Secure Working from Home in an Industrial Context

Fredrik Kilemark

MASTER'S THESIS
Technical University of Denmark
LYNGBY
IMM-THESIS-2004-06

IMM

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

Front page image courtesy of Learn the Net. Copyright 1996-2004 by Michael Lerner Productions. http://www.learnthenet.com

IMM-THESIS: ISSN 1601-233X

Printed by IMM, DTU

Abstract

This thesis project investigates the security risks that need to be considered when companies are opening their networks for remote access over the Internet. The focus is on employees connecting from home or from other remote locations using the VPN technology. Especially considered is the case where employees want to take advantage of their private PCs and broadband connections to do some work in the evening or during the weekend. The main goal is to find out what the company policy should be when employees want to do this.

The situation at a particular company in Sweden has been studied to see how this is handled in practice. Important concepts related to remote access like authentication, data protection, firewalls and intrusion detection are addressed. Focus is on Windows related issues since this company operates in a Windows-based environment. The risks associated with remote access have been identified and assessed. Mitigation actions that may be used to reduce these risks are described. The report presents general recommendations for good IT security practice for both companies and home users. More specific recommendations for companies in the same situation as this particular company are also given.

The usage of private PCs is not as widespread as initially thought, mainly because many employees are still using dial-up modem connections. But broadband connections are becoming more and more common and it is wise for companies to have a policy ready that addresses these security issues.

Keywords: remote access, security, risks, VPN, home users

Preface

This thesis project was performed to fulfill the final part of the requirements for obtaining the degree Master of Science in Computer Systems Engineering. The work has been carried out over a period of 5 months, from 1 October 2003 to 29 February 2004. It took place at the department of Informatics and Mathematical Modelling at the Technical University of Denmark. The project was supervised by Dr. Robin Sharp.

Acknowledgments

There are a lot of people who I would like to thank, who have all contributed in one way or the other during my work with this thesis.

First of all, the people at the company with which I have cooperated. The time spent at the office has allowed me to take part of your views and experiences in this area. The surveys, interviews and discussions have supplied me with a large part of the information this thesis is based on. I would especially like to thank the network administrator for always taking time for discussions.

My supervisor, Robin Sharp, for patiently giving me advice in technical as well as practical issues during our meetings.

Margareta and Mats for taking time to proofread and comment on my English writing.

My family for always encouraging and supporting my studies, even financially when the study assistance was not sufficient.

Finally, my girlfriend, for her understanding during the time I have spent on this project and for always giving me feedback during discussions of different ideas.

Fredrik Kilemark, February 2004

Contents

Chapter 1

Introduction

Working from home or working from a location other than the company office is today a part of everyday life for many people. The increased use of IT systems has changed the way we store, access and communicate information. For a lot of people this has led to the computer becoming the most important tool at work.

The technologies available today with mobile phones, laptops and Internet access allows for these people to connect to the corporate network from almost anywhere. This enables them to work from home, from business partners or customers and during business trips. The widespread use of these technologies has made them available at an economically feasible cost.

Traditionally only people who traveled a lot was given equipment by the company to take advantage of these possibilities. Today it has become very common for people in Sweden to have one or more computers at home. It is also becoming more and more common to have high-speed Internet connections at home for personal use. In this situation it is not uncommon for the employee to ask the employer to get access to the corporate network from home. The employee would often like to have the possibility to do some work from home. Maybe leave the office early and finish up in the evening or do some work in the weekend. Since the computer and the Internet connection are already available, all that is necessary for the company, is to open up their network for remote connections.

This situation gives rise to a lot of security issues that need to be considered. The IT security awareness of the average home user is not very high. Often the security measures available on a home computer is not much more than a free trial version of an anti-virus program that was installed by the computer manufacturer and has not been updated since the computer was bought.

Everybody have heard about hackers breaking into computers. Viruses and worms spreading through the Internet. The home user often says that there is no reason for protection since there is nothing to protect. Is this true? What risks are there when connecting to the Internet? Which actions are reasonable for the company to require from employees that are connecting from remote locations over the Internet?

This thesis will focus on the security aspects associated with employees connecting to the corporate network over the Internet. The questions above are some of the things that I was wondering about when I started working on this thesis and which I will try to give answers to.

To be able to find out the concerns about these issues from a company's perspective, I have worked in cooperation with a company. Since security issues are considered sensitive I will not discuss any unnecessary details about the company or their actual security configuration. Hopefully this will result in that the information presented here will be applicable for other similar companies as well. Some information about the company and the requirements it has for a remote access solution are presented in Chapter 2.

Chapter 3 describes common threat-sources and the attack methods they are using. The risks associated with deploying a remote access solution are presented, categorized and assessed.

Concepts that are important concerning remote access solutions are described in Chapters 4-8. These include technologies for remote access, user authentication, data protection, firewalls and intrusion detection. These chapters naturally contain discussions that are a bit more technical than the rest of the chapters.

Chapter 9 contains advice about what needs to be considered to achieve good IT security practice. This information applies to companies as well as home users.

Recommendations of mitigation actions that are suitable for mitigating the risks that are present in a remote access solution are presented in Chapter 10.

The final chapter contains conclusions that have been drawn during the work with this thesis. Suggestions of areas that would be interesting to study further are also made.

Appendix A contains a glossary to aid readers not familiar with all concepts discussed in this report. The OSI model commonly used when discussing network architecture is found in Appendix B. Introduction to the basic concepts of cryptography and malicious code are found in Appendix C and Appendix D respectively.

Chapter 2

Requirements

This chapter describes the current remote access situation at the company with which I have cooperated. The parties that have an interest in a remote access solution will be identified and their requirements will be clarified.

2.1 Background

The company with which I have cooperated, is involved in research, development, manufacturing, sales, marketing and support of the company's products. The corporate network has about 120 users and about 150 computers. It is a Windows-based network environment, even if a few Linux systems have been deployed. At the moment remote access to the corporate network is useful for about 20-30 employees working in various departments in the organization. Some of these have laptop or desktop computers that belong to the company while others use private computers to connect from home. The connections to the Internet from remote locations vary from case to case, some use old fashioned dial-up modem connections, while some have permanent broadband connections.

The task is to look at the current solution for remote access from a security perspective and find out which improvements can be made to make the system as secure as possible, with regards to the company operation.

In a situation like this when a system is constructed or modified it is important to identify the requirements for the system. Otherwise the final system will probably not fulfill the expectations of the people that will interact with it. In this case the stake-holders may be divided into three groups, the users who will actually use the system, the IT department which will be responsible for installation, configuration, maintenance and support and finally management which is ultimately responsible for the company operation. The requirements from these groups have been identified through surveys, interviews and discussions with representatives from the different groups. These requirements are presented in sections 2.2-2.4 below. In addition to these, there are also requirements that are based on practical and economical aspects. These have to do with that the current systems, already in place, should be kept unchanged as far as possible. The reasons for this are that a lot of money have been invested in the systems as well as a lot of time to configure them. These requirements are presented in section 2.5 below.

2.2 Management requirements

- **Flexibility**
  The main goal is to provide a solution for employees that need to be able to access resources on the corporate network when working from remote locations, e.g. during business trips.

  The remote access solution may also be used by other employees at home to allow for flexibility in their work.

- **No unauthorized access**
  It is important to prevent unauthorized access to information that is sensitive for the company.

- **Authorization routines**
  It is important to have clear rules about who is responsible for granting an employee access to connect to the corporate network from a remote location.

- **Clear rules**
  Clear rules about how the computer at the remote location may be used. Who may use it, for which purpose, which applications may be installed etc.

2.3 IT department requirements

- **Central control**
  As many features as possible should be centrally controlled to make management of the system as easy as possible.

- **Clear rules**
  Clear rules about how the computer at the remote location may be used. Who may use it, for which purpose, which applications may be installed etc.

  The case where the computer is a private computer that is owned by the employee must be especially considered.

- **Verification**
  A way to monitor and verify that the rules and procedures that apply are actually enforced in practice.

- **Incident overview**
  A better way to detect and investigate incidents than to just go through log-files after they have occurred.

- **Adaptability**
  A system that easily can be adapted to new threats as they arise.

2.4 User requirements

- **Functionality**
  The system should allow employees access to the resources that they need to be able to perform their work from a remote location. Users from different departments have different needs regarding which kind of resources they need to access. Some only need access to their mailbox while others need to be able to work on resources that are shared between several employees. The resources which are accessed on the corporate network may later be used locally when the user is offline. Many also need to be able to connect hardware locally to their PC.

- **User friendliness**
  The system should be as easy and flexible to use as possible.

- **Clear rules**
  Clear rules about how the computer at the remote location may be used. Who may use it, for which purpose, which applications may be installed etc.

2.5 Other requirements

The Windows-based network environment contains systems that should not be changed if possible. There have been investments both in time and money to install and configure these systems, which include:

- **Firewall**
  The current firewall which has support for remote access VPN using common protocols like Point-to-Point Tunneling Protocol and IP Security.

- **E-mail server**
  The current e-mail server which has support for remote access through a web-based interface.

- **Application server**
  The current Citrix MetaFrame application server.

- **Remote systems**
  Remote PCs using the Windows operating system which are familiar to the users.

- **Anti-virus**
  The centrally controlled anti-virus solution for hosts on the network.

2.6 Summary

The requirements presented above will not be treated as requirements in the strictest sense, they will be considered more as wishes of the company. The reason for this is that it may not be possible to combine all requirements with the goal of the task, to make the system reasonably secure for use in the company operation. Instead it is likely that compromises need to be made to achieve this.

Chapter 3

Risks

This chapter begins with a short overview of what IT security and risk management is about, followed by a description of different threat-sources and the attack methods they use. Finally there is a presentation of the risks that have been identified for a remote access solution together with a description of how they have been categorized and assessed. The main goal is to find out which threats cause the highest risks.

3.1 Overview

3.1.1 IT security

IT security is about ensuring three things; confidentiality, integrity and availability.

- Confidentiality is about making sure that information is not accessible by unauthorized parties.
- Integrity is about making sure that information is not modified by unauthorized parties.
- Availability is about making sure that information and systems are available to authorized parties when needed.

3.1.2 Risk management

It is not possible to make a system 100 percent secure, i.e. ensuring confidentiality, integrity and availability under all circumstances. This would imply that nothing could make the system behave in a way that was not intended no matter what happens to it. This includes viruses, hackers, floods, fires and even the administrator smashing a sledge hammer into the main server. The system could of course be made as secure as possible by implementing all available technical and physical safeguards. But in practice this is not done, since security is not the main goal of the company operation. Instead security measures should be taken to ensure that the security level is reasonable for the company operation. The process of ensuring a reasonable security level in a structured way is called risk management. The description of risk management as given by the National Institute of Standards and Technology (NIST) [SGF02] is shown below.

> *"Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level."*

3.2 Threat-sources

Security threats come from many different sources. These sources have very different objectives, competence, motivation and resources. The following sections will give a short description of the most important threat-sources and finally a description of common attack methods that these threat-sources use.

3.2.1 Hackers[1]

Hackers are technically competent persons who break into computer systems. Their motivation vary a lot and can be anything from curiosity to revenge. Some even claim that they are actually doing a good thing since by breaking into a system they prove that the system is not safe. This opinion is probably not shared by the company that spend time to investigate and restore the compromised system. Their objectives may also vary from just accessing the system to modifying or destroying it or the information that is stored and processed by it. One example is the defacing of web-sites which often get media attention. Other incidents that are not as visible to the outside are probably kept secret by the company to prevent unnecessary negative attention.

3.2.2 Script kiddies

Script kiddies are persons who think they are, or want to be hackers. They lack the technical expertise that is required and use malicious code written by others. This code is used to attack systems and exploit vulnerabilities in different ways but the script kiddie might not even understand how it should be used or what consequences there may be. It is even possible that the target system is of a completely different kind than the code was intended for, e.g. using an exploit for a Linux system on a Windows system. There is a large amount of attack tools available on the Internet for anyone to download and execute.

3.2.3 Computer criminals

Just like in the real world there are criminals in cyberspace. With monetary motivation their objective may be to steal the customer credit card database from an e-commerce company or to perform identity theft. The book Tangled Web [Pow00] contains some

[1] The word hacker means different things to different people. Some would rather use one of the terms cracker or black hat hacker when talking about persons that uses their technical skills to break into systems.

true stories in this area. Less severe actions may be to manipulate the input of poorly constructed web-based shopping systems to be able to order products at reduced price or even for free. Also, organized crime is taking advantage of new technologies, using it to serve their malicious purpose [EUR03].

3.2.4 Terrorists

Since IT systems have become essential tools for many kinds of organizations, they have become interesting targets for terrorists. Attacks on IT systems are of course different from physical attacks like bombs but may cause severe damage anyway.

3.2.5 Industrial espionage

The threat-source may also be professionals engaged in industrial espionage. It could be competitive companies or foreign governments. The motivation of these are competitive advantage. Their financial and technical resources are much higher than for the groups discussed in the previous sections.

The worldwide counter intelligence collection system known as Echelon is run jointly by the United States, Great Britain, Canada, Australia and New Zealand. Information collected by this system was allegedly used for industrial espionage to favor the American company Boeing over its European competitor Airbus when trying to break into the Saudi Arabian market [BBC00]. The United States Federal Bureau of Investigation (FBI) is using surveillance systems like Carnivore to be able to tap data communications at ISPs. The Swedish national authority for signals intelligence is called Försvarets radioanstalt (FRA), or the National Defence Radio Establishment. New laws in Sweden and recommendations from the EU are opening possibilities for this kind of surveillance operations here as well.

For most companies the information collected by these systems is probably not something that they need to worry about. Instead a more likely threat is the one from the competing companies themselves. These have not got the same technical resources as counter intelligence agencies and have to access information in other ways, e.g. through hacking.

3.2.6 Insiders

Insiders pose threats in several different ways. A disgruntled employee or a dishonest employee may deliberately attack the system. These attacks include employees who destroy or falsify information as revenge against the company, steal information like the customer database or other business secrets and sell them to a competitive company or take it with them when they leave the company. According to [And01, NBC03] inside threats are more common than external threats. The biggest concern are the unintentional non-malicious mistakes that users make. There may be many reasons for these mistakes, e.g. poor education of users, negligence or just human error. Systems used by humans will naturally and unavoidably be subject to human error.

3.2.7 Natural disasters

Threats which come from natural disasters, like earthquakes and floods must of course also be taken into consideration. In the current case though, the geographical location is not especially exposed to these kind of threats and they will therefore not be further considered.

3.2.8 Attack methods

Attackers who do not have a particular reason for targeting a specific system will naturally look for a target that is easy to attack. As described in [MSK03] attackers try to find out information about the target before the actual attack. This is done through foot-printing, scanning and enumeration. The information collected through these methods can reveal a lot, e.g. IP addresses, open ports, operating system version, running applications, file-shares and user accounts. This will tell the attacker which known vulnerabilities that can be used to gain access to the system. There are a lot of advanced attack tools available on the Internet and it is not necessary to be a highly skilled attacker to use these tools. If the system has some basic security then then these attackers will find out little or no information about the system and move on to find an easier target.

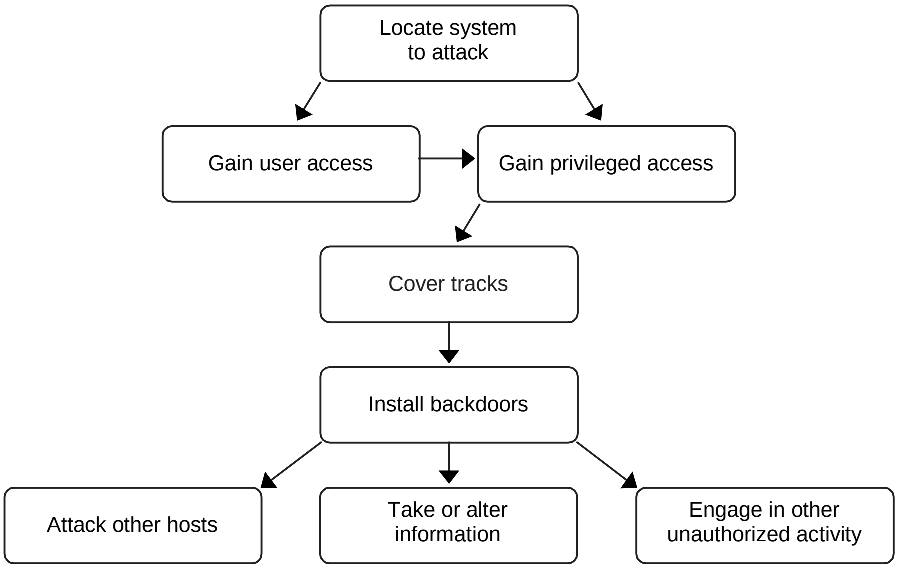


Figure 3.1: Typical steps taken by an attacker during the attack of a network [CER03b].

