietary, For Internal Use Only, or Organization Sensitive. The categories used in the security policy should be consistent with any existing categories. Data should be broken into four sensitivity classifications with separate handling requirements: sensitive, confidential, private and public. This standard data sensitivity classification system should be used throughout the organization. These classifications are defined as follows: [12]

- Sensitive. This classification applies to information that needs protection from unauthorized modification or deletion to assure its integrity. It is information that requires a higher than normal assurance of accuracy and completeness. Examples of sensitive information include organizational financial transactions and regulatory actions.
- Confidential. This classification applies to the most sensitive business information that is intended strictly for use within the organization. Its unauthorized disclosure could seriously and adversely impact the organization, its stockholders, its business partners and/or its customers. Health care-related information should be considered at least confidential.
- Private. This classification applies to personal information that is intended for use within the organization. Its unauthorized disclosure could seriously and adversely impact the organization and/or its employees.
- Public. This classification applies to all other information that does not clearly fit into any of the above three classifications. While its unauthorized disclosure is against policy, it is not expected to impact seriously or adversely affect the organization, its employees and/or its customers.

After identifying the risks and the sensitivity of data, the likelihood of each risk occurring has to be estimated. Quantifying the threat of a risk is hard work. Some ways to estimate risk include:

- Obtaining estimates from third parties, such as insurance companies.
- Basing estimates on the company's records, if the event happens on a regular basis.
- Investigating collected statistics or published reports from industry organizations.

Once all the risks have been realized for each asset, it is necessary to identify whether the damage caused will be intentional or accidental.

As we saw also in the chapter about Security Strategies, after assessing the risks, the next step is to define a plan for proactive and reactive security planning.

In the flowchart that follows, it becomes clear that a company's security plan consists of security policies, which give specific guidelines for areas of responsibility.

Security Planning
- **For each type of Threat (e.g. Malicious Attacker**
  - **For each type of Method of Attack (e.g. Virus)**
    - **Proactive Planning**
      - Develop Security Policies and Controls
      - Implement Tools and Techniques to aid in security
        - Secure Access, Secure Date, Secure Code
        - Technologies to secure network connectivity
        - Detection Tools
      - Technologies to keep system running in the event of a failure
    - **Reactive Planning**
      - Contigency Plan

Figure 4.2: Security Planning Flowchart

Due to the fact that a big part of the proactive security planning is done in Chapter 7, where a variety of security solutions and technologies for Plasdan's current network are being presented, a detailed description of the individual steps of the above flowchart would be redundant. Therefore, and only in the interest of completeness, a brief description of the steps is being added.

1. **Developing Security Polices and Controls.** Policies can be defined for any area of security. There could be policies for the whole company, or policies for various sections within the company. The various types of policies that could be included are:
   - Password policies (Administrative responsibilities, User responsibilities)
   - E-mail policies
   - Internet policies
   - Backup and restore policies
2. **Tools and Techniques to Aid in Security.** There are various technologies, tools, and techniques to help aid in securing networks and computers:[1]
   - Secure Access, Secure Data, Secure Code (Public Key Infrastructures (PKI), Digital Signatures, Secure E-mail, Encryption File System, Authentication, etc.)

[1] Details on various of the technologies will be presented in Chapter 7

   - Technologies to Secure Network Connectivity (Firewalls, Packet Filtering Gateways, Application Gateways, Virtual Private Networks (VPN's), remote access, dial-in, etc.)
   - Detection Tools (Intrusion detection, virus detection, etc.)
3. **Technologies to keep the system running in the event of a failure.** Computers are not failure proof. Companies can only make computers more failure resistant. Faulty hardware, attackers, natural disasters, power failures, and errors from users can corrupt, damage or delete data from a system. There are several ways of preventing this from happening:
   - Spares
   - Disk Mirroring
   - Disk Striping
   - Cluster Servers
   - Standby Servers

To summarize, it must be stated that the policies and strategies outlined in the above sections are merely guidelines. It is important to keep in mind that each organization is different and needs to plan and create security policies based upon its individual security goals and needs.

## 4.2 Common Criteria

Chapter 3 and 4 included a methodology on how to analyze a company's Information Technology (IT) system and how to setup a security strategy and policies, in order to protect standard information security services.

Due to the fact that the application of this methodology is different for every organization, like mentioned at the end of the previous section, security agencies and centers around the world proposed the standardization of such a security evaluation scheme, in order to be recognized internationally. This proposal was made reality in late 1998, where the United States and other national governments adopted a security evaluation scheme called the Common Criteria (CC).[2] Because the Common Criteria are an international standard[3], IT evaluation results will be meaningful to a much wider audience and valid on an international level. In this way they can provide a standard basis for evaluation of security properties and permit compatibility between the results of independent security evaluations.

### 4.2.1 Security Evaluation Scheme

Under the Common Criteria, classes of products are evaluated against the requirements of "Protection Profiles" (PP) that specify security functional requirements. Protection Profiles may be developed to apply to Operating Systems (OS), firewalls, smart cards or any other product that can be expected to meet security requirements. The Common Criteria specify a series of Evaluation Assurance Levels (EAL's) for evaluated products. A higher EAL specifies a higher level of confidence that a product's security functions will be performed correctly and effectively.

Going into a more detailed analysis of the Common Criteria Security Evaluation Scheme would go beyond the scope of this thesis.[4] Nevertheless, it becomes obvious that the general methodology presented in the previous sections, is not just some simple guideline, but is actually a standardized procedure for evaluating security properties. Plasdan, or any other company which is planning to

[2] Before the CC other computer system security evaluations existed, like the Trusted Computer Systems Evaluation Criteria (TCSEC), or the Information Technology Security Evaluation Criteria (ITSEC), processes which have been replaced now by the Common Criteria

[3] ISO/IEC 15408 [13]

[4] For more information about specific Common Criteria evaluation activities refer to the National Computer Security Center (NCSC) Web site [14]

develop or use a product related to security, can profit substantially by applying this standard. Personally I believe that in the future the Common Criteria will not only be a basis for evaluating single or classes of products, but also entire businesses that are expected to meet certain security requirements. Today's most wanted and used security products are the ones providing the highest Evaluation Assurance Levels. I am confident that the same thing will be the case when choosing business partners or evaluating entire companies.[5] It becomes clear that the incorporation of standards in a company's security planning should have a very high priority.

In the next chapter, based on the theoretical approach and methodology presented in the previous two chapters, an analysis of Plasdan's network configuration will be done. This analysis will be very helpful, when solutions and related technologies which are best suited to Plasdan's security needs, will be extracted.

[5] Maybe it is already happening.

# Chapter 5

# Plasdan Lda

In this chapter the organization of the Danish-Portuguese company Plasdan will be described and the current network architecture and configuration analyzed. The methodology for conducting a Security Strategy and Planning[1] will be the basis for the analysis.

Due to the fact that the full scale development of security policies and controls for Plasdan, is not the goal of this thesis, the analysis will concentrate mainly on the risk assessment and the extraction of possible solutions for the purpose of secure interconnection of the company's branches. The risk management at the end of the chapter is done only on a theoretical level, in order to point out the importance of such, to the entire process of planning the deployment of a security solution.

## 5.1 Organization

In the following figure Plasdan's organizational structure is being presented:

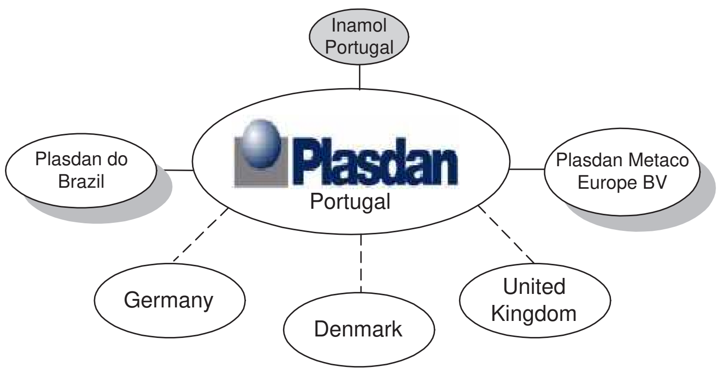



Figure 5.1: Plasdan's Organization

Plasdan is an international mould engineering company with a series of branches, cooperative agents and customers around Europe and in Brazil. The main headquarters are located in Portugal, where Inamol,[2] a mouldmaking company was acquired some years ago. Apart from Portugal, there

[1]Please refer to Figures 3.1 and 4.2
[2]www.inamol.pt

are two other physical locations present, namely Plasdan do Brazil in São Paulo Brazil and Plasdan-Metaco Europe BV in Reuver Netherlands.[3] The dotted lines in the figure represent future branch locations, or cooperative agents in the presented countries. A branch office in Denmark is already in the phase of being setup and is almost available.

A part of Plasdan's philosophy is the existence of modern communication technologies, for achieving the best possible results when leading such an international organization. Therefore, Plasdan is planning to interconnect the various branches, customers and agents around the globe, in order to enable the best service possible, by exchanging information efficiently, effectively and most important securely between the different locations.

As mentioned in the Methodology section of the Introduction, the company's analysis started by producing a requirement document. The document is included in Appendix A, where the purposes of expanding the existing network and interconnecting the individual branches are being described. In the following section, this existing computer network, at Plasdan's headquarters in Portugal is being analyzed.

## 5.2 Network Architecture Analysis

The computer network has the following layout:

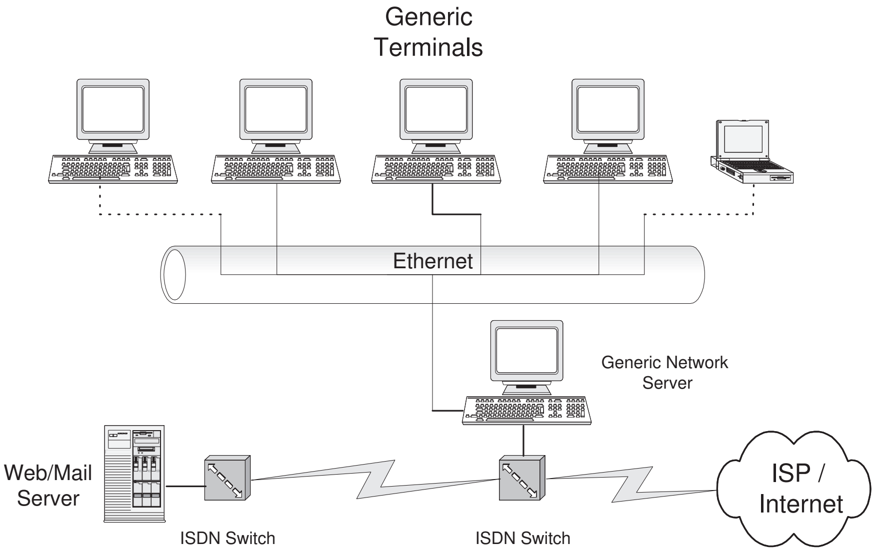



Figure 5.2: Plasdan's Network Diagram

At the current point, Plasdan connects to the Internet through a Integrated Services Digital Network (ISDN) which was acquired at the local Internet Service Provider (ISP). For technological reasons, Sitework,[4] an Internet company in a nearby city[5] was bought by Plasdan to host the company's Web and Mail Server. Apart from that, Sitework deals with other projects, independent from Plasdan, in the area of Web design, multimedia and Internet applications. Plasdan's

[3]http://www.tref.nl/bbrt/metaco
[4]www.sitework.pt Unfortunately only available in Portuguese.
[5]Sitework is located around 10 km from Plasdan's headquarters.

internal network is a LAN (Local Area Network) and is being administrated by a generic network server. Apart from that there exist several Terminals (Workstations and Laptops) for the individual departments, as part of the stub domain. The stub domain uses unregistered IP addresses. The current operating system running on most of the machines is Microsoft©Windows 2000. The company is planning at the moment to obtain a file server.

### Risk Assessment

The basic methodology of risk assessment has been described in section 4.1. In order to be able to plan security policies and controls to minimize the realization of risks in the company, this particular methodology has to be followed. A complete identification of Plasdan's assets, the related risks and the methods used to take advantage of vulnerabilities, is due to time restrictions, not possible.[6] Therefore, I have chosen to focus on my personal observations during my visit at Plasdan's headquarters, by looking at the daily activities of the employees when using the Internet and the current security implementations and measures implemented at the company. In this way at least some of the important assets and risks can be identified.

As stated in the requirement document, Plasdan's employees are using the Internet mainly for gathering work related information, e-mails and file transfer. The CAD-department uses the Internet daily as a medium for exchanging CAD/CAM files of various sizes, between the individual branches or with customers. On the other hand the mould division receives projects, drawings and customer related information by mail and sends out offers, prizing material and other valuable information about prototypes, moulds and tools. It becomes clear that Plasdan uses valuable assets daily at their business relations and that this kind of information needs to be protected.

At my visit in Portugal, in order to gain an insight on the various aspects related to the company's network architecture and security configuration, I was rather surprised to find out, that Plasdan did not have any security policy or control at all in place. It became clear that identifying risks to the above described assets, would actually involve most of the threats and vulnerabilities pointed out in chapter 3. In order to illustrate the use of the introduced methodology for Security Strategies and Planning[7] and to visualize how the risk analysis looks, a possible scenario has been chosen that can affect Plasdan's network at any time.

**Scenario (Malicious Threat (Outside Attacker)):** A cracker is contacted by the competition of Plasdan and is offered a large amount of money to find information on Plasdan's prizes for their latest Multi-Component Moulding Systems. The cracker uses E-mail hacking in order to eavesdrop on the e-mails send out from Plasdan's Moulding Division. He succeeds in reading the contents of a mail sent out to one of Plasdan's exclusive customers. Plasdan loses the deal, because the competitors offered the project cheaper.

The individual steps for the security strategy for the above example are:

1. **Predict Attack:** Information can be stolen by eavesdropping on mails sent by employees
2. **For each type of Threat:** Malicious Attacker from the outside
3. **For each type of method of Attack:** E-mail hacking
4. **Proactive Strategy:**
   (a) **Predict possible damage:** If sensitive and valuable information is stolen, there is a loss in profits
   (b) **Determine Vulnerabilities:** No encryption is used with the current mail client. No mail encryption protocols

[6] My one visit at the company's headquarters was not enough to conduct a full scale risk assessment
[7] Please refer to Figure 3.1 and 4.2

   (c) **Minimize Vulnerabilities:** Implement an mail protection protocol
5. **Reactive Strategy:**
   (a) **Assess Damage:** Loss of profits and sensitive information
   (b) **Determine the cause of damage:** Mail content was revealed due to lack of encryption
   (c) **Repair damage:** Implement a mail encryption protocol to the current mail application
6. **Review Outcome:** Sensitive information could be stolen, because the mail application had no encryption protocol, which would result in a loss of income
7. **Review Policy Effectiveness:** Review implementation of an encryption protocol
8. **Adjust Policy Accordingly:** ... (Cannot be specified yet)

The above example shows only one case of possible scenarios that could occur. Security policies should be defined for all valuable assets and risks present. It might seem at this point rather useless to define a policy for each and every type of asset and risk, but it is important to keep in mind that by having a security policy in place, a written set of steps and rules exists, which defines when, how, and by whom the steps and rules are implemented. The organization's policy is the way for emphasizing the management's commitment to computer security and making clear their expectations for employee performance, behavior and accountability.

After having the company's security policies and controls in place the next step would be to implement tools and techniques to aid in security.[8] The possible security solutions and tools which could be deployed by Plasdan are being described in the next chapter. Before investigating these solutions and the technologies involved, a last, very important aspect has to be investigated, namely risk management.

## 5.3 Risk Management

The formal, quantitative risk assessment, like we saw it in the previous section, is the foundation and starting point of a much wider defined term in the area of Internet Security, namely Risk Management. [15] The risk management process does not only determine what kind of controls are needed to protect an organization's information systems adequately, but most importantly also cost-effectively. In other words the risk management process uses the risk assessment process, analyzes the cost associated with it and correlates this information to determine feasibility.

It becomes very clear, that this kind of information, demands an analysis at a very high level which was, due to time limitations, not possible at this point. It is however important to mention, even theoretically, how the process of risk management makes this kind of financial analysis:

The information obtained by the vulnerability assessment, along with relevant threat data and asset information[9] is being combined to a cost benefit analysis for the system under review. The result of the cost benefit analysis will be then to create a so called Return on Investment (RoI) ratio, balancing the value of information against the cost of controls to protect it. By establishing RoI data, managers and directors can make more informed decisions regarding which controls to implement, based on the current threat exposure of the organization.[10]

Although it was not possible for me to apply this approach to Plasdan's company in practice, it is clear that risk management is becoming an increasingly important tool in corporate management strategies, and that every company should take this in consideration.

[8]According to Figure 4.2, this is the second step of proactive planning.

[9]Such information could be, present day replacement values, criticality, integrity and availability of the information contained in the system, etc.

[10]The big emphasis on the need for risk management is causing heightened interest in actually automating the risk management process with the help of risk analysis tool.

# Chapter 6

# Analysis of possible solutions and technologies

As shown in the previous chapters, the technology involved when planning or implementing a successful security solution for a company, is just a small part of the entire process.[1] We saw that a security policy, as well as the cooperation and security sensitiveness of the employees are equally important. It is crucial however, that the chosen solution, independently of being hardware or software, delivers the right balance of cost, functionality, and ease of access. In the following sections such security solutions and the involved technologies will be presented and analyzed.

In order to present the individual proposals in a systemized order, the seven-layered Open Systems Interconnection (OSI) reference model is being used. According to the International Organization for Standardization (ISO)[2] the layers in which no particular security services can be provided are the Session and Presentation Layer. Therefore, only the other layers will be taken into consideration. Apart from security implementations at the individual layers, the last two sections of this chapter include security solutions which could be implemented independently.[3]

Before starting with the investigation of the individual solutions and their involved technologies it is important to mention, that it is not recommended to deploy any of the presented major security solutions or technologies, without having an associated security policy in place.

## 6.1 Application Layer Security

Application layer security provides end-to-end security from an application running on one host through the network to the application on another host. This type of security does not care about the underlying transport mechanism. Complete coverage of security requirements, integrity, confidentiality and non-repudiation, can be provided at this layer. Applications have a fine granularity of control over the nature and content of the transactions. However, application layer security is not a general solution, because each application and client must be adapted to provide the security services. Several examples of application security extensions are given below:

[1] Figure 4.2 step 2

[2] International Standard ISO 7498-2 First edition 1989-02-15 [16]

[3] The usage of cryptography and authentication is possible at several layers

### 6.1.1 E-Mail Applications

#### Pretty Good Privacy (PGP)

Phil Zimmerman created PGP in 1991.[4] It is widely used by individuals worldwide for privacy and digital signing of email messages. PGP provides end-to-end security from the sender to the receiver. It can also be used to encrypt files. PGP has traditionally used Rivest-Shamir-Adleman (RSA) public key cryptography to exchange keys and the International Data Encryption Algorithm (IDEA) to encrypt messages.

PGP uses a web of trust or network trust model, where any users can vouch for the identity of other users. Getting the public keys of the intended person can be difficult to achieve in a secure manner. For example somebode can get a person's public key directly from that person and then communicate the hash of the key in an out-of-band pathway. Keys are stored in files called key rings. There are some servers on the Internet with public key rings. These servers do not authenticate the keys, but merely store them. It is important not to trust keys that have an unknown heritage.

#### S/MIME

S/MIME is a specification for secure electronic mail. S/MIME stands for Secure/Multipurpose Internet Mail Extensions and was designed to add security to e-mail messages in MIME format. [18] The security services offered are authentication (using digital signatures) and privacy (using encryption).

There is a growing demand for e-mail security. S/MIME melds proven cryptographic constructs with standard e-mail practices. More importantly, it was designed to be interoperable, so that any two packages that implement S/MIME can communicate securely.

The S/MIME specification consists of two documents:

- S/MIME Message Specification
- S/MIME Certificate Handling

Both of these are Internet Drafts. The S/MIME community has submitted these to the The Internet Engineering Task Force (IETF). The goal is to form a working group and produce an Internet standard.

#### Privacy Enhanced Email (PEM)

PEM is an electronic mail application which provides confidentiality, authentication and message integrity using various encryption methods. [19]

PEM is the outgrowth of work by the Privacy and Security Research Group (PSRG) of the Internet Research Task Force (IRTF). At the heart of PEM is a set of procedures for transforming RFC 822[5] messages in such a fashion as to provide integrity, data origin authenticity, and, optionally, confidentiality. PEM may be employed with either symmetric or asymmetric cryptographic key distribution mechanisms. Because the asymmetric (public-key) mechanisms are better suited to the large scale, heterogeneously administered environment characteristic of the Internet, only those mechanisms have been standardized. The standard form adopted by PEM is largely a profile of the CCITT X.509 (Directory Authentication Framework) recommendation. PEM is defined by a series of documents. These documents have been issued as RFCs and as Internet-Drafts.

[4] http://www.pgpi.org/ [17]

[5] Standard for the format of ARPA Internet Text Messages

### 6.1.2 S-HTTP

S-HTTP is not widely used, but it was designed to provide security for web-based applications. Secure HTTP is a secure message-oriented communications protocol and can transmit individual messages securely. It provides transaction confidentiality, authentication and message integrity. It extends HTTP to include tags for encrypted and secure transactions. S-HTTP is implemented in some commercial web servers and most browsers. The S-HTTP server negotiates with the client for the type of encryption that will be used. Transactions can involve several types of encryption between a particular server and client.

S-HTTP does not require clients to have public key certificates, because it can use symmetric keys to provide private transactions. The symmetric keys would be provided in advance using out of band communication.

### 6.1.3 Secure Shell (SSH)

Secure shell protocol is specified in a set of Internet draft documents. SSH provides secure remote login and other secure network services over an insecure network. SSH is being promoted free to colleges and universities, as a means for reducing cleartext passwords on networks. SSH version 2 is completely rewritten to use different security protocols and has added public key cryptography. [20]

The SSH protocol provides channels for establishing secure, interactive shell sessions and tunnelling other TCP applications. There are three major components to SSH:

- Transport layer protocol provides authentication, confidentiality and integrity for the server. It can also compress the data stream. The SSH transport runs on top of TCP. The transport protocol negotiates key exchange method, public key, symmetric encryption, authentication and hash algorithms.
- User authentication protocol authenticates the user-level client to the server and runs on top of SSH transport layer. It assumes that the transport layer provides integrity and confidentiality. The method of authentication is negotiated between the server and the client.
- Connection protocol multiplexes an encrypted tunnel into several channels. It is run on top of SSH transport and authentication protocols. The two ends negotiate the channel, window size and type of data. The connection protocol can tunnel X11 or any arbitrary TCP port traffic.

There are several authentication methods that can be used with SSH:[6]

| | Windows Client | Windows Server | Unix Client/Server |
|---|---|---|---|
| Password | Yes | Yes | Yes |
| Public Key | Yes | Yes | Yes |
| PKI | Yes | Yes | Yes |
| Smart Cards | Yes | N/A | Yes |
| Host-based | N/A | N/A | Yes |
| Kerberos | N/A | N/A | Yes |
| PAM | Yes | Yes | Yes |
| SecureID | Yes | Yes | Yes |
| Keyboard Interactive | Yes | Yes | Yes |

Table 6.1: Supported authentication methods in Secure Shell

[6] An analysis of the authentication methods listed here is provided at the end of this chapter

### 6.1.4 Firewalls

#### Application Level Firewall

A proxy server or firewall (sometimes referred to as an application gateway) is an application that intercepts traffic flowing between a protected network and the Internet. Proxies prevent traffic from passing directly between networks and are often used instead of router-based traffic controls. These sophisticated devices work at the application layer. They can also implement protocol specific security such as passing incoming FTP and blocking outgoing FTP.

This type of device deals with user level commands. They provide a much higher level of intelligence making it easier to implement the security policy. Configuring the system to only allow Web requests from the purchasing department between 8 AM and 6 PM is an example of such an configuration. The servers perform elaborate logging and auditing of the traffic passing through them. The trade-off for this functionality tends to be speed as well as increased complexity when adding new applications.

## 6.2 Transport Layer Security

Transport layer security is directed at providing process-to-process security between hosts. Most schemes are designed for TCP to provide reliable, connection-oriented communication. Many transport layer security mechanisms require changes in applications to access the security benefits. The secure applications are replacements for standard unsecure applications and use different ports.

### 6.2.1 Secure Sockets Layer (SSL) and Transport Layer Security (TLS)

SSL was designed by Netscape and is widely used on the Internet for web transactions such as sending credit card data. SSL can also be utilized for other protocols such as telnet, ftp, ldap, imap, and smtp, but these are not commonly used. TLS is an open, IETF proposed standard based on SSL 3.0. RFCs 2246, 2712, 2817, and 2818 define TLS. The two protocols are not interoperable, but TLS has the capability to drop down into SSL 3.0 mode for backwards compatibility. SSL and TLS provide security for a single TCP session. [21]

SSL and TLS provide a connection between a client and a server, over which any amount of data can be sent securely. Server and browser must be SSL or TLS enabled to facilitate secure web connections. Applications must be SSL or TLS enabled to allow their use of the secure connection.