Attackers that do have a reason for targeting a specific company are harder to protect against. They will of course use other means than just technical if that makes it easier to get what they want. This includes social engineering, dumpster-diving, wardriving, theft and break-ins. To resist attackers like these, it is important to consider not only the technical security measures but also the physical security and the security awareness of the employees. It is more likely that these attackers will take a simpler way like through a stolen laptop than to hack through the main firewall. For the company that we are looking at in this case threats from these professional attackers are not considered very likely.

3.3 Risk identification and assessment

The risks associated with a remote access solution have been identified and divided into three categories, loss of confidentiality, loss of integrity and loss of availability. To be able to calculate the risk level for each identified risk, the risk level matrix from [SGF02] have been used. The way this works is by assessing the likelihood of a threat and assessing the impact of a threat. These assessments are based on scales with three grades. The definitions of the threat impact grades are shown in Table 3.1 and the definitions of the threat likelihood grades are shown in Table 3.2 below.

Impact level	**Definition**
High (100)	Sensitive information that is important for the company operation may become known by competitors. This includes business strategies for the future and core technical expertise that is vital for maintaining a strong position in the market. The longterm effect is that the company may become less competitive. Another type of incident that will also have a high impact is if normal operation on the corporate network is prevented. This could be caused by for example a virus or worm infection spreading on the network.
Medium (50)	Information that is intended only for close partners will become known by competitors. This will give them an advantage that might result in some longterm financial loss for the company.
Low (10)	The system on the company side will not be accessible for remote users to connect to or individual remote users will lose information (without it being disclosed to unauthorized persons).

Table 3.1: Description of the threat impact level grades. The higher the grade the greater the damage is for the company.

Likelihood level	**Definition**
High (1.0)	The likelihood of this to occur is almost certain.
Medium (0.5)	There is a fair chance that this will occur sometime.
Low (0.1)	This is not likely to occur.

Table 3.2: Description of the threat likelihood level grades.

Each of the grades high, medium and low is assigned a value to be able to calculate the risk level. This calculation is done by multiplying the threat impact and the threat likelihood, as shown in Table 3.3 below. The calculated risk level is a value in the interval 1-100, the

Threat likelihood	**Threat impact**		
	Low (10)	**Medium** (50)	**High** (100)
High (1.0)	Low (10 x 1.0 = 10)	Medium (50 x 1.0 = 50)	High (100 x 1.0 = 100)
Medium (0.5)	Low (10 x 0.5 = 5)	Medium (50 x 0.5 = 25)	Medium (100 x 0.5 = 50)
Low (0.1)	Low (10 x 0.1 = 1)	Low (50 x 0.1 = 5)	Low (100 x 0.1 = 10)

Table 3.3: Risk level matrix. The risk level is calculated by multiplying the assessed values of the threat likelihood and the threat impact.

higher the value the larger the risk. The definitions of what these values mean in practice are shown in Table 3.4. Just like with the threat impact and threat likelihood assessments the risk level is divided into three grades, high, medium and low.

Risk level	**Description**
High (51 - 100)	Mitigation actions must be taken right away to reduce the risk regardless of the cost.
Medium (11 - 50)	Mitigation actions should be taken if the cost is reasonable.
Low (1 - 10)	No mitigation actions are needed, the risk must be accepted. An exception may be done if the mitigation cost is very low.

Table 3.4: Descriptions of which actions that should be taken by the company based on the calculated risk level associated with a threat.

In the following sections the threats in each of the three categories, loss of confidentiality, loss of integrity and loss of availability, are listed. Together with each threat is the impact assessment and a list of attack descriptions, i.e. methods or reasons for how the threat may be realized. The likelihood assessment for each of these attacks is also presented as well as the calculated risk level.

These assessments are based on the scenario where no special security safeguards are implemented on the remote PCs. The security safeguards taken on the corporate network itself is not the focus of this report and therefore only threats to the corporate network that arise because of the remote access solution or the remote access users are considered.

3.3.1 Loss of confidentiality: corporate information

Threat description	**Impact**
Unauthorized read access to sensitive corporate information which may lead to the information becoming available to a competitor.	High

This threat is categorized as loss of confidentiality which is generally the least likely threat category compared to loss of availability and loss of integrity.

The highest likelihood for this threat to occur is probably through an attack that is aimed specifically at this kind of information, e.g. by a competitor. The most likely way for this to occur is through the theft of a portable device like a laptop computer. The information on this device is then accessible to the attacker, this may also include account information that may be used to access the corporate network or the employee's mail account.

Another approach from these professional attackers may be to hack into the corporate network directly or through a compromised remote PC. This attack requires more skill from the attacker and is therefore less likely.

A completely different scenario is if the employee accidentally shares sensitive information using Windows file sharing or some other Peer-to-Peer (P2P) files sharing application. P2P applications have become a very popular way of sharing files, by making part of, or all of, the hard drive accessible for other users on the Internet. Often the files which are shared contain information which is copyright protected, like music or movies. Another common type of files are cracks for popular applications which will enable users to run these applications without purchasing a license. The SANS Institute has ranked P2P file sharing as item number nine on their list of the most critical security vulnerabilities for Windows systems [SAN03]. It may not even be the employee who installed or configured this application, it may have been someone else using the computer, e.g. another member of the family. The employee might not even be aware that this application is actually running on the PC.

Attack description	**Likelihood**	**Risk level**
On the remote PC:		
Theft of the PC.	Medium	**50**
The PC is compromised by an attacker on the Internet or the LAN.	Low	**10**
The PC is compromised by an attacker through social engineering techniques (malicious web-site, e-mail with an attached trojan horse etc.).	Low	**10**
Non-employees using the PC (friends, family members etc.).	Medium	**50**
User makes it available by mistake (Windows file sharing, P2P file sharing etc.).	Medium	**50**
Theft of old backup media.	Low	**10**
Information is not removed when old PC is sold or thrown away.	Low	**10**
In transit:		
Sniffing the LAN to which the remote PC is connected.	Low	**10**
Compromised network device on the Internet (router etc.).	Low	**10**
On the corporate network:		
System is compromised (VPN server, firewall etc.).	Low	**10**
A compromised remote PC is used as a back-door to access the system.	Low	**10**
A stolen remote PC is used to access the system.	Medium	**50**
An old remote PC is used to access the system.	Low	**10**

3.3.2 Loss of integrity: corporate information

Threat description	**Impact**
Unauthorized write access that allows an attacker to modify sensitive corporate information so that it can not be trusted.	High

An attack that corrupts data is more likely to come from some kind of system crash than from an attacker actively trying to modify it.

Attack description	**Likelihood**	**Risk level**
On the remote PC:		
The PC is compromised by an attacker on the Internet or the LAN.	Low	**10**
The PC is compromised by an attacker through social engineering techniques (malicious web-site, e-mail with an attached trojan horse etc.).	Low	**10**
User deletes information by mistake.	Low	**10**
System software crash.	Medium	**50**
System hardware crash.	Medium	**50**
Virus or worm infection.	Low	**10**
Non-employees using the PC (friends, family members etc.).	Low	**10**
User makes it available by mistake (Windows file sharing, P2P file sharing etc.).	Low	**10**
In transit:		
Manipulating traffic on the LAN to which the remote PC is connected.	Low	**10**
Manipulating traffic on the Internet (at an ISP, etc.).	Low	**10**
Replaying old traffic.	Low	**10**
On the corporate network:		
System is compromised (VPN server, firewall etc.).	Low	**10**
A compromised remote PC is used as a back-door to access the system.	Low	**10**
A stolen remote PC is used to access the system.	Low	**10**
An old remote PC is used to access the system.	Low	**10**

3.3.3 Loss of availability: corporate information

Threat description	**Impact**
Unauthorized write access that allows an attacker to delete sensitive corporate information.	High

A professional attacker is probably more interested in finding and copying information than of destroying it, even if there is a slight possibility of a blackmail scenario. The most likely way for information to be destroyed is because of a user deleting it by mistake or because of a system crash.

It may also occur if the information is mistakenly shared with write access, for example by using Windows file sharing. A person with ill intent, who just finds the information on the

LAN by coincidence, may delete it. During business trips the laptop computer might be connected to a LAN where other users may not be trusted. Some buildings offer Internet access through a shared LAN, this will enable other people living in the building to access the information. Wireless LANs will allow access to everybody within signal range.

Attack description	**Likelihood**	**Risk level**
On the remote PC:		
The PC is compromised by an attacker on the Internet or the LAN.	Low	**10**
The PC is compromised by an attacker through social engineering techniques (malicious web-site, e-mail with an attached trojan horse etc.).	Low	**10**
User deletes information by mistake.	Medium	**50**
System software crash.	Low	**10**
System hardware crash.	Medium	**50**
Virus or worm infection.	Low	**10**
Non-employees using the PC (friends, family members etc.).	Low	**10**
User makes it available by mistake (Windows file sharing, P2P file sharing etc.).	Medium	**50**
In transit:		
Manipulating traffic on the LAN to which the remote PC is connected.	Low	**10**
Manipulating traffic on the Internet (at an ISP etc.).	Low	**10**
Replaying old traffic.	Low	**10**
On the corporate network:		
System is compromised (VPN server, firewall etc.).	Low	**10**
A compromised remote PC is used as a back-door to access the system.	Low	**10**
A stolen remote PC is used to access the system.	Low	**10**
An old remote PC is used to access the system.	Low	**10**

3.3.4 Loss of availability: remote PC

Threat description	**Impact**
The remote PC becomes unavailable for a few hours or days (need software configuration, software reinstallation, hardware repair etc.).	Low

The most likely cause for this threat is a virus or worm infection. A PC which is connected to the Internet without any security safeguards will be infected. Depending on the type of malicious code with which the system is infected, the downtime will vary. Other likely causes are software or hardware crashes. There are many different natural reasons for these and they will happen from time to time. Information stored on the hard drive will be fragmented over time as files are modified, removed and added. This will reduce the performance over time and may eventually lead to information being lost in a software crash. When it comes to hardware crashes the hard drive is the most sensitive part of the PC since it is a mechanical device and it contains all the information.

It is also common that users download applications from the Internet which cause the system to become unstable. Sometimes this is simply because the application is badly written and interferes with other applications on the system. Other times the application is not correctly installed or configured by the user. It may even be as simple as the user not having patience enough to allow the installation process to finish properly.

Attack description	**Likelihood**	**Risk level**
Theft of the PC.	Medium	**5**
The PC is compromised by an attacker on the Internet or the LAN.	Low	**1**
The PC is compromised by an attacker through social engineering techniques (malicious web-site, e-mail with an attached trojan horse etc.).	Low	**1**
User destroys system configuration by mistake.	Medium	**5**
System software crash.	Medium	**5**
System hardware crash.	Medium	**5**
Virus or worm infection.	High	**10**

3.3.5 Loss of availability: remote access point

Threat description	**Impact**
The system on the company side is not available to receive connections from remote users for a few hours or days.	Low

The systems at the company side that accepts connections from the remote PCs are not as likely to crash or being compromised as a remote PC. This is because these systems are usually implemented as a hardware devices or as hardened software systems.

Attack description	**Likelihood**	**Risk level**
Denial-of-service attack.	Low	**1**
Virus or worm infection from remote PC.	Low	**1**
Virus or worm infection from the Internet.	Low	**1**
System is compromised (VPN server, firewall etc.).	Low	**1**
System crash.	Low	**1**
Administrator misconfigures the system.	Low	**1**

3.3.6 Loss of availability: corporate network

Threat description	**Impact**
The corporate network will not be available for normal operation for a few hours or days.	High

This threat most likely comes from a virus or a worm infection, spreading to the corporate network from a remote PC. Either an infected PC which is connected from a remote location, or from an infected PC, i.e. a laptop, that is carried into the office and connected directly to the network.

Attack description	**Likelihood**	**Risk level**
Virus or worm infection on the remote PC spreading to the corporate network.	Medium	**50**
Vital network resource compromised by an attacker through a remote PC (mail server etc.).	Low	**10**

3.3.7 Information sources

The assessments that have been done of the threat likelihood and the threat impact are based on information collected from several sources. The threat impact assessments have been based mainly on discussions with representatives from the company management. The threat likelihood assessments have been based on discussions with the IT department about the frequency of previous incidents, incident statistics [NIS03b, NIS03a, Fed04], incident trend analysis [CER03b] and the required skill and availability of tools to perform such attacks [SM01, MSK03].

It is very hard to do these kinds of assessments, the main reason for this is that there are no definite answers, in the end it comes down to subjective feelings. On the same time it is very important to do these assessments. The result will be used to make sure that the future mitigation actions are implemented to reduce the highest risk levels, as will be discussed in Chapter 10. Implementing mitigation actions before the risks have been identified and assessed will probably lead to misdirected actions and is not recommended [SGF02, FE97, And01].

3.4 Summary

The main threat-sources have been described as well as the attack methods that they use. For the current case the most common threats are the ones that come from mistakes by users, system crashes and malicious code like viruses and worms. Attackers that actively are trying to hack systems to get access are not considered very likely by this company.

Risk assessment is a difficult process that is based on probabilities and not on scientific facts. The main goal in this case was to identify the highest risks and thereby identify what is important to protect. The result is that losing sensitive corporate information to a competitor or not being able to use the corporate network resources for normal operation will have most impact on the company. Threats that only affect a single or a few employees does not have a high impact for the company. The remote access solution itself is considered to be a system like that, since only a limited number of employees rely on.

Chapter 4

Remote access technologies

Traditionally employees have connected from home, or from other remote locations, to the corporate network by dialing directly into the office over the Public Switched Telephone Network (PSTN) or the Integrated Services Digital Network (ISDN). But today higher speed connections are available through the cable television network and by using Digital Subscriber Line (DSL) technologies, i.e. ADSL and VDSL. These types of connections are becoming more and more common at home to connect to the Internet. A company may use the Internet as the access point to the corporate network and in this way take

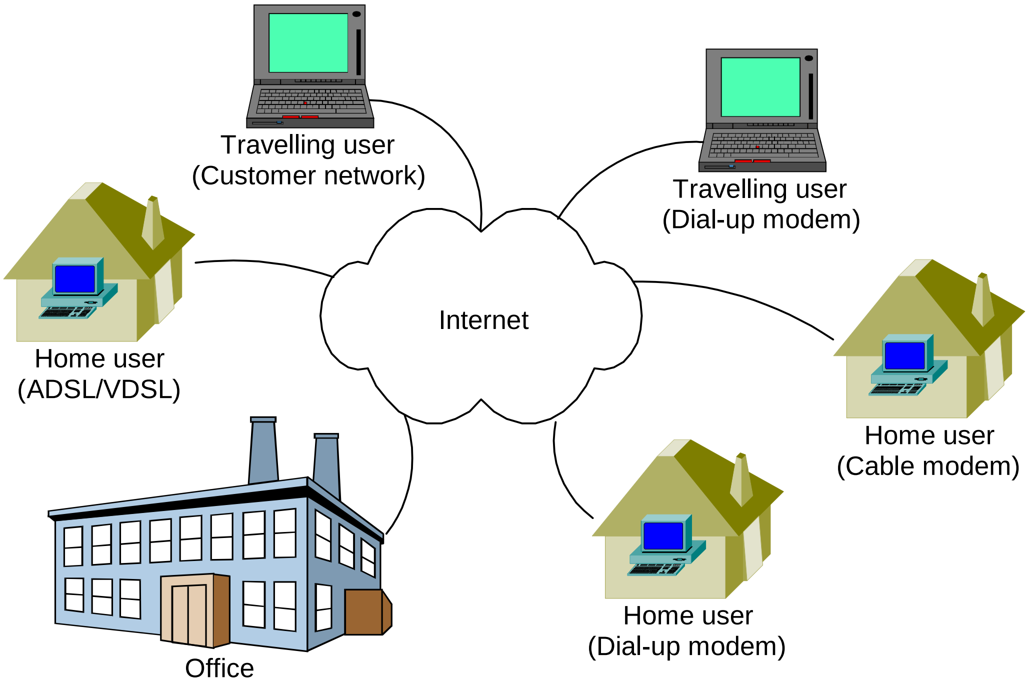


Figure 4.1: Connecting to the corporate network through the Internet allows remote users to take advantage of a variety of Internet access technologies, while the connections are handled in the same way at the office.

advantage of these high-speed connections. The flexibility of allowing a variety of Internet access technologies at the user-end will not be a burden on the company-end since all connections are handled in the same way.

In this chapter the most common and powerful technology for remote access in this scenario is described, the Virtual Private Network. Two other techniques that offer more limited access are also described, an application server based solution and a web-based interface for mail access.

The information about Virtual Private Networks is mainly based on [Cis03a, Mic99, Mic03g, Wat03, IBM99].

4.1 Virtual Private Network

With Virtual Private Networks (VPNs) the idea is to create a secure private network between two parties over an insecure public network. Before the VPN may be set up it is assumed that there already is connectivity between the involved parties over the public network. Here the Internet will be used as the public network and this means that both parties first will have to get access through an Internet Service Provider (ISP) and have IP connectivity before the VPN can be set up. The VPN is then set up by creating a secure connection between the two points. Data sent between these points are encrypted, this is called a tunnel.

VPNs may be used both for connecting two company sites, site-to-site VPN, as well as connecting a single remote computer to the company site, remote access VPN. This report will naturally focus on remote access VPNs.

To create a remote access VPN we need a VPN server at the company side and a VPN client at the user side. The VPN server can be either a device for this purpose only, or it can be firewall or a router with built-in VPN support. Modern solutions often use a device with built-in VPN support. This effectively eliminates the need to decide where the VPN server should be placed in relation to the firewall. The VPN client on the user side can be implemented either in software or in hardware. A software client is the most flexible solution for users that connect from more than one location.

The VPN tunnel may be created on different layers in the Open Systems Interconnection (OSI) reference model, and there are several different protocols available. In the following sections the most common ones that may be used for remote access VPNs over the Internet, will be discussed. See Appendix B for a description of the OSI model.

4.1.1 Point-to-Point Tunneling Protocol

The Point-to-Point Tunneling Protocol (PPTP) [HPV$^+$99] is a protocol created by Microsoft. It operates at the data-link layer, layer 2 of the OSI model, and depends on another layer 2 protocol, the Point-to-Point Protocol (PPP) [SE94]. PPP is like the name indicates used for communication over point-to-point links. Data from an arbitrary layer 3 protocol is encapsulated inside PPP frames. PPTP then encapsulates PPP frames inside

IP packets using a modified version of Generic Routing Encapsulation (GRE). This makes it possible to send data over the Internet like any other IP packet. See Figure 4.2 below.

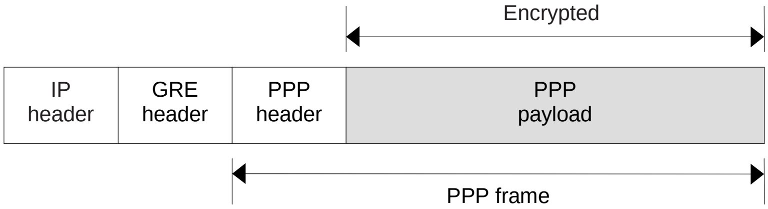


Figure 4.2: PPTP packet structure.

To achieve confidentiality of the transmitted data, PPTP encrypts the payload that is stored inside the PPP frames using Microsoft Point-to-Point Encryption (MPPE). MPPE is based on the symmetric RC4 encryption algorithm.

During connection establishment and user authentication the control protocols specified in PPP are used. This includes either the clear text Password Authentication Protocol (PAP) or one of the encrypted protocols in the form of Challenge Handshake Authentication Protocol (CHAP), MS-CHAP version 1 or MS-CHAP version 2. There is also a standard extension to PPP, called Extensible Authentication Protocol (EAP), that allows for an arbitrary authentication protocol to be implemented. The most common authentication protocol actually in use is probably MS-CHAP version 2.

Regardless of which of these PPP protocols that are used, the communication activities takes place on a control channel which is initiated from the client to port 1723 on the PPTP server using TCP. The actual data is sent on a separate channel using the GRE encapsulated packets previously described.

Using PPTP is very convenient since all Microsoft Windows operating systems since Windows 95[1] have built-in client software for it. Unfortunately Microsoft's implementation of PPTP is not considered secure. Cryptanalysis of the protocol have shown several vulnerabilities due to the the way Microsoft have implemented it [SM98, SMW99]. There are vulnerabilities in the most common authentication protocols used with PPTP, both in the original MS-CHAP version 1 as well as the improved MS-CHAP version 2. Weaknesses in the implementation of the RC4 encryption algorithm are also pointed out. The main concern is that encryption keys are generated based on the user password. Windows passwords will be discussed in more detail in Chapter 5.

There are also a few other issues that makes PPTP questionable as a secure VPN protocol. The communication over the control channel is done in clear text. This can reveal information to eavesdroppers or be used to cause Denial-of-Service (DoS) attacks. Another issue is that even though there is encryption of the payload to achieve confidentiality, there are no authentication or integrity mechanisms that prevent packets from being picked up by an attacker and then replayed, either modified or unchanged.

[1] Windows 95 systems do need to have an update from Microsoft installed.

4.1.2 IP Security

IP Security (IPSec) [KA98b] is a security architecture for the Internet Protocol (IP). Since it is developed specifically for IP it operates at the network layer, layer 3 of the OSI-model.

Two different protocols are specified in the architecture, the IP Authentication Header (AH), and the IP Encapsulation Security Payload (ESP) [KA98a]. These protocols may be used separately or in combination. AH is not appropriate in this case since it includes a packet integrity checksum which is calculated partly from the packet IP header. Because of this it is not compatible with Network Address Translation (NAT), which is a very widespread technique on the Internet today. See section 7.5 for more information about NAT. As a result of this incompatibility most IPSec implementations use ESP.

IPSec operates in either tunnel mode or traffic mode. For the current case the best way to use IPSec is in tunnel mode. This mode of operation will provide the following security features:

- Confidentiality of data through encryption.
- Integrity of data and authentication of the sender through the inclusion of a key based hash value.
- Anti-replay protection through the inclusion of packet sequence numbers.

IPSec is algorithm independent. This means that the communicating parties have come to an agreement about which encryption algorithms should be used. This agreement is called a Security Association (SA). Even though the IPSec architecture does not require a specific encryption algorithm to be used, there are some algorithms that an implementation must include to be considered compliant. Common encryption algorithms in use today include Data Encryption Standard (DES) with a 56-bit key and Triple DES (3DES) with a 168-bit key. Common hash functions are Message Digest 5 (MD5) and Secure Hash Algorithm 1 (SHA1).

The encryption keys should not be the same during the whole session, instead they should be changed regularly. To automate this process a key management protocol is used. Just like it is possible to use different encryption algorithms, it is possible to use different key management protocols. A common choice today is to use Internet Key Exchange (IKE).

The authentication process is much different from the PPTP protocol. While PPTP performs user authentication based on a user password, IPSec allows for both device authentication and user authentication through shared secrets or through certificates. This is a much more secure configuration, but it also requires more work to configure it.

4.1.3 Layer 2 Tunneling Protocol/IP Security

Since the company in this case is primarily using Microsoft's Windows operating systems, it is interesting to look at the VPN support in these system. Microsoft's latest operating systems Windows 2000 and Windows XP have apart from PPTP also built-in client software for the L2TP/IPSec protocol.

Layer 2 Tunneling Protocol

Layer 2 Tunneling Protocol (L2TP) was created as a replacement for PPTP. It was influenced by both PPTP from Microsoft as well as the Layer 2 Forwarding protocol (L2F) from Cisco Systems.

Just like in PPTP, L2TP depends on the PPP protocol but in contrast it does not use GRE to encapsulate the PPP frames. Instead the PPP frames are encapsulated inside L2TP frames which are then sent over the Internet using the User Datagram Protocol (UDP), see Figure 4.3 below. L2TP allows for the payload in the PPP frame to be encrypted just like in PPTP.

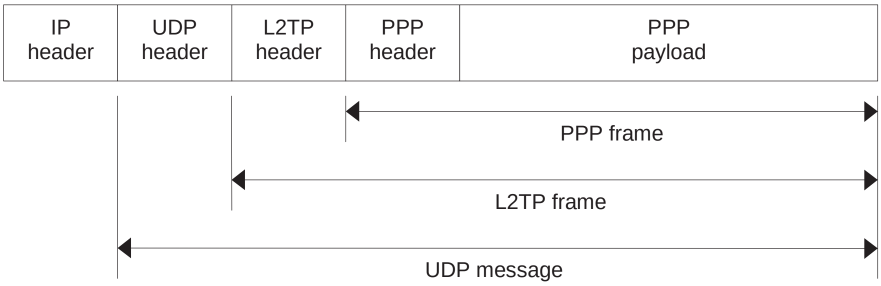


Figure 4.3: L2TP packet structure.

L2TP operates in one of two modes, voluntary tunnel mode or compulsory tunnel mode. For remote access VPNs the voluntary tunnel mode is the most interesting since in contrast to compulsory tunnel mode it does not require support from the ISP.

L2TP/IPSec

In Microsoft's implementation of L2TP the optional encryption of the PPP payload is not included. Instead the whole UDP datagram is encrypted using IPSec ESP in tunnel mode, see Figure 4.4 below. This is referred to as L2TP/IPSec and is a significant improvement compared to PPTP since it relies on the security features provided by IPSec.

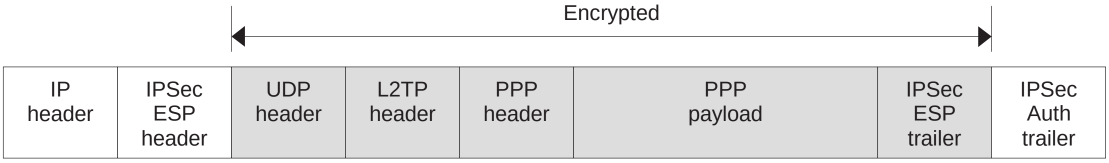


Figure 4.4: L2TP/IPSec packet structure.

4.1.4 Split Tunneling

When it comes to accessing systems outside the corporate network, e.g. browsing web pages on the Internet, the VPN connection may be configured in one of two ways.

The first way is to send all traffic from the remote computer through the VPN tunnel, even traffic which is destined for the Internet. This traffic is then sent out onto the Internet from the corporate network and returned the same way. This may cause performance implications since the traffic is sent twice between the corporate network and the Internet.

The second way is to only send traffic that is destined for the corporate network through the tunnel. Traffic destined for the Internet is sent directly onto the Internet from the remote PC. This configuration is called split tunneling.

Not using split tunneling will enable intrusion detection systems and firewalls on the corporate network to detect and prevent malicious and inappropriate traffic. Because of this, not using split tunneling is considered more secure. This depends of course on the VPN configuration. In this case with remote access VPN the remote computer will send all traffic directly onto the Internet whenever the VPN tunnel is not established and then the security precautions implemented on the corporate network will not help the remote user anyway.

4.1.5 Conclusion

VPN based solutions are often use either PPTP or IPSec. IPSec is the recommended solution and it is superior to PPTP when considering security aspects such as authentication, confidentiality and integrity. PPTP remain popular because aspects other than security are considered important for many companies, such as widespread client support and simple configuration. Another problem with IPSec is that implementations from different vendors are not always compatible, which is a problem if products from different vendors are used. This is not a problem for PPTP.

4.2 Application server

An application server based solution is very different from the VPN based solution previously described. Instead of providing users with access to corporate resources on the network layer, this solution operates at the application layer.

Remote users connect to a server on the corporate network and are given access to the resources which this server is configured to provide. This includes both applications and data. The applications are executed on the application server instead of on the remote PC. The remote PC only executes a small client application that allows the remote user to receive the screen image from the server and to send keystrokes and mouse clicks to the server. This kind of solution has many advantages over the VPN solution. Some of these are:

- No applications are installed on the remote PC, which makes the configuration of the remote PC very simple.
- No data is stored on the remote PC, which eliminates the need for backup and encryption for locally stored data.

- Only the screen image, keystrokes and mouse clicks need to be sent over the Internet, which increases performance.
- Remote users are only given access to the resources that they actually need, this increases security since they do not have unnecessary access to the complete network.

4.2.1 Citrix MetaFrame Access Suite

One of the most well know application server solutions is the MetaFrame Access Suite from Citrix. For the current case the MetaFrame XP Presentation Server together with the MetaFrame Secure Access Manager is a good solution for users with always-on connections. The XP Presentation Server is configured by the network administrator to publish applications, files and other resources that should be available for remote users. The client application is available as a Java-applet that allows remote users access using any PC with a web-browser. The browser will automatically download and execute this applet as the user connects to the server. The communication between the client and the server is secured using the Secure Sockets Layer which is described in Section 4.3.1. From a security aspect this solution is very attractive, but in the current case there are a few situations in which this solution is not appropriate. These are:

- Users with private dial-up connections do not want to be connected to the server during long periods.
- Some users need to be able to connect resources locally on the remote PC.
- Some users need to work from locations were Internet access is not available, e.g. during business trips.

This solution can be made even more secure by using a thin client at the remote location instead of a regular PC [Mai03].

4.3 Microsoft Outlook Web Access

The dominant e-mail server for companies working with the Windows platform is Microsoft Exchange Server. This handles in addition to e-mail also contact lists, calendars and shared folders. The most common client software used with Exchange is Microsoft Outlook which is included in Microsoft's Office suite.

The latest version of the server software, Exchange 2003, was hopefully developed while considering the "Trustworthy Computing" initiative that was introduced by Microsoft in early 2002 [Mic03f]. This is an initiative that many people hope will lead to increased security in Microsoft's products, which are very widespread and therefore popular targets for attackers.

For many companies, upgrading to Exchange 2000 or Exchange 2003 is not as simple as just upgrading the software on a single server. This is because it requires older NT domains to be migrated to the newer Active Directory (AD) structure. This has led to many companies continuing to use the older Exchange 5.x versions.

To allow remote users to take advantage of the same functionality as local users running Outlook, Microsoft have developed Outlook Web Access (OWA). This is a web application running on Microsoft's Internet Information Server (IIS). IIS and OWA are usually installed on a server separate from the Exchange Server. This server gives remote users access to a web-based interface similar to that available in Outlook, this front-end server then communicates with the back-end Exchange server. Security for the connection between the remote user and OWA is achieved by using the Secure Sockets Layer which is described in the following section.

4.3.1 Secure Sockets Layer

Secure Sockets Layer (SSL) [Net96] is a security protocol that was developed by Netscape Communication Corporation. SSL is also the basis for another security protocol, Transport Layer Security (TLS), that is currently being developed by the Internet Engineering Task Force (IETF).

The most common use of SSL is to provide security for the Hypertext Transfer Protocol (HTTP) and allow secure communications over the web. This is called HTTP over SSL or Secure HTTP (HTTPS) and is supported by most web-browsers. Figure 4.5 shows the padlock icon that is displayed in the Microsoft Internet Explorer status-bar when HTTPS is used to secure the current web session.

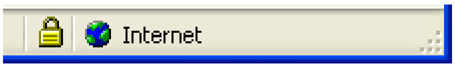


Figure 4.5: Microsoft Internet Explorer uses a padlock icon to indicate that the current web session is secured using HTTPS.

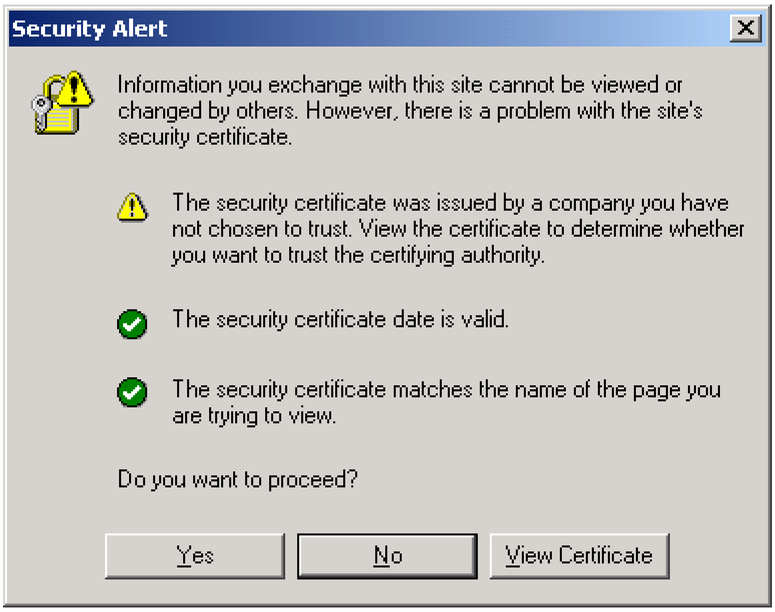
To establish a secure session with a web-server the browser connects to a server denoted by the URL scheme "https://". The browser will connect to the server on TCP port 443 instead of port 80 which is used for regular HTTP traffic. To make it easy for the user, the server may of course also be set up to automatically redirect from HTTP to HTTPS. This will relieve the user from having to worry about entering "http" or "https".

The first step in setting up an SSL session between the browser and the server is the handshake phase. During this phase the browser and the server will agree on which security capabilities that will be used during the rest of the session, e.g. encryption algorithms, compression etc. SSL is based on the RSA public-key cryptosystem and common encryption algorithms are RC2 or RC4 with 40-bit or 128-bit key lengths. During this phase the server will send its certificate to the browser, which contains the server's public key. The browser then uses this key to encrypt a master key that is sent to the server. Since the browser generated the master key and sent it encrypted to the server, this is a secret known by no one except the browser and the server. From this master key it is possible to derive keys that are used to encrypt the actual data sent between the client and server during the session.