For the browser and server to communicate securely, each needs to have the shared session key. SSL/TLS use public key encryption to exchange session keys during communication initialization. When a browser is installed on a workstation, it generates a unique private/public key pair.

The Figure on the following page shows the relative location in the protocol stack of the SSL and TLS protocols.

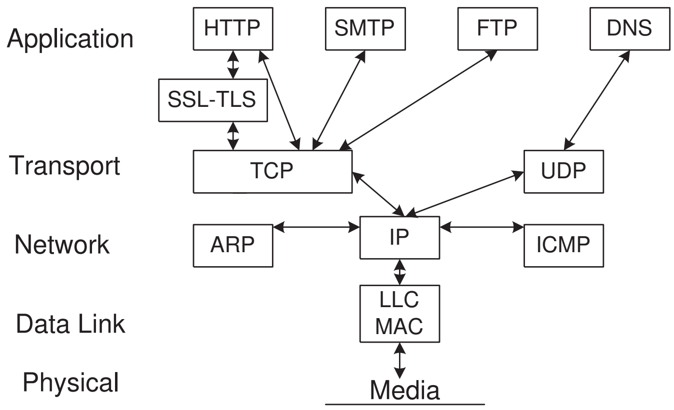



Figure 6.1: The Secure Socket Layer

### 6.2.2 Packet Filtering

#### Stateful Inspection and Stateful Filtering

A firewall of this type analyzes individual data packets as they pass through the gateway. In addition to the packet header, stateful inspection will also assess the packet's payload and look at the application protocol.

Most importantly, stateful inspection tracks information about past packets and builds a context for each data stream in memory. Only the first packet in a connection needs to be compared to the set of rules. All subsequent packets can pass quickly through the firewall. Packet filters can be implemented on routers and layer 3 devices to control the packets that will be blocked or forwarded at each interface. Routing decisions about whether to forward or drop the packet are made based on the rules in the access list. Standard access lists cannot filter on transport layer information. Only extended access lists can specify a protocol, and a parameter related to that protocol. TCP filtering options include established connections, port numbers or ranges of port numbers, and type of service values. UDP filter options only specify port numbers, since it is not a connection-oriented protocol.

## 6.3 Network Layer Security

Network layer security can be applied to secure traffic for all applications or transport protocols in the above layers. Applications do not need to be modified since they communicate with the transport layer above.

### 6.3.1 Internet Protocol Security (IPSec)

#### Introducing IPSec

The IP Security (IPSec) Protocol is a standardsbased method of providing privacy, integrity and authenticity to information transferred across IP networks and is the long term direction for secure networking. It provides a key line of defense against private network and Internet attacks, balancing ease of use with security. The goal of IPSec is to address all of the threats in the network infrastructure itself, which were pointed out thoroughly in previous chapters, without requiring expensive host and application modifications. This goal is met through the use of cryptography-based protection services, security protocols and dynamic key management. This foundation provides both the strength and flexibility to protect communications between private network computers, domain sites, remote sites, extranets, and dial-up clients. It can even be used to block receipt or transmission of specific traffic types. [22]

IPSec is based on an end-to-end security model, meaning that the only computers that must know about the traffic being secured, are the sending and receiving computers. Each handles security at its respective end, with the assumption that the medium over which the communication takes place is not secure. Any computers that only route data from source to destination are not required to support IPSec. This feature allows IPSec to be successfully deployed for most of the existing enterprize scenarios, like:

- Local area network (LAN): client/server, peer to peer.
- Wide area network (WAN): router to router, gateway to gateway.
- Remote access: dial-up clients; Internet access from private networks.

### IPSec Protocol Types

IPSec protocols provide data and identity protection services for each IP packet by adding their own security protocol header to each IP packet.

### Authentication Header

Authentication Header (AH) provides authentication, integrity, and anti-replay for the entire packet (both the IP header and the data payload carried in the packet). It does not provide confidentiality, which means it does not encrypt the data. The data is readable, but protected from modification. AH uses the Hash message authentication code (HMAC) algorithms[7] to sign the packet for integrity.

For example, Alice on Computer A sends data to Bob on Computer B. The IP header, the AH header, and the data are protected with integrity. This means Alice can be certain it was really Bob who sent the data and that the data was unmodified.

Integrity and authentication are provided by the placement of the AH header between the IP header and the transport (layer 4) protocol header, which is shown as TCP/UDP in the following Figure. AH uses an IP protocol ID of 51 to identify itself in the IP header.

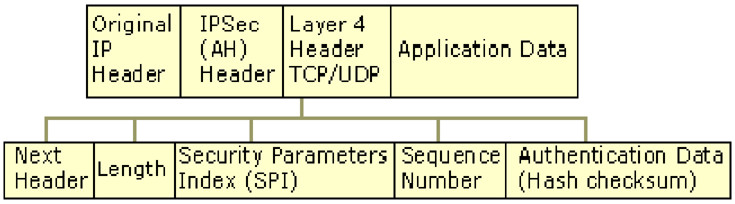



Figure 6.2: Authentication Header

AH can be used alone or in combination with the Encapsulating Security Payload (ESP) protocol.[8]

The AH header contains the following fields:

[7]Please refer to Appendix D for further information
[8]Please refer further down for more information.

- **Next Header** Identifies the next header that uses the IP protocol ID. For example, the value might be "6" to indicate TCP.
- **Length** Indicates the length of the AH header.
- **Security Parameters Index (SPI)** Used in combination with the destination address and the security protocol (AH or ESP) to identify the correct security association (SA) for the communication. The receiver uses this value to determine with which security association this packet is identified.
- **Sequence Number** Provides anti-replay protection for the SA. It is 32-bit, incrementally increasing number (starting from 1) that is never allowed to cycle and that indicates the packet number sent over the security association for the communication. The receiver checks this field to verify that a packet for a security association with this number has not been received already. If one has been received, the packet is rejected.
- **Authentication Data** Contains the Integrity Check Value (ICV) that is used to verify the integrity of the message. The receiver calculates the hash value and checks it against this value (calculated by the sender) to verify integrity.

## Packet Signature

AH is inserted after the IP header and before an upper layer protocol such as TCP, UDP, or ICMP. If another security protocol is being used in addition to AH, the AH header is inserted before any other IPSec headers. The packet signature is shown graphically in the following Figure.

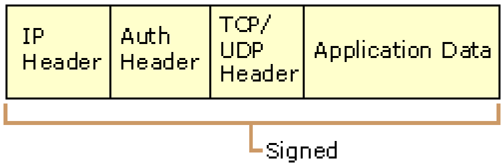



Figure 6.3: AH Integrity Signature

AH signs the entire packet for integrity, except certain fields in the IP header which may change such as the Time To Live and Type of Service fields.

## Encapsulating Security Payload

Encapsulating Security Payload (ESP) provides confidentiality, in addition to authentication, integrity and anti-replay. ESP can be used alone, or in combination with AH.

ESP does not normally sign the entire packet unless it is being tunnelled ordinarily. Just the IP data payload is protected, not the IP header.

For example, Alice on Computer A sends data to Bob on Computer B. The data payload is encrypted and signed for integrity. Upon receipt, after the integrity verification process is complete, the data payload in the packet is decrypted. Bob can be certain it was really Alice who sent the data, that the data is unmodified, and that no one else was able to read it.

ESP indicates itself in the IP header using the IP protocol ID of 50. As shown in the following Figure, the ESP header is placed prior to the transport layer header (TCP or UDP) or the IP payload data for other IP protocol types.

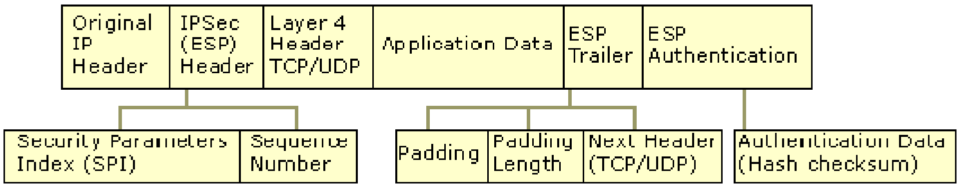



Figure 6.4: ESP

The ESP header contains the following fields:

- **Security Parameters Index** Identifies, when used in combination with the destination address and the security protocol (AH or ESP), the correct security association for the communication. The receiver uses this value to determine the security association with which this packet should be identified.
- **Sequence Number** Provides anti-replay protection for the SA. It is 32-bit, incrementally increasing number (starting from 1) that indicates the packet number sent over the security association for the communication. The sequence number is never allowed to cycle. The receiver checks this field to verify that a packet for a security association with this number has not been received already. If one has been received, the packet is rejected.

The ESP trailer contains the following fields:

- **Padding** 0 to 255 bytes is used for 32-bit alignment and with the block size of the block cipher.
- **Padding Length** Indicates the length of the Padding field in bytes. This field is used by the receiver to discard the Padding field.
- **Next Header** Identifies the nature of the payload, such as TCP or UDP.

The ESP Authentication Trailer contains the following field:

- **Authentication Data** Contains the Integrity Check Value (ICV), and a message authentication code that is used to verify the sender's identity and message integrity. The ICV is calculated over the ESP header, the payload data and the ESP trailer.

## Packet Signature and Encryption

As shown in the next Figure, ESP provides protection for upper layer protocols. The Signed area indicates where the packet has been signed for integrity. The Encrypted area indicates what information is protected with confidentiality.

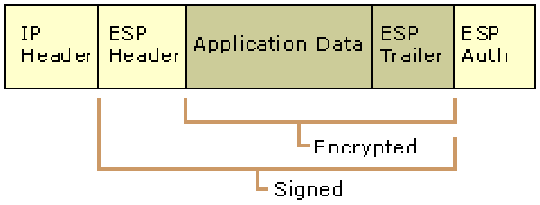



Figure 6.5: ESP: Signature and Encryption

ESP is inserted after the IP header and before an upper layer protocol, such as TCP, UDP, or ICMP, or before any other IPSec headers that have already been inserted. Everything following ESP (the upper layer protocol, the data, and the ESP trailer) is signed. The IP header is not signed, and therefore not necessarily protected from modification. The upper layer protocol information, the data, and the ESP trailer are encrypted.

### Tunnelling

Tunnelling is also referred to as encapsulation because the original packet is hidden or encapsulated inside of a new packet. A tunnel is the logical data path through which the encapsulated packets travel to their destination.[9]

### ESP Tunnel Mode

As shown in the following Figure, when in tunnel mode the inner IP header (the original packet header) carries the ultimate source and destination addresses, and the outer IP header might contain addresses of security gateways.

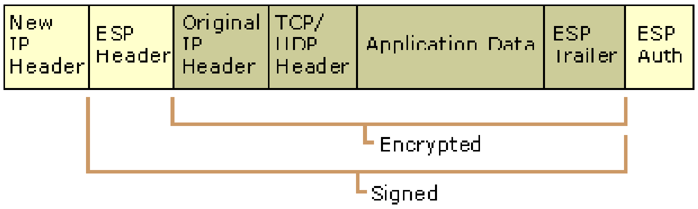



Figure 6.6: ESP Tunnel Mode

The Signed area indicates where the packet has been signed for integrity and authentication. The Encrypted area indicates what information is protected with confidentiality.

Because a new header for tunnelling is placed on the packet, everything following the ESP header is signed (except for the ESP authentication trailer), as it is now encapsulated in the tunnelled packet. The original header is placed after the ESP header.

The entire packet is appended with an ESP trailer prior to encryption. Everything following the ESP header, except for the ESP authentication trailer, is encrypted, including the original header because it is now considered to be part of the data portion.

The entire ESP payload is then encapsulated within the new tunnel header, which is not encrypted. The information in the new tunnel header is only used to route the packet from origin to destination.

If the packet is being sent across a public network, the packet is routed to the IP address of the tunnel server for the receiving intranet. The packet itself is most likely destined for an intranet computer. The tunnel server decrypts the packet, throws away the ESP header, and uses the original IP header to route the packet to the intranet computer.

### AH Tunnel Mode

The only difference between AH tunnel mode and ESP tunnel mode is how the packet is handled. As shown in the next Figure, AH signs the entire packet for integrity, including the new Tunnel Header (ESP does not sign the tunnel header), and encryption is not provided by AH.

ESP and AH can be combined to provide tunnelling which includes both integrity for the entire packet and confidentiality for the original IP packet, which contains the data being sent.

[9] Additional information about tunnelling concepts and the integration with L2TP will be provided in the section about Virtual Private Networks. The issues here are related to IPSec tunnelling only.

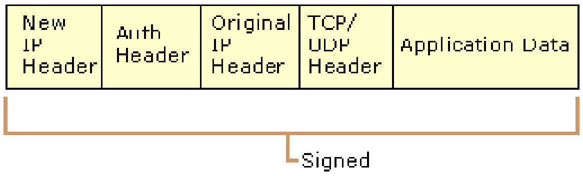



Figure 6.7: AH Tunnel Mode

### Transport mode

Transport mode provides the protection of an IP payload through an AH or ESP header. Typical IP payloads are TCP segments (containing a TCP header and TCP segment data), a UDP message (containing a UDP header and UDP message data), and an ICMP message (containing an ICMP header and ICMP message data). Transport mode was developed for use by end systems. Its use is predicated on full deployment to all systems in the group and most cases will require reprogramming of applications.

### AH Transport Mode

In AH transport mode, an authentication header is inserted between the IP header and payload. The AH provides a security parameter index, sequence number and other data required for authenticating the source of the data.

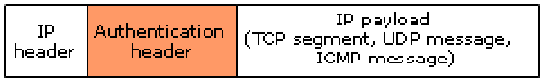



Figure 6.8: AH Transport Mode

### ESP Transport Mode

In ESP transport mode, an ESP header is inserted between the IP header and the payload, and an ESP trailer and authentication MAC are added to the end of the packet. In tunnel mode ESP, the entire packet is encrypted and appended to a new ESP header and IP header and an authentication trailer added.

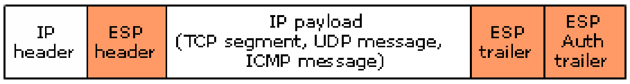



Figure 6.9: ESP Transport Mode

### Provided Protection Against Attacks

After this technical analysis of IPSec, this section provides information on the protection capabilities. The best level of protection is provided with IPSec's end-to-end model: the sending computer secures the data prior to transmission (before it ever reaches the network wires), and the receiving computer "unsecures" the data only after it has been received. For this reason, IPSec should be one of the components in a layered enterprize security plan. It protects the private data in a public environment by providing a strong, cryptography-based defense against attacks. All network traffic is secured packet by packet rather than for a whole communication (that is, a flow of packets). Used in combination with strong user access control, perimeter, and possibly physical level security, IPSec ensures an in-depth defense for data. IPSec can be combined also with other security solutions, providing a allround security package. Some of the combinations which are possible with IPSec will be described later.

IPSec protects the data so that an attacker finds it extremely difficult or impossible to interpret. The level of protection provided is determined by the strength of the security levels specified in a company's IPSec policy structure.

The following list provides an overview on how IPSec significantly reduces or even prevents some of the attacks we saw in Chapter 3:

- **Sniffers, Lack of Privacy** IPSec's Encapsulating Security Payload (ESP) protocol provides data privacy by encrypting the IP packets.
- **Data Modification** IPSec uses cryptography-based keys, shared only by the sending and receiving computers, to create a digital checksum for each IP packet. Any modifications to the packet data alter the checksum, which indicates to the receiving computer that the packet was modified in transit.
- **Identity Spoofing, Password-Based, Application-Layer, and Denial-of-Service** IPSec allows the exchange and verification of identities without exposing that information to interpretation by an attacker. Mutual verification (authentication) is used to establish trust between the communicating systems; only trusted systems can communicate with each other.
- **Man-in-the-Middle** IPSec combines mutual authentication with shared, cryptography-based keys.
- **Denial-of-Service** IPSec uses IP packet filtering methodology as the basis for determining whether communication is allowed, secured, or blocked, according to the IP address ranges, protocols, or even specific protocol ports.

### Provided Security Properties

IPSec provides the following properties for secured communications:

**Non-Repudiation** Verifies that the sender of the message is the only person who could have sent it. The sender cannot deny having sent the message. Non-repudiation is a property of messages containing digital signatures when using public key technology. With public key technology, the sender's private key is used to create a digital signature that is sent with the message. The receiver uses the sender's public key to verify the digital signature. Because only the sender has possession of the private key, only the sender could have generated the digital signature. Non-repudiation is not a property of message authentication codes and hashes on messages using secret key technologies, because both the sender and the receiver have the secret key.

**Anti-Replay** Also called replay prevention, it ensures the uniqueness of each IP packet. Anti-replay ensures that data captured by an attacker cannot be re-used or "re-played" to establish a session or gain information illegally. This protects against attempts to intercept a message and then use the identical message to illegally gain access to resources, possibly even months later.

**Integrity** The definition of this property was given in Chapter 3. Hash functions sign each packet with a cryptographic checksum using one of the shared keys, which the receiving computer checks before opening the packet. Only the sender and receiver have the key used to calculate the checksum. If the packet and therefore the signature has changed, the packet is discarded.

**Confidentiality** Another of the basic security feature we saw in Chapter 3. Confidentiality is achieved by encrypting the data before transmission. This ensures that the data cannot be read during transmission, even if the packet is monitored or intercepted. Only the party with the shared, secret key is able to read the data (after decryption). This property is optional and is dependent on IPSec policy settings.

**Authentication** Verifies the origin of a message through the process of one side sending a credential and the receiver verifying the legitimacy of the credential.

### 6.3.2 Virtual Private Networks (VPN)

#### Overview

A virtual private network (VPN) is the extension of a private network that encompasses links across shared or public networks like the Internet. A VPN enables data to be sent between two computers across a shared or public internetwork in a manner that emulates the properties of a point-to-point private link. The act of configuring and creating a virtual private network is known as virtual private networking. [23]

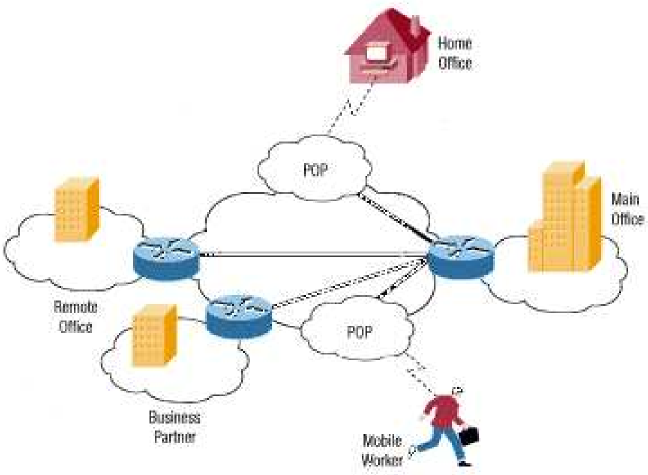



Figure 6.10: Typical Virtual Private Network

To emulate a point-to-point link, data is encapsulated, or wrapped, with a header that provides routing information allowing it to traverse the shared or public internetwork to reach its endpoint. To emulate a private link, the data being sent is encrypted for confidentiality. Packets that are intercepted on the shared or public network are indecipherable without the encryption keys. The link in which the private data is encapsulated and encrypted is known as a virtual private network (VPN) connection. The following Figure illustrates the logical concept of a VPN.

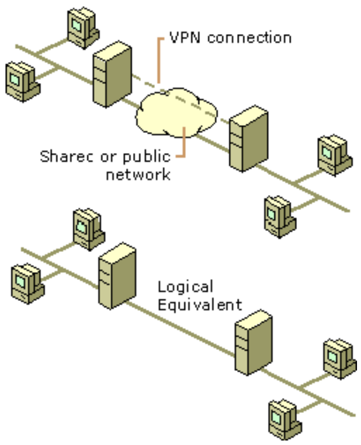



Figure 6.11: Logical concept of a VPN

VPN connections allow users working at home, or on the road to obtain a remote access connection to an organization server using the infrastructure provided by a public internetwork, such as the Internet. From the user's perspective, the VPN is a point-to-point connection between the computer, the VPN client and an organization server, the VPN server. The exact infrastructure of the shared or public network is irrelevant, because it appears logically as if the data is sent over a dedicated private link.

VPN connections also allow organizations to have routed connections with geographically separate offices or with other organizations over a public internetwork such as the Internet, while maintaining secure communications. A routed VPN connection across the Internet logically operates as a dedicated WAN link.

With both the remote access connection and with the routed connection, VPN connections allow an organization to trade in long distance dial-up or leased lines for local dial-up or leased lines to an Internet service provider (ISP).

## Elements of a VPN Connection

A VPN connection includes the following components as illustrated in the following Figure:

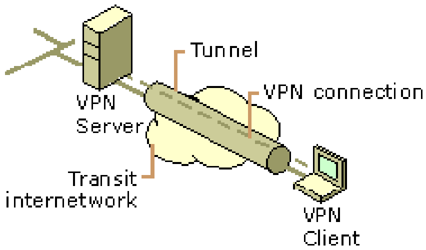



Figure 6.12: VPN Components

**VPN server:** A computer that accepts VPN connections from VPN clients. A VPN server can provide a remote access VPN connection or a router-to-router VPN connection.

**VPN client:** A computer that initiates a VPN connection to a VPN server. A VPN client can be an individual computer that obtains a remote access VPN connection or a router that obtains a router-to-router VPN connection. There are no limitation in the particular Operating system when using a VPN client.

**Tunnel:** The portion of the connection in which the data is encapsulated.

**VPN connection:** The portion of the connection in which the data is encrypted. For secure VPN connections, the data is encrypted and encapsulated along the same portion of the connection.[10]

**Tunnelling protocols:** Communication standards used to manage tunnels and encapsulate private data. (Data that is tunnelled must also be encrypted to be a VPN connection.) The most widely used protocols are the PPTP and L2TP tunnelling protocols.[11]

**Tunnelled data:** Data that is usually sent across a private point-to-point link.

**Transit internetwork:** The shared or public internetwork crossed by the encapsulated data. The transit internetwork can be the Internet or a private IP-based intranet.

[10] It is possible to create a tunnel and send the data through the tunnel without encryption. This is not a VPN connection, because the private data is sent across a shared or public network in an unencrypted and easily readable form.

[11] An analysis of the two protocols has been added to Appendix C

### VPN Connections

Creating the VPN is very similar to establishing a point-to-point connection using dial-up networking and demand-dial routing procedures. There are two types of VPN connections:

- The remote access VPN connection and
- The site-to-site VPN connection

The following Figure illustrates the different VPN types:

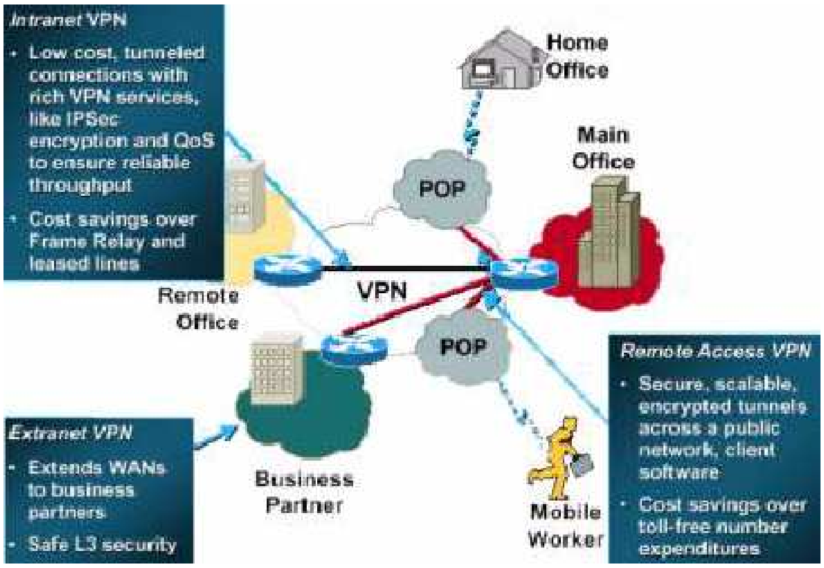



Figure 6.13: VPN Types

### Remote Access VPN Connection

A remote access VPN connection is made by a remote access client or a single user computer, that connects to a private network. The VPN server provides access to the resources of the VPN server or to the entire network to which the VPN server is attached. The packets sent across the VPN connection originate at the remote access client.

The remote access client (the VPN client) authenticates itself to the remote access server (the VPN server) and, for mutual authentication, the server authenticates itself to the client.