Usually the browser is preconfigured to accept certificates that are signed by well known and trusted Certificate Authorities (CA), e.g. Thwate or VeriSign. Sometimes the browser will not be able to determine by itself if the server should be trusted. This might be due to one of the following things:

- The certificate is signed by a company that the browser is not configured to trust.
- The certificate is used before or after the period for which it is valid.
- The certificate is used by a server other than the one specified in the certificate.

The alert dialog, shown in Figure 4.6, is asking the user to decide if the current server should be trusted even though the company that signed the certificate is not trusted. Many users just clicks "Yes", continues and then think that everything is fine just because the padlock icon is displayed. This is not true. The padlock icon indicates that the communication with the server is secured using SSL. It does not ensure that the server should be trusted with sensitive information. The certificate contains information that the user should use to decide if the server should be trusted or not. The certificate itself does not ensure anything. A rogue server may present a certificate that is signed by itself and hope that the user will accept it. For more information about certificates see Appendix C.



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

✓ The security certificate date is valid.

✓ The security certificate matches the name of the page you are trying to view.

Do you want to proceed?

Figure 4.6: Microsoft Internet Explorer security alert dialog asking the user to decide if the current server should be trusted or not.

Previously USA had export restrictions that prevented US products that included strong encryption technology to be exported. Today these restrictions only apply to US embargoed destinations. So for most countries, including Sweden, 128-bit support is available in Microsoft's Internet Explorer.

SSL is a solution that is considered secure, provided that it is handled correctly by the users and implemented correctly in the browser and the server. It is commonly used by e-commerce companies as well as banks.

4.4 Summary

The solutions described in this chapter fulfill very different needs for remote users. In an organization where different users perform different tasks it might be necessary to use more than one of these.

A VPN based solution is the most powerful and flexible choice. This technology can be configured to allow remote users access to resources on the corporate network in the exact same way as they would if they had physically connected the PC at the office. In the current case surveys have shown that this is the solution that users feel they have a need for, with exception for users that only want access to their mail.

An application server based solution has many advantages over a VPN based solution, both for practical and for security reasons. The practical reason is that employees do not have to install any special software on the remote PC, a web-browser is enough. This allows them to access both applications as well as data that is stored on corporate network resources. There are several security reasons, no data is stored locally on the remote PC, effectively eliminating the need for backup and the risk of losing data in case of a crashed or stolen PC. The resources that remote users are allowed to access, both in form of applications and data, are centrally controlled by the network administrator. Users in the current case are not too enthusiastic about this solution. The main reason is skepticism about performance. For modem users the requirement to be connected during the whole session is not very attractive.

Solutions like OWA offer the most limited access of these solutions, basically only mail access. At the same time surveys with users have showed that this is one of the most common tasks that they want to be able to perform from remote locations. For many users this solution alone will fulfill their needs.

Chapter 5

User authentication

User authentication is an important process used to make sure that only authorized users have access systems. In remote access systems this is even more important than in regular systems since these do not require the the user to have physical access to it. In this chapter the traditional and most common way of performing user authentication is discussed, i.e. using static passwords. The Windows authentication mechanisms are described in some detail. Finally two modern ways of performing user authentication based on one-time passwords and biometrics are presented.

5.1 Ways to authenticate users

User authentication is the process of verifying that a user really is the person she claims to be. There are three things a user may present to a system to authenticate herself:

- Something the user knows. - This is usually a password or some other information which is likely that only this person will know.
- Something the user has. - This can be a magnetic strip card, a key, smart-card or another similar token.
- Something the user is. - This can be something like fingerprint, hand-print, retina pattern or DNA.

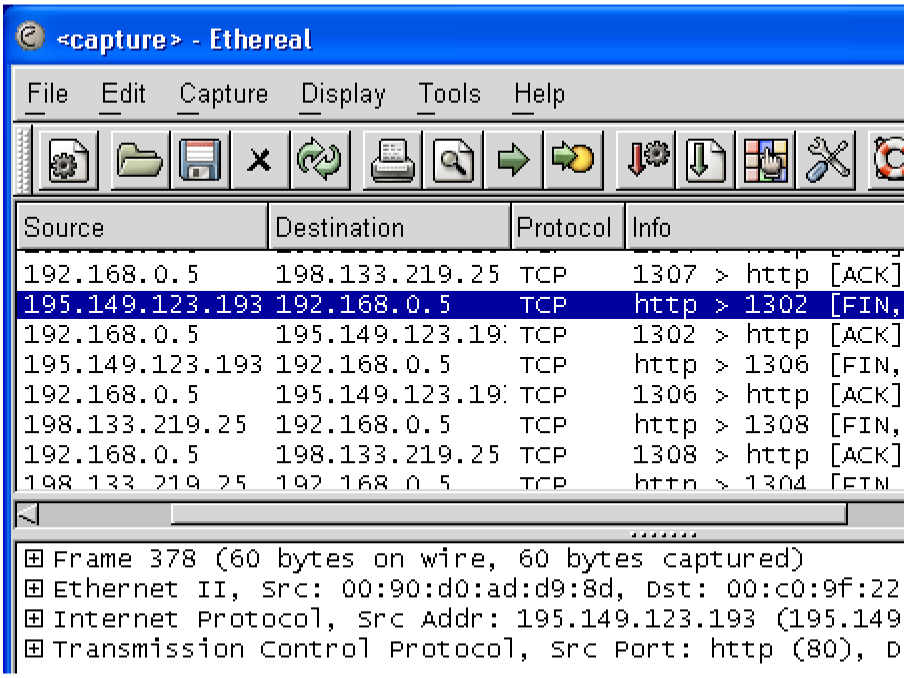
If two, or all three, of these things are used in combination, it will be more difficult for an attacker to gain access the system. For the authentication method to be considered strong, it is required that at least two of these three things are used in combination.

5.2 Static passwords

The most common way of performing authentication is still through the traditional static username/password pair. There are several ways to crack these passwords either by pure technical means or in other ways.

5.2.1 Password cracking

The static password authentication method has been around for a long time and is susceptible to many types of attacks. Someone may pick up the username and password while the user is typing it in by looking over the shoulder. If the computer has already been compromised, or if a public computer is used, then it it possible that a keylogger application is capturing keystrokes and sending them secretly to a hacker somewhere. A sniffer application may be used to pick it up while it is being transmitted over a network. There are both freeware and commercial sniffer and keylogger applications which may be used by anyone to do this. Two examples are the open source network analyzer application, Ethereal [eth03], see Figure 5.1, and the Ghost Keylogger application from Sureshot Software [key03]. Using applications like these is not something which requires the competence of a highly skilled hacker. An application that is specialized in sniffing passwords is Dsniff [mon01]. This application will simply display the username and password on the screen whenever the traffic from a user who is logging in to a service over the network is picked up. Dsniff will recognize login information for services like FTP, Telnet, POP, IMAP, SNMP, LDAP, Rlogin, NFS, SOCKS, CVS, ICQ, Citrix ICA, Symantec pcAnywhere, Microsoft SMB and more. Several of these protocols are almost 20 years old and do not even encrypt the passwords.



```
Source            Destination      Protocol  Info
192.168.0.5       198.133.219.25   TCP       1307 > http [ACK]
195.149.123.193   192.168.0.5      TCP       http > 1302 [FIN,
192.168.0.5       195.149.123.19:  TCP       1302 > http [ACK]
195.149.123.193   192.168.0.5      TCP       http > 1306 [FIN,
192.168.0.5       195.149.123.19:  TCP       1306 > http [ACK]
198.133.219.25    192.168.0.5      TCP       http > 1308 [FIN,
192.168.0.5       198.133.219.25   TCP       1308 > http [ACK]
198.133.219.25    192.168.0.5      TCP       http > 1304 [FIN
```

```
⊞ Frame 378 (60 bytes on wire, 60 bytes captured)
⊞ Ethernet II, Src: 00:90:d0:ad:d9:8d, Dst: 00:c0:9f:22
⊞ Internet Protocol, Src Addr: 195.149.123.193 (195.149
⊞ Transmission Control Protocol, Src Port: http (80), D
```

Figure 5.1: The Ethereal network analyzer can be used to sniff traffic, including passwords, on a network.

Another attack approach may be to target the server instead. Many users still choose easy-to-guess passwords and on many systems the default passwords are not changed. There are several sites on the Internet that lists default passwords for various systems [phe03, cir03]. So it is not impossible to gain access to a system by simply connecting to the server and trying common username and password combinations. In fact some viruses and worms use this technique when trying to spread to other systems. One example of this was the Deloder worm [F-S03b] that appeared in March 2003. It spread by guessing passwords for resources on other systems which had been made available for remote users through Windows file sharing. An audit at the company in this case, a few years ago, showed that 80 percent of the user passwords could be cracked within 1 minute. After this a new password policy was implemented.

Another way to prevent this kind of attack is to disable an account if the correct password is not entered within a few login attempts. This will make it hard for an attacker to gain access but could be used to cause DoS instead. By guess the wrong passwords for several accounts the accounts would be disabled and thereby the legitimate users would be denied access to the system. Usually the administrator account can not be disabled in this way to prevent the administrator from being locked-out from the system.

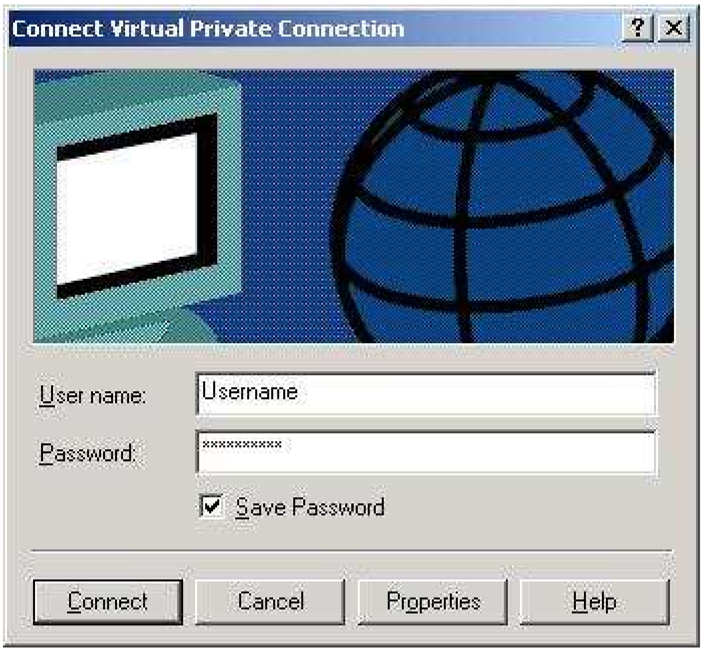
A more advanced attack method is to get access to the password file for a system. Attempts to crack passwords in it may then be performed offline. Password files are usually encrypted using hash functions but may be cracked by guessing a password and encrypting it with the same hash function as the target system uses. The resulting hash value is then compared to the entries in the password file, a match means that the password has been found. There are different attack methods available to do this. The dictionary attack makes use of all words from a dictionary to guess the password. Many people tend to choose passwords which are easy to remember and often this is a word that exists in a dictionary. The ultimate method though is to use the brute force attack. Here every possible combination of characters is used to guess the password. This attack will always work but it requires a lot of time or computing resources.

To avoid passwords being cracked with the dictionary attack some users are trying to disguise a word from a dictionary by for example appending special characters at the end of the word or replacing parts of the word, e.g. occurrences of the alphabetic character o with the numeric character 0. Common tools for password cracking uses hybrid attacks to crack the passwords in spite of this. This attack is a mixture of the dictionary attack and the brute force attack since it will guess passwords by using variations of the words from a dictionary. This will require more time and computing resources than a dictionary attack but will still be much faster than the brute force attack. Just like with sniffer and keylogger applications there are a lot of password cracking applications which are simple to use. One famous application is LC 4 from @stake [ats03], previously known as L0phtCrack. Just like the sniffer and keylogger applications mentioned above, this tool is not made available as a tool for crackers but rather as a tool for network administrators. Intended for securing networks and to recover lost passwords etc. but it may of course also be used with malicious intent. The hard part is to get hold of the password file, but there are of course tools available for this as well.

Guessing passwords and performing dictionary attacks is nothing new, this has been going on for a long time. It was used successfully during the mid 1980-ies by a hacker in Europe to access military systems in the USA [Sto88, Sto00].

5.2.2 Managing passwords

There are several inappropriate ways to handle a password which may give unauthorized persons access to the system. Obvious ones are to just give out the password to another person or to write it down on a note next to the keyboard. Other ways are to use the same password on several systems, this will allow administrators on all systems to have access to it. From an attacker's point of view it may be easier to retrieve a password by attacking a system that is less secure and then use this password to login to the user's account on a more secure system, e.g. using the password found on an employee's home computer to access resources on the corporate network. In Windows it is very common for users to check the save password box in the login dialog, see Figure 5.2. This is convenient since the user does not have to enter the password in the future. But this will also allow other users or applications on the computer to login to this account. Someone could steal the PC and get instant remote access to the corporate network. Malicious code, like trojan horses, can use this to access the corporate network without the user noticing it.



User name: Username

Password: ***********

☑ Save Password

Figure 5.2: Save password check-box available when connecting to the corporate network through VPN in Windows.

To make sure that weak passwords are not used in an organization a good password policy can be implemented. This is usually implemented as a technical mechanism that will force users to follow it. Some common things controlled by the password policy are:

- Minimum password length. - A minimum number of characters that the password must contain.
- Password complexity. - The password must contain a certain mixture of characters from different groups, i.e. lower case, upper case, numeric etc.

- Maximum password age. - A maximum time a password may be used before it must be changed.
- Password history. - A number of previously used password must not be reused.

This is an effective way to make sure that users follow the policy, but it is not foolproof. There are people that will change the password 15 times in a row to exhaust the password history, just to be able to reuse their favorite password. If the rules are too hard, users might no be able to remember their passwords and write them down or use the save password check-box previously mentioned. Making sure that users choose good passwords and handle them with care is not an easy task.

5.2.3 Windows authentication

One of the reasons behind Windows success is its backward compatibility. It is still possible to run old applications and share resources with Windows systems that are over 10 years old. This is usually considered to be a good thing but in the area of security it is not, as we will see.

Password hash functions

Passwords on Windows systems are stored in the local Security Accounts Manager (SAM) database. For security reasons a hash value of the password is stored instead of the cleartext password. See Appendix C for more information about hash functions. There are two hash functions in use today to create the password hash:

- LanManager hash (LM hash)
- Windows NT hash (NT hash)

The original LM hash was replaced by the NT hash because of two main weaknesses. The first weakness is that it divides passwords into two 7 character blocks which are hashed independently. Passwords shorter than 14 characters are padded with blanks, while passwords longer than 14 characters are truncated. The second weakness is that lower case characters in the password are converted to upper case before the hash is generated. An attacker will benefit from this by attacking the two hashes independently as if they were two separate 7 character passwords without lower case characters.

The NT hash is a significant improvement since it removes these two weaknesses. It will not convert lower case characters and uses all 14 characters when generating the hash value. The attack methods described earlier will of course still be possible but a password with mixed characters, or a password longer than 7 characters will be much harder to crack if the NT hash is used instead of the LM hash. It is important to note that even with these improvements the main security factor is still the user's choice of password. A password, e.g. based on a word from a dictionary, will still be cracked within seconds on a regular PC using the dictionary or hybrid attack method, no matter which one of these hash algorithms that is used.

Challenge/response authentication

The LM and NT password hashes are also used in challenge/response schemes for authentication over a network. There are several different schemes in use:

- LanManager (LM) challenge/response
- Windows NT version 1 (NTLM) challenge/response
- Windows NT version 2 (NTLMv2) challenge/response
- Kerberos

The LanManager challenge/response authentication scheme uses the LM hash, while the other schemes uses the NT hash. For backward compatibility reasons systems that use the NT hash also store and send the corresponding LM hash over the network. So even if a system is configured to use NTLM it is still possible to pick up the LM hash on the network or locally on the system. This allows an attacker to crack the LM hash as the first step and with this password in cleartext it is much easier to crack the NT hash.

Microsoft have release knowledge base articles to help users disable the storing of the LM hash [Mic03b] and enabling the use of NTLMv2 [Mic03a]. Doing this will of course limit the ability to communicate with older systems that rely on the LM hash[1].