### Site-to-Site VPN Connection

A site-to-site VPN connection is made by a router and connects two portions of a private network. The VPN server provides a routed connection to the network to which the VPN server is attached. On a site-to-site VPN connection, the packets sent from either router across the VPN connection typically do not originate at the routers. The calling router (the VPN client) authenticates itself to the answering router (the VPN server), and, for mutual authentication, the answering router authenticates itself to the calling router. Site-to-site VPNs can be either:

**Intranet-based** If a company has one or more remote locations that they wish to join in a single private network, they can create an intranet VPN to connect LAN to LAN.

**Extranet-based** When a company has a close relationship with another company (for example, a partner, supplier or customer), they can build an extranet VPN that connects LAN to LAN, and that allows all of the various companies to work in a shared environment.

In the following section, the two subcategories of a site-to-site VPN Connection will be analyzed deeper by looking at some examples of site-to-site VPN network structures.

### Internet-Based VPN Connections

Using an Internet-based VPN connection, long-distance telephone charges can be avoided, while taking advantage of the global availability of the Internet.

**Remote Access over the Internet** Rather than a remote access client having to make a long distance call to a corporate or outsourced network access server (NAS), the client can call a local ISP. By using the established physical connection to the local ISP, the remote access client initiates a VPN connection across the Internet to the organization's VPN server. When the VPN connection is created, the remote access client can access the resources of the private intranet. The next Figure illustrates remote access over the Internet.

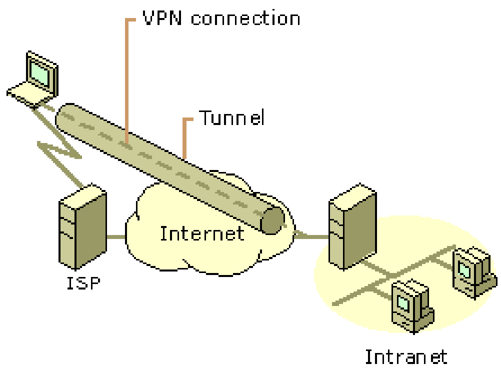



Figure 6.14: Connecting a Remote Client to a Private Intranet

**Connecting Networks over the Internet** When networks are connected over the Internet (illustrated in Figure 6.12), a router forwards packets to another router across a VPN connection. To the routers, the VPN operates as a data-link layer link.

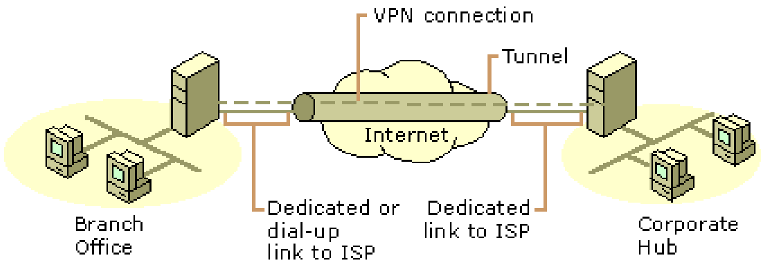



Figure 6.15: Connecting Two Remote Sites Across the Internet

**Connecting Networks Using Dedicated WAN Links** Rather than using an expensive long-distance dedicated WAN link between offices, the office routers are connected to the Internet using local dedicated wide area network (WAN) links to a local ISP. A router-to-router VPN connection is then initiated by either router across the Internet. When connected, routers can forward directed or routing protocol traffic to each other using the VPN connection.

**Connecting Networks Using Dial-Up WAN Links** Rather than having a branch office router make a long distance call to a corporate or outsourced NAS, the branch office router calls a local ISP. Using the established connection to the local ISP, a router-to-router VPN connection is initiated by the branch office router to the corporate hub router across the Internet. The corporate hub router acting as a VPN server must be connected to a local ISP using a dedicated WAN link. It is possible to have both offices connected to the Internet using a dial-up WAN link. However, this is only feasible if the ISP supports demand-dial routing to customers; the ISP calls the customer router when an IP datagram is to be delivered to the customer. Demand-dial routing to customers is not widely supported by ISPs.

### Intranet-Based VPN Connections

The intranet-based VPN connection takes advantage of IP connectivity in an organization intranet.

**Remote Access over an Intranet** In some organization intranets, the data of a department, such as a human resources department, is so sensitive that the department's network segment is physically disconnected from the rest of the organization's intranet. While this protects the department's data, it creates information accessibility problems for those users not physically connected to the separate network segment.

VPN connections allow the sensitive department's network segment to be physically connected to the organization intranet but separated by a VPN server. The VPN server does not provide a direct routed connection between the corporate intranet and the separate network segment. Users on the corporate intranet with the appropriate permissions can establish a remote access VPN connection with the VPN server and can gain access to the protected resources of the sensitive department's network. Additionally, all communication across the VPN connection is encrypted for data confidentiality. For those users who do not have permissions to establish a VPN connection, the separate network segment is hidden from view. The following Figure illustrates remote access over an intranet.

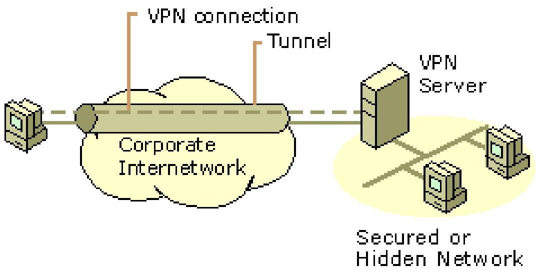



Figure 6.16: Remote Access to a Secured Network over an Intranet

**Connecting Networks over an Intranet** It is also possible to connect two networks over an intranet using a router-to-router VPN connection. This type of VPN connection might be necessary, for example, for two departments in separate locations, whose data is highly sensitive, to communicate with each other. For instance, the finance department might need to communicate with the human resources department to exchange payroll information.

The finance department and the human resources department are connected to the common intranet with computers that can act as VPN clients or VPN servers. When the VPN connection is established, users on computers on either network can exchange sensitive data across the corporate intranet. The next Figure illustrates networks connected over an intranet.

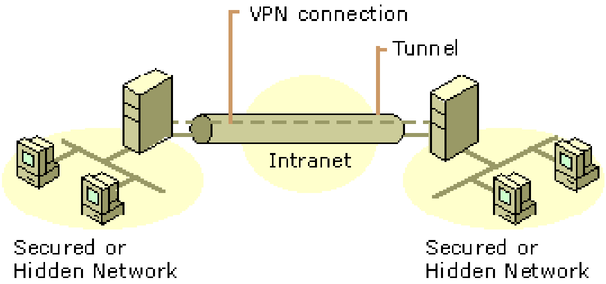



Figure 6.17: Connecting Two Networks over an Intranet

Due to the fact that a VPN connection is a networking tool that can provide secured point-to-point connections in whatever manner fit the company's requirements, there exist also a possibility of combining the individual internet and intranet based solutions. This less common combined Internet and intranet VPN connection, called a pass-through VPN connection, illustrated in the following Figure, allows a remote access client connected to one company's intranet to access the resources of another company's intranet using the Internet. In this scenario, a remote access VPN connection passes through one intranet and the Internet to access a second intranet.

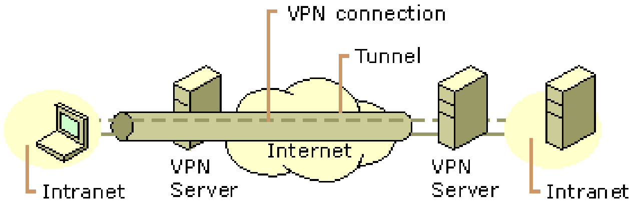



Figure 6.18: Connecting Two Networks over an Intranet

## Properties of VPN Connections

VPN connections[12] have the following properties:

- Encapsulation
- Authentication
- Data encryption
- Address and name server assignment

**Encapsulation:** VPN technology provides a way of encapsulating private data with a header that allows the data to traverse the transit internetwork.

[12]Connections that use PPTP and L2TP over IPSec

**Authentication:** Authentication for VPN connections takes two forms:

- User authentication
  For the VPN connection to be established, the VPN server authenticates the VPN client attempting the connection and verifies that the VPN client has the appropriate permissions. If mutual authentication is being used, the VPN client also authenticates the VPN server, providing protection against masquerading VPN servers.
- Data authentication and integrity
  To verify that the data being sent on the VPN connection originated at the other end of the connection and was not modified in transit, the data can contain a cryptographic checksum based on an encryption key known only to the sender and the receiver.

**Data Encryption:** To ensure confidentiality of the data as it traverses the shared or public transit internetwork, it is encrypted by the sender and decrypted by the receiver. The encryption and decryption processes depend on both the sender and the receiver having knowledge of a common encryption key.

Intercepted packets sent along the VPN connection in the transit internetwork are unintelligible to anyone who does not have the common encryption key. The length of the encryption key is an important security parameter. Computational techniques can be used to determine the encryption key. Such techniques require more computing power and computational time as the encryption key gets larger. Therefore, it is important to use the largest possible key size.

In addition, the more information that is encrypted with the same key, the easier it is to decipher the encrypted data. With some encryption technologies, you are given the option to configure how often the encryption keys are changed during a connection.

**Address and Name Server Allocation:** When a VPN server is configured, it creates a virtual interface that represents the interface on which all VPN connections are made. When a VPN client establishes a VPN connection, a virtual interface is created on the VPN client that represents the interface connected to the VPN server. The virtual interface on VPN client is connected to the virtual interface on the VPN server creating the point-to-point VPN connection.

The virtual interfaces of the VPN client and the VPN server must be assigned IP addresses. The assignment of these addresses is done by the VPN server. By default, the VPN server obtains IP addresses for itself and VPN clients using the Dynamic Host Configuration Protocol (DHCP). There is the possibility to configure a static pool of IP addresses defined by an IP network ID and a subnet mask.

Name server assignment, the assignment of domain name system (DNS) servers, also occurs during the VPN connection establishment process. The VPN client obtains the IP addresses of the DNS servers from the VPN server for the intranet to which the VPN server is attached.

### Managing Virtual Private Networks

Virtual private networks must be managed just like any other network resource, and VPN security issues, particularly with Internet VPN connections, must be addressed carefully. In the following section, an outline on the various management issues will be given.

**Managing Users** Because it is administratively unsupportable to have separate user accounts on separate servers for the same user and try to keep them all simultaneously current, most administrators set up a master account database at a domain controller (PDC) or on a Remote

Authentication Dial-in User Service (RADIUS) server. This allows the VPN server to send the authentication credentials to a central authenticating device. The same user account is used for both dial-in remote access and VPN-based remote access.

**Managing Addresses and Name Servers** The VPN server must have IP addresses available in order to assign them to the VPN server's virtual interface and to VPN clients during the IP Control Protocol (IPCP) negotiation phase of the connection establishment process. The IP address assigned to the VPN client is assigned to the virtual interface of the VPN client. The VPN server must also be configured with DNS and WINS server addresses to assign to the VPN client during IPCP negotiation.

**Managing Authentication** The VPN server can be configured to use RADIUS as an authentication provider, where user credentials and parameters of the connection request are sent as a series of RADIUS request messages to a RADIUS server.

The RADIUS server receives a user-connection request from the VPN server and authenticates the user using its authentication database. A RADIUS server can also maintain a central storage database of other relevant user properties. In addition to a yes or no response to an authentication request, RADIUS can inform the VPN server of other applicable connection parameters for this user - such as maximum session time, static IP address assignment and so on.

RADIUS can respond to authentication requests based on its own database, or it can be a front end to another database server, such as a generic Open Database Connectivity (ODBC) server. In addition, a RADIUS server can act as a proxy client to a remote RADIUS server. The RADIUS protocol is described in RFC 2138 and RFC 2139.

**Managing Accounting** The VPN server can be configured to use RADIUS as an accounting provider, where accounting messages are sent to the RADIUS server for accumulation and later analysis.

Most RADIUS servers can be configured to place authentication request records into an accounting file. A number of third parties have written billing and audit packages that read RADIUS accounting records and produce various useful reports. For more information about RADIUS accounting, see RFC 2139.

## VPN and Tunelling

Most VPNs rely on tunnelling to create a private network that reaches across the Internet. Essentially, tunnelling is the process of placing an entire packet within another packet and sending it over a network. The protocol of the outer packet is understood by the network and both points, called tunnel interfaces, where the packet enters and exits the network. Tunnelling requires three different protocols:

**Carrier protocol** The protocol used by the network that the information is traveling over

**Encapsulating protocol** The protocol (GRE, IPSec, L2F, PPTP, L2TP) that is wrapped around the original data

**Passenger protocol** The original data (IPX, NetBeui, IP) being carried

Tunnelling has amazing implications for VPNs. For example, a packet that uses a protocol not supported on the Internet (such as NetBeui) could be placed inside an IP packet and send it safely over the Internet. Or a packet that uses a private (non-routable) IP address could be put inside a packet that uses a globally unique IP address to extend a private network over the Internet.

In a site-to-site VPN, GRE (generic routing encapsulation) is normally the encapsulating protocol that provides the framework for how to package the passenger protocol for transport over the carrier protocol, which is typically IP-based. This includes information on what type of packet there is encapsulated and information about the connection between the client and server. Instead of GRE, IPSec in tunnel mode is sometimes used as the encapsulating protocol. IPSec works well on both remote-access and site-to-site VPNs. IPSec must be supported at both tunnel interfaces to use.

In a remote-access VPN, tunnelling normally takes place using PPP. Part of the TCP/IP stack, PPP is the carrier for other IP protocols when communicating over the network between the host computer and a remote system. Remote-access VPN tunneling relies on PPP.

Each of the protocols listed below were built using the basic structure of PPP and are used by remote-access VPNs:

- L2F (Layer 2 Forwarding) - Developed by Cisco, L2F uses any authentication scheme supported by PPP.
- PPTP (Point-to-Point Tunneling Protocol) - PPTP was created by the PPTP Forum, a consortium which includes US Robotics, Microsoft, 3COM, Ascend and ECI Telematics. PPTP supports 40-bit and 128-bit encryption and uses any authentication scheme supported by PPP.
- L2TP (Layer 2 Tunneling Protocol) - L2TP is the product of a partnership between the members of the PPTP Forum, Cisco and the IETF (Internet Engineering Task Force). Combining features of both PPTP and L2F, L2TP also fully supports IPSec. L2TP can be used as a tunneling protocol for site-to-site VPNs as well as remote-access VPNs. In fact, L2TP can create a tunnel between:
  - A client and a router
  - A NAS and a router or
  - A router and a router

A very easy way to imagine what tunnelling is about is to think of it like having a computer delivered to a location by UPS. The vendor packs the computer (passenger protocol) into a box (encapsulating protocol) which is then put on a UPS truck (carrier protocol) at the vendor's warehouse (entry tunnel interface). The truck (carrier protocol) travels over the highways (Internet) to the specific location (exit tunnel interface) and delivers the computer. Then the receiver opens the box (encapsulating protocol) and removes the computer (passenger protocol).

As there are many details involved with the VPN technology, the protocols related to tunnelling have been added to Appendix C.

Before proceeding the further analysis of the security solutions at the different layers of the OSI model, there has to be mentioned that the suggestions some of the VPN solutions, assume that the VPN gear exists on the customer premises and is managed by the customer. Though the topologies may not change significantly, if the VPN is managed by a service provider, the management and provisioning of that type of network would be very different.

### 6.3.3 Network Layer Firewalls

Routers form connections between different parts of a network and seem like a logical place to implement security. Routers filter packets and can allow or deny access to system resources based upon information contained within the packet header, such as the source address or destination address. The Filtering is stateless in that each packet is examined in isolation with access granted according to a defined set of rules. The logging of packets also takes no account of any history.

Security is not the primary function of a router. They contain little intelligence and cannot perform complex decisions. This simplicity helps to keep operating speeds high and ensures that it is relatively easy to introduce new applications. Unfortunately translating the company's security policy into a set of instructions for the router is extremely arduous.

## 6.4 Data Link Layer Security

The Data Link layer describes the network technology connected to the Physical layer. This layer deals with the network equipment such as ethernet hubs and switches and network interface cards (NIC) installed in the computers. Data Link security is done point-to-point, such as over a leased line or frame relay permanent virtual circuits. Dedicated hardware devices attached to each end of the link do encryption and decryption. This is called link encryption. Link encryption protects against intruders from outside the network that share that data link, but it does not distinguish authorized parties within the network. When a communication path is formed over a network consisting of multiple data links, link encryption allows intrusion by members of the "trusted" community of every data link traversed by the path. Military, governments, and banking are the most common users of this approach. It is not scalable to large internetworks, because the packets are not routable in their encrypted state. This method does have the advantage that an eavesdropper cannot determine the source or destination addresses in the packets. It can also be used for any upper layer protocols. Searching for particular security solutions at the data link level was quit difficult. Most of the solutions found were kept very general and the main concept is described above. Therefore, no particular solutions are presented.

## 6.5 Physical Layer Security

At the physical layer, security can be achieved by various non-cryptographic techniques that prevent tampering with the communication medium itself.

### 6.5.1 Secure Cable Conduits

A pretty unconventional possibility of preventing somebody from tampering the actual communication medium (e.g network cables) ist to encase them for example in concrete. In this way the physical protection is provided. Although I personally believe this is quite ridiculous, there were certain companies that actually "implemented" such a solution.

### 6.5.2 Shielding

A keyword that is used when talking about shielding of electronic equipment is TEMPEST. TEMPEST is a U.S. government code word that identifies a classified set of standards for limiting electric or electromagnetic radiation emanations from electronic equipment. It has been simulated and proven that emanations like this could be captured and then reconstructed. The purpose of the program was to introduce standards that would reduce the chances of "leakage" from devices used to process, transmit or store sensitive information. Solutions to this problem have already been implemented by government agencies. This is done by shielding the device (or sometimes a room or entire building) with copper or other conductive materials, in order to block the emanation and the electromagnetic signals.

### 6.5.3 Choice of a Special Medium

The choice of particular mediums (cables) could be another security solution at the physical layer. Except from advantages of for example Fiber Optic Cables, like the expanded data handling capacity, electrical noise immunity and electrical isolation, there are also some security features involved which come along with the mediums characteristics. In other words, it is for example harder to tap an optical cable than a normal phone line cable.

At the end of this chapter there are some general security solutions which can be incorporated layer-independently and could be combined with some of the previous implementations.

## 6.6 Authentication

Authentication can be provided locally on each device on the network, but using an authentication server offers improved scalability, flexibility and control. Firewalls, routers and remote access servers enforce network access security. Configuring these devices to use one centralized database of accounts, is easier on the administrator and the users who may access the network through multiple pathways. [24]

### 6.6.1 Terminal Access Controller Access System (TACACS+)

TACACS+ is an enhanced version of TACACS developed by Cisco. The enhancements include the separation of authentication, authorization and accounting into three distinct functions. These services can be used independently or together. For example, Kerberos[13] could be used for authentication and TACACS+ used for authorization and accounting. Some of the characteristics of TACACS+ are:

- While older versions of TACACS and RADIUS use UDP for transport, TACACS+ uses TCP (port 49) for reliable and acknowledged transport.
- TACACS+ can encrypt the entire payload of the packet, so it protects the password, username and other information sent between the access client and the server. The encryption can be turned off for troubleshooting. Communication from the workstation to the client providing access services is not encrypted.
- TACACS+ supports multiple protocols such as IP, Appletalk Remote Access (ARA), Novell, Asynchronous Services Interface (NASI), X.25 PAD connection and NetBIOS.
- TACACS+ can be used to provide greater control over router management in either nonprivileged or privileged mode, because it can authenticate individual users or groups rather than a shared password. Router commands can be specified explicitly on the TACACS+ server to allow specific commands.

### 6.6.2 Remote Dial In User System (RADIUS)

We saw the incorporation of RADIUS in the section about VPNs. Here it will be investigated separately. RADIUS is an open standard and available from many vendors. RADIUS can be a good choice in a heterogeneous network environment because of its widespread support, but some vendors have implemented proprietary attributes in RADIUS that hinder interoperability. Some of the characteristics are:

- RADIUS uses UDP, so only offers best effort delivery.

[13] Please refer to section 6.6.3

- For authentication, RADIUS encrypts only the password sent between the access client and the RADIUS server.
- RADIUS does not provide encryption between the workstation and the access client. RADIUS does not support multiple protocols, and only works on IP networks.
- It does not provide the ability to control the commands that can be executed on a router

### 6.6.3 Kerberos

Kerberos protocol can be used for network authentication and host authentication. Host-based applications must be adapted to use the Kerberos protocol. A Kerberos realm includes all users, hosts and network services that are registered with a Kerberos server. Kerberos uses symmetric key cryptography and stores a shared key for each user and each network resource that is participating in its realm. Every user and network resource needs a Kerberos account. Knowing its shared key is proof of identity for each of those entities. Kerberos stores all passwords encrypted with a single system key. If that system key is compromised, all passwords need to be recreated.

The process of authenticating using Kerberos involves three systems:

- A client
- A network resource, and
- The Kerberos server

The Kerberos server is called the Key Distribution Center (KDC). For remote network access, the client and network resource is the boundary network device, such as network access server or router. The remote user establishes a PPP connection to the boundary device, and the device prompts the user for username and password. The device, acting as the client, requests a ticket granting ticket from the Kerberos authentication server. If the user has an account, the authentication server generates a session key, and sends it to the ticket-granting server (TGS). The ticket-granting ticket (TGT) is a credential that specifies the user's verified identity, the Kerberos server identity, and the expiration time of the ticket. By default, tickets expire after eight hours. The ticket granting ticket is encrypted with a key known only to the ticket-granting server and the authentication server. The Kerberos server using a DES key generated from the users password encrypts the TGT, session key and other info. Only the user and the Kerberos server should know the password. The access server will attempt to decrypt the TGT with the password that the user entered. If successful, the user is authenticated to the access server, and the user's workstation becomes part of the protected network.

Users who want to access services that are part of the Kerberos realm on the network, must now authenticate against the Kerberos server and get authorization to access the services. The user first gets a ticket-granting ticket as described above, which is used to request access to other services. The difference is that the client is now the user's workstation. The user then sends the ticket granting ticket to the ticket granting service to request access for a specific service on a specific server. The ticket granting service generates a random session key and sends a server ticket containing the key to the client that requested the service. The client presents the new server ticket to the server in order to gain access. A server ticket must be created for each service that the client will access. [25]

## 6.7 Cryptography

Cryptography is a method which was incorporated in most of the previous security solutions. In this section the aspects of cryptography and the related algorithms will be investigated. Many of the algorithms have been mentioned on the side of the previous solutions, but will be analyzed in more detail. Cryptography is the science of writing and reading in code or cipher. Information security uses cryptosystems to keep information private and to authenticate the identity of the sender or receiver of the information. Cryptography can also provide integrity for information, because it allows only authorized people or processes to access it and can detect corruption or modification of the original message or file. Cryptography works by making the effort required to break the encryption much more expensive than the value of the data, or by taking much longer to break than the data will hold its value.

There are three categories of cryptographic functions: symmetric key, asymmetric key, and hash functions. Most of the standard algorithms are public knowledge and have been thoroughly tested by many experts. Their security depends on the strength of the algorithm and the strength of the key. A key is a sequence that is used for the mathematical process of enciphering and deciphering information. The hash functions do not use a key. The hash is performed by a specialized mathematical function.

There are many algorithms for encrypting information. To exchange encrypted messages, the parties must agree on the algorithms that will be used and the keys for each algorithm. The protocols will be configured or negotiate a particular algorithm and a key management system will generate, distribute and manage the keys. [26]

### 6.7.1 Symmetric Cryptography

Symmetric key cryptography uses the same key to encrypt and decrypt the message. Each pair of users shares a key for exchanging messages. By being able to encrypt or decrypt a message, each partner assumes that the other entity is the same entity with which they exchanged keys. It provides some degree of authentication. For this scheme to work, the key must be kept secret between the two parties involved.

Examples of symmetric key algorithms are:

- Data Encryption Standard (DES) (56 bits)
- Triple DES (3DES) (168 bits)
- International Data Encryption Algorithm (IDEA) (128 bits)
- Rivest Cipher 4 (RC4) (variable length key)
- Advanced Encryption Standard (AES) (will replace DES as a federal standard)

For stored files that are encrypted, the loss or destruction of the sole copy of a symmetric key could result in the loss of access to the files. Sometimes keys are archived or backed up to protect the organization from such potential loss. For network transfers, this vulnerability is not an issue. New keys can be generated, exchanged, and the information resent.

A symmetric key, including any backup copies, has to be protected to the same extent as the information that it protects. The distribution of the keys must be accomplished by a secure means. If someone intercepted a key during the exchange or acquired a key from a user's system, they could also participate in the exchange of encrypted information. Privacy and integrity would be lost.

Symmetric key algorithms are fast and can encrypt a lot of information in a short period of time. They are strong when large keys are used. Symmetric key algorithms are used for the bulk of communication link encryption.

### 6.7.2 Asymmetric Cryptography

Asymmetric key cryptography is also known as public key cryptography. It uses a pair of keys that are mathematically related, but given one key, the other is very unlikely to be calculated. One key is for encrypting or signing, and the other is used for decrypting or verifying. One of the keys is kept private or secret, and the other is distributed publicly.

Examples of asymmetric key algorithms are:

- Diffie-Hellman
- Rivest, Shamir, Adleman (RSA)
- Digital Signature Algorithm (DSA) / El Gamal
- Elliptic Curve Cryptosystem (ECC)

The asymmetric algorithms are trapdoor one-way functions. They are easy to compute in one direction, but extremely difficult to calculate in the reverse direction, unless you have the other key to the trapdoor. Even with the keys, asymmetric key functions are very compute intensive. They are about one hundred times slower than symmetric key algorithms. They are not practical for encrypting and decrypting large amounts of data.

When used to provide confidentiality, the sender encrypts the message using the public key of the receiver. Only the intended receiver's private key can decrypt the message. Messages going to multiple receivers must be encrypted for each one of the receivers. When used for authentication in digital signatures, the message is encrypted with the sender's private key. Only the sender's public key can decrypt it, verifying that it came from the sender. Confidentiality is the most common use for public key cryptography. It is used to exchange the session keys for symmetric key algorithms.

### 6.7.3 Hash Function

A hash function is used to condense a variable-length message into a fixed-length code, known as a hash or message digest. Different algorithms will produce different length hashes. Some examples of hash functions are:

- Message Digest 5 (MD5) (128 bits)
- Secure Hash Algorithm (SHA) (160 bits)
- Haval (variable length)

Hashes are a cryptographic checksum used to provide an integrity check on messages. A change of just one character in the original message can produce a change in a significant number of the hash bits. A hash function is a one-way function, and it is mathematically infeasible to compute the original message from the hash. The sender computes a hash of the original message and sends it with the encrypted message. The receiver decrypts the message, and also computes a hash. If the original hash and the computed hash are the same, then the receiver is confident that the message is complete and unmodified.

Computing a hash of the message, and encrypting the hash with the sender's private key can create a digital signature. The sender attaches this digital signature to the message. The receiver separates the digital signature and decrypts it with the sender's public key. A hash of the message received is computed. If the two hash values match, then it verifies that this is the authentic message from the sender.

### 6.7.4 Public Key Certificates

Public key certificates are data structures, signed by a trusted certificate authority (CA) that binds an identity to a public key and additional information. They provide a means of distributing public keys. The degree of trust that somebody puts into the identity, is dependent upon the procedures and trust that he places in the certificate authority. Public key certificates are used to support authentication, confidentiality and integrity for such things as Web transactions, email exchange and IPSec, like we saw. The certificate is signed with the private key of the certificate authority. The CA's public key is used to authenticate the certificate. Signed public key certificates, traceable via a hierarchical chain of trust, provide authentication and integrity of the public key and data included in the certificate.

The public key infrastructure provides a mechanism for generating keys, managing certificates and ensuring integrity of the keys. Certificates are issued with expiration dates, after which they are no longer valid. Certificates may be revoked prior to the expiration date, for example due to personnel or organizational changes. Certificates are verified against recent certificate revocation lists (CRL) or online query mechanism to determine their validity. Certificate revocation lists can be downloaded from certificate authorities and used offline, but they need to be updated periodically.

# Chapter 7

# Comparison of proposed Security Solutions

Due to the fact that the analysis of the proposed solutions in the previous chapter was very detailed, it was difficult to point out particular features, advantages or disadvantages of the security solutions. Therefore, this part of the report will try and give an overall view and assessment of the individual proposals and try to point out important aspects of comparison. Many of the analyzed characteristics will be in a tabular form, in order to make their comparison transparent.

## 7.1 Comparison of Email Encryption Protocols

S/MIME, PGP and PEM, all specify methods for securing electronic mail. Each is capable of adequate security and all of them offer privacy and authentication, but also suffer from the lack of good implementation, in the context of transparent email encryption. Since PGP and PEM are quite different, they need to be compared with S/MIME individually.

PGP can be thought of as both a specification and an application and its underlying cryptography is quite sound: RSA (up to 2048 bits with the most recent implementation), IDEA with a 128 bit key, and MD5. PGP is entirely in accordance with the recent recommendations on minimum key length, and in fact does not include a mode of operation in violation of those recommendations. PGP is packaged in a single application (i.e. a single binary) which performs encryption, decryption, signing, verification and key management. It does not depend on the existence of great deal of infrastructure. These factors have, in my opinion, been decisive in PGP's popularity.

However, PGP is still not suitable for fully transparent email encryption. PGP contains a number of implementation flaws (including silly things like not locking files, so that concurrent invocations fail). In addition, key management has some problems. Mostly, key management is hard to learn, time consuming, and requires a great deal of manual intervention. The "Web of trust" is supposed to fix this, by providing transitive trust of key authenticity. However, in practice the Web of trust has not delivered.[1] Moreover, this informal "web of trust" works well only for small workgroups, but can become unmanageable for large numbers of users. S/MIME on the other hand, utilizes hierarchies in which the roles of the user and the certifier are formalized. This means that S/MIME is both more secure and more scalable than PGP implementations. S/MIME has flexible guidelines for establishing hierarchies of users and will be equally easy for small groups and scalable to large

[1] Personally I could not get more than 2 keys trusted

enterprizes. S/MIME will also be well integrated into many e-mail applications, making it simple for users and ubiquitous.

S/MIME is an attempt to graft MIME support onto underlying PKCS standards, which are in turn a backwards-compatible extension of PEM. The PEM message format is based on 7-bit text messages, whereas S/MIME is designed to work with MIME binary attachments as well as text. The guidelines for hierarchies are also more flexible in S/MIME. This should allow for both easy set-up for small workgroups that don't need to be part of an all-encompassing hierarchy, and an easy path to move workgroups to the hierarchy that best suits their needs.

One cryptographic weakness of S/MIME is that eavesdroppers can distinguish between encrypted and signed-and-encrypted messages, and more importantly, tell who the signers of the message were. This violates the principle of disclosing a minimum amount of information. PGP and PEM do not have this problem.

To conclude, all of the proposals described here can be used for secure email and their application is a great improvement in comparison to no security implementation at all.[2]

## 7.2 S-HTTP

S-HTTP resides, like we saw, at the application layer and is designed to transmit individual messages securely. Due to this fact it cannot accommodate other applications such as email and newsgroups. This limitation of S-HTTP can also be considered an advantage, however. Since S-HTTP was designed specifically for browsers, it can be tuned to be more efficient in its transmission and receipt of data. It has to be mentioned though, that its use is diminishing and other technologies have emerged as the method of choice. Therefore, no further analysis will be made.

## 7.3 SSH

SSH provides adequate security. It protects against a wide variety of potential security breaches and solves the most important security problem on the Internet: hackers stealing passwords. Its interoperability is also one of the advantages. There are a wide variety of SSH clients that run on Linux, Macintosh, UNIX and Windows that work with the Process Software SSH server. Also, a user can select from a wide variety ciphers to use for strong encryption. Moreover, SSH is a flexible protocol. By using the port forwarding feature, any application that has a static port assignment, such as POP, SMTP and Oracle database connections can be encrypted. A systems administrator may only choose to encrypt his telnet session and not POP. The End-to-End security makes it possible for SSH to encrypt the connection from the source system to its destination. This provides security on the public and internal corporate network. It can also restrict the user from accessing any other system on the internal network other then the target system. SSH is a de-facto standard for encrypted terminal connections and secure file transfers.

There also some drawbacks associated with SSH. SSH cannot secure (encrypt) all applications, only if there is a known port number. Therefore applications can not be protected using SSH port forwarding. A special setup has to be made on a per-client basis, so that SSH can't be used from a random machine. Moreover, port ranges and dynamic ports can't be forwarded. Some of the characteristics of SSH will also become more clear, when it will be compared to other security implementations.

[2] Plasdan is not using any E-mail encrypting application at the moment

## 7.4 Firewalls

Although we saw firewalls reside on more than one layer of the OSI model, it is much better to compare this different types at once, in order to visualize their advantages and disadvantages. In the following table a firewall performance summary is presented:

| Technology | Speed | Flexibility | Intelligence |
|---|---|---|---|
| Packet Filtering | Very Good | Very Good | Low |
| Application proxy | Low | Low | Very Good |
| Stateful Inspection | Good | Good | Good |
| Circuit gateway | Low | Low | Low |

Table 7.1: Firewall Performance

Companies that plan to implement a firewall have to weigh their individual requirements with the above characteristics. The future promises solutions which combine the best features and functionality of each of the different firewall technologies.

## 7.5 SSL

The fact that SSL resides below applications such as e-mail (SMTP), web browsers (HTTP), and news groups (NNTP) has some significant advantages. SSL can work with any network that supports TCP/IP. This allows applications written for the Internet to be completely unaware as to what data transformations are taking place before they receive their data. New applications that come to market need not be concerned with how SSL works. This design of SSL, however, has its limitations. Since it is a general-purpose encryption technology, it may be slower than those written for specific application layer programs. Another drawback, as with any TCP/IP dependent technology, is that SSL is a communication oriented technology, which requires a dedicated port to communicate. Despite these minor limitations, SSL has been the largest single solution in use for secure transmissions over the Internet and is actually a standard on most browsers. This makes the establishment of SSL sessions easy. On the other hand there is no guarantee of where the information is from or by who it was generated and whether it is secure at either end of the pathway. SSL is just a simple "highway" with no rules, where anyone can relatively easy fake identities. From the described attacks, SSL provides no denial-of-service defense (i.e. TCP-SYN flooding is possible possible).

## 7.6 IPSec

During the analysis of IPSec many features were already pointed out. In the following section a summary of the advantages and disadvantages will be presented. IPSec's deployment has the following main advantages:

- It provides a transparent security solution
- The old and new TCP/IP applications are instantly secured with no modification.
- It has become an international industry (IETF) standard
- The deployment is simplified, due to its integration in a variety of products, like Microsoft, Solaris, HP, Cisco, Linux, BSD, telecom and datacom hardware (e.g. router) vendors etc.
- It provides flexible and configurable security, because the security services within each policy can be customized to meet the majority of security requirements for the network and data traffic.

- Security is configurable per TCP/IP application, source and/or destination host(s). Due to its tight integration at the IP layer (Layer 3), it provides security for any protocol in the TCP/IP suite. There is no need to separate security packages for each protocol in the TCP/IP suite, because applications using TCP/IP pass the data to the IP protocol layer, where it is secured.
- With the help of IPSec policies, rather than applications programming interfaces (APIs) or operations systems, a variable level of protection for most traffic types in most existing networks is provided.
- The known security services, such as authentication, encryption, integrity and replay protection are provided.
- IPSec provides a high level of security by using cryptography-based mechanisms. Cryptography allows information to be transmitted securely by hashing (integrity) and encrypting (confidentiality) the information.

In order to make some of IPSec's features more clear it was chosen to compare it with SSL. The following table summarizes the features of IPSec and SSL.

| Feature | IPSec | SSL |
|---|---|---|
| Protection | IP Packet | Applications |
| Performance | Fast (one handshake) | Handshake for each connection |
| Platform | Any | Client/Server |
| Current Uses | VPN Security | WWW Security |
| Scalability | Large number of public keys | Increasing processing needs |
| IPv6 | Inclusion in IPv6 | Cannot be included |

Table 7.2: IPSec and SSL Features

### Analysis of the above Features

Due to the fact that IPSec only needs one handshake between source and destination addresses, this gives it better performance and lower overhead on large amounts of data than SSL and makes it a better security protocol for VPNs. On the other hand, it lacks the access control due to its position. SSL's access control makes it better protocol in extranets where this extra access control is needed. Since each protocol has its advantages and disadvantages due to where they reside in the OSI model, the deciding factor on the future of the two is probably IPSec's inclusion in IPv6. The incredible advantage that this inclusion gives IPSec is that inclusion in IPv6 makes it interoperable with any other system that uses IPv6. Since this is the case and the only real drawback to IPSec is it lack of access control, I personally believe that IPSec will prevail as the predominant Internet security protocol

## 7.7 VPN

In the previous chapter we saw many possibilities to deploy a VPN solution. But many would ask themselves why a company should use a VPN? There are several advantages related with the choice of a VPN solution.

- Scalability: The cost to an organization of traditional leased lines may be reasonable at first, but can increase exponentially as the organization grows. A company with two branch offices, for example, can deploy just one dedicated line to connect the two locations. However, as an organization grows and more companies must be added to the network, the number of leased lines required, increases dramatically. This combinatorial explosion of needed lines

limits the flexibility for growth. VPNs that utilize the Internet avoid this problem by simply tapping into the geographically-distributed access already available. It becomes clear that a VPN service is an economical alternative to setting up a private network with expensive leased lines, as it can use existing IP infrastructure and equipment to connect remote users and offices.
- Extend geographic connectivity: With a VPN it is possible to interconnect many different types of network structure.
- Operational costs: By outsourcing the management of equipment used for remote access, as well as reducing the number of access line running into a corporate site companies can cut down on operational costs. In some cases, the company can even "borrow" the necessary hardware from a VPN service provider, at no extra charge. Finally, a VPN can theoretically alleviate the support burden, as the public service provider is generally responsible for supporting its dial-up customers.
- Security: For users the greatest strength of the internet is its ubiquity and its greatest weakness is the lack of security. VPNs have the security of a private network and the scalability and availability of the internet. Interoperable authentication and encryption protocols provide the necessary encryption in the VPN tunnel.

Except from the advantages of a VPN there are also certain concerns and drawbacks:

- Difficult to set-up and manage: Remote clients need to be configured with the right security parameters. Additionally, the secure tunnels between the client and tunnel must be integrated with the firewall. VPN do not easily inter-operate with NAT devices, because NAT uses private IP addresses that VPN devices do not recognize.
- All traffic over the VPN is encrypted, regardless of need. This can potentially cause bottlenecks, since encrypting data creates network overhead.
- Performance: With unpredictability of the internet performance is also a main concern. Private lines have guaranteed bandwidth that is agreed upon in the contract. An internet connection is also bought by the amount of bandwidth but can't be guaranteed across the entire internet. If there is overload of traffic in the internet it will greatly effect the performance. VPN industry needs to come up with a way to guaranty bandwidth across the internet.
- Currently there are many different VPN products, protocols, authentication and encryption algorithms. All of the different options add to the confusion of configuring a VPN. To add to the complexity, some vendors are creating their own proprietary solutions that only work with their products. The VPN industry needs more standards to be successful, options are good but too many confuse consumers.

Before analyzing the influence of the individual countries on the deployment of specific security solutions, it has to be mentioned that Plasdan has to try to understand the current technology landscape that exists. At this point it might seem very difficult to decide upon a particular solution, but it is crucial to understand how to choose the right solutions dependent on the underlying problems that must be addressed, the restrictions that have to be considered and of course the several characteristics that each of the Security solutions provide. Moreover, it is important to understand also, where the technology will likely head in the future, in order to be able to make the right choice which will be also up to date in the future.

# Chapter 8

# Country dependent Requirements and Dedicated Security Solutions

In this chapter I will investigate the different countries Plasdan operates in and plans to expand to, for aspects related to Internet Security and try to point out their influence on the proposed solutions in the previous chapters. In addition to these country dependent requirements, I will outline some existing security solutions which are proposed by one of the known vendors in the area of Internet and Network Security.

## 8.1 Country Requirements

It is of great importance for a company that plans to expand and operate in different countries, to have information about the various differences and characteristics of these countries, before marketing particular products or services. It is very important that an organization considers its environment before beginning this marketing process. In fact, such an analysis of the environment should be continuous and feed all aspects of planning. In the case of Plasdan it is essential for the company to investigate certain regulations and extraordinary features of the countries the company's branches are located in, before starting with the deployment of any of the proposed Security solutions.

In order to gain such information a macroeconomical analysis with the help of a PEST-Model has to be done. This means an analysis of the **P**olitical, **E**conomical, **S**ociocultural and **T**echnological aspects of Plasdans external macro-environment. [27] Due to the fact that many of this macro-environmental factors are country-specific, a PEST-analysis will need to be performed for all countries of interest. It is rather obvious that a precise and full scale PEST analysis of the individual countries is a huge project by itself and would go beyond the scope of this Master Thesis. Therefore, the form of the PEST-Analysis will be used, only to point out important and general issues related to the deployment of security solutions in the individual countries and induce Plasdan to take further actions in this area. This section will concentrate mainly on the political and technological factors of the model, while the economical and sociocultural aspects, will be described very briefly and in the interest of completeness, as they are not directly related to the Internet Security solutions. There can be found more detailed information about the different regulations and laws in the individual countries in Appendix D.

### 8.1.1 PEST-Analysis

The concept of the PEST analysis is to look at external factors which influence the business:

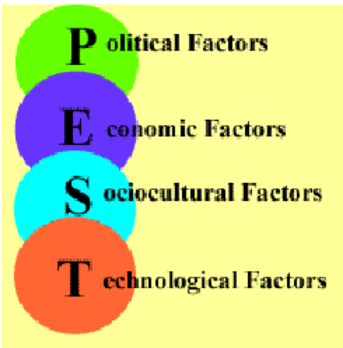



Figure 8.1: PEST-Analysis

#### Political Factors

The political arena has a huge influence upon the regulation of businesses and the spending power of consumers and other businesses. There must be considered issues such as the stability of the political environment, the legal framework and aspects related to governments policies. In the case of Plasdan the important parameters are the individual countries law regulations and guidelines concerning aspects related to Internet Security and the deployment of relevant solutions.

The Internet is of course no space free of law. All regulations and laws apply also to the Internet. According to Professor Michael Jaeger, the problem consists in the application and the necessary extension of the Law.[1] Many issues are still not clear, when applying laws to the Internet. There are certain regulations which have been renewed and rewritten in order to handle also Internet related issues. Some of them are:

- Trademark Law
- Copyright Law
- Legal Aspects of Electronic Commerce
- Taxation of Information Connected Activities
- Data Protection Law
- Cryptography Law

In the following I will concentrate on pointing out some important issues about some of these regulations.[2] Due to the uncertain state of a global legal framework for the Internet, the information in this section and the detailed explanation in the Appendix, should not be construed as legal advice or opinion on any specific facts or circumstances. There is a lot of movement on regulations regarding the Internet, both on a national and international basis. Therefore, Plasdan, or any other company operating in different countries, is advised to contact a qualified lawyer for specific advice. The contents are intended for general information purposes only and like I stated previously for motivation of further action on behalf of the reader.

[1] http://homepages.fh-giessen/~hg52/lv/eh/root.html [28]
[2] In Appendix D can be found detailed information on the individual laws in the different countries.

**Jurisdiction on the Internet** As the Internet creates a global village without global laws, jurisdiction on the Internet is a very important topic. When business is done over the Internet, it is important to know if it is covered by the jurisdictions of other countries. The concept of extra territoriality is critical for any type of business on the Web.

**Trademark Law** Globalization and the extensive use of the Internet has generated new challenges for the protection of intellectual property. Companies must act in an interactive way, but respecting cultural and legal aspects of each country. The Trademark Law finds its usage mainly in issues concerning the Internet Domain Name Application (the so called Domain Name Battle) and the registration of Software products.

**Copyright Law** The Internet is the sort of place where it is extraordinarily easy to copy and link information on any other Web page. A problem arises as soon as links are used to pretend to provide pieces of information that have been created by others. Although there are no rules regarding linking and copying, over the past few years it has become clear that so-called *deep linking* (i.e., direct linking of a particular Web page) is considered pirating a Web site, if done in large scale (there are numerous of examples of companies involved in accusations and legal charges, concerning linking and framing issues[3]). There is a pretty simple rule when it comes to the Internet. "If you didn't write it and you want to reproduce it, ask the creator". For a company like Plasdan it is important to be prepared and informed about issues like this.[4]

**Legal Aspects of Electronic Commerce** For E-Commerce related issues, most of the traditional laws are applicable. Companies which operate in the area of E-Commerce should especially be aware of problems occurring in the demonstrability of an act in the law. Special problems could occur also with the valency and validity of proof material concerning E-Commerce. If Plasdan is planning to expand also to E-Commerce it is important to get some legal advice in this field.

**Taxation of Information Connected Activities** The future of taxation of Internet related business is still uncertain. The Internet Tax Freedom Act (ITFA) is scheduled to sunset in the fall of 2002. State and local taxing authorities, who are well aware of the continued exponential growth of doing business on the Internet, are fighting for the right to tax this type of business, conducted within their states or by their residents. These state and local taxing authorities are expressing concern that their tax revenues - arguably the sole source of funding for some - will dry up if they are not permitted to tax Internet business. Others view the Internet as the greatest contribution to business since the industrial revolution and are wary of actions that might stunt its growth. In addition, opponents of Internet taxation have expressed a valid concern that, unless properly regulated, sellers on the Internet will be subject to multiple and discriminatory taxing.

**Data Protection Law and Cryptography Law** From the above laws applicable to Internet related issues, the Data Protection and Cryptography Law are the ones of most importance to Plasdan, when planning the deployment of security solutions in different countries. These two particular laws are closely connected to many of the features of the proposed solutions and could enforce or compromise the choice of deployment of particular solutions.

**Data Protection:** As a result of the rapid development in computer technology large quantities of information relating to individuals ("personal data") are routinely collected and used by public

[3] Microsoft was sued by Ticketmaster because it was providing direct links to the ticket sales portion on the Web site, by bypassing the Ticketmaster home page [29]

[4] Brad Templeton has written a very interesting article about intellectual property on the Web [30]

administrations and in every sector of business. Several Member states of the European Union have passed legislation protecting the fundamental rights of individuals and in particular their right to privacy from abuses resulting from the processing (i.e. the collection, the use, the storage etc.) of personal data.

Data protection laws provide for a series of rights for individuals such as the right to receive certain information whenever data are collected, the right of access to the data and if necessary, the right to have the data corrected and the right to object to certain types of data processing. These laws generally demand good data management practices on the part of the entities who process data ("data controllers") and include a series of obligations. These include the obligation to use personal data for specified, explicit and legitimate purposes, the obligation to guarantee the security of the data against accidental or unauthorized access or manipulation and in some cases the obligation to notify a specific independent supervisory body before carrying out all or certain types of data processing operations. These laws normally provide for certain safeguards or special procedures to be applied in case of transfers of data abroad. Although national data protection laws are to a certain extent similar, a number of differences exist between them. The level of protection guaranteed to the citizens in the Member States of the EU is not uniform (two Member states are still in the process of passing data protection laws). This situation creates potential obstacles to the free flow of information and additional burdens for economic operators and citizens, such as the need to register or be authorized to process data by supervisory authorities in several Member States, the need to comply with different standards and the possibility to be restricted from transferring data in other Member States of the EU. [31]

**Cryptography:** In the last few years there have been very controversial debates on possible restrictions on the use, import and export of cryptography. With more and more users starting to use cryptography as a means to hide their conversations from intruders, official bureaus regard it as necessary to be able to gain access to the encrypted data (Key Escrow[5] and law enforcement agencies and governments discuss the possibility of even disallowing encryption in order to keep up public safety.

Recent trends in international law and policy though, point toward continued relaxation of controls on cryptography. The Organization for Economic Cooperation and Development's (OECD) Cryptography Policy Guidelines and the Ministerial Declaration of the European Union, both released in 1997, argue for the liberalization of controls on cryptography and the development of market-based, user driven cryptography products and services. There is a growing awareness worldwide of encryption and an increasing number of countries have developed policies, driven by the OECD guidelines.

Export controls remain the most powerful obstacle to the development and free flow of encryption. The revised December 1998 Wassenaar Arrangement rolled back some of the liberalization sought by the OECD, particularly by restricting the key lengths of encryption products that can be exported without approval licenses. However, several major countries have already indicated that they do not plan to adopt new restrictions. [?]

For Plasdan it is important to research into depth the particular regulations for the different countries the company is operating or plans to operate. Appendix D might give some important guidelines on the individual countries.

### Economic Factors and Sociocultural Factors

The economic and social analysis of the individual countries a company is operating in, are of great importance when planning to market particular products and services. The fact that for Plasdan

[5] The concept of Key Escrow is that it allows the government and the police to decipher encrypted messages, because it allows the use of encryption only if a copy of the keys that are used for encryption have been sent to a governmental agency

this information is of minor interest for the deployment of any of the proposed Internet Security solutions, I have chosen to mention them epigrammatically and due to completeness, without going into detail for each country. Nevertheless it could be of interest for Plasdan to perform such an analysis, if they plan to market internationally some of their moulding systems.