A drawback with both the LM hash and the NT hash functions are that the password is the only input to the hash function. This will result in the same hash value for two users who choose the same password. On Linux systems this is solved by using a salt value in addition to the password as input to the hash function. The salt value is generated in a way that will make it unique for every user. This is stored in clear text next to the username and password hash in the password file and ensure that the same password will result in different password hashes for different users. For an attacker this makes it harder since hash values for words from a dictionary can not be generated in advance and then compared to all password hashes in the password file. Instead individual password hashes for each user must be created after the salt value has been obtained.

SysKey

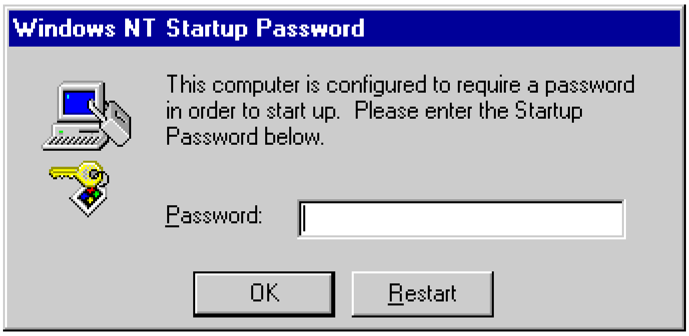
Microsoft have developed a tool called SysKey, to provide another level of protection for the password hashes. This will encrypt the entire SAM database using the RC4 encryption algorithm. This makes it harder for an attacker to access the information stored in the SAM database, since a 128-bit encryption key is required to decrypt it. This encryption key is also needed by the system at boot time to be able to decrypt the SAM database. There are three configurations for how to store the key:

1. Stored in the registry and made available automatically at boot time.

[1] The Active Directory Client Extension (DSClient) can be installed on these older systems to allow them to perform NTLM and NTLMv2 authentication.

2. Stored in the registry but protected with a password that must be supplied at boot time.

3. Stored on a floppy disk that must be supplied at boot time.



Windows NT Startup Password

This computer is configured to require a password in order to start up. Please enter the Startup Password below.

Password:

Figure 5.3: Windows NT dialog asking the user to enter the startup password that is required to decrypt the SysKey encrypted SAM database.

In Windows 2000 and Windows XP the default is configuration is number 1. This is the least secure, but the most convenient since no user intervention is required. A more secure configuration is number 2, Figure 5.3 shows the dialog that is presented to the user if this is used. The most secure configuration is number 3, provided of course that the floppy disk is kept in a safe place when it is not used.

Conclusion

User authentication is a very important mechanism in Windows. It is involved when granting access to resources both locally and remotely. The need for backward compatibility and the use of weak passwords are common in systems today, this leads to a security level that is not as high as the technique allows. As shown in the previous chapter one of the main issues with the PPTP protocol was that it depends on the user password, the same applies for most configurations of the encrypting file systems that is described in Chapter 6. So it is not strange that Windows authentication is rated as the third item on SANS Institute's list of the most critical Internet security vulnerabilities [SAN03].

5.3 One-time passwords

A technique that recently have become very popular is the use of one-time passwords. The most common implementation of this, is to equip every user with a device that generates a password that is valid only for a limited time, e.g. 3 minutes. This require that the server is synchronized with this device.

As opposed to the static passwords described so far, this is considered as a strong authentication method. It combines a PIN-code or a password, i.e. something the user knows, with the fact that the device must be in the user's possession, i.e. something the user has, hence it is a two factor authentication method.

Figure 5.4: Digipass PRO 300 authentication device from Vasco.

Some Swedish banks which offer services over the Internet or over the phone use a solution with a device like the one shown in Figure 5.4. This requires the user to enter a PIN-code to activate the device. A challenge value is then given by the bank, the user enters this value into the device and is presented with a response value which is given back to the bank.

This challenge/response scheme is not so interesting in the current case since it requires modifications of the current system both on the server-side and the client-side. Instead a more popular solution is to give users a device that generates a password without the user having to enter a challenge value. This password is then entered together with a static password in the login dialog. If someone picks up this password when it is sent over the network it will not be of any use to the attacker since it is only valid for a limited time. An attacker that steals the device will not be able to login since the static password is not known.

This scheme is supported on the server-side by all three remote access technologies that was presented in Chapter 4. In practice this is achieved by introducing an extra server that will contain the user accounts and handle the verification of the passwords sent from the users. Figure 5.5 shows how a solution from Vasco works for a VPN based solution. The Digipass GO1 authentication device is shown in Figure 5.6.

The most well known system that uses this scheme is called SecurID and comes from RSA Security. In this system the authentication device could be the 600 Fob shown in Figure 5.7 and the server application is called ACE/Server.

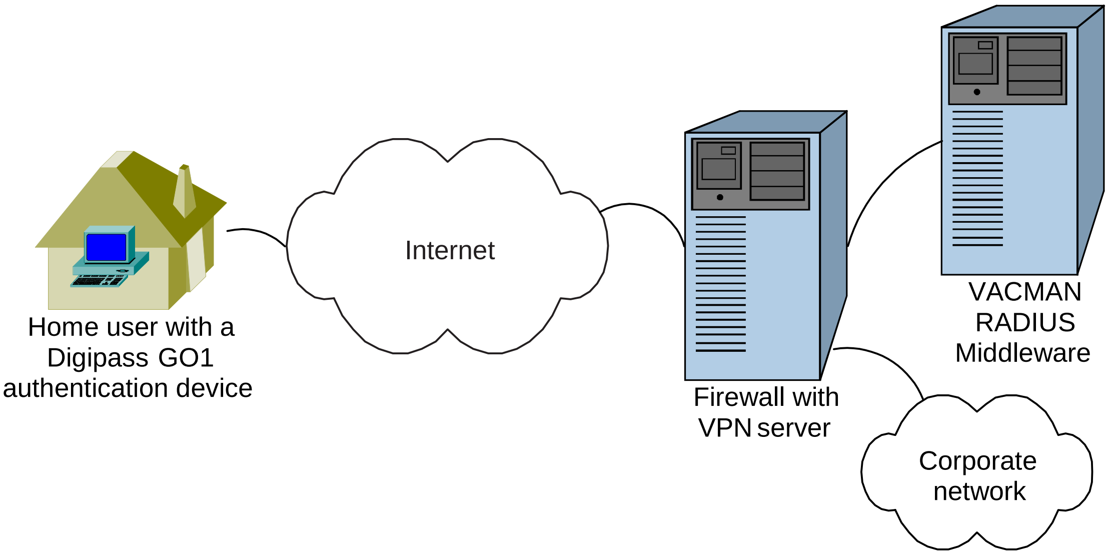


Figure 5.5: User authentication when connecting to the corporate network is achieved through a solution from Vasco. The user is equipped with a Digipass authentication token and the VPN server relies on the VACMAN RADIUS Middleware to verify the password received from the user.

Figure 5.6: Digipass GO1 authentication device from Vasco.

Figure 5.7: SecurID 600 Fob from RSA Security.

5.4 Biometrics

Biometric authentication solutions are based on something the user is. The most common among biometric products today is to use fingerprint scanning, but other biometrics are also used, e.g hand, face, iris and speech. This is a popular research area and new products are continuously appearing on the market.

Figure 5.8: Precise 100 MC combined fingerprint and smart card reader. Image courtesy of Precise Biometrics.

Compared to the one-time password generators previously described there are a few disadvantages of using biometric authentication, reasons for this are:

- Hardware devices must be installed on the remote PCs.
- It is more expensive than using one-time password generators.
- It is likely that some users do not feel comfortable with using a part of themselves to access a system.

5.5 Summary

Static passwords is the most common way of authentication, this is a very old technique and it still suffers from the same vulnerabilities as it did 20 years ago. The main weakness being the way users choose and handle their passwords. This is dangerous since a compromised user account is a common first step for attackers aiming for administrator privileges.

A one-time password scheme is a good way of solving many of these problems and there are solutions which do not require any modifications on the client-side. This makes this solution an attractive improvement for existing systems.

Biometric authentication methods are still a popular research area and they are continuously being improved. They are still a bit expensive and require hardware devices connected to the client systems.

Chapter 6

Data protection

Working from a remote location often involves storing data locally on the PC. There are two main security issues related to this behavior, either that the data is revealed to unauthorized parties or that the data is lost. In this chapter two possible solutions for data protection, namely encryption and backup, are discussed. For an introduction to the basic concepts of cryptography, see Appendix C.

6.1 Encryption

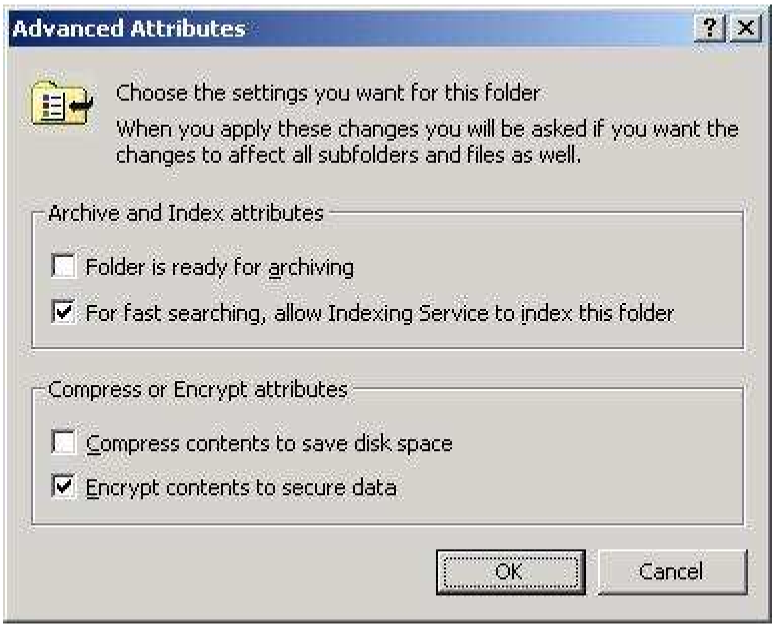
Since remote PCs are used at locations that are not as protected as the corporate office the risk for theft of the PC is higher. During business trips laptops are brought to places like airports and hotels where they may be left unattended. Other remote PCs are kept at employees homes or in vacation houses where they may be stolen during a break-in.

An attacker who gains physical access to the PC will have different possibilities to access data stored on it than an attacker who gains remote access to it. One way to prevent data like business strategies, e-mail or other sensitive information from getting into the wrong hands, is to use some kind of encryption mechanism. There are many different products available for this purpose. Since many companies, including the one that is considered in this case, use the Windows operating system the feature included in this system is discussed.

6.1.1 Encrypting File System

The Encrypting File System (EFS) is built-into the Windows 2000 and Windows XP Professional operating systems. This is a feature that allows for encryption of files in a way which is transparent to the user.

EFS is based on the NTFS filesystem and can be used on drives that are created with this filesystem. It is activated by simply checking a box in the folder attributes dialog, see Figure 6.1. Checking this box will encrypt files that are created in this folder.



Choose the settings you want for this folder

When you apply these changes you will be asked if you want the changes to affect all subfolders and files as well.

Archive and Index attributes

□ Folder is ready for archiving

☑ For fast searching, allow Indexing Service to index this folder

Compress or Encrypt attributes

□ Compress contents to save disk space

☑ Encrypt contents to secure data

Figure 6.1: The dialog for advanced folder attributes in Windows 2000 includes an encryption check-box.

EFS uses a combination of symmetric and asymmetric encryption algorithms. The actual data stored in the files are encrypted using a symmetric encryption algorithm. This is either the Expanded Data Encryption Standard (DESX) or Triple Data Encryption Standard (3DES). The choice of a symmetric encryption algorithm is natural because of the speed advantage compared to an asymmetric encryption algorithm. The secret key that is used to encrypt the data is called the File Encryption Key (FEK) and is unique for each file.

The FEK must be available for everybody that should be able to decrypt the data. Apart from the user who creates the file, a recovery agent should also be able to decrypt it. This is useful in case something happens the user account, e.g. the employee quits. By default the recovery agent is the local administrator account.

Each user is assigned a key-pair consisting of one private and one public key. For each file, the FEK is encrypted with an asymmetric encryption algorithm twice. Once with the user's public key and once with the recovery agent's public key. These encrypted versions of the FEK are then stored in the header of the file and makes it possible for both the user and the recovery agent to decrypt the file even though they have different private keys, see Figure 6.2.

The main advantage of using EFS instead of another product is that it is built-into the operating system. This eliminates the need to buy and install additional software or hardware. It is also very userfriendly since it is transparent once it has been activated.

As described in Chapter 5 the password hashes for the user accounts are stored in the SAM. With physical access to the PC it is possible to boot the PC from a floppy disk and bypass the operating system's access controls. This method makes it possible to access

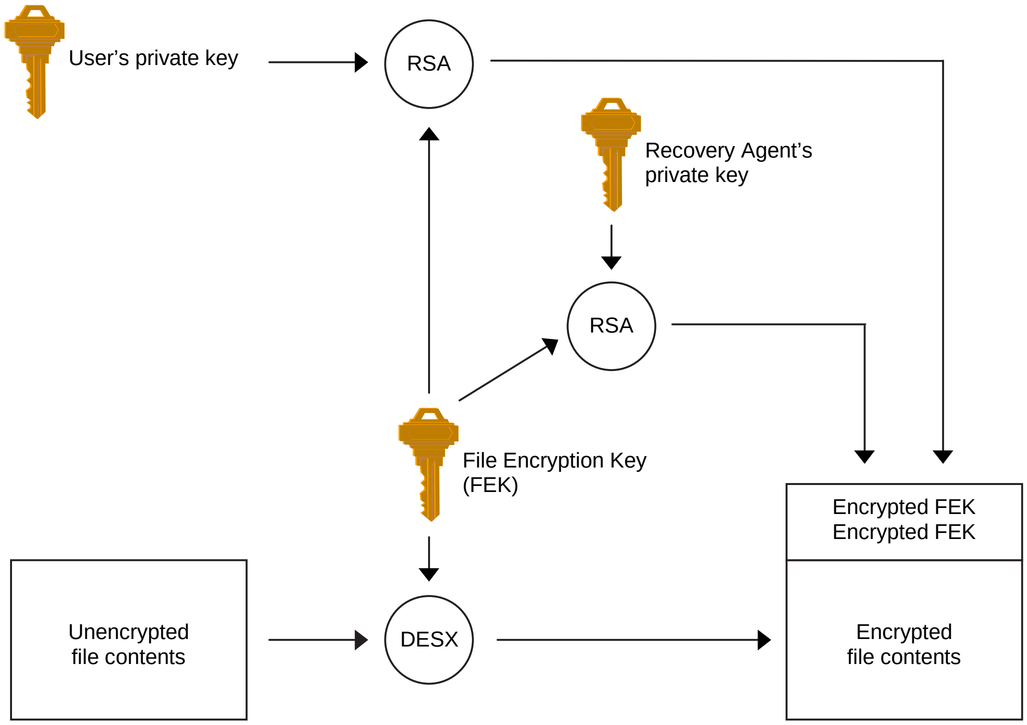

User's private key
RSA
Recovery Agent's private key
RSA
File Encryption Key (FEK)
Encrypted FEK
Encrypted FEK
Unencrypted file contents
DESX
Encrypted file contents

Figure 6.2: The EFS encryption process takes advantage of both the symmetric encryption algorithm DESX as well as the RSA public-key cryptosystem.

the SAM and use this information to crack the passwords. It is also possible to modify the SAM in ways that will change passwords for users or simply delete the SAM and login with the blank administrator password which Windows will create when it discovers that the SAM is corrupt or missing.

The only way to configure the PC so that the encrypted files will not be accessible through these kinds of attacks is to use SysKey and protect the SysKey encryption key either by placing it on a floppy disk or by using a password, according to [SM01]. Although this will allow attackers access to the rest of the system the encrypted files are still protected. This is because the private user key that is used to decrypt the FEK is encrypted by SysKey. This configuration also requires that the recovery agent's private key is exported from the system so that an attacker than gains administrator privileges will no be able to use that to access the encrypted files.

For Active Directory domains the configuration is a bit simpler since the domain administrator account can be configured as the default recovery agent instead of the local administrator account. This eliminates the need to export the recovery agent's key manually from every system. Copies of the SysKey passwords or the floppy disks which are used to store the SysKey encryption key must still be kept by the IT department in case a user forgets their password or the floppy disk breaks.

Some new features have been introduced in Windows XP Professional that allows for encryption of the FEK for additional users. This is dangerous to rely on if older applications that are not aware of this are used. Files saved with these applications will still use the older encryption functions and only encrypt the FEK with the user's and the the recovery agent's public keys other uses will be ignored and are not able to decrypt the file in the future. For the current case this is not an useful function anyway.

6.2 Backup

Data that is stored on a computer system may be lost for several reasons. It may be because of a malicious attack that information is destroyed or modified, but it is more likely that the reason is a system hardware crash, software crash or a user mistake. The best way to protect against losing data has been the same for a long time, save your work often and backup data regularly.