**Economical Factors:** It is important to consider factors such as:

- The type of economic system in countries of operation
- Government intervention in the free market
- Comparative advantages of host country
- Exchange rates & stability of host country currency
- Efficiency of financial markets
- Infrastructure quality
- Skill level of workforce
- Labor costs
- Business cycle stage (e.g. prosperity, recession, recovery)
- Economic growth rate
- Discretionary income
- Unemployment rate
- Inflation rate
- Interest rates
- etc.

**Sociocultural Factors:** Important factors include:

- Demographics
- Class structure
- Education Culture (gender roles, etc.)
- Entrepreneurial spirit
- Attitudes (health, environmental consciousness, etc.)
- Leisure interests
- etc.

### Technological Factors

Another important part of the PEST-analysis which is of great importance for Plasdan for the deployment of Security solutions in the individual countries, is the technological aspect. Technology is not only vital for competitive advantage and a major driver of globalization, but it has also a big impact on the possibilities that Plasdan has, in applying some of the proposed, advanced security solutions. Factors like the Web-infrastructure and the service benefits by the Internet Service Providers (ISP's) in the individual countries, as well as the telecommunication and equipment in the Information Technology (IT) sector, can often decide about whether it is possible to deploy a certain solution or not.

From a more general point of view, the technological factors being extracted in the PEST analysis, include everything that affects a company's product, its market, or information-gathering efforts of the market that come as a result of changes in technology. Some of the features and aspects that have to be considered are:

- The recent technological developments in the area which is of interest for the company.
- The technology's impact on the product offering, or the implementation of certain services.
- The impact on the cost structure.[6]

[6]The important question to answer at this point is whether the technology researched, does allow for products and services to be made more cheaply.

- The impact on the value chain structure of the company.[7]
- The rate of technological diffusion

As mentioned also above in the section with the political factors of the PEST-analysis, a detailed investigation of the different technological aspects in the individual countries, Plasdan operates in, would go beyond the scope of the thesis. Therefore, in Appendix E has been included a summarization of some of the important issues for the deployment of the security solutions, in each country separately.[8]

## 8.2 Hardware and Software Solutions

This section of the report will describe existing Security solutions by one of the leading vendors of Internet and Network Security Systems. The chosen vendor is not any commitment for the deployment of a Security solution.

Moreover, it is rather obvious that the initial proposed solutions, mainly the ones at the application layer, do not need any further investigation from an availability point of view, because most of them can be obtained as free-or-shareware from their developers. Therefore, the following section will only concentrate on one of the major Security solutions, namely the deployment of a VPN.

### 8.2.1 Cisco Inc. Security Hardware and Software

Depending on the type of VPN (remote-access or site-to-site), a company will need to put in place certain components to build a security solution in that area. These might include:

- Desktop software client for each remote user
- Dedicated hardware such as a VPN concentrator or secure PIX firewall
- Dedicated VPN server for dial-up services
- NAS (network access server) used by service provider for remote-user VPN access
- VPN network and policy-management center

Like it has been mentioned before, because there is no widely accepted standard for implementing a VPN, many companies have developed turn-key solutions on their own. Cisco Inc. provides a combination of dedicated security solutions, security options available for networking products and consulting services and offers several VPN solutions. [33] Below are listed some of the products that make up the Cisco offerings. The breadth of these products provides a fairly complete set of security solutions for organizations to protect the availability, confidentiality and integrity of their systems.

- VPN concentrator: Incorporating the most advanced encryption and authentication techniques available, Cisco VPN concentrators are built specifically for creating a remote-access VPN. They provide high availability, high performance and scalability and include components, called scalable encryption processing (SEP) modules, that enable users to easily increase capacity and throughput. The concentrators are offered in models suitable for everything from small businesses with up to 100 remote-access users to large organizations with up to 10,000 simultaneous remote users.

[7] Given the difficulty in creating and maintaining value in an intensively competitive world of changing markets and technologies, business are forming value chains to meet new demands and remain viable.

[8] The information was extracted from booklets published by the Foreign Ministry of Denmark about the market profiles for the individual countries. This market profiles can be purchased for the particular information that is needed, namely in the case of Plasdan the IT sector.

- VPN-optimized routers: Cisco's VPN-optimized routers provide scalability, routing, security and QoS (quality of service). Based on the Cisco IOS (Internet Operating System) software, there is a router suitable for every situation, from small-office/home-office (SOHO) access through central-site VPN aggregation, to large-scale enterprize needs.
- Cisco secure PIX firewall: The PIX (private Internet exchange) firewall combines dynamic network address translation, proxy server, packet filtration, firewall and VPN capabilities in a single piece of hardware. Instead of using Cisco IOS, this device has a highly streamlined OS that trades the ability to handle a variety of protocols for extreme robustness and performance by focusing on IP. In the next table the different models available are compared on their performance characteristics

| Model | Throughput | Simultaneous Sessions |
|---|---|---|
| 506 | 10 Mbps | N/A |
| 515-R | 120 Mbps | 50,000 |
| 515-UR | 120 Mbps | 125,000 |
| 520 | 370 Mbps | 250,000 |

Table 8.1: Cisco Secure PIX Firewall Performance

- Cisco Secure Integrated Software: The Cisco Secure Integrated Software is a bundle of security features that integrate with Cisco IOS software. It can add firewall, intrusion detection, Data Encryption Standard (DES) (56-bit) encryption and secure administration capabilities to most of Cisco routers.
- Cisco Secure Access Control Server: The Cisco Secure Access Control Server (ACS) provides authentication, authorization and accounting (AAA) for users accessing network services. Cisco Secure ACS supports TACACS+ and RADIUS protocols. The ACS can be used as a centralized server or a distributed system comprised of multiple ACS systems. It can also interface to other third-party RADIUS or TACACS+ systems in a distributed configuration. In a distributed environment, the ACS can act as a proxy and automatically forward an authentication request to another AAA server
- Cisco Secure Intrusion Detection System: An intrusion detection system (IDS) can help to make you aware of the nature and frequency of attacks against your network and systems. From the information provided by the IDS, a company can design an appropriate response to reduce the risks to your systems from these attacks.It is a real-time network intrusion detection system. The system consists of sensors and a director. A system can be implemented with a single sensor at a strategic location, or multiple sensors placed at many well-chosen locations in the network. Sensors operate in promiscuous mode and passively analyze the network traffic that appears on its interface for unauthorized activity. The IDS sensor will report traffic matching attack signatures to the director. The sensor can also be configured to actively change ACLs on Cisco routers in response to attack signatures. The sensor is a hardware and software appliance. The Director is the management station. It receives the alerts from sensors locally or remotely located.
- Cisco Secure Policy Manager: The Cisco Secure Policy Manager is a comprehensive security management system for Cisco Secure products. Security policies can be defined, distributed, enforced, and audited for multiple PIX Firewalls and VPN routers from a central location. Cisco Secure Policy Manager supports IPSec VPN, user authentication, and in a future version will support intrusion detection, and vulnerability scanning technologies. Its use on routers requires that Cisco Secure Integrated Software be installed. The Policy Manager centralizes the management of security policies, monitoring of status, and reporting of policy events. It can help to ensure a consistent application of policies across hundreds of devices, and will save the company's time by automating portions of the policy creation and distribution.

- Cisco Secure Consulting Services: Cisco Secure Consulting Services are targeted to large corporate and government customers. It offers two types of professional services:
  - Security Posture Assessments: This service provides comprehensive security analysis of large, complex networks. Cisco will test your network security from the perspective of external attackers, disgruntled employees, or contractors. They will make recommendations on security measures needed to improve network security.
  - Incident Control and Recovery: This service is an emergency response to a hostile network incident. Cisco can provide short-notice assistance to restore control and availability of your network.

It becomes clear that there are almost unlimited possibilities when it comes to the choice of deployment of a particular Security solution. The offers and proposals vary from just individual security components that can be integrated to the existing network, to complete solution packages, like we saw with Cisco. Some of the vendors even give the possibility to automate through their system the entire process of building up a Security Strategy and Policy, issues we saw in Chapter 3 and 4.

Personally I believe that Plasdan, or any company that plans to extend their network, should take the discussed issues related with Internet Security to heart, before rushing to buy some expensive security package, which might turn out to be not suitable after all.

# Chapter 9

# Conclusion

The growth of the Internet and its reach into the fabric of business and personal life has outdistanced most organization's ability to protect their information systems. This increased exposure and the constant escalation of threats to network security have increased the need for effective controls that can restore availability, confidentiality and integrity of the compromised information systems.

This master thesis describes this growing problem of protecting networked systems, by identifying security threats and risks of networks, that don't take the necessary security measures. A detailed methodology on how to plan and realize a security policy provides necessary information to address systematically the growing vulnerabilities. As part of the implementation of such a security policy, a number of security solutions are presented, which are being compared on various features and characteristics.

The entire investigation and analysis is based on Plasdan's current network architecture and configuration, where all of the proposed security solutions can be deployed. An analysis of the different countries Plasdan operates in, provides necessary information also for the surounding environment, enabling a multidisciplinary evaluation.

This thesis, with the level of information that it provides, gives Plasdan the opportunity to start with the realization of a security policy for their company. The various proposed solutions give an overview of the existing technologies, making the choice for deployment easier.

## Personal Preference

Setting the various characteristics and advantages of the proposed solutions to contrast with Plasdan's ambitions and reasons for implementing a security solution, left no doubt about which would be most suitable. Personally I think that a deployment of a Virtual Private Network, in combination with IPSec, will give Plasdan exactly what they wanted, from an organizational point of view, providing at the same time security features which overexceed any other implementation.

At the moment there is no security measure present at the company. Due to the fact that just the planning of a VPN solution is very time consuming, it is recommended that Plasdan deploys a security solution as fast as possible, which addresses the most crucial threats and vulnerabilities the company has. By having a certain level of security already in place, it is easier in the future to expand, or change the existing solution.

It has to be mentioned, that following the guidelines and procedures in this master thesis, does not guarantee a secure environment, nor does it guarantee that it will prevent all penetrations. It has been stated from the beginnig that absolute security cannot be achieved. However, it is possible to achieve reasonable security by establishing a good security policy and maintaining and monitoring all systems with sound system administration practices.

While no one product or system can provide complete protection, security can be layered to provide reasonable risk management reduction of vulnerabilities.

## Future Work

Due to the limited time provided for such a wide subject, it was not possible to undergo all individual steps of a full scale security planning for Plasdan. Many steps where just left as guidelines, or where done on a theoretical level. It would be very interesting to actually go through the entire process of security planning for a security solution. Moreover, the physical deployment of a chosen solution together with a comparison with the initial security level could be very helpful for future development and backup of the entire theory provided.

To conclude, it has to be stated that the Internet offers many more opportunities than threats. It is necessary however to take precautions to safeguard Plasdan's or any company's information assets. A wealth of presented solutions are available to help your company secure its network and establish access controls at each point of risk. Technology alone is only part of the solution. Probably the most vital element is a written security policy or statement that explains the guidelines and procedures that should be followed. The sentiment and content of the document needs to be shared with the organization. Only with the cooperation of your staff wiil your network be truly secure.

# Appendix A

# Requirement Document for Plasdan

The following requirement document is the document that was proposed to the contact persons at Plasdan and was approved after some minor changes. It was build according to the proposed layout of Ian Sommervilles book Software Engineering. [2] It has to be denoted though that due to the very initial stage the project was at the time the document was produced, it is only a rough layout of the proposed steps in the book and is intended only to provide to the company an overview of the project and its objectives and to exclude misunderstandings about the goals and technics used.

## Introduction

This document is intended to provide the requirements for possible secure internet/network solutions for the mould engineering company Plasdan. The proposed solutions will involve an upgrade to the already existing network of Plasdan.

## Internet Security Project

### Project Objectives

The objective of this Internet security project is to research and suggest a variety of network/internet solutions for the company Plasdan, in order to interconnect the different branches of the company which are located in different countries in Europe and one in Brazil. Concerning the internationally distributed locations of the company, these different solutions must be applied to the companies needs and objectives which will be described as part of this requirement document. The solutions will be compared and evaluated according to different aspects like security, cost, implementation effort and availability in the different locations of the branches. Their advantages and disadvantages will be pointed out, in order to make the right choice easier.

### Project Goals

1. To research different ways of secure interconnection between the branches of Plasdan
2. To adjust the different solutions to specific extracted needs and characteristics of the company
3. To investigate into depth the security aspects involved and the limitations that have to be taken into consideration

4. If time permits to set-up and simulate a chosen solution on Plasdans network in order to visualise the enhanced possibilities it provides and offers

### Project Guiding Principles

1. Take advantage of a number of existing enabling technologies
2. Leverage the existing infrastructure of the company
3. The system must conform to standards including those mandated by the different governments involved for on-line transfer of metadata and data
4. The user should experience a single information system and not be forced, if possible, to learn to manage several.

### Intended Users of the system

The users of the system consist of the broad spectrum of Plasdans employees and also the company's customers. These users include, but are not limited to engineers, administrative stuff, CAD- and Maintanceengineerrs, accounting personnel and the general customers involved with Plasdan. It should be recognised that the broad base of users described above implies also a broad range of computing technologies will be used to access the system.

### Overview of Plasdans structure ( Domain Analysis)

Plasdan is a mould engineering company which links clients to particular mould making processes. They are active in many countries like Portugal, Brazil and Holland and are planning to expand also in Denmark and Germany. It would be a big improvement and of great importance, if possible solutions of an interconnection of these different branches, for purposes like data transfer, communication, customer relations, remote access etc. would be researched and proposed. It is rather obvious that due to this co-operational working style, a fast, secure and stable communication is essential for a company like Plasdan.

### Problems/Drawbacks of the current system/network

Due to the fast expanding structure of Plasdan the existing network is lacking in many aspects, like speed, reliability and security. Due to the fact that except from normal mail traffic, file transfers of bigger sized files are a daily routine, the existing ISDN connection is not adequate. At the moment no secure transfer is being used, so the company's files and data are very vulnerable to attacks of any kind. Apart from that, no additional security technologies are implemented in order to protect the networks integrity from outside threats. Moreover the existing network, does not provide any facilities of interconnecting the different branches securely and exchanging data. All this is done openly over the internet at moment.

### Assumptions

Due to the limited time provided, this project will provide Plasdan a number of different solutions for their network architecture which will enable a secure interconnection between the different locations. These different solutions will be compared according to individual criteria and in the end a full evaluation will be presented. If time still permits, a choice of an individual solution is possible to be simulated and tried on Plasdans existing network.

### General Requirements

- The suggested solutions shall provide a possibility for the users to connect between different branches of the company securely
- The solutions shall provide a facility for users to communicate with eachother over NetMeeting technologies
- The proposed systems shall enable a fast and secure file transfer between the different locations
- A possibility for customers to view their individual orders and the progress of their projects shall be provided by the system
- Viewing work activity at the different branches of Plasdan should be possible
- Customers and employees shall have the possibility of connecting to the existing network from remote locations
- The proposed solutions shall conform with governmental rules in the individual countries Plasdan is located
- An expansion of the network beyond immediate geographic areas shall be provided
- Immediate, fast, secure and reliable communication shall be possible
- United Kingdom was added to the list of the cooperate partners of Plasdan
- Further suggestions by the company

This requirement document is just a main outline of the requirements I extracted while being down in Portugal and looking at the location and interviewing people. It would be a great advantage and very helpful for the further successful development of the project if I would get a feedback on this requirement document. I'm positive that by the time you will be reading this a number of comments, suggestions and even further requirements will come up and be extracted which you should mention in your answer. I'm planning that by middle/end of March we will have finalised this requirements document in order for me to base my further research upon that. It will be a much more successful project and the result will be more useful and efficient if we can agree on the final requirements for Plasdan and adjust the proposed solutions exactly upon this agreement.

# Appendix B

# Methods, Tools and Techniques for Attacks

Malicious attackers use various method, tools, and techniques to enter, disrupt, and steal information from a system.

## B.1 E-mail Hacking

The most common mail transfer protocols (SMTP, POP3, IMAP4) do not typically include provisions for reliable authentication as part of the core protocol, allowing e-mail messages to be easily forged. Nor do these protocols require the use of encryption that could ensure the privacy or confidentiality of e-mail messages. Although extensions to these basic protocols do exist, the decision whether to use them needs to be established as part of the mail server administration policy. Some of the extensions use a previously established means of authentication while others allow the client and server to negotiate a type of authentication that both ends support.

## B.2 Social Engineering

This is a common form of cracking. It can be used both by outsiders and by people within an organization. Social engineering is a hacker term for tricking people into revealing their password or some form of security information.

Users should be made aware of various security issues, even those that are not common. A common example of social engineering would be where a hacker sends e-mail to an employee, claiming to be an administrator who needs the employee's password to do some administrative work. The normal user who has not been taught about security might not know the difference between the actual administrator and the imposter administrator, especially in a large organization. Other variations of this type of social engineering would be where someone claiming to be the administrator phones a user and asks for the user's password and logon credentials. The user unwittingly gives out the logon and password and the imposter now has full access.

"Shoulder surfing" is also common among hackers and users who wish to learn someone's password. In this case, they hang around a user's desk, talking and waiting for the user to type in a password. Company employees with malicious intent could also do this. Users should be informed not to type in their passwords in front of others or, if they have and suspect that someone else now has their password, that they should change the password immediately.

Another form of social engineering is guessing a user's password. When people can learn things about certain users' personal and social lives, they can use this against them. For example, users might choose a daughter or son's name or birth date or a friend's name as a password. Users also often use passwords that they can read on their desks or on posters in the work area. This gives the hacker a chance at guessing the password.

## B.3 Intrusion Attacks

Attackers using well-known techniques can penetrate many networks. This often happens when attackers use known vulnerabilities in the network. In updateable systems, administrators may not have or take the time to install all the necessary patches in a large number of hosts. In addition, it is usually not possible to perfectly map an organization's policy on computer use to its access-control mechanisms and thus authorized users often can perform unauthorized actions.

Users may also demand network services and protocols that are known to be flawed and subject to attack. For example, a user might ask, "Why can't I just FTP the files down?" It is very important that security policies deal not only with end-user demands but also with the threats and vulnerabilities associated with those demands. Realistically, however, it is seldom possible to remove all vulnerabilities.

Intrusion detection is the process of detecting unauthorized use of, or an attack upon, a computer or network. Intrusion detection provides two important functions in protecting information system assets.

The first function is that of a feedback mechanism that informs the security staff about the effectiveness of other components of the security system. The lack of detected intrusions is an indication that there are no known intrusions, not that the system is completely impenetrable.

The second function is to provide a trigger or gating mechanism that determines when to activate planned responses to an incident. A computer or network without an intrusion detection system (IDS) may allow attackers to leisurely explore its weaknesses. If vulnerabilities exist in networks, a determined attacker will eventually find them and exploit them. The same network with an IDS installed is a much more formidable challenge to an attacker. Although the attacker may continue to probe the network for weaknesses, the IDS should be able to detect these attempts if the vulnerabilities are known, block these attempts, and alert security personnel who can take appropriate action.

## B.4 Denial-of-Service Attacks

### Background

DoS attacks are designed to prevent legitimate use of a service. Attackers achieve this by flooding a network with more traffic than it can handle. Examples of this include:

- Saturating network resources, thereby preventing users from using network resources.
- Disrupting connections between two computers, preventing communications between services.
- Preventing a particular individual from accessing a service.
- Disrupting services to a specific system or client.

DoS attacks flood a remote network with an enormous amount of protocol packets. Routers and servers eventually become overloaded by attempting to route or handle each packet. Within minutes, network activity exponentially rises and the network stops responding to normal traffic and service requests from clients. This is also known as a network saturation attack or bandwidth consumption attack. Attackers strike with various tools, including Trin00 and Tribe Flood Network (TFN, TFN2K).

### Types of Denial-of-Service Attacks

Computers use certain core resources to operate and function correctly. Failure or disruption of resources could cause the computer to crash. Some of these resources include network bandwidth, memory, CPU time, and hard drive space. The operating system and applications than run on the system play an important role in managing these resources correctly. When the operating system or the resources are overrun by malicious attacks, one or more of these core resources breaks down, causing the system to crash or stop responding. An attacker can cause resources to be overrun by various means, including consuming server resources, saturating network resources, and mail bombing.

### Consuming Server Resources

The goal of a DoS attack is to prevent hosts or networks from communicating on the network. An example of this type of attack is the SYN flood attack:

When a client attempts to contact a server service, the client and server exchange a series of messages. The client starts by sending a TCP connection request or SYN message to the server. The server responds to the SYN message with an acknowledgement ACK-SYN message. The client then acknowledges the server's ACK-SYN message with an ACK message. After these three actions take place, the connection between the client and server is open and they can exchange service-specific data.

The problem arises when the server has sent the SYN-ACK message back to the client but has not yet received an ACK response from the client. This is now a half-open connection. The server keeps the pending connection in memory, waiting for a response from the client. The half-open connections in memory eventually will time out on the server, freeing up valuable resources again.

Creating these half-open connections is accomplished with IP spoofing. The attacker's system sends a SYN message to the victim's server. These messages seem to be legitimate but in fact are references to a client system that is unable to respond to the server's SYN-ACK message. This means that the server will never be able to send an ACK message to the client computer. The server now has half-open connections in memory and eventually will fill up the server connections. The server now is unable to accept any new connections. The time limit on half-open connections will expire. However, the attacker's system keeps sending IP-spoofed packets faster than the expire limit on the victim's server. In most cases the victim of such an attack will have difficulty accepting any new, legitimate incoming connections.

This type of attack does not really affect any of the current connections or outgoing connections. Normally it consumes an enormous amount of memory and processing power on the server, causing it to crash. The location of the attacking system is difficult to trace because the attacker's system address was masquerading as a legitimate IP address. Since the network forwards packets based on destination address, the only way to validate the source of a packet is to use input source filtering.

This type of attack does not depend on the attacker being able to consume network bandwidth. In this case, the intruder is consuming valuable server resources. The implication is that an intruder can execute this attack from a dial-up connection against a computer on a very fast network.

## Saturating Network Resources

An intruder may also be able to consume all the available bandwidth on a network by generating a large number of packets directed to the network. Typically, these packets are Internet Control Message Protocol (ICMP) echo packets, but in principle they may be anything. Further, the intruder need not be operating from a single computer; he or she may be able to coordinate or co-opt several computers on different networks to achieve the same effect. This is known as a distributed denial-of-service attack (DDoS).

The ICMP is used to convey status and error information including notification of network congestion and other network-related problems. ICMP can be used to determine if a computer on the Internet is responding. To do this, an ICMP echo request packet is sent to a computer on the network. If the computer is operating, it will respond to the request by sending an ICMP echo reply packet. A common example of this is the PING command.

On TCP/IP networks, a packet can be sent to an individual computer or broadcast to all computers on the network. When an IP packet is sent to an IP broadcast address from a computer on the same local area network, all computers on that network receive the IP packet. When a computer outside the local area network sends an IP broadcast packet, all computers on the target network receive the broadcast packet (as long as the routers have been configured to forward these broadcast packets).

Three parties are involved in these attacks: the attacker, the intermediary, and the victim. The intermediary can also be a victim. The intermediary receives an ICMP echo request packet that is directed to the IP broadcast network address. If nothing is filtering these ICMP echo requests, all computers on the network will receive the ICMP echo request packet and respond with an ICMP echo reply packet. When all computers respond to these packets, severe network congestion or outages are possible.

When the attackers create these packets, they do not use their own IP source address. Instead, they use the source address of their intended victim. This is known as IP spoofing. The result is that when the intermediary computers respond to the ICMP echo request packet, they send the reply packet to the victim's IP address. The victim's computer is now subjected to network congestion that could cause the network to stop responding.

Attackers have developed a variety of tools for this purpose. The tools enable the hackers to send ICMP echo request packets to multiple intermediary computers, causing all of them to respond to the same victim's source IP address. These tools could also be used to scan for network routers that do not filter broadcast traffic.

DDoS attacks involve breaking in to hundreds or thousands of computers across the Internet. Then the attacker installs DDoS software on them, allowing the attacker to control all of these computers and launch coordinated attacks on victim sites. These attacks typically exhaust bandwidth, router processing capacity, or network stack resources, breaking network connectivity to the victims.

The perpetrator starts by breaking into weakly secured computers, using well-known defects in standard network service programs, and common, weak configurations in operating systems. Then they perform some additional steps on each system. First, they install software to conceal the break-in and to hide the traces of their subsequent activity. For example, they replace the standard commands for displaying running processes with versions that fail to display the attacker's processes.

Then they install a special process used to remotely control the burgled computer. This process accepts commands from over the Internet, letting the intruder launch an attack over the Internet against some designated victim site. Finally, they make a note of the IP address of the computer they've taken over.

All these steps are highly automated. A cautious intruder will begin by breaking in to just a few sites, then using them to break into some more, and repeating this cycle for several steps. By the time they are ready to mount the attacks, they have taken over thousands of computers and assembled them into a DDoS network. Once the attacker has installed the DDoS software, the attacker runs a single command that sends command packets to all the captured computers, instructing them to launch an attack (from a menu of different varieties of flooding attacks) against a specific victim. When the attacker decides to stop the attack, he or she sends another single command.

The controlled computers being used to mount the attacks send a stream of packets. For most of the attacks, these packets are directed at the victim computer. For one variant (called "smurf," after the first circulated program to perform this attack), the packets are aimed at other networks, where they provoke multiple echoes all aimed at the victim as described earlier.

The packets used in DoS attacks use forged source addresses or spoofed IP addresses. If a packet arrives at the first router, and the source IP address doesn't match the IP network it's coming from, the router should discard the packet. This style of packet checking is called ingress or egress filtering, depending on the point of view; it is egress from the customer network, or ingress to the heart of the Internet.

The first signs of an attack may be when thousands of compromised systems all over the world begin to flood the victim's network with traffic all at once. The first symptom is likely to be a router crash, or something that looks a lot like one; traffic simply stops flowing between the victim and the Internet.

## B.5 Mail Bombing

Mail bombing is an e-mail-based attack. E-mail floods the attacked system until it fails. A system will fail in different ways, depending on the type of server and how it is configured. Some Internet service providers give temporary accounts to anyone who signs up for a trial subscription, and those accounts can be used to launch e-mail attacks.

Here are typical failure modes:

- The e-mail server accepts e-mail messages until the disk where e-mail is stored fills up. Subsequent e-mail is not accepted. If the e-mail disk is also the main system disk, it may crash the system.
- The incoming queue is filled with messages to be forwarded until the queue reaches its limit. Subsequent messages can't be queued.
- A particular user's server disk quota can be exceeded. This prevents subsequent mail from being received and may keep the user from getting work done. Recovery can be difficult because the user may need to use more disk space just to delete the e-mail.

## B.6 Virus Attacks

### History

All administrators have heard about viruses and their effects. Viruses can be very destructive, causing loss of information. Fred Cohen formally defined the term "computer virus" in 1983 when he performed academic experiments on a Digital Equipment Corporation VAX system.

Viruses are classified as being one of two types: research or "in the wild." A research virus is one that has been written for research or study purposes and has received almost no distribution to the public. Viruses that have been seen with regularity are termed "in the wild."

The first computer viruses were developed in the early 1980s. The first viruses found in the wild were Apple II viruses such as Elk Cloner, which was reported in 1981. Viruses now have been found on the following platforms: Apple II, IBM PC, Macintosh, Atari, and Amiga.

When personal computers first came onto the market, operating systems like Microsoft MS-DOSő were intended for a single user who was in total control of the computer. There were no security mechanisms to separate users, to separate the user from the system, or to stop intentional modification of system or user files.

Given the ways computers were used, these mechanisms were not required. However, the spread of computers instigated a new industry that grew around them. This included the emergence of:

- Commercial software products such as spreadsheets and word processors.
- Computer games.
- Shared use of computers, whether it be several employees using the same computer or large organizations connecting computers on a LAN.

Note that all viruses found in the wild target personal computers. As of today, the overwhelming numbers of virus strains are IBM PC viruses.

Viruses have evolved over the years due to efforts by their authors to make the code more difficult to detect, disassemble, and eradicate. This evolution has been especially apparent in the IBM PC viruses. An examination of the IBM PC family of viruses indicates that the most commonly detected viruses vary according to continent, but that "Stoned," "Brain," "Cascade," and members of the "Jerusalem" family have spread widely and continue to appear. This implies that highly survivable viruses tend to be benign, replicate many times before activation, or are somewhat innovative, utilizing some technique never used before in a virus.

Personal computer viruses exploit the lack of effective access controls in these systems. The viruses modify files and even the operating system itself. These are legal actions within the context of the operating system. While more stringent controls are in place on multitasking, multiuser operating systems, configuration errors and security holes (security bugs) make viruses on these systems more than theoretically possible.

With the advent of the personal computer, software was exchanged on floppy disks, software for professional and private use ran on the same computer, and companies moved information onto computers that no longer were controlled by a central IT department but by individual users. The lack of security mechanisms and security awareness on these systems started to make itself felt.

Virus researchers have put considerable effort into developing schemes for describing, naming, and classifying computer viruses and on defining the distinctive features that distinguish computer viruses from other malicious software

## How Viruses Work

A computer virus is a piece of self-replicating code attached to some other piece of code. This code can be harmlessŮfor example, it might display a message or play a tune. Or it might be harmful and proceed to delete and modify files.

The virus code searches users' files for an uninfected executable program for which the user has security write privileges. The virus infects the file by putting a piece of code in the selected program file. When a program that is infected with a virus is executed, the virus immediately takes command, finding and infecting other programs and files.

Some viruses are "memory resident" viruses. When a user executes an executable file that is infected with this type of virus, the virus loads itself into memory and remains there even if the original program is shut down. Subsequent programs that are executed are infected with the virus until the computer is shut down or turned off. Some viruses have a "dormant" phase and will appear only at certain times or when certain actions are performed.

A **variant** is a virus that is generated by modifying a known virus. Examples are modifications that add functionality or evade detection. The term "variant" usually applies only when the modifications are minor. An example would be changing the trigger date from Friday the 13th to Thursday the 12th.

An **overwriting** virus will destroy code or data in the host program by replacing it with the virus code. It should be noted that most viruses attempt to retain the original host program's code and functionality after infection because the virus is more likely to be detected and deleted if the program ceases to work. A non-overwriting virus is designed to append the virus code to the physical end of the program or to move the original code to another location.

A **self-recognition** procedure is a technique whereby a virus determines whether or not an executable is already infected. The procedure usually involves searching for a particular value at a known position in the executable. Self-recognition is required if the virus is to avoid multiple infections of a single executable. Multiple infections cause excessive growth in size of infected executables and corresponding excessive storage space, contributing to the detection of the virus.

A **resident** virus installs itself as part of the operating system upon execution of an infected host program. The virus will remain resident until the system is shut down. Once installed in memory, a resident virus is available to infect all suitable hosts that are accessed.

A **stealth** virus is a resident virus that attempts to evade detection by concealing its presence in infected files. To achieve this, the virus intercepts system calls that examine the contents or attributes of infected files. The results of these calls must be altered to correspond to the file's original state. For example, a stealth virus might remove the virus code from an executable when it is read (rather than executed) so that an anti-virus software package will examine the original, uninfected host program.

An **encrypted** virus has two parts: a small decryptor and the encrypted virus body. When the virus is executed, the decryptor will execute first and decrypt the virus body. Then the virus body can execute, replicating or becoming resident. The virus body will include an encryptor to apply during replication. A variably encrypted virus will use different encryption keys or encryption algorithms. Encrypted viruses are more difficult to disassemble and study since the researcher must decrypt the code.

A **polymorphic** virus creates copies during replication that are functionally equivalent but have distinctly different byte streams. To achieve this, the virus may randomly insert superfluous instructions, interchange the order of independent instructions, or choose from a number of different encryption schemes. This variable quality makes the virus difficult to locate, identify, or remove.

A **research** virus is one that has been written, but has never been unleashed on the public. These include the samples that have been sent to researchers by virus writers. Viruses that have been seen outside the research community are termed "in the wild."

## How Are Computer Viruses Spread?

The following are necessary characteristics of a virus:

- It is able to replicate.
- It requires a host program as a carrier.

- It is activated by external action.
- Its replication ability is limited to the (virtual) system.

Computer viruses move from computer to computer by attaching themselves to files or boot records of disks and diskettes. These days it is not uncommon to find them in e-mail attachments and other programs that can be downloaded from the Internet.

A virus is a relatively passive agent that relies on ordinary users for its activation and propagation. It can travel from one file to another on the same computer if the infected file is executed, from computer memory to a file on disk, on a disk that is carried from one computer to another (some companies prohibit floppy drives, thereby preventing users from copying information onto their computers), on e-mail attachment executable files, and over a modem or network connection.

### Damage that Viruses Cause

Viruses can destroy file allocation tables (FAT) and lead to the corruption of an entire file system, resulting in the need to fully reinstall and reload the system. Viruses also can create bad sectors on the disk, destroying parts of programs and files. They can decrease the space on hard disks by duplicating files. They also can format specific tracks on the disks or format the entire disk.

Viruses can destroy specific executable files and alter data in data files, causing a loss of integrity in the data. Viruses can cause the system to hang so that it does not respond to any keyboard or mouse movements.

## B.7 Trojan Horses Background

The term "Trojan horse" comes from a myth in which the Greeks gave a giant wooden horse to their foes, the Trojans, seemingly as a peace offering. After the Trojans dragged the horse inside the city walls of Troy, Greek soldiers sneaked out of the horse's hollow belly and opened the city gates, allowing their compatriots to pour in and capture Troy.

### What Are Trojan Horses?

A Trojan horse is code hidden in a program such as a game or spreadsheet that looks safe to run but has hidden side effects. When the program is run, it seems to function as the user expects, but in actuality it is destroying, damaging, or altering information in the background. It is a program on its own and does not require a host program in which to embed itself. An example of a Trojan horse would be a Christmas executable that, when executed, pops up with an animated figure of Santa Claus and a caption saying "Merry Christmas." In the background, extra code could be deleting files or performing other malicious actions.

### How Trojan Horses Are Spread

Trojan horses generally are spread through e-mail and exchange of disks and information between computers. Worms could also spread Trojan horses.

### Damage Caused by Trojan Horses

The damage that Trojan horses cause is much the same as what a virus causes. Most of the time the users are unaware of the damage it is causing because of the Trojan horse's masking effect.

## B.8 Worms Background

Worms first were used as a legitimate mechanism for performing tasks in a distributed environment. Network worms were considered promising for the performance of network management tasks in a series of experiments at the Xerox Palo Alto Research Center in 1982. The key problem noted was worm management; controlling the number of copies executing at a single time.

Worms were first noticed as a potential computer security threat when the Christmas Tree Exec attacked IBM mainframes in December 1987. It brought down both the worldwide IBM network and BITNET. The Christmas Tree Exec wasn't a true worm. It was a Trojan horse with a replicating mechanism. A user would receive a Christmas card by e-mail that included executable (REXX) code. If executed, the program claimed to draw a Christmas tree on the display. That much was true, but it also sent a copy to everyone on the user's address lists.

The Internet Worm was a true worm. It was released on November 2, 1988. It attacked Sun and DEC UNIX systems attached to the Internet (it included two sets of binaries, one for each system). It utilized the TCP/IP protocols and vulnerabilities in sendmail, common application layer protocols, operating system bugs, and a variety of system administration flaws to propagate. Various problems with worm management resulted in extremely poor system performance and a denial of network service. It exploited operating system flaws and common system management problems.

### What Are Worms?

The following are necessary characteristics of a worm:

- It is able to replicate.
- It is self-contained and does not require a host.
- It is activated by creating process (it needs a multitasking system).
- If it is a network worm, it can replicate across communication links.

A worm is a program designed to replicate. The program may perform any variety of additional tasks as well. The first network worms were intended to perform useful network management functions. They took advantage of system properties to perform useful actions. However, a malicious worm takes advantage of the same system properties. The facilities that allow such programs to replicate do not always discriminate between malicious and good code. Worms exploit flaws (that is, bugs) in the operating system or inadequate system management to replicate. Release of a worm usually results in brief outbreaks, shutting down entire networks.

Worms are programs that run independently and travel from computer to computer across network connections. Worms may have portions of themselves running on many different computers. Worms do not change other programs, although they may carry other code that does.

### How Worms Affect Network Systems

Developing a worm requires a network environment and an author who is familiar not only with the network services and facilities, but also with the operating facilities required to support them once they've reached the computer. Protection against worm programs is like protection against break-ins. If an intruder can enter your computer, so can a worm program. If the computer is secure from unauthorized access, it should be secure from a worm program.

### How Worms Are Spread

Worms are autonomous agents capable of propagating themselves without the use of another program or intervention or action by a user. Worms are found primarily on computers that are capable of multitasking and are connected by a network.

### Damage that Worms Can Cause

Most worms disrupt services and create system management problems. Some worms scan for passwords and other loopholes and then send the information back to the attacker. In some cases worms can install Trojan horses or viruses that cause damage to the systems.

Macro Viruses A macro virus is a virus that attaches itself to a spreadsheet worksheet, or is programmed into the spreadsheet. It also could be programmed into other products such as Word documents and Microsoft PowerPoint©presentations and so on.

Macro viruses are written in high-level languages like Visual Basic©for applications used by Microsoft©Office products, Lotus©scripting, WordPerfect©macros, and so on. Macro viruses bypass integrity protection mechanisms for normal executables because macro viruses are embedded in the data file. Documents are widely exchanged by e-mail and therefore are a good medium for spreading a virus. Users opening a file may not even be aware of the fact that they are running a program. All instructions available for writing macros are also available to virus writers who now can hide viral code in a macro file.

An example of a macro virus is the Melissa macro virus. The Melissa macro virus was spread via e-mail. The virus was programmed into a Word document. When the document was opened, the macro virus would send a copy of it to the first 50 e-mail addresses from the global address list. This caused major e-mail systems to crash throughout the world and also saturated network bandwidth.

# Appendix C

# Tunnelling Protocols

## C.1 Point-to-Point Tunnelling Protocol

The Point-to-Point Tunnelling Protocol (PPTP) encapsulates Point-to-Point Protocol (PPP) frames into IP datagrams for transmission over an IP-based internetwork, such as the Internet or a private intranet. PPTP is documented in RFC 2637. [?]

The PPTP uses a TCP connection known as the PPTP control connection to create, maintain, and terminate the tunnel and a modified version of Generic Routing Encapsulation (GRE) to encapsulate PPP frames as tunnelled data. The payloads of the encapsulated PPP frames can be encrypted or compressed or both.

PPTP assumes the availability of an IP internetwork between a PPTP client (a VPN client using the PPTP tunnelling protocol) and a PPTP server (a VPN server using the PPTP tunnelling protocol). The PPTP client might already be attached to an IP internetwork that can reach the PPTP server, or the PPTP client might have to dial into a network access server (NAS) to establish IP connectivity as in the case of dial-up Internet users.

Authentication that occurs during the creation of a PPTP-based VPN connection uses the same authentication mechanisms as PPP connections.

For Internet-based PPTP servers, the PPTP server is a PPTP-enabled VPN server with one interface on the Internet and a second interface on the intranet.

### C.1.1 Tunnel Maintenance with the PPTP Control Connection

The PPTP control connection is between the IP address of the PPTP client using a dynamically allocated TCP port and the IP address of the PPTP server using the reserved TCP port 1723. The PPTP control connection carries the PPTP call control and management messages that are used to maintain the PPTP tunnel. This includes the transmission of periodic PPTP Echo-Request and PPTP Echo-Reply messages to detect a connectivity failure between the PPTP client and PPTP server. PPTP control connection packets consist of an IP header, a TCP header, and a PPTP control message as illustrated in the following Figure. The PPTP control connection packet in the following Figure also includes a data-link layer header and trailer.

For information about the exact structure of PPTP control connection messages, see RFC 2637.

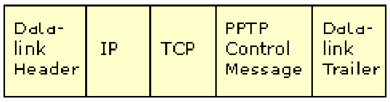



Figure C.1: PPTP Control Connection Packet

### C.1.2 PPTP Data Tunnelling

PPTP data tunnelling is performed through multiple levels of encapsulation.

The following Figure shows the resulting structure of PPTP tunnelled data.

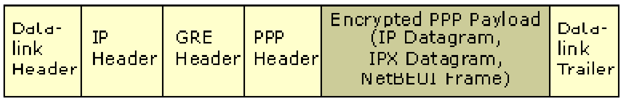



Figure C.2: PPTP Tunnelled Data

#### Encapsulation of PPP Frame

The initial PPP payload is encrypted and encapsulated with a PPP header to create a PPP frame. The PPP frame is then encapsulated with a modified GRE header. GRE is documented in RFC 1701 and RFC 1702 and was designed to provide a simple, lightweight, general purpose mechanism for encapsulating data sent over IP internetworks. GRE is a client protocol of IP using IP protocol 47.

For PPTP, the GRE header is modified in the following ways:

- An acknowledgement bit is used to indicate that a 32-bit acknowledgement field is present and significant.
- The Key field is replaced with a 16-bit Payload Length field and a 16-bit Call ID field. The Call ID field is set by the PPTP client during the creation of the PPTP tunnel.
- A 32-bit Acknowledgement field is added.

#### Encapsulation of GRE Packet

The resulting GRE and PPP-encapsulated payload is then encapsulated with an IP header containing the appropriate source and destination IP addresses for the PPTP client and PPTP server.

### C.1.3 Data-Link Layer Encapsulation

To be sent on a local area network (LAN) or WAN link, the IP datagram is finally encapsulated with a header and trailer for the data-link layer technology of the outgoing physical interface. For example, when IP datagrams are sent on an Ethernet interface, the IP datagram is encapsulated with an Ethernet header and trailer. When IP datagrams are sent over a point-to-point WAN link, such as an analog phone line or ISDN, the IP datagram is encapsulated with a PPP header and trailer.

### Processing of the PPTP Tunnelled Data

Upon receipt of the PPTP tunneled data, the PPTP client or PPTP server:

- Processes and removes the data-link header and trailer.
- Processes and removes the IP header.
- Processes and removes the GRE and PPP headers.
- Decrypts or decompresses, or both, the PPP payload (if needed).
- Processes the payload for receipt or forwarding.

## C.2 Layer Two Tunnelling Protocol

Layer Two Tunnelling Protocol (L2TP) is a combination of PPTP and Layer 2 Forwarding (L2F), a technology proposed by Cisco©Systems, Inc. Rather than having two incompatible tunnelling protocols competing in the marketplace and causing customer confusion, the IETF mandated that the two technologies be combined into a single tunnelling protocol that represents the best features of PPTP and L2F. L2TP is documented in RFC 2661.

L2TP encapsulates PPP frames to be sent over IP, X.25, Frame Relay, or ATM networks. Currently, only L2TP over IP networks is defined. When sent over an IP internetwork, L2TP frames are encapsulated as User Datagram Protocol (UDP) messages. L2TP can be used as a tunnelling protocol over the Internet or over private intranets.

L2TP uses UDP messages over IP internetworks for both tunnel maintenance and tunnelled data. The payloads of encapsulated PPP frames can be encrypted or compressed, or both. Encryption for L2TP connections is provided by IPSec ESP.

It is possible to create L2TP connections that are not encrypted by IPSec. However, this is not a VPN connection because the private data being encapsulated by L2TP is not encrypted. Non-encrypted L2TP connections can be used temporarily to troubleshoot an L2TP over IPSec connection by eliminating the IPSec authentication and negotiation process.

L2TP assumes the availability of an IP internetwork between a L2TP client (a VPN client using the L2TP tunnelling protocol and IPSec) and a L2TP server (a VPN server using the L2TP tunnelling protocol and IPSec). The L2TP client might already be attached to an IP internetwork that can reach the L2TP server, or the L2TP client might have to dial into a NAS to establish IP connectivity as in the case of dial-up Internet users.

For Internet-based L2TP servers, the L2TP server is an L2TP-enabled dial-up server with one interface on the external network, the Internet, and a second interface on the target private network.

L2TP tunnel maintenance and tunneled data have the same packet structure.

### C.2.1 Tunnel Maintenance with L2TP Control Messages

Unlike PPTP, L2TP tunnel maintenance is not performed over a separate TCP connection. L2TP call control and management traffic is sent as UDP messages between the L2TP client and the L2TP server.

L2TP control messages over IP are sent as UDP datagrams, as the encrypted payload of IPSec ESP as illustrated in the following Figure.

Because a TCP connection is not used, L2TP uses message sequencing to ensure delivery of L2TP messages. Within the L2TP control message, the Next-Received field (similar to the TCP Acknowledgment field) and the Next-Sent field (similar to the TCP Sequence Number field) are used

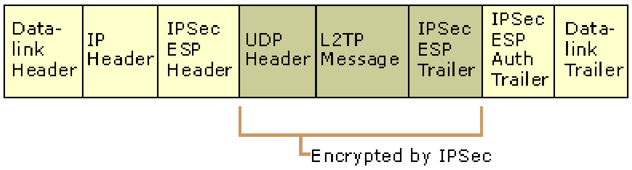



Figure C.3: L2TP Control Message

to maintain the sequence of control messages. Out-of-sequence packets are dropped. The Next-Sent and Next-Received fields can also be used for sequenced delivery and flow control for tunneled data.

L2TP supports multiple calls for each tunnel. In the L2TP control message and the L2TP header for tunneled data is a Tunnel ID that identifies the tunnel and a Call ID that identifies a call within the tunnel.

For the exact structure of L2TP control messages, please see the L2TP Internet draft.

### C.2.2 L2TP Data Tunnelling

L2TP data tunneling is performed through multiple levels of encapsulation. The next Figure shows the resulting structure of L2TP over IPSec tunneled data.

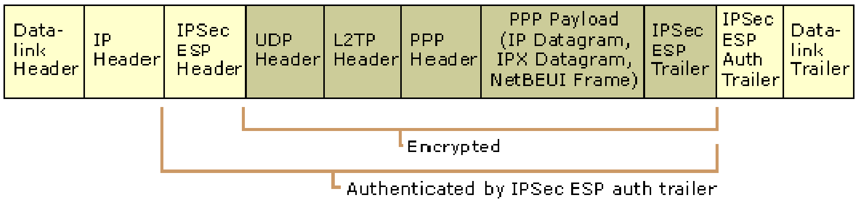



Figure C.4: L2TP Packet Encapsulation

#### L2TP Encapsulation

The initial PPP payload is encapsulated with a PPP header and an L2TP header.

#### UDP Encapsulation

The L2TP encapsulated packet is then encapsulated with a UDP header with the source and destination ports set to 1701.

#### IPSec Encapsulation

Based on IPSec policy, the UDP message is encrypted and encapsulated with an IPSec Encapsulating Security Payload (ESP) header and trailer and an IPSec Authentication (Auth) trailer.

### IP Encapsulation

The IPSec packet is encapsulated with a final IP header containing the source and destination IP addresses of the VPN client and VPN server.

## C.2.3 Data-Link Layer Encapsulation

To be sent on a LAN or WAN link, the IP datagram is finally encapsulated with a header and trailer for the data-link layer technology of the outgoing physical interface. For example, when IP datagrams are sent on an Ethernet interface, the IP datagram is encapsulated with an Ethernet header and trailer. When IP datagrams are sent over a point-to-point WAN link such as an analog phone line or ISDN, the IP datagram is encapsulated with a PPP header and trailer.

### De-encapsulation of L2TP over IPSec Tunneled Data

Upon receipt of the L2TP over IPSec tunneled data, the L2TP client or L2TP server:

- Processes and removes the data-link header and trailer.
- Processes and removes the IP header.
- Uses the IPSec ESP Auth trailer to authenticate the IP payload and the IPSec ESP header.
- Uses the IPSec ESP header to decrypt the encrypted portion of the packet.
- Processes the UDP header and sends the L2TP packet to L2TP.
- L2TP uses the Tunnel ID and Call ID in the L2TP header to identify the specific L2TP tunnel.
- Uses the PPP header to identify the PPP payload and forward it to the proper protocol driver for processing.

# Appendix D

# Laws and Regulations

## D.1 Trademark Law

**Brazil** It was rather difficult to gather information about particular regulations considering the trademark law in Brazil, but there doesn't seem to be any extraordinary legal aspects involved. Most of the legal issues concerning the Internet, were the registration of a Software product, the Internet Domain Name Application and the Electronic Commerce Property. Companies, in particular Plasdan should contact the "National Institute for the Industrial Property" (Instituto Nacional da Propriedade Industrial) and Registro BR, in order to check on certain regulations. Speaking the native language is very helpful!

**Portugal** Portugal is a member of the International Union for the Protection of Industrial Property (WIPO) and a party to the Madrid Agreement on International Registration of Trademarks and Prevention of the Use of False Origins. Portugal's current trademark law entered into force on June 1, 1995. The law, however, is not considered to be entirely consistent with the terms of the trade related intellectual property provisions of GATT (TRIPS).