At an office the usual backup routine is to have all users store their data on a server on the network. Backup is then taken of this data at least a few times a week. This will relieve the users from having to worry about backup and just contact the IT department in case data is lost and needs to be recovered.

When working from a location other than the office the same backup approach may be appropriate, but this depends on which remote access technology is used. Since a VPN solution can be setup to provide the remote user with access to network resources just like when working at the office there is no reason to change anything in this backup routine. If an application server technology is used, then applications as well as the data which they operate on, are stored on servers in the office. This does not require any new backup routines either.

This scheme seems simple enough but there are some cases in which this is not an appropriate solution. Some people still use modems to connect to the Internet over the PSTN. The connection to the company will then have a limited bandwidth. The remote user will use this for downloading data that is necessary to be able to work and to upload data that other people depend on. But it is not likely that this limited bandwidth will be used to backup data, at least not if the size is more than a few megabytes. This is especially true if it is a private line and there are other family members who want to use the phone or are expecting a call. For other people who primarily use broadband connections this is also a problem when they go away on business trips and needs to rely on modem connections.

These people look for other backup solutions or ignore it altogether. The simplest backup method is to just copy the data to another part of the local hard drive or to copy it to another local hard drive. This is sufficient protection against most user mistakes and probably even software crashes. Against hardware crashes, theft or compromise of the computer, it is not enough. If the data is burnt on a CD-R or stored on some other media then it will still be available even if something happens to the computer. Then the risk of loosing data comes down to how the backup media is handled. If it is stored in a bag with the laptop computer then it is not much use if the bag is stolen. The thief will even have easier access to the data on the backup media than on the computer hard drive, at least if the data is not encrypted on the backup media. The backup media must be protected just as well as the original data on the PC since it contains the same data. Backup media that is reused is more likely to be handled with care than write-once media like CD-Rs.

An interesting reusable media that is available in may different varieties is the USB Flash Memory. This is a small device that is plugged into the USB port on the computer and then accessed by the user like a regular hard drive. Today devices with capacities up to a few gigabytes are available. Some offer protection in the form of encryption. There are even more advanced ones like the ClipDrive Bio, shown in Figure 6.3, which have built-in biometric access control through fingerprint scanning.

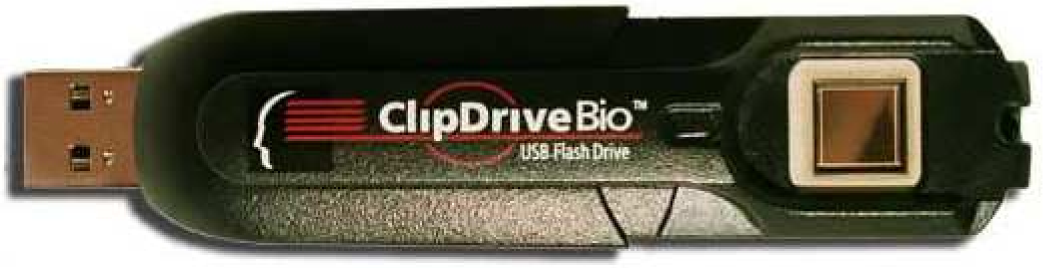


Figure 6.3: ClipDrive Bio USB Flash Drive includes biometric access control to encrypted data through fingerprint scanning. Image courtesy of Memory Experts International.

6.3 Summary

Backup is important. It makes it possible to restore data that is lost regardless of the reason for losing it. Because of confidentiality and integrity concerns the backup media should not be available to unauthorized users. It needs to have the same protection level as the original data on the PC. This may be achieved by some technical solution like encryption or by storing the backup media were it is physically protected from unauthorized persons, or by a combination of the two.

Protecting data from attackers which have physical access to the PC is very hard. The built-in EFS feature in Windows 2000 and Windows XP Professional provides a good and cheap encryption solution. To achieve a secure EFS configuration it is paramount to follow the implementation guidelines including the use of SysKey. The sensitive part concerning encryption, regardless of the product, is how the encryption keys are handled.

The simplest and most effective way to solve these problems, is to simply avoid storing data locally on the remote PC if that is possible.

Chapter 7

Firewalls

This chapter describes the different types of firewalls available to protect networks and hosts. This is followed by a discussion that will focus on ways that an attacker may circumvent the firewall in relation to remote users. This includes some of the risks related to deploying wireless networks without protection at home. This chapter is primarily based on information from [WCP02, CBR03].

7.1 Basic types of firewalls

A corporate network is usually connected to the Internet through a firewall. This is often considered the main protection for the company concerning attacks from the Internet. There are different types of firewalls which may be used separately or in combination. The three basic types of firewalls are briefly described in the following sections.

7.1.1 Packet filtering firewalls

The most basic type of firewall is called a packet filter. This form of firewall operates at the network layer, i.e. layer 3 of the OSI model. It looks at the information found in the header of network packets and based on a predefined ruleset it makes decisions for each packet. The packet may either be allowed or denied to pass through the firewall. The ruleset contain information about which source and destination IP addresses and ports that should be allowed or denied.

7.1.2 Stateful inspection firewalls

A stateful inspection firewall is basically a packet filtering firewall with extended knowledge of the protocols operating at the transport layer, i.e. layer 4 of the OSI model. In practice this means the connection oriented TCP protocol. This form of firewall is able to keep track of the current state of TCP connections. The advantage of this is that it may be configured to only allow traffic from the Internet to a host on the internal network if the internal host initiated the connection. Since most common traffic like, web-browsing, sending and receiving e-mail etc. is initiated from the internal host this is a very useful feature. This was not possible with the packet filtering firewall previously described and because of this the stateful inspection firewall is considered more secure.

7.1.3 Application-proxy gateway firewalls

The application-proxy gateway firewall is the most advanced form of firewall. It operates on the application layer, i.e. layer 7 of the OSI model. This means that the firewall must have knowledge of the specific application protocol in use. This makes it possible to filter traffic based on more sophisticated parameters like traffic content and not just source and destination information in the packet headers. To be able to do this it is required that there exists proxies for each protocol that should be filtered. Proxies exist for many protocols, two of the most common are Simple Mail Transfer Protocol (SMTP) and Hypertext Transfer Protocol (HTTP). The proxy makes the protocol understandable and allows the firewall to filter traffic based on things like inappropriate contents on websites, possible virus attachments in e-mail, spam etc.

7.2 Hybrid firewalls

Modern firewalls are usually hardware devices implemented as hybrids of the three different forms of firewalls discussed so far. These give a very good protection for the company network if configured correctly.

7.3 Demilitarized Zone

One problem with firewall configuration is that different systems have different requirements concerning the level of Internet connectivity that should be available. Web-servers, mail-servers etc. require more connectivity than systems that are used only for browsing the web and reading e-mail. One common solution to this problem is to create a Demilitarized Zone (DMZ). This is a network that is placed between the corporate network and the Internet. One firewall is placed between the Internet and the DMZ and another firewall is

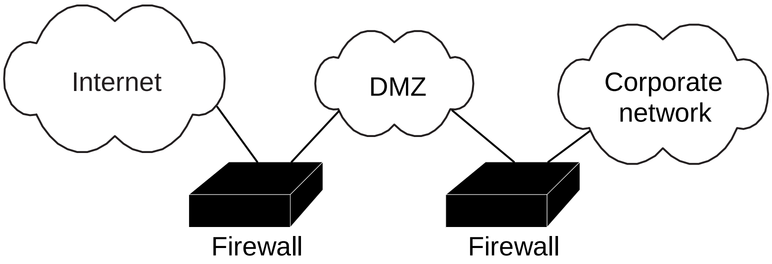


Figure 7.1: DMZ configuration using two firewalls.

placed between the DMZ and the corporate network, see Figure 7.1. Systems like servers that need a high level of connectivity are placed in the DMZ, while systems that need a high level of protection are placed in the corporate network. The two firewalls may then be configured to allow appropriate access between the networks. Several modern firewalls are designed to support the DMZ configuration. These have three network interfaces, instead of two, like the one shown in Figure 7.2. For this kind of firewall it is possible to set up rules for how the traffic between the three interfaces should be handled.

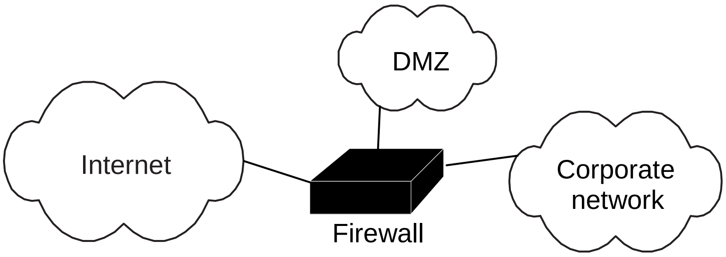
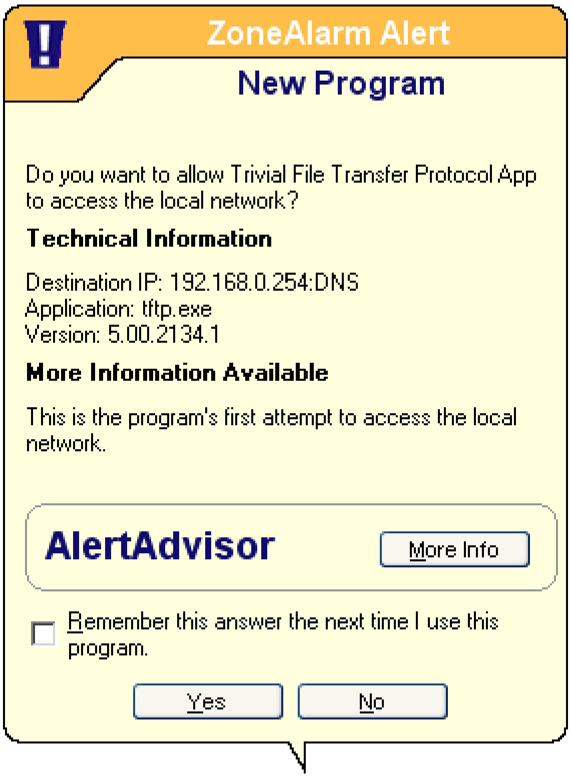


Figure 7.2: DMZ configuration using one firewall.

7.4 Personal firewalls

There is also another kind of firewall that is intended to protect not a whole network but a single host. These are software based firewalls called personal firewalls. A personal firewall will give a good protection for the host if it is configured correctly. The problem is that it requires more knowledge than an average user has to configure it correctly. One of the most common personal firewalls is ZoneAlarm from Zone Labs [zon04]. Figure 7.3 shows a ZoneAlarm Alert-dialog asking the user to decide if the current program should be allowed to access the network or not. For the firewall to work properly the user have to understand what this means and how to respond to alerts like these.

In Microsoft's Windows XP operating system there is a built-in firewall called Internet Connection Firewall (ICF). ICF will not display dialogs like ZoneAlarm does, instead all connections initiated from the host will be allowed, while all connections initiated from the Internet will be blocked. It is possible to open up specific ports if the computer needs to run a service that should be accessible from the Internet. A solution like this will prevent most attackers from connecting to the host from the Internet. But the user does not have the possibility to block programs on the host from connecting to the Internet. Many attackers use social engineering to make the user run a program on the computer. One example of this was the Swen worm that began spreading in September 2003. This worm propagated partly through an e-mail that claimed to be an Microsoft Internet Explorer update. The recipient was encouraged to run the attached update file, which actually contained malicious code. Once the user ran it the program would take several actions, turning of security products, mailing itself to other people and place itself in folders that are known to be used by peer-to-peer file sharing applications. This method is successful since many people are curious and still run unknown attachments that they receive by e-mail or that they download from the Web or through peer-to-peer file sharing applications.



ZoneAlarm Alert

New Program

Do you want to allow Trivial File Transfer Protocol App to access the local network?

Technical Information

Destination IP: 192.168.0.254:DNS
Application: tftp.exe
Version: 5.00.2134.1

More Information Available

This is the program's first attempt to access the local network.

AlertAdvisor

□ Remember this answer the next time I use this program.

Figure 7.3: ZoneAlarm personal firewall alert-dialog asking for user response.

There is nothing that says that these programs are not malicious. By default the ICF is disabled on a Windows XP system.

Another protection mechanism available in Microsoft Windows 2000 and Windows XP Professional is IPSec filters. IPSec was described in Section 4.1.2 as a protocol for providing security for IP. Microsoft's implementation of IPSec offers a filtering feature that allows IP traffic to be filtered even if IPSec is not used. The IPSec filters may be set up either as a local policy on a single host or as a group policy which can be distributed to several hosts on a network.

Another feature available in Windows 2000 and Windows XP is TCP/IP filtering which makes it possible to filter IP traffic arriving at a host based on destination TCP or UDP port numbers or IP protocol. This is much simpler to setup but it is not as advanced as the IP filtering mechanism previously mentioned.

7.4.1 Distributed firewalls

A distributed firewall is a firewall that operate on host systems, just like a personal firewall, but is centrally controlled by the network administrator. This idea was presented in 1999 [Bel99]. Today many vendors offer products that implement this idea. In the case of remote access users this is a way for the network administrator to make sure that the company security policy is enforced even on remote PCs where the Internet traffic is not handled by the company firewall.

7.5 Network Address Translation

Network Address Translation (NAT) [SE01] is a technology that allows for hosts to have different IP addresses on different subnets. Typically a router or firewall implements NAT to allow hosts on the company network to have one IP address that is used internally while it is mapped to another IP address when the host communicates with hosts on the Internet on the outside of the NAT device.

The NAT device achieves this by changing the IP header of packets that pass through. On out-bound packets the source address is changed from the hosts internal address to the corresponding public address. On in-bound traffic the destination address is changed from the public address to the hosts corresponding internal address. This simple IP address to IP address mapping is also referred to as basic NAT.

7.5.1 Network Address Port Translation

The enormous growth of the Internet together with the limited address space of IP version 4 prevents every host from having a globally unique IP address. The Network Address Port Translation (NAPT) technology makes it possible to have several hosts on a subnet to appear on the Internet as one single IP address. A very common configuration is to connect the local network, both company networks and small home networks, to the Internet trough a device that implements NAPT. Figure 7.4 shows this configuration for a home network with two hosts.

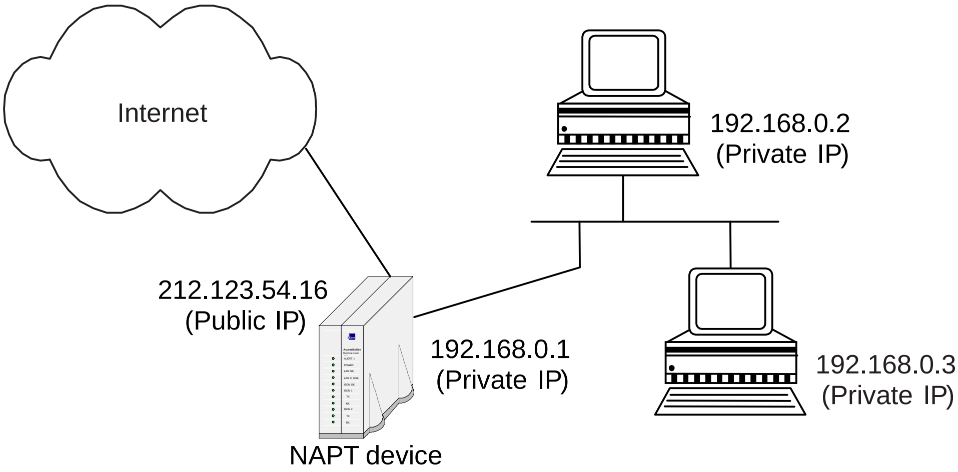


Figure 7.4: A home network with two hosts connected to the Internet trough a NAPT device.

NAPT is also referred to as traditional NAT and is a bit different from basic NAT since there is no one-to-one mapping between IP addresses. Usually the NAPT device is connected to several internal hosts but has only one public IP address that is valid on the Internet. So all traffic from the internal hosts destined for the Internet will be manipulated to appear to originate from that address. The NAPT device will keep track of which internal host the traffic originated from so that it will be able to handle reply traffic.

This technique is somewhat limited since the NAPT device will not know to which internal host traffic is intended for if it originates from the Internet. This is not a problem for most users since almost all traffic are requests originating from internal host and the traffic from hosts on the Internet are just replies to those requests. For internal hosts that do need to be accessible from the Internet there is the possibility to set up static mappings in the NAPT device. If the internal host 192.168.0.2 is running a web-server the NAPT device might be set up to forward all in-bound traffic addressed to port 80 of the public IP address to port 80 on the internal host with IP address 192.168.0.2.