**Germany** The requirements for the application of a trademark and other signs in Germany are governed by the following provisions:

- The Law on the Protection of Trademarks and Other Signs (German Trademark Act) of October 25, 1994 (Bundesgesetzblatt I, p.3082)
- The Law on Patent Office and Patent Court Fees of August 18, 1976 (Bundesgesetzblatt I, p.2188), last amended by Article 20 of the Law on the Reform of the Trademark Law and on the Incorporation of the First Council Directive of December 21, 1988, to approximate the Laws of the Member States Relating to Trademarks (89/104/EEC) (Trademark Reform Law) of October 25, 1994 (Bundesgesetzblatt I, p.3082);
- The Trademark Regulations of November 30, 1994 (Bundesgesetzblatt I, p.3555). [35]

**Holland** The New Trademark-act has been approved by the Government and Parliament of the Netherlands Antilles. A date for the new act to become effective however has not yet been set. Under the new Trademark-act it will be possible to register service marks. Within one year after the new Trademark-Act has become effective, all current trademark owners will be required to file a confirmation of the exsisting registration to maintain their rights to the already registered trademark under the new Act.

**Denmark** The Trademarks Act was amended on January 1, 1997, in order to enable Denmark to ratify the Trademark Law Treaty, and to bring the Danish Trademark Law into conformity with the TRIPS Agreement and the European Union Harmonization Directive. The amendments will enable the following principal changes:

1. the Patent Office may in the future refrain from examining all new trademark applications for inherent or relative registrability;
2. it will be possible for applicants or owners of trademark registrations to request an administrative re-examination of a trademark registration after the registration procedure (including the opposition and appeal procedure) has been finalized;
3. owners of foreign trademarks may oppose similar marks for similar goods if the applicant was or should have been aware of the foreign trademark.

It is not yet clear if and when the changes outlined in 1) and 2) above will take effect.

**United Kingdom** The Trade Marks Act 1994 entered into force on October 31, 1994, thereby implementing the EU Directive on Harmonization of Trademark Laws within the Member States of EU and paving the way for ratification of the Madrid Protocol by the United Kingdom. Although the new Act follows substantially the Bill introduced into Parliament in November 1993 and referred to in our Information Letter N.S. 182, several changes were made to the Bill while it was debated in committee. Here is a summary of the principal provisions of the new law:

- Registrability
- Conflicting Prior Rights and Registrations
- Practice and Procedure
- Infringement and Counterfeiting
- Licensing and Assignment

## D.2 Copyright Law

**Brazil** Brazil has enacted new copyright and software laws which came into effect on June 19, 1998 and February 20, 1998, respectively.

Major changes in the copyright law include the following:

1. the term of protection for economic rights under the copyright law is in general standardized at 70 years from the first of January next following the author's death or in the case of audiovisual works 70 years from publication of the work
2. the payment due to the copyright owner under the droit de suite is reduced to 5% of the sale price
3. it is made clear that sale of a work itself does not imply sale of the copyright therein and
4. assignment of copyright is to be presumed to be limited to a five-year period and confined to the country in which the assignment is executed unless there are express provisions to the contrary.

The copyright law also establishes that computer software and databases are copyrightable subject matter but copyright protection for computer software is subject to the new software law.

Under the new software law the formalities previously required before software of foreign origin could be marketed in Brazil have been removed.

**European Union** Ministers from the 15 nations of the European Union (EU) adopted a copyright directive, which aimed at updating copyright laws for the digital age to prevent Internet and high-tech piracy of music, books and other copyrighted works.

It is important to look still at the individual countries, because not all of them have adapted to the new regulations.

## D.3 Data Protection Law

**Brazil** Brazil Constitution of 1998 voted on the personal data protection act. The purpose of this Act is the full protection of personal information recorded in data files, registers, banks or other technical means of data-treatment, either public or private for purposes of providing reports, in order to guarantee the honor and intimacy of persons, as well as the access to the information that may be recorded about such persons, in accordance with the provisions of Section 43, Third Paragraph of the National Constitution.

**United Kingdom** The UK which is part of the EU has signed on to the EU Data Protection Directive. They did this by enacting the Data Protection Act of 1998. This laws allows the a UK citizen to not have to give up personal information on the internet as well as letting internet companies sell that information without permission from the internet consumer. Many ISPŠs and other e-business protect the privacy of their customers to certain extent. (This excludes the selling of names, addresses and market histories of consumers.) It is monitored by the Data Protection Commissioner which is an independent agency that enforces the Act.

As part of being in the EU the UK has to enforce this Data Privacy Directive. This means that UK companies have to meet these standards to trade within the EU. Also other countries not in EU must meet these standards as well. The US and EU have come to a tentative agreement that companies could become a Śsafe harborŠ if they meet certain guidelines.

**Germany** Personal data protection is guaranteed in Germany through the federal data protection law (Bundesdatenschutzgesetz) and also through the European Commission Directive on Data Protection. Issues related to internet activities and telecommunication were introduced in August 1997 through the Information and Communication Services Bill.

**EU** Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector

## D.4 Cryptography Law

Generally speaking, there can be as many different cryptography laws as there are different states. In most states, cryptography technology is regarded to be some kind of "conventional arm". Therefore it is amenable to the laws on export and import of arms. Of course, in most regulations it is separately mentioned, and separate regulations have been established for cryptography.

In the past few years efforts have been made to find a solution that is suitable for many states. The so called "Wassenaar Agreement" has been signed by 31 countries.

Wassenaar Agreement (7/1996): In 1995, 28 countries decided to establish the Wassenaar Agreement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies was established. The Wassenaar Agreement, controlling the export of weapons and dual-use goods (both for a military and civil purpose) , was signed by 31 countries. Cryptography is regarded as a dual-use good and therefore is subject to the Agreement. The initial provisions were largely the same as the old COCOM regulations. A "General Software Note" was added, which was applicable until the December 1998 revision of the agreement. The General Software Note said that mass market and public domain crypto software is excepted from the controls.

Wassenaar Meeting (12/1998) During the Wassenaar Meeting in December 1998 it was stated that more export controls would cause more insecurities. However, neither the United States' with its restricted view nor Germany with its liberal view could enforce their regulations.

Both the Military and the Economy regard cryptography as a very important factor. Only a strong encryption would guarantee confidential communication that cannot be spied out. The Wassenaar Agreement does only grant a minimum of harmonization for export controls. Every state can freely design the applied regulation methods. So it is in the national responsibility of every state to determine what can be exported under what circumstances.

The following new agreements in this Wassenaar Meeting were made: Free for export are

- all symmetric crypto products up to 56 bit all asymmetric crypto products up to 512 bit mass market symmetric crypto soft- and hardware up to 64 bits equal treatment of hard- and software no more export controls for keylenghts smaller 56 bit now also export controls for strong mass market cryptography (bigger 64 bit). Export was relaxed for products that use encryption to protect intellectual property (such as DVDs). Exceptions from export controls are:
- methods for digital signature and authentification for banking, pay-tv and copyright-protection public domain, as long as there are no restrictions on the furter distribution of the software

That means, even if only a further distribution without documentation is forbidden, the software does not meet the Wassenaar requirements for being public domain. PGP therefore is not public domain from the Wassenaar point of view. The security of company-internal secrets and personal confidential communication was seen as a high good, even regarding the fact that single persons can transport illegal content via a network. During that Wassenaar meeting the USA deviated from key recovery and key escrow and since has been content with having access to the plain text using just any method. However, the US still uses key recovery with US-internal data .

Wassenaar Meeting (12/2000) In their meeting in December 2000 the Wassenaar States lifted the 64 bit limit for export controls on mass market crypto soft- and hardware. The participating states recognized that it is important "to continue deepening the Wassenaar Arrangement understanding of how and how much to control". In the following we will look at the individual situation and regulations for the countries Plasdan is operating in:

**Brazil** Brazil does not regulate the export, import or domestic use of encryption. However, there are indications that this situation may be changing. The Brazilian government is considering a law that would require importers and domestic users of encryption to register their products and systems with the government. [37]

**Denmark** Denmark reported to the OECD that there are no domestic use prohibitions on the use of cryptography in Denmark.

In April 1997, an Export Committee on Cryptography, meeting under the auspices of the Ministry of Research and Technology and including representatives of other ministries, issued a report on the use and sale of cryptographic products. The Committee recommended that Denmark not impose new regulations on cryptography. However, it did state that Danish cryptography policy should take into consideration international developments (an obvious reference to Wassenaar and other regimes). The Committee particularly recommended against the establishment in Denmark of a key recovery scheme. In June 1998, the Committee issued its final recommendation. Although the Committee recommended that key recovery regulations and incentive schemes should not be implemented, international developments might necessitate a reconsideration of such controls in the future.

Denmark has implemented Wassenaar export controls in its Executive Order on Exports of Dual-Use Goods Technologies and Know-how. Denmark adheres to the amended Wassenaar Dual-Use Control list agreed to in Vienna in December 1998. This has caused some political controversy in Denmark and hearings may be held in the Parliament this year.

The Danish Agency for Trade and Industry licenses exports of cryptographic products. Danish export controls cover both tangible and intangible software transfers. Criminal sanctions can be levied against those who illegally transfer unlicensed cryptographic products subject to export controls. The Danish Defense Intelligence Service (Forsvarets Efterretningstjeneste) determines what and to whom cryptographic products may be exported.

Denmark originally regulated the export of strategic goods under a Ministry of Industry executive order dated November 12, 1993. The executive order has been subsumed by the EU dual-use regulation. [38]

**Germany** Germany has been at the forefront of opposing restrictions on encryption. It has been a counter-balance to U.S. efforts to promote key escrow and international restrictions. It had a significant role in the EU's 1997 paper on Encryption and Digital Signatures. In 1999, German efforts prevented key escrow from becoming part of the Wassenaar Arrangement.

According to the Embassy of the Federal Republic of Germany in Washington and the Federal Ministry of Economics and Technology.

There are no controls on the use of encryption software or hardware; There are no controls on the import of encryption; Export controls on encryption are comparable to those of the United States as they existed until early in 1997; Export controls are overseen by the Federal Exports Office of the Ministry of Economics (Bundesamt *für* Aussenwirtschaft- BMWi). Germany enacted a Digital Signature Law (SigG) on June 11, 1997. The digital signature system mandated uses asymmetric encryption. This system requires a secret key to be held by the signer and a public key that is certified by a Certificate Authority. The encryption algorithm to be used is not defined in the law. The law does not specify Certificate Authorities, but it requires that such parties be licensed by the government communications authority. This authority will certify Certificate Authorities and create a digital chain of trust for purposes of public key verification.

According to GermanyŠs report to the OECD, the "Electronic Commerce Initiative of the Federal Government" states that "the German government does not plan to regulate by statute the marketing and use of encryption products. In Germany, encryption systems may be freely chosen and used." In its progress report on the German action plan "Info 2000: GermanyŠs Way to an Information Society" (Autumn 1997), the government states its policy is to:

Ensure availability of reliable and strong encryption in Germany on a sustainable basis; Guard the interests of German security and criminal prosecution authorities; and Promote the strength of the market position of German producers of encryption systems. Cryptographic exports are regulated by the implementation of the EU Dual-Use Regulation. Encryption equipment is listed individually in the German export list in Part 1 C, paragraph 5 part 2 "Information Security." In 1998, the German Green Party posed the following question to the Federal Government: "Is the

Federal Government aware of the view of cryptographic experts that certain encryption standards and systems have been watered down by the influence of agencies responsible for cryptography matters, in particular the NSA, and what is its response to this viewpoint?" The governmentŠs answer was surprisingly candid, "The restrictive export control policy of the USA with regard to encryption technology is generally known; in its advisory role the BSI (Bundesamt für Sicherheit der Informationstechnik - the German Federal Information Security Agency, a department of the Ministry of the Interior) is, therefore, cautious with regard to recommending U.S. products to the public administration and to private German companies."

In December 1998, Germany adhered to the revised Wassenaar Arrangement export controls, tightening up its own export criteria. However, the Ministry of Economics has indicated that they do not plan to impose new restrictions on the export of cryptographic products. [39]

**Netherlands** There are no restrictions on the domestic use of cryptography in the Netherlands, including that used for public and private radio systems. In March 1994, the Netherlands government advanced a draft parliamentary bill that would have prohibited the possession, use, and marketing of powerful encryption products without a license. After a national outcry, the bill was withdrawn.

The Netherlands applies export controls on cryptographic hardware and software in accordance with the Wassenaar Arrangement and the European Union Dual-Use Regulation. It also supported the changes to the Wassenaar control list announced in December 1998. The export of cryptographic equipment from the Netherlands requires an individual license for all nations except Belgium and Luxembourg. The applicable statutes are the 1962 Law on Import and Export (Dutch Statute Book 1962, 295) and the ministerial Decree on Export of Strategic Goods and its Annex (Dutch Statute Book 1963, 128).

The licensing authority for exports is the Central Agency of Import and Export, a component of the Ministry of Economic Affairs. The National Communications Security Agency (NCSA) has the responsibility for determining the impact that specific exports of cryptographic equipment may have on national security. The Commerce/NSA report heavily redacts further information on the activities of the NCSA, although it is known that this agency performs many of the functions of the NSA. Dutch export law only applies to tangible products, not intangible software transmitted electronically.

There are no import controls on cryptography. [40]

**Netherlands Antilles** The Cabinet Minister for the Netherlands Antilles in s'Gravenhage, the Netherlands informed us that the Department of Justice of the Netherlands Antilles located in Willemstad, Curcaao had responsibility for establishing a policy on the use of cryptography.

Significantly, the Netherlands Antilles was not on the list of countries eligible to receive U.S. general purpose encryption commodities and software under a U.S. Commerce Department license exception, while the neighboring island of Aruba was granted such an exception. This indicates that there are mutual legal assistance difficulties between the U.S. and the Netherlands Antilles. [41]

**Portugal** There are no controls on the import of cryptography or its domestic use.

Portugal regulates the export of encryption in accordance with its participation in the Wassenaar Arrangement and its implementation of the EU Dual-Use Regulation. According to PortugalŠs report to the OECD, the licensing authority is the Directorate-General for Commerce.

**United Kingdom** There are currently neither domestic use restrictions nor are there any import controls on encryption products in the United Kingdom.

The UK has been the strongest supporter of the US's efforts to promote key escrow and limitations on encryption. The government began a Public Consultation on the regulation of Trusted Third Parties (TTPs) for the provision of encryption services in 1996 and released a Public Consultation Paper on detailed proposals for legislation on the Licensing of TTPs for the provision of encryption services in March 1997. In April 1998, the Department of Trade and Industry released a "Secure Electronic Commerce Statement" which sets out the details of the government proposal:

"We therefore intend to introduce legislation to license those bodies providing, or facilitating the provision of cryptography services. Principally these will be Trusted Third Parties, Certification Authorities and Key Recovery Agents. Such licensing arrangements will be voluntary, as business has requested, although we would hope that organisations providing services to the public will see the benefit of adhering to a high standard, and the public confidence that this will bring. Organisations facilitating encryption services (for example through offering key recovery or providing key management services for confidentiality) will also be encouraged to seek licences."

Licensed service providers that provide encryption services will, therefore, be required to make recovery of keys (or other information protecting the secrecy of the information) possible through suitable storage arrangements.

The Government intends to introduce legislation to enable law enforcement agencies to obtain a warrant for lawful access to information necessary to decrypt the content of communications or stored data.

In December 1998, the Queen Elizabeth II announced that a Secure Electronic Commerce Bill would be introduced in 1999. The bill should be introduced in the summer of 1999.

In March 1999, Prime Minister Tony Blair met with industry representatives and announced that the government was backing away from support for the linking of licensing with escrow requirements. A task force of industry and government will examine alternatives to assist law enforcement. Blair suggested that escrow might be adopted if alternatives were not sufficient.

The United Kingdom maintains export controls on cryptography pursuant to its participation in the Wassenaar Arrangement and adherence to the EU Dual-Use Control List. The United Kingdom strongly supported the amendment to the Wassenaar Dual-Use Control List announced in December 1998. Export controls are implemented under the Export of Goods (Control) Order 1994 as amended by the Dual-Use and Related Goods (Export Control) Regulations 1996. The licensing authority is the Export Control Department of the Department of Trade and Industry (DTI). It has recently taken steps, spelled out in a Strategic Export Controls White Paper, to extend export controls beyond tangible cryptography to intangible exports of encryption programs over the Internet.

According to the Department of Trade and Industry (DTI), "an export license may be obtained by applying to the DTI. In practice, however, UK vendors of these goods also send a fax of their applications to the Communications and Electronics Security Group (CESG), simultaneously with the transmittal of the application to DTI so as to speed up the decision process. CESG is part of GCHQ, the UKŠs NSA equivalent, but has a separate identity to facilitate work with unclassified commercial entities. CESG reviews the application and (on paper) advises DTI of its view. In practice, DTI generally follows the CESG recommendation and does not approve the export item that CESG finds unacceptable."

On January 28, 1998, the DTI authorized an "Open General Export License" for personal computers accompanying their users that contain encryption. On-line voice encryption/decryption programs are not covered by the special permit. citeuk

## D.5 Taxation

The ITFA, 47 USCA Paragraph 151 (1998), is a federal law that established a three-year moratorium on state and local governments ability to tax certain aspects of Internet commerce. The moratorium applies to taxation of Internet access provided to individuals and businesses through ISP's unless the access tax was in force before October 1, 1998. In addition, the moratorium prohibits states from assessing discriminatory taxes. A tax is discriminatory if it taxes groups of otherwise similarly situated taxpayers differently because one group conducts business via the Internet. A tax is also discriminatory if it is applies to an out-of-state retailer whose only presence within the state is via the Internet. Finally, the moratorium prohibits the assessment by state or local governments of a bit tax, which is a tax that varies according to the volume of electronic information transferred through the Internet.

# Appendix E

# Technological Factors

Like mentioned also in the main report, the following information was extracted from market profile information, published by the Foreign Ministry of Denmark for the individual countries. [36]

## E.1 Portugal

Data Transmission Services (DTS), including Internet services, are fully liberalized in Portugal. Presently, there are 30 licensed operators offering services, such as:

- data transmission services,
- E-mail,
- EDI,
- fax storage and transmission and
- videotext

Internet linkage is an important DTS in Portugal, especially for large companies. The Internet has also become very popular and as a result, Internet-based services have expanded quickly. However, growth has been slower than experienced in other Western European countries, but since January, 2000, this situation has been changing due to the great majority of Portuguese ISP's which are offering free access to the Internet.

Telepac, a Portugal Telecom (PT) owned company, is chartered to provide all types of DTS (Data Transmission Services) and is the principal Internet service provider. DTS, excluding Internet services, accounted for 95% of Telepac's business in 1996. However, Telepac has started to face some competition from other operators offering DTS. The most important is Comnexo with a market share of 9%. Comnexo maintains a strategic agreement with British Telecom. Other operators are starting to offer a growing presence in DTS. They include AT&T, Global One, TMI, Eunet, and Compensa (100% owned by IBM).

Internet services are new to Portugal. In fact, there were only about 50,000 paying subscribers and 250,000 non-paying users in 1999. Approximately one quarter of the total investment contributed to this sector was made for the offering of Internet services. Presently, 23 companies offer Internet access. Telepac still controls more than 78% of the market with 256 POPs (Points of Presence) throughout the country serving some 125,000 clients.

The telecommunications market is the most important business area of the Portuguese economy. The market reflects all of the dynamics originated by total liberalization of the market which began two years ago and shall be completed before the end of year 2003. Portugal's telecommunications market offers huge opportunities for investors, service providers, and equipment suppliers.

The strong performance of the telecommunications industry in Portugal has been a result of improved infrastructure accompanied by a significant decrease in equipment costs, and gradual liberalization of the sector.

The equipment market is expected to grow at a remarkable annual rate of 20% over the next two years. Imports constitute 73% of the total market and the U.S. real share is much higher than the 3% reported because most U.S. exports to Portugal are made through other European countries.

High-Speed Services, like T1, commercial ISDN, leased lines are available through Portugal Telecom. A piloted Integrated Services Digital Network (ISDN) was consolidated in 1994, with a total of 1,556 basic accesses and 281 primary accesses. International Euro-ISDN connections have been established with most other European countries. Speeds range from 64kbit to 120Mbit/s.

## E.2 Germany

Germany has one of the world's most technologically advanced telecommunications systems. With a share of 28%, Germany is the single largest Telecommunication market in Europe and is fully liberalized since January 1, 1998. As a result of intensive capital expenditures since reunification, the formerly backward system of the eastern part of the country is being rapidly updated to the most advanced technology. Germany is served by an digitized switching system connected by modern networks of fiber-optic cable, coaxial cable, microwave radio relay, and a domestic satellite system. The fiber-optic cables build up the most dense network in the world. Cellular telephone service is widely available and includes roaming service to many foreign countries.

Deutsche Telekom AG is EuropeŠs largest telecommunications company and the third largest carrier worldwide. It provides universal services including the online service "T-online" and a TV cable network. The number of telephone lines grew to over 44 million (including 7.3 million ISDN B channels). The basis for the high developed and widespread infrastructure in Germany is the network of the Deutsche Telekom.

Although in 1997 almost 30% of all companies with more than 10 employees were connected to the internet, online activities were still strongly correlated to size. Nevertheless, the small business market segment showed that it has a high potential. The degree of internet usage sky rocketed. Trading companies are the main users, followed by the banking/insurance and service industry.

The internet is mainly used for Information gathering (86%), communication (67%), marketing (32%), distribution (23commerce (19%).

The number of German companies that are present in the World Wide Web may be estimated from the number of domains .de which add up to 344,045 in April 2000. In addition, 26% of all companies being present in the WWW used the .com domain.

## E.3 Netherlands

The Dutch wireline market was completely liberalized in 1997 which was ahead of the EU mandated January 1, 1998 deadline. The act provided interconnect access to KPNŠs lines and MCI WorldCom was one of the first competitors who began offering services. The act also created the OPTA, which is an independent administrative body that oversees the opening of the market and is responsible for insuring a competitive environment. In 1998, a new Telecommunications Act was introduced that defined the relationships between incumbents and new carriers. The Dutch Government required all wireline carriers to offer number portability in 1999 that mandated customers could keep their phone numbers if they choose to changes carriers.

The leading telecommunications provider, KPN Telecom, is facing heavy demands on its system spurred by 100% a year Internet growth. Certain areas of the country, such as Amsterdam, are growing so fast that KPN is having trouble keeping service up. This is a result of problems they are facing meeting demands for the necessary materials, manpower and equipment for installing new lines and networks. Infrastructure spending is expected to increase to over NLG 3 billion.

The wireless sector is becoming a competitive market as there are presently five wireless companies serving the 6.8 million wireless users. While KPN is still the leader in market share with 52%, they face stiff competition from new companies entering the mix bidding on spectrum licenses for new 3G next generation services. The number of wireless users is expected to grow to 8.6 million users in 2002.

The Dutch also have very good cable coverage, as cable is available to approximately 94% of the population. Although there has not been much activity in using the cable infrastructure for telephony and Internet access it may provide an excellent option to improve the telecom infrastructure. With increased demand on the wireline system from voice and data application the cable market finds itself in a very good position although substantial upgrades will be required.

KPN dominates another area, the satellite market, which is used to reach outlying areas and to facilitate the Netherlands as a heavy trading hub. This gives the ability to provide broadband access to areas not served by the traditional wireline infrastructure. Since the Netherlands has heavy rural areas, satellites may provide a solution that is able to solve the "digital divide".

Internet coverage is also very high, as there are some 50 national Internet providers and at least 150 more operating on a regional basis. This adds up to 20 Internet hosts per 1000 people in Holland, second only to the United States. This has placed high demands on the telecom infrastructure as greater demands, led by data applications, are exhausting the present system. This will require substantial investments in new infrastructure equipment to provide greater capacity.

Key Statistics are:

- 54.33 main telephone lines/100 inhabitants.
- 8.431 million main telephone lines.
- Network characteristics: 100 percent automatic, 100 percent digital.
- International telephone traffic: 29,300 circuits; minutes per subscriber 182.
- Network infrastructure investment 1997: approximately $1.45 billion.
- Internet Service Providers (ISPs): 70 (1999)
- By January 1, 2000, there were 6.8 million wireless users

## E.4 Brazil

AlterNex, operated by IBASE since 1989, is the first provider of Internet services outside of the academic community in Brazil. IBASE is a founding member of the Association for Progressive Communications (APC), and AlterNex is an APC member network. services provider. Number of users:6,000. Currently with dial-up centers in Rio and Sao Paulo.

There are basically four players right now in the backbone business:

- Embratel (MCI-Worldcom)
- Netstream (high speed fiber in metro areas, owned by AT&T)
- MetroRed (similar to Netstream, owned by Fidelity Investments, seems much smaller than Netstream)

- Rede Nacional de Pesquisa (RNP), which operates the academic network and is funded by the Ministry of Science and Technology. This is slowly implementing Internet II type metropolitan networks in some cities (Rio, Sao Paulo, Brasilia, Salvador, Belo Horizonte, Porto Alegre etc), using 155 to 622 Mb/s ATM beds.

Jointly, these backbones have a gross bandwidth to the Internet at large (links to the US, Canada, Europe and some border Latin American countries) in the range of 450 - 500 Mb/s, most of which (about 300 Mb/s) is operated by Embratel.