It is possible to use any IP addresses on the local network, even IP addresses that exist on the Internet since the NAPT device will translate them into addresses that are unique. But the most common solution is to use ranges of IP addresses that have been reserved as private and may not be routed on the Internet [RMK+96].

7.5.2 Security issues

The reason for describing NAPT is that it is used very extensively and there are some network security issues that needs to be considered in relation to it. Often remote users do not connect directly to the Internet. Instead they connect to a small home network or to a network at another company or organization. The device that connects these networks to the Internet will often implement NAPT. This may cause implications for the remote user that connect using the VPN technology.

With PPTP there is no problem with the control channel which is a regular TCP connection initiated from the client. The NAPT device will be able to handle this connection as usual by keeping track of the client's IP address and TCP port number. But the GRE packets containing the actual data is an IP protocol and does not use ports. The NAPT device must allow some form of NAT traversal functionality to be able to handle this traffic correctly.

During the description of IPSec in Section 4.1.2 the AH protocol was mentioned. This protocol does not work with NAPT at all. This is because the checksum that is calculated from the IP header will be invalidated by the NAPT device as it replaces parts of the header information. Instead the ESP protocol must be used for IPSec to work. But even here there are problems, the Windows 2000 and Windows XP VPN clients does not work with NAPT unless a NAT Traversal (NAT-T) update is installed [Mic03c]. There are discussions about these problems but no standard yet [IET04]. Modern NAPT devices usually include some NAT-T feature to handle IPSec traffic.

One positive thing about NAPT is that it serves as a security measure in the form address hiding. Simply because internal host addresses are not visible from the Internet and therefore much harder to attack.

7.6 Circumventing the firewall

Even though a correctly configured firewall provides a very good protection for the company network it should not be relied on as the only protection mechanism. There are several ways to circumvent the firewall and attack hosts on the internal network. The following sections will describe a few ways which are all related to remote users. On the list of the top 14 security vulnerabilities presented in [MSK03] the second item is the following one.

> *"Unsecured and unmonitored remote access points provide one of the easiest means of access to your corporate network. Telecommuters often connect to the Internet with little protection, exposing sensitive files to attack."*

7.6.1 Laptops

It is common that remote users bring their laptop to the company network from outside. These are employees that use the same PC both at the office and at other remote locations. In many cases this PC have been used in environments that are not as protected as the company network. If the PC have been exposed for some malicious code then this may spread onto the company network once the PC is connected. Even if the other hosts on the internal network are not vulnerable to this attack there may still be implications for the company. The Nachi worm that appeared in August 2003 a few days after the Blaster worm [CER03a] was actually designed to clean and patch hosts infected by Blaster. Nachi generated a lot of network traffic as it used the Internet Control Message Protocol (ICMP) [Pos81] to scan for other systems to target. Even a single host on the internal network starting to scan for target systems out on the Internet with its 100 Mbps network interface card will easily generate large amounts of traffic. A firewall connected to the Internet with a bandwidth of only a few Mbps will not be able to handle this load and other users on the internal network will suffer from this DoS attack as they are not able to connect to the Internet. This scenario could of course have been much worse if the hosts on the internal network were vulnerable to this attack, in this case just one PC have to be cleaned to restore the network to normal operation.

7.6.2 Remote computers

Employees working from home and have access to the company network may also pose a threat that the company firewall will not protect against. If the employee is using the VPN technology to connect to the company network, then the logical connection is equal to physically connecting the computer at the office. Since the VPN connection is established over the Internet the remote computer must have a connection to the Internet. This means that a remote user without a firewall will expose the company network to the Internet. The expensive firewall at the office will not be of any use when an attacker chooses to target the remote user's computer and access the company network this way instead.

7.6.3 Wireless networks

Wireless networks have rapidly become very popular. The most widespread standard is probably IEEE 802.11b while 802.11g is becoming more and more popular [IEE04]. These standards allow for communication speeds up to 54 Mbps and support a range of over 100 meters, depending on the surrounding environment. The signals may be picked up from even further distances if a better antenna than the default one is used.

All that is needed to create a wireless network is a wireless Access Point (AP) that is plugged in to the wired network and an wireless network interface card for the computer. Because of the increased popularity for wireless networking equipment the prices have dropped and are still dropping. A wireless network interface card is not much more expensive than a wired one. People will buy and install this kind of equipment at home. It is very convenient to be able to move around the house with the laptop and to be able to avoid long wires through the house.

The most common way is to install this equipment with the default configuration, which is almost always the least secure. This will enable people within signal range to access the network. Even if the home network is protected from attackers on the Internet the same measures may not apply to an attacker that gains direct access to the home network through the AP. Broadband router devices with NAPT or firewall functionality will only protect against attacks coming from the Internet. Personal firewall software on hosts are usually configured with much more relaxed rules for traffic on the home network than for Internet traffic. This is useful for allowing things like file and printer sharing on the home network but not on the Internet. So an attacker with access to the home network will have it much easier than an attacker out on the Internet.

Wired Equivalent Privacy

A security scheme called Wired Equivalent Privacy (WEP) have been developed for wireless networks. The goal of this is to achieve a security level that is equivalent to a wired network. WEP enables confidentiality through encryption of the traffic based on the symmetric RC4 encryption algorithm, with a key length of 64, 128 or 256 bits. Most implementations support key lengths of 64 and 128 bits. The WEP encryption process is shown i Figure 7.5 below.

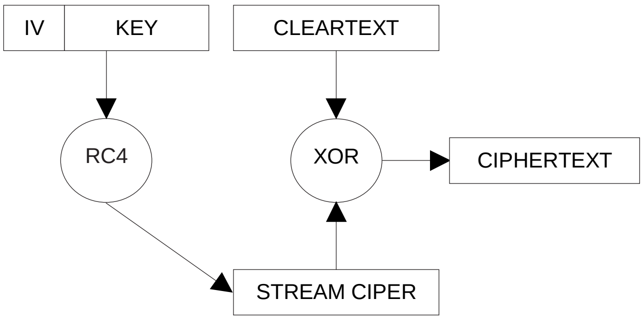


Figure 7.5: Wired Equivalent Privacy encryption process.

There are several weaknesses in WEP that enables attackers to crack it. One reason for this is that to prevent the same cleartext from always being encrypted to the same cipertext a random 24 bit Initialization Vector (IV) is used as part of the encryption key. This IV is generated by the sender and included unencrypted in the transmitted packet so that the receiver will be able to decrypt it. This makes it possible for an eavesdropper to pick it up, hence reducing the effective key length with 24 bits. Another reason is that when a client connects to the AP a challenge response authentication scheme is used to verify that the client has a correctly configured WEP key. This scheme will give an eavesdropper access to both the cleartext and the corresponding ciptertext. Also there is no key exchange protocol which means that the same key will be used until it is manually changed in all devices on the network. By passively analyzing the wireless traffic an attacker can perform offline attacks to crack the key. The speed of this process depends somewhat on how much traffic the attacker is able to pick up. For a lightly loaded network the process might take weeks while it may be a matter of hours or minutes for a heavily loaded network. Also there are no mechanisms in WEP for integrity or authenticity of the transmitted packets. The general opinion is that these issues prevent WEP from being a good solution when it comes to protecting sensitive data.

Other security measures

There are also some security measures that are not part of the wireless standard but are implemented in APs by many vendors anyway. Two of these are the following ones.

- MAC address access control which allow users to specify the MAC addresses for the wireless network interface cards that should be allowed to connect to the AP. Passive attacks are still possible by just sniffing the traffic. It is also possible to circumvent the MAC access control by spoofing a valid MAC address. There are simple tools available on the Internet for this purpose. With a spoofed MAC address the attacker can connect to the AP and pretend to be a valid client. It is also possible to perform a denial-of-service attack by spoofing the MAC address of the AP and forcing the clients to disconnect.

- Possibility to disable broadcast of the Service Set Identifier (SSID), i.e. the name of the wireless network. This makes it harder to detect the wireless network. But since the SSID is still sent by clients when connecting to the AP it is still possible for an attacker to find out the SSID by using freely available software tools. It might also be a good idea to choose a SSID name that does not attract attackers.

As we have seen all of these measures can be circumvented one way or the other but they will at least make it harder for an attacker than if they are not used. If sensitive data is to be sent on the network the same higher layer encryption mechanisms that are available for wired networks should be used, e.g. IPSec or SSL.

This section was primary based on information from these sources [MSK03, Cis03b].

7.7 Summary

Almost all companies connecting to the Internet have a firewall to protect the company network. For companies this is often a hybrid firewall that allows an advanced filtering configuration. This provides a good first line of defense if it is configured correctly. Home users sometimes have a personal firewall on their PC or a small broadband router implementing NAPT for their home network.

Remote users must have some form of firewall protection to avoid creating holes in the perimeter defense when connecting to the company network. It is also becoming more and more common for companies to consider providing an in-depth defense by implementing some type of filter to control traffic between hosts on the internal network. This will prevent attacks that break through the perimeter defense from reaching the internal hosts or spreading between hosts. Distributed firewalls or Microsoft's group policies will allow central control of these filtering rules and they may also be applied to remote hosts.

Chapter 8

Intrusion Detection Systems

This chapter describes a type of system that is used to detect malicious activities on networks and hosts, this system is called an Intrusion Detection System (IDS). Focus will be on the most common kind of IDS, anti-virus software. A variant of an IDS called a honeypot is also briefly described. This information is primarily based on [CBR03].

8.1 Overview

On many companies security incidents are not detected until they result in noticeable things like degrade network performance, system crashes or missing data. On most systems log-files are created and these are used to go back and see what has happened on the system. There are three problems with this way of handling incidents:

- The incident has already occurred or been going on for a while before actions against it can be taken.
- Attackers often remove their tracks by modifying log-files, leaving the company without information concerning the incident.
- Incidents that do not have effects that will disrupt normal operation will not be detected.

This is why an IDS can be useful. The operation of an IDS is either anomaly-based or signature-based. An anomaly-based IDS looks for unusual system behavior. This may be things like network traffic patterns or system call patterns, that do not look normal. It is very difficult to determine what is normal and what is not normal, this is currently a popular research area. A signature-based IDS uses a database of signatures for known malicious activity. This makes it easy to detect malicious behavior but it depends on a signature database that is kept up-to-date with current attack patterns. If the signatures are too detailed it is possible for an attacker to just make a small change to the attack pattern and slip through undetected, this is called false negatives. On the other hand, if the signatures are not detailed it is possible that normal harmless traffic is detected as an attack, this is called false positives. It is hard to configure the IDS so that the rate of false positives and false negatives do not become too high.

An IDS is categorized as either Host-based or Network-based.

8.2 Host-based Intrusion Detection Systems

A Host-based Intrusion Detection System (HIDS) is a system that is used to detect malicious activity directed against a specific host. The most common kind of software that can be categorized as a HIDS is anti-virus software.

8.2.1 Anti-virus software

Anti-virus software is a signature-based IDS and the most important part of this software is the virus definitions database. This is a collection of signatures for known malicious code, like viruses and trojan horses. The anti-virus software operates by scanning files on the host for content that matches the signatures in the virus definitions database. Usually the anti-virus software is running in the background and scans all files that are used on the system. There is also another feature that allows the user to scan all files on hard drives or on removable media.

Some vendors also include additional features that allows for scanning of files that are sent or received by e-mail or instant messaging. A trend is that anti-virus software and personal firewalls are moving closer together. Sometimes it is necessary to disable some features in either the anti-virus software, or the firewall, since they might interfere with each other when using products from different vendors. This trend is probably due to the increase of blended threats, see Appendix D for a description of blended threats.

Many users consider anti-virus software to be the most important security mechanism there is. This is probably because many users are familiar with it. It is true that anti-virus software provides a good safety-net for malicious code that manages to get into the system, but it should not be relied on as the only security mechanism. The reason for this is that although it can detect and remove malicious code from the system it does not prevent it from entering the system. This is instead achieved by having a firewall, patching known software vulnerabilities and acting with caution when opening e-mail attachments and installing downloaded applications.

Even though many people have installed anti-virus software, they fail when it comes to to the most important part, i.e. making sure that the virus definitions are up-to-date. New viruses are discovered all the time and for the anti-virus software to be able to detect them, their signatures must be known. Usually there is an automatic update feature that will allow automatic updates of the virus definitions. Sometimes there are performance implications when running applications that access a lot of files. The simplest solution when problems like this occur, is to turn off the anti-virus software. This is dangerous because it is very easy to forget to turn it back on again. Maybe there are better solutions to problems like these that do not require the anti-virus software to be turned off altogether. This can include, configuration of it to exclude a particular directory or certain file types from being scanned.

For companies, there are many vendors which offer centrally controlled and monitored anti-virus software. This allows the network administrator to make sure that the software is running on all hosts on the network and that the virus definitions are up-to-date.

8.2.2 Tripwire

Another HIDS is Tripwire [Tri04]. This is a program that is used to detect undesired changes to a system. It monitors file attributes like size and date stamp. At first, a snapshot of the current system state is taken, this is then used as a reference. Changes compared to this snapshot are logged so that is is possible to detect undesired behavior. These changes can be the result of malicious activities but also of normal activities like software upgrades etc. If a detected change is not desirable, it is possible to restore the file to a previous known good state. Another possibility is to configure Tripwire so that certain files are automatically restored when changes are detected.

8.3 Network-based Intrusion Detection Systems

A Network-based Intrusion Detection System (NIDS) is used to detect malicious activities on a network. This is useful since a single system can be used to detect malicious activities, that can potentially effect all hosts on the network. A problem with a NIDS is that it is not aware of the state of the individual hosts on the network. This may lead to that it is not as efficient as a HIDS. Another problem is that encrypted traffic can not be analyzed by the NIDS since it is unable to decrypt it.

NIDS exist in many different forms, from dedicated hardware implementations to open source software, like Snort [sno04]. Modern firewalls often include some kind of IDS functionality.

It can be hard to decide where on the network the NIDS should be located, to detect malicious behavior as efficiently as possible. It is necessary to carefully plan which kinds of attacks the IDS is supposed to detect.

8.4 Honeypots

A honeypot is a special kind of IDS. It is setup in a network environment in a way such that no normal traffic is sent to it. All traffic that is received by this system is therefore considered potentially malicious. There are different types of honeypots, some will act as a single host, while some will act as several hosts.

8.5 Summary

An IDS can be useful to detect malicious activities that would otherwise not have been detected. Not having an IDS can be dangerous since not being able to detect malicious behavior may contribute to a false sense of security. The hard part of an IDS is to tune it so that it does not generate high amounts of false positives or false negatives. The most common IDS is anti-virus software which provides a good way of detecting viruses.

Chapter 9

Good IT security practice

As we have seen there are many technical mechanisms that can be implemented to make a system more secure. We have also seen that if users do not understand how these mechanisms work or why they are there, they will not handle them correctly.

The following was written by Nils Gunnar Billinger the Director-General of the Swedish governmental authority for issues related to telecoms, called Post- och telestyrelsen (PTS), or the National Post and Telecom Agency [PTS03b].

> *"Det är min fasta övertygelse att det mest effektiva sättet att uppnå IT-säkerhet är att vi användare är informerade och kunniga."*

This basically translates into something like, the most effective way to achieve IT security is through user awareness.

This chapter gives some advice that all users who operate PCs which are connected to the Internet should be aware of, both employees at companies as well as home users. Finally, some of the consequences that may follow from not taking this advice are presented.

9.1 Patch management

Installing patches for known vulnerabilities on IT systems is probably the cheapest and most underestimated security precaution that may be taken. It is very common that malicious attacks are based on known vulnerabilities in the target systems. Instead of applying patches for these vulnerabilities in a pro-active manner many users and system administrators do not pay attention to vulnerabilities until there are actual exploits of them.

One good example of this was the Remote Procedure Call (RPC) interface buffer overrun vulnerability in Microsoft's Windows NT, Windows 2000 and Windows XP operating systems. This was described in a Microsoft Security Bulletin [Mic03e] on July 16 2003. On August 11 CERT Coordination Center issued an Advisory [CER03a] about a worm called Blaster that exploited this vulnerability to spread. Systems that already had been patched were of course not affected by this worm.

To aid in the process of making sure that all systems have patches for known vulnerabilities there are some tools available. For the Windows operating systems the Windows Update tool checks if there are any updates available for the system. If the Critical Update Notification Feature is activated, then an icon will automatically appear in the system tray when a critical update is available on the Windows Update site. Another tool from Microsoft is the Microsoft Baseline Security Analyzer [Mic03d] which allows a single computer or several computers on a network to be analyzed. A report for each computer is then created. This report shows which patches are missing on the system as well as if there are any common security misconfigurations like weak passwords etc. This tool does not only analyze the Windows operating system, but also products like SQL Server, Exchange Server and IIS. For networks with many computers there are tools like Ecora Patch Manager [Eco03], which allows advanced configuration of patch policies and central control of the patch management process.