Other companies (like IBM, Global One and Unisys) operate backbones with links through Embratel, so they are counted in the figures above.

Players in the cable IP and KU band business are starting to appear (like Ajato - Abril/UOL Group - and Virtua - Globo Group) but their impact is so far negligible.

At the oeratos individual sites there is detailed info, including network maps and, in some cases, speed data.

## E.5 Denmark

The Danish are generally regarded as having a high quality telecommunication infrastructure. With regard to both conventional telephones and mobile telephones, Denmark is in the forefront within the global community. During the 1980's, in cooperation with its Nordic neighbors, Denmark developed the analog Nordic Mobile Telephone (NMT) system that was later exported to a number of countries. In 1992 it was one of the first countries to introduce the digital GSM pan-European cellular telephone system, which provides among the best GSM coverage in Europe. On a per capita basis, Denmark is among the world's largest users of cellular telephones. At year-end 1994 the number of NMT subscribers was 271,593 while the number of subscribers to the GSM system has grown even more rapidly from zero in 1992 to 231,907 by year-end 1994. As a result of such growth within the GSM system, Denmark is considering establishing a new service, the DCS 1800 system in approximately 1998. (USDOC, International Trade Association)

Today the situation looks very promising: Denmark is embracing the concept of knowledge-based and networked New Economy. Industry and community are co-operating closely in the process of rapid transformation towards the creation of a full-scale "Digital Denmark". Denmark's strength in the IT industry is based on the Danes ability to make technology and content blend seamlessly together. Combined with a talent for staying ahead with cutting edge technologies, this enables Danish communities and businesses to navigate the networked New Economy.

Denmark offers:

- World-class software development and integration capabilities.
- Cutting edge areas include pervasive computing, e-business, wireless Internet technologies and e-learning
- High penetration, use and familiarity with the Internet (75% according to GfK Worldwide, Q2 2001). This makes Denmark an ideal test market for new technology
- Highly skilled workforce
- Stated ambition by the Government for Denmark to be a world leading IT nation. The country is already well on its way
- Innovative entrepreneurial environment. According to the Innovation Index published by the US Council of Competitiveness, Denmark will be the worldŠs fourth most

## E.6 United Kingdom

The United Kingdom (UK) is very advanced in Information technology (IT). The UK is using the Internet as tool for business. They have the second highest international broadband rate in the world. Yet access to the Internet is very expensive because of the high taxation on phone service. The UK is one of the most advanced IT countries in the world. They develop both hardware and software products, yet they have not reached the status of the US. This is because they are behind in their deployment of high speed Internet connections. It is also because of their conservative views on investment and growth in the IT sector, although this is beginning to change as Europe is beginning to look at the UK as a center for IT development.

The United Kingdom has several competitive advantages, with the primary advantage as the language and culture. Since the "language of the internet" is English, and all residents of the UK speak English, there is an automatic advantage in the fact that there is nothing lost to translation. Strengths of the UK include governmental policies supporting IT, a strong and sophisticated financial system, one of the most respected educational systems in the world, and world-class R & D parks.

The domestic mobile telecom companies in the UK are:

- Vodafone
- Cellnet
- Orange
- One2One

The above providers provide today a variety of telecommunication solutions.

# Glossary

## A

- Active X - This set of technologies from Microsoft provides tools for linking desktop applications to the World Wide Web. Using a variety of programming tools–including Java, Visual Basic, and C++–developers can create interactive Web content. For instance, ActiveX technology can allow users to view Word and Excel documents directly in a browser.
- Access Control List(ACL) - Most network security subsystems operate by allowing selective use of services. An Access Control List is the usual means by which access to, and denial of, services are controlled. It is simply a list of the services available, each with a list of the hosts permitted to use the service.
- Algorithm - A set of ordered steps for solving a problem, such as a mathematical formula or the instructions in a program.
- Anti-virus - A program that detects and removes a virus.
- Authentication - Verifying the identity of a user that is in the process of logging onto or has already logged onto a network.
- Authorization - The process of determining what types of activities are permitted. Usually, authorization is in the context of authentication: once you have authenticated a user, they may be authorized different types of access or activity.
- Assets The resources owned by a company, fund or person. Assets can be tangible, eg. cash, investments, property and equipment, or intangible

## B

- Bandwidth - In a general sense, this term describes information-carrying capacity. It can apply to telephone or network wiring as well as system buses, radio frequency signals, and monitors. Bandwidth is most accurately measured in cycles per second, or hertz (Hz), which is the difference between the lowest and highest frequencies transmitted. But it's also common to use bits or bytes per second instead.
- Browser - If you can read this, it's highly likely that you're using a Web browser. In brief, a browser is your interface to the World Wide Web; it interprets hypertext links and lets you view sites and navigate from one Internet node to another. Among the companies that produce browsers are NCSA Mosaic, Netscape, and Microsoft, as well as commercial services like CompuServe, Prodigy, and America Online.
- Browser Sniffing - Browser sniffing describes the process by which a Web site detects which versions of various browsers users are running, in order to determine whether or not they can access certain Web site features. Browser sniffing–usually accomplished with JavaScript–can also be used to detect whether or not a user has a specific plug-in required to access the site.
- BIOS - (Basic Input Output System). Detailed instructions that activate peripheral devices.

## C

- Cache - Caches come in many types, but they all work the same way: they store information where you can get to it fast. A Web browser cache stores the pages, graphics, sounds, and URLs of online places you visit on your hard drive; that way, when you go back to the page, everything doesn't have to be downloaded all over again. Since disk access is much faster than Internet access, this speeds things up. Of course, disk access is slower than RAM access, so there's also disk caching, which stores information you might need from your hard disk in faster RAM.
- CGI - common gateway interface - The CGI standard lays down the rules for running external programs in a Web HTTP server. External programs are called gateways because they open up an outside world of information to the server.
- Client - The customer side of a client/server setup. To confuse matters, when you log on to a server, the word client can refer to you, to your computer, or to the software running on your computer. For example, to download something from an ftp site, you use ftp client software.+
- Certificate Authority - An individual, organization, or agency, public or private, that acts as a "notary" to authenticate the identity of users of public-key encryption.
- Cryptography - Conversion of data into a secret code for security purposes. Known as keeping communications private. It deals with encryption, decryption, and authentication.

## D

- Data packet - Although your computer and modem can send data one character at a time, when you're surfing the Internet, downloading files, or sending email, it's more efficient to send information in larger blocks called data packets. Modems generally send packets of around 64 characters along with some extras for error checking. When downloading files using a protocol like Xmodem, however, the packets are larger. And when using Internet protocols such as TCP/IP, the packets are larger still–around 1,500 characters.
- Digital certificate - Citing concerns about security, many people are still wary of online transactions. In an attempt to assuage those fears, software vendors, security specialists, and online vendors have developed the concept of digital certificates. A digital certificate is a password-protected file that includes a variety of information: the name and email address of the certificate holder, an encryption key that can be used to verify the digital signature of the holder, the name of the company issuing the certificate, and the period during which the certificate is valid. Certificate authorities (CAs) gather information about a person or company and then issue certificates. These certificates can be used as online identification, much in the same way a driver's license can verify your identity in the physical world. If an email message or order form comes through with an attached digital certificate, the recipient can be more confident that the document is genuine. Several technologies (including SET, SSL, and Authenticode) are currently competing for market share, each hoping to become the certificate of choice.
- Digital signature - Forgery is a growing concern among Netcitizens. After all, who's to say that a message with your name on it is really from you and not somebody pretending to be you? Digital signatures are a means of proving that a file or email message belongs to a specific person, much as a driver's license proves identity in real life. Digital signatures have the added benefit of verifying that your message has not been tampered with. When you sign a message, a hash function–a computation that leaves a specific code, or "digital fingerprint"–is applied to it. If the fingerprint on the recipient's message doesn't match the original fingerprint, the message has been altered. Digital signatures are often used in combination with strong-encryption software to create a secure channel of communication,

in which both privacy and identity are protected.

- DNS - domain name system - When you send email or point a browser to an Internet domain such as cnet.com, the domain name system translates the names into Internet addresses (a series of numbers looking something like this: 123.123.23.2). The term refers to two things: the conventions for naming hosts and the way the names are handled across the Internet.
- Domain name - Domain names are issued by the National Science Foundation (NSF), and they come with different extensions based on whether the domain belongs to a commerical enterprise (.com), an educational establishment (.edu), a government body (.gov), the military (.mil), a network (.net), or a nonprofit organization (.org). Some domains use a geographical notation too (such as the San Francisco, California-based well.sf.ca.us).
- DES - (Data Encryption Standard). An NIST-standard encryption technique that scrambles data into an unbreakable code for public transmission.
- Decryption - applies the algorithm in reverse to restore the data to its original form.
- Dial-Up - A type of communication that is established by a switched circuit connection using the telephone network.

# E

- email - electronic mail - Whenever you send messages to people using a computer and they read it later, you've sent a piece of email. You can send email in several ways–across a local area network, via the Internet, or through an online service like CompuServe or America Online–and you can send it to a single recipient or to a whole slew of them. But all email behaves pretty much the same way: you send it to a virtual mailbox, and the recipient has to pick it up or can use software that does it automatically.
- Encryption - Encryption is the process of changing data into a form that can be read only by the intended receiver. To decipher the message, the receiver of the encrypted data must have the proper decryption key. In traditional encryption schemes, the sender and the receiver use the same key to encrypt and decrypt data. Public-key encryption schemes use two keys: a public key, which anyone may use, and a corresponding private key, which is possessed only by the person who created it. With this method, anyone may send a message encrypted with the owner's public key, but only the owner has the private key necessary to decrypt it. PGP (Pretty Good Privacy) and DES (data encryption standard) are two of the most popular public-key encryption schemes.
- Extranet - Companies often use extranets to provide nonpublic information to a select group of people, such as business partners or customers. So while an extranet may look like an ordinary Web site, you have to enter a password or use digital encryption to access it. For example, Federal Express's customers can track packages on the company's extranet by simply entering a tracking number. And Bank of America's extranet lets users transfer funds or look up account balances online. Using an extranet can help companies save money by allowing customers to find information themselves, without having to call and talk to a person.
- Electronic Signature - Ranges from Personal Identification Number (PIN) to the actual "burning in" of a bitmap of a user's signature on a document.
- Encapsulation - In communications, a method for transmitting multiple protocols within the same network.
- E-Commerce - E-commerce, ecommerce, or electronic commerce is defined as the conduct of a financial transactions by electronic means. With the growth of commerce on the Internet and the Web, ecommerce often refers to purchases from online stores on the Web, otherwise knows as e-commerce Web sites. They may also be referred to as "virtual-stores" or Cyber stores. Since the transaction goes through the Internet and the Web, some have suggested another term: I-commerce (Internet commerce), or icommerce. Few have referred to it as

Web-commerce. E-commerce can be business to business (B to B) or business to consumer (B to C).

## F

- Firewall - If you want to protect any networked server from damage (intentional or otherwise) by those who log in to it, you put up a firewall. This could be a dedicated computer equipped with security measures such as a dial-back feature, or it could be software-based protection called defensive coding.
- Finger - Finger is a program that you point at the username of someone on a networked system. It uncovers that person's full name, most recent log-in time, and other information. It's also used as a verb, meaning to apply the program to a username.
- FTP - file transfer protocol - This Internet protocol is used to copy files between computers– usually a client and an archive site. It's old-fashioned, it's a bit on the slow side, it doesn't support compression, and it uses cryptic Unix command parameters. But the good news is that you can download shareware or freeware apps that shield you from the complexities of Unix, and you can connect to FTP sites using a Web browser

## G

- Gateway - A gateway is a program or piece of hardware that passes data between networks. You'll see this term most often when you either log in to an Internet site or when you're passing email between different servers.

## H

- Hacker - A person who attempts to gain access to computer systems he / she is not authorised to do so.
- Http - hypertext transfer protocol - The protocol used to transmit and receive all data over the World Wide Web. When you type a URL into your browser, you're actually sending an HTTP request to a Web server for a page of information (that's why URLs all begin with "http://"). HTTP1.1, the latest version, is currently undergoing revisions to make it work more efficiently with TCP/IP
- HTML - Hypertext Markup Language - As its name suggests, HTML is a collection of formatting commands that create hypertext documents–Web pages, to be exact. When you point your Web browser to a URL, the browser interprets the HTML commands embedded in the page and uses them to format the page's text and graphic elements. HTML commands cover many types of text formatting (bold and italic text, lists, headline fonts in various sizes, and so on), and also have the ability to include graphics and other non-text elements.
- Host - A central computer or server in a network. It is usually referred to as a large centralized mainframe, but also can refer to any computer that functions as the source of information or services. It can be a server in a network as well as a desktop PC that functions as a host to its peripherals

## I

- Internet - The Internet originated in 1969, in the midst of the Cold War, as a "nuke-proof" communications network. As you might guess, it received most of its early financing from the U.S. defense department. Now, however, it consists of countless networks and computers across the world that allow millions of people to share information. The lines that carry the majority of the information are know as the Internet backbone. While the government used to run things, now major Internet service providers (ISPs) such as MCI, GTE, Sprint, UUNET, and ANS own portions of the backbone–a good thing as they have the motivation and the revenue to maintain the quality of these large networks.

- IP Address - Internet protocol address - This address is a unique string of numbers that identifies a computer on the Internet. These numbers are usually shown in groups separated by periods, like this: 123.123.23.2. All resources on the Internet must have an IP address–or else they're not on the Internet at all.
- ISDN - Integrated Services Digital Network - The plain old telephone system doesn't handle large quantities of data, and the phone companies realized this a long time ago. So the ISDN spec was hammered out in 1984 to allow for wide-bandwidth digital transmission using the public switched telephone network. Under ISDN, a phone call can transfer 64 kilobits of digital data per second. But it's not always easy to adopt.
- ISP - Internet Service Provider - Once upon a time, you could only connect to the Internet if you belonged to a major university or had a note from the Pentagon. Not anymore: ISPs have arrived to act as your (ideally) user-friendly front end to all that the Internet offers. Most ISPs have a network of servers (mail, news, Web, and the like), routers, and modems attached to a permanent, high-speed Internet "backbone" connection. Subscribers can then dial into the local network to gain Internet access–without having to maintain servers, file for domain names, or learn Unix.
- Insider Attack - An attack originating from inside a protected network.
- Internet Access - The method by which users connect to the Internet.
- Intranet - A private network that uses Internet software and standards.
- IP Spoofing - An attack whereby a system attempts to illicitly impersonate another system by using its IP network address. Routers and other firewall implementations can be programmed to identify this discrepancy.

## J

## K

- Kbps - Your modem's speed is measured in the number of bits it can transfer in a second. Modems rated in kilobits per second are now the standard.
- Kerberos - A security system developed at MIT that authenticates users. It does not provide authorization to services or databases; it establishes identity at logon, which is used throughout this session

## L

## M

- MIME - multipurpose Internet mail extensions - MIME has absolutely nothing to do with Marcel Marceau. It's a way to extend the power of Web browsers to handle graphics, sound, multimedia–anything but text. (Remember, HTML handles nothing but text–everything else is an extension.) MIME is also used for binary email attachments. Browsers recognize MIME types in categories and file types, separated by a slash (such as image/gif). If you've registered a MIME type, the browser decodes the file and launches a helper application

## N

- NetBEUI - Network BIOS Enhanced User Interface - IBM developed this standard protocol, which is a set of rules that an operating system uses to control how computers on a network to talk to each other. This protocol is now also used by Microsoft and Novell on many network operating systems including LAN Server, LAN Manager, Windows NT, and Windows 95.
- NCSC - (National Computer Security Center). The arm of the U.S. National Security Agency that defines criteria for trusted computer products. Following are the levels:
- Network - A collection of computers and other devices that are able to communicate with each other over some network medium.
- Network Security - The authorization of access to files and directories in a network. Users are assigned ID numbers and passwords that allow them access to information and programs.

## O

## P

- POP - Post Office Protocol - The current champ in Internet email mailbox access standards, but its limitations–basically, you connect to a server and download all your messages, which are then deleted from the server–discourage flexibility. Of course, some clients let you leave all messages on the server, and/or refuse to download messages above a certain size. Still, as messages become longer–with multimedia (such as sound or video) objects and the likes–we'll want some flexibility in what we retrieve and when we retrieve it. That's where IMAP comes in. The current version of POP is POP3.
- Proxy servers - A proxy server is a system that caches items from other servers to speed up access. On the Web, a proxy first attempts to find data locally, and if it's not there, fetches it from the remote server where the data resides permanently.
- Packet - A logical grouping of information that includes a header and usually user data (a frame) that is used for transmission in LANs and packet switching systems.
- Packet Filtering - A second layer of filtering on top of the standard filtering provided by a traditional transparent bridge. Can improve network performance, provide additional security, or logically segment a network to support virtual workgroups.
- Packet Switching - Type of data transfer that occupies a communication link only during the time of actual data transmission. Messages are split into packets and reassembled at the receiving end of the communication link.
- Private-Key Cryptography - The traditional method of encryption that uses a secret key. Both sender and receiver use the same key. This is the fastest method, but transmitting the secret key to the recipient in the first place is not secure.
- Protocol Address - Also called a network address. A network layer address referring to a logical, rather than a physical, network device.
- Public-Key Cryptography - This term deals with each person having a pair of keys, one called the public key, and the other called the private key. Each person's public key is published while the private key is kept secret. Public-Key cryptography can be used for privacy (encryption) and also for authentication (digital signatures).

## Q

## R

- Router - This piece of hardware does what it says: it routes data from a local area network (LAN) to a phone line's long distance line. Routers also act as traffic cops, allowing only authorized machines to transmit data into the local network so that private information can remain secure. In addition to supporting these dial-in and leased connections, routers also handle errors, keep network usage statistics, and handle security issues.
- Remote Access - the process of allowing remote workers to access a corporate LAN over analog or digital telephone lines.

## S

- SHTTP - secure hypertext transfer protocol - This protocol was developed by Enterprise Integration Technologies to keep your money safe on its way from your wallet to a commercial transaction on the Internet.
- System life cycle (SLC) - The course of developmental changes through which a system passes from its conception to the termination of its use and subsequent salvage. Note: For example, a system life cycle might include the phases and activities associated with the analysis, acquisition, design, development, test, integration, operation, maintenance, and modification of the system.
- SMTP - simple mail transfer protocol - When you're exchanging electronic mail on the Internet, SMTP is what keeps the process orderly. It's a protocol that regulates what goes on between the mail servers.
- SSL - Secure Sockets Layer - SSL is a transaction security standard developed by Netscape Communications to enable commercial transactions to take place over the otherwise notoriously non-secure Internet. It's one of a few competing security standards.
- Security - Protection against unwanted behavior. The most widely used definition of computer security is security = confidentiality + integrity + availability.
- Security Policy - A security policy is the set of rules, principles, and practices that determine how security is implemented in an organization. It must maintain the principles of the organization's general security policy.
- Smart Card - A credit card with a built-in microprocessor and memory used for identification or financial transactions. It is more secure than a magnetic stripe card and can be programmed to self-destruct if the wrong password is entered too many times.

## T

- TCP/IP - transmission control protocol/Internet protocol - These two protocols were developed by the U.S. military to allow computers to talk to each other over long distance networks. IP is responsible for moving packets of data between nodes. TCP is responsible for verifying delivery from client to server. TCP/IP forms the basis of the Internet, and is built into every common modern operating system (including all flavors of Unix, the Mac OS, and the latest versions of Windows).
- Telnet - Telnet is an application that lets you log on to a Unix computer. Provided you have an account on that Telnet server, you can then use its resources. A drawback of Telnet is that it's character-based, so you need to speak Unix to the other computer. Traceroute - Originally a Unix program, Traceroute is now available on most platforms. Traceroute is a

utility that allows you to see how and where information travels on the Net. It traces the path a packet takes as it is sent from your computer to a destination computer (such as the server for a Web site). When encountering a particularly slow Web site, a Traceroute program can help you evaluate which link in the Internet chain is responsible for the lag time.

## U

## V

- Virus - A malicious piece of code that infects computers. It is most commonly transmitted by e-mail and its effects can range from mildly annoying to total devastation.
- Virtual Private Network (VPN) - A network service offered by public carriers in which the customer is provided a network that in many ways appears as if it is a private network, but which, in fact, is provided over the carrier's public network facilities. It allows a private network to be configured within a public network.

## W

- WAN - (Wide Area Network). - A communications network that covers a wide geographic area, such as a state or country.

## X

## Z

# Bibliography


[1] http://www.gocsi.com/

[2] Software Engineering (6th Edition) by Ian Sommerville Addison-Wesley Pub Co; ISBN: 020139815X; 6th edition (August 7, 2000)

[3] CERT©Advisory CA-2000-04 Love Letter Worm http://www.cert.org/advisories/CA-2000-04.html

[4] Hack Attacks Encyclopedia: A Complete History of Hacks, Cracks, Phreaks, and Spies over Time by John Chirillo Publisher: John Wiley & Sons; ISBN: 0471055891; Bk&Cd-Rom edition (August 22, 2001)

[5] System Security: Confidentiality Integrity Continuity Brookfield Pub Co; ASIN: 0863530591; (December 1996)

[6] Cyber Threats and Information Security: Meeting the 21st Century Challenge (Csis Report) Center for Strategic and International Studies; ISBN: 0892063882; (May 21, 2001)

[7] Gollmann, Dieter. Computer Security. John Wiley and Sons, August 1999

[8] Garfinkel, Simson, and Gene Spafford. Practical Unix, Windows and Internet Security. O'Reilly & Associates, Inc., April 1996.

[9] Securing Business Information: Strategies to Protect the Enterprise and Its Network Addison-Wesley Pub Co; ISBN: 020176735X; 1st edition (January 30, 2002)

[10] Internet Security Strategy: A technical guide by Barbara and Robert Bagwill: National Institute os Standards and Technology Computer Security Division http://csrc.nist.gov/

[11] Information Security Risk Analysis Auerbach Publications; ISBN: 0849308801; 1st edition (January 23, 2001)

[12] Data Analysis and Classification Bay Press; ISBN: 0970029705; (August 1, 2000)

[13] Common Criteria for Information Technology Security Evaluation Part 1, 2, 3. Version 2.1 CCIMB-99-031,032,033 ISO/IEC 15408:1999

[14] http://www.radium.ncsc.mil

[15] IRMI - Risk Management and insurance informartion resource http://www.irmi.com/

[16] Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture

[17] The International PGP Home Page http://www.pgpi.org/

[18] Internet Mail Consortium http://www.imc.org/smime-pgpmime.html

[19] PEM Web Resources http://asg.web.cmu.edu/cyrus/email/standards-PEMPGP.html

[20] SSH Communications Security http://www.ssh.com/

[21] Netscape developers homepage http://developer.netscape.com/docs/manuals/security/sslin/contents.htm

[22] IPSec Developers Forum http://www.ip-sec.com

[23] Virtual Private Network Consortium htt://www.vpnc.org/

[24] Authentication: From Passwords to Public Keys Addison-Wesley Pub Co; ISBN: 0201615991; 1st edition (October 1, 2001)

[25] Kerberos: A Network Authentication System Addison-Wesley Pub Co; ISBN: 0201379244; 1st edition (May 4, 1999)

[26] security.tao.ca Encryption Technology http://security.tao.ca/crypt.shtml

[27] PEST Analysis http://www.corex.net/visitors/pest.htm

[28] University of Giessen Law Department http://homepages.fh-giessen/h̃g52/lv/eh/root.html

[29] http://www.ticketmaster.com/

[30] http://www.templetons.com/brad/copymyths.html

[31] http://europa.eu.int/index_en.htm

[32] MEGALAW.COM Cryptography / Encryption Law http://www.megalaw.com/top/encryption.php

[33] Cisco Connection Online http://www.cisco.com

[34] Stein, Lincoln D. Web Security; Addison-Wesley (1998)

[35] Bundesgesetzblatt http://www.jura.uni-sb.de/BGBl/

[36] Udenrigsministeriet (Royal Danish Ministry of Foreign Affairs) Markedsprofil (Portugal, Tyskland, Brasilien, Holland, England)

[37] NIST Preliminary Results of Study of Non - U.S. Cryptography Laws/Regulations.

[38] OECD Group of Experts on Information Security and Privacy, Inventory of Controls on Cryptographic Technologies (DSTI/ICCP/REG(98)4/REV3), September 23, 1998.

[39] E-mail from the German Ministry of Economics and Technology, January 19, 1999.

[40] http://www.db.nl/english/Legal.html

[41] Het Kabinet Van De Gevolmachtigde Minister Van De Nederlandse Antillen.

[42] Cyber-Rights & Cyber-Liberties (UK) Response to the Secure Electronic Commerce Statement, April 28, 1998 http://www.cyber-rights.org/crypto/ecsresp.htm