Patches must be installed not only for the operating system but for all critical software on the PC. This includes all software that communicates over the network. For home users this is often software like web-browsers, e-mail readers, firewall and anti-virus software etc[1].

As it very often is in the area of network security there are no simple answers. Writing software is a relatively new area and there are no scientific rules, only best practices, for how to construct software without introducing bugs. So for new patches there is no way to be sure that even if the vulnerability is removed another one will not be introduced.

9.2 Passwords

Using passwords is the most common way of performing authentication. As we have seen the main problem with this method are the weak passwords that users choose. Here are some rules that should be followed when handling passwords:

- Do not choose passwords that are based on common words, e.g. words from a dictionary. This applies even if some character from the word are replaced or appended.
- Do not choose passwords that are based on personal information, e.g. part of your name or a pets name etc.
- Use a mixture of lowercase, uppercase, numeric and special characters.
- Use at least 8 characters in the password.
- Do not share the password with anyone.
- Do not write the password down, unless the note is kept in a safe place.
- Do not check the save password box in login dialogs.

[1] Applications that operate on data which does not seem to be executable content, like word processors and Postscript previewers should also be considered. Microsoft Word contains a powerful macro language that have been used to create viruses and Postscript is actually a language.

- Do not use the same password on different systems.
- Change the password regularly.

One good method of choosing a password is to think of a phrase and make up the password from this phase e.g. the phrase “Do not Forget to Choose a Good Password!” can be used to remember the password “DnF2CaGP!”.

9.3 Virus definitions

Many users have anti-virus software installed on their PCs. Still they fail with the most important part, i.e. making sure that the virus definitions are updated and that it is actually running.

It is impossible to say how often the virus definitions database should be updated, this depends on how often new viruses are discovered. Sometimes the anti-virus software vendor updates the definitions several times a day and sometimes only a few times a week. The best way is to use the automatic update feature that is available in all modern anti-virus software. This will download updated virus definitions when they become available.

9.4 Spam and e-mail

Unsolicited bulk e-mail, called spam, is a problem that has increased dramatically during the last year. Some source now claim that over 50 percent of all e-mails are spam.

At companies this is usually handled by some filter in the mail server, which prevents it from reaching the employee’s PC. For home users this can be a real nuisance. Here are some recommendations for how to avoid encouraging spammers.

- Do not give out your e-mail address unnecessary. Use a trash e-mail address on all web-sites that require you to enter an address for different reasons. There are free web-based e-mail services that may be used to create this account.
- Do not reply to spam, this will just confirm to the spammer that someone is using the address.
- Do not read or preview spam, just delete it. HTML-code that is included in many e-mails to make them more attractive to the reader can also be used in ways that will inform the spammer that someone is using the e-mail address.

Often just seeing the from and the subject fields of a mail will reveal that it is spam. It is often from someone unknown with a strange subject and in addition it is usually in English.

Just like spam filters, companies often have filters to remove executables from e-mails since this is a very popular way to distribute malicious code. This is working because users are curious and open both suspect e-mails and attached files instead of just deleting them. Home users usually do not have the safeguards which companies do and are therefore more vulnerable.

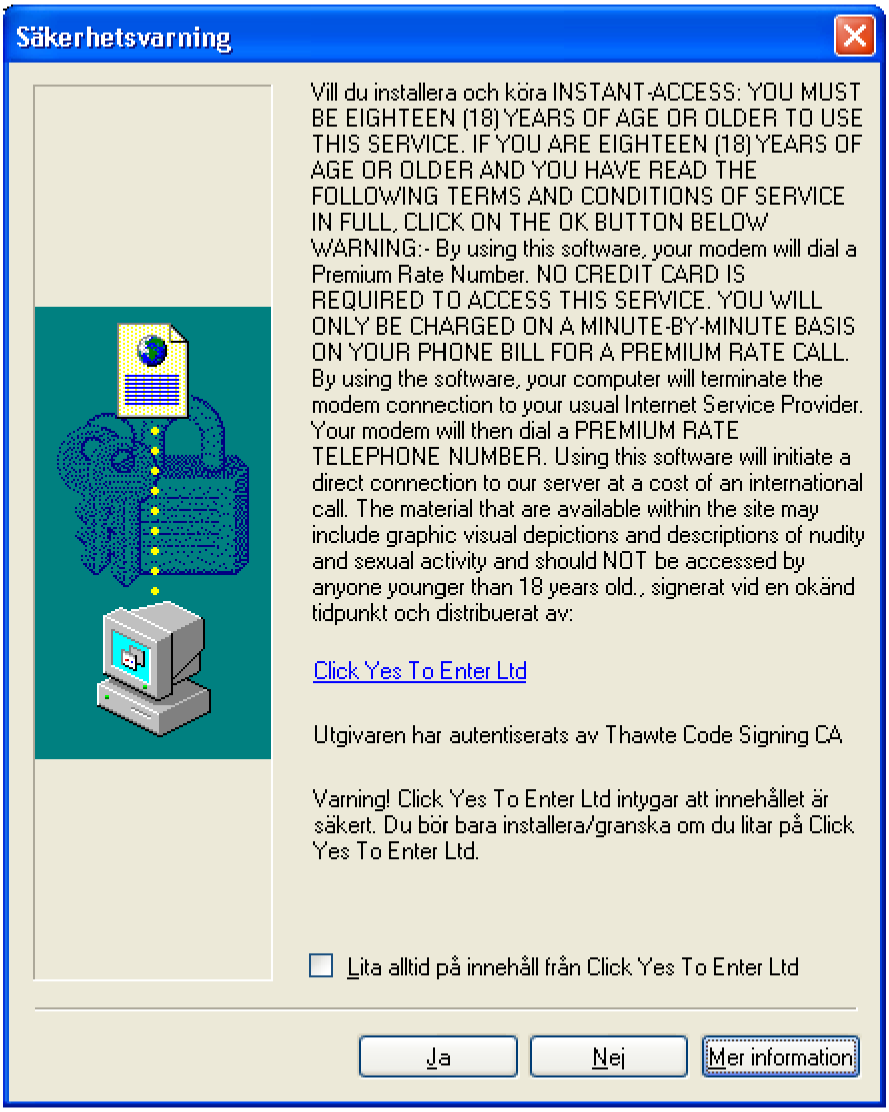
The BugBear.B worm that was discovered in the beginning of June 2003 spread through e-mail [F-S03a]. A known vulnerability in common e-mail readers allowed it to infect a PC even if the user just viewed the e-mail without opening the attached file. It contained a back-door that allowed anybody to access an infected PC and take control of it as well as a keylogger that could be used to capture passwords or credit card information etc.

9.5 Possible consequences

Even if home users often do not have sensitive information on their computer there are still many reasons for protection.

- The system may be used for Distributed Denial-of-Service (DDoS) attacks on other systems.
- The system may be used to send spam to other systems.
- The system may be used to attack other systems, making it hard for the victim to find out who the actual attacker is.
- The system may be used as a temporary storage for piracy software or child pornography etc.
- The system may become unstable and crash.
- Files on the system may be modified or deleted.
- A back-door may be installed and used by an attacker at a later time.
- The user may receive increased amounts of spam.
- The modem may be hijacked and used to call premium rate numbers at the owner's expense, see Figure 9.1.

Computers connected to the Internet will be attacked, there is no question about it. A small test was performed in the middle of January 2004 with a normal Windows 2000 system connected to the Internet through a regular 0.5 Mbps ADSL connection while another computer was used to monitoring the traffic sent to it. In less than 40 minutes 20 distinct IP addresses tried to connect to it. Most of the connections were from computers infected with Blaster or its successors that tried to spread. Luckily, the computer was patched against this vulnerability and was not infected. This is not confined to just ADSL but applies to all other Internet access technologies as well, like dial-up modem, cable modem and building LANs.



Säkerhetsvarning

Vill du installera och köra INSTANT-ACCESS: YOU MUST BE EIGHTEEN (18) YEARS OF AGE OR OLDER TO USE THIS SERVICE. IF YOU ARE EIGHTEEN (18) YEARS OF AGE OR OLDER AND YOU HAVE READ THE FOLLOWING TERMS AND CONDITIONS OF SERVICE IN FULL, CLICK ON THE OK BUTTON BELOW WARNING:- By using this software, your modem will dial a Premium Rate Number. NO CREDIT CARD IS REQUIRED TO ACCESS THIS SERVICE. YOU WILL ONLY BE CHARGED ON A MINUTE-BY-MINUTE BASIS ON YOUR PHONE BILL FOR A PREMIUM RATE CALL. By using the software, your computer will terminate the modem connection to your usual Internet Service Provider. Your modem will then dial a PREMIUM RATE TELEPHONE NUMBER. Using this software will initiate a direct connection to our server at a cost of an international call. The material that are available within the site may include graphic visual depictions and descriptions of nudity and sexual activity and should NOT be accessed by anyone younger than 18 years old., signerat vid en okänd tidpunkt och distribuerat av:

Click Yes To Enter Ltd

Utgivaren har autentiserats av Thawte Code Signing CA

Varning! Click Yes To Enter Ltd intygar att innehållet är säkert. Du bör bara installera/granska om du litar på Click Yes To Enter Ltd.

□ Lita alltid på innehåll från Click Yes To Enter Ltd

Figure 9.1: Security alert dialog that popped up automatically during a web-browsing session asking for the user's approval to run a program the will use the modem to dial a premium rate number. Many users do not bother to read messages like this and just clicks "Yes".

Once an attacker gains access to a computer there are no limits to what might happen. As we have seen the impact of an attack is not just about disclosure of confidential information or destruction of data. One problem is that users are many times not aware that the computer has been attacked and is under the control of an attacker. This problem have become so extensive that since late 2003 several large ISPs in Sweden have begun disconnecting users who's computers are used to send spam without the user's knowledge [Tel03]. The same applies for viruses, users say that they have not been affected even though there may be several viruses on the system that they simply have not detected.

9.6 User awareness

That user awareness is an important part of IT security is also shown by increased non-technical information being made available for users. Here are some web-sites that are useful for keeping up with important issues in this area.

9.6.1 Information in English

The United States-Computer Emergency Readiness Team (US-CERT) was established in September 2003. It offers non-technical information for home and corporate computer users through what they call Cyber Security Tips and Cyber Security Alerts. These are made available on their web-site or subscribed to through e-mail.

Cyber Security Tips: http://www.us-cert.gov/cas/tips/index.html

Cyber Security Alerts: http://www.us-cert.gov/cas/alerts/index.html

The CERT Coordination Center is a major reporting center for Internet security problems. It was established in November 1988 right after the first major Internet worm, the Morris worm, was released. Part of the information found on their web-site is articles and tips aimed at home users.

http://www.cert.org/homeusers/

9.6.2 Information in Swedish

PTS has opened a web-site that focuses on Internet security. The target audience is home uses as well as small and medium-sized companies.

http://www.pts.se/internetsakerhet/

PTS has also created a Center to support activities against IT incidents. It is called Sveriges IT-incidentcentrum (Sitic), or the Swedish IT Incident Center and was opened in January 2003.

http://www.sitic.se

9.7 Summary

By following the advice given here many incidents that occur because the attacker or the malicious code writer relies on foolish user actions will be prevented.

It is common that users are not aware of what the computer is actually doing. Users think that their systems are not affected just because they do not know about it. Increased user awareness is very important in the area of IT security.

Chapter 10

Recommendations

This chapter presents mitigation actions that should be used to reduce the risks related to a VPN based remote access solution. Possible mitigation actions for the highest risks in this case are presented. This is followed by recommendations for both technical and non-technical actions. Considerations concerning the usage of private PCs are also included.

10.1 Possible mitigation actions

As we saw in Chapter 3 the risks associated with a remote access solution can be realized through many different attacks. To prevent these attacks, there are different mitigation actions that may be taken. Table 3.4 in Chapter 3 describes guidelines for implementing mitigation actions in relation the the calculated risk level.

In this case all the risks had a calculated risk level of either 1, 5, 10 or 50. We will focus on the highest risks levels of those and therefore ignore 1 and 5. 50 falls into the high-end of the medium risk grade while 10 falls into the high-end of the low risk grade. Table 10.1 below lists the attacks that were associated these risks and the possible mitigation actions that may be implemented.

Attack description	**Highest risk level**	**Possible mitigation actions**
On the remote PC:		
Theft of the PC.	50	Encryption. Do not store data locally. Backup policy.
Non-employees using the PC (friends, family members etc.).	50	Policy about who may use the computer and for which purposes.
User deletes information by mistake.	50	Backup policy.

User makes it available by mistake (Windows file sharing, P2P file sharing etc.).	50	Policy about which applications may be installed. Firewall.
System software crash.	50	Backup policy.
System hardware crash.	50	Backup policy.
The PC is compromised by an attacker on the Internet or the LAN.	10	Firewall. Patch management policy.
The PC is compromised by an attacker through social engineering techniques (malicious website, e-mail with an attached trojan horse etc.).	10	Anti-virus software. Firewall. Policy about handling e-mail attachments. Policy about which applications may be installed.
Virus or worm infection.	10	Policy about handling e-mail attachments. Policy about which applications may be installed. Firewall. Patch management policy. Anti-virus software.
Theft of old backup media.	10	Backup policy.
Information is not removed when old PC is sold or thrown away.	10	Policy about how to handle old PCs.
In transit:		
Sniffing the LAN to which the remote PC is connected.	10	Secure communications protocols. Well chosen and regularly changed passwords. Strong authentication.
Manipulating traffic on the LAN to which the remote PC is connected.	10	Secure communications protocols. Well chosen and regularly changed passwords. Strong authentication.
Manipulating traffic on the Internet (at an ISP etc.).	10	Secure communications protocols. Well chosen and regularly changed passwords. Strong authentication.

Compromised network device on the Internet (router etc.).	10	Secure communications protocols. Well chosen and regularly changed passwords. Strong authentication.
Replaying old traffic.	10	Secure communications protocols. Well chosen and regularly changed passwords. Strong authentication.
On the corporate network:		
Virus or worm infection on the remote PC spreading to the corporate network.	50	Firewall. Patch management policy. Anti-virus software.
A stolen remote PC is used to access the system.	50	Policy about saving passwords. Well chosen and regularly changed passwords. Strong authentication.
System is compromised (VPN server, firewall etc.).	10	Well chosen and regularly changed passwords. Strong authentication.
A compromised remote PC is used as a back-door to access the system.	10	Firewall. Patch management policy. Anti-virus software. Policy about saving passwords. Well chosen and regularly changed passwords. Strong authentication.
Vital network resource compromised by an attacker through a remote PC (mail server etc.).	10	Firewall. Patch management policy. Anti-virus software. Policy about saving passwords. Well chosen and regularly changed passwords. Strong authentication.
An old remote PC is used to access the system.	10	Policy about how to handle old PCs.

Table 10.1: Possible mitigation actions for attacks that are associated with the highest risks.

As we can see most of the attack methods can be mitigated by using one of several actions or by using a combination of them. These actions are either technical in the form of a hardware or software mechanism, or rules in the form of a corporate policy. The most effective way to reduce the risks are by a combination of the two.

The security policies must be combined with information and user education to achieve the desired effect. If users are not convinced that the actions taken by the company are motivated, chances are that they will ignore them if they feel that the actions are unnecessary or cause problems. This can lead to that users do not handle security products in the way which they were intended or do not use them at all. In this case it does not matter how technically advanced the products are, since if they are not used they will not provide any protection.

10.2 Recommended technical actions

The following sections contain recommendations for technical actions that should be taken by the company. These recommendations are the result of considering the requirements presented in Chapter 2, the issues described throughout this report and the possible mitigation actions presented in Table 10.1.

10.2.1 Remote PC configuration

Operating system

The recommended Windows operating system is either Windows 2000 or its successor Windows XP. These contain several new security features that was introduced in Windows 2000 and improved in Windows XP. Windows XP exists in a Home edition that is often preinstalled on PCs. This edition does not contain all security features that are included in the Professional edition. There are also limitations in the Home edition when it comes to operating in a Windows domain environment. So if Windows XP is used then the Professional edition is the preferred one.

Firewall

Remote PCs connecting to the corporate network will create a new path between the Internet and the corporate network which is not protected by the corporate firewall. To prevent this from becoming a security risk the remote PC should have a firewall. The best solution would be a distributed firewall that can be centrally configured. This relieves the user from having to worry about the configuration hence increases the user friendliness. At the same time it is possible to centrally monitor the operation of the firewall to make sure that the corporate security policy is enforced.

Anti-virus software

Anti-virus software is a good safety-net since it is able to detect malicious code no matter which way it manages to enter the system. The important thing is to have virus definitions that are up-to-date, automatic update features can ensure this. Just like with distributed firewalls there are solutions that will allow central control of anti-virus software, this is of course preferred.

Patch management

Making sure that critical software is up-to-date is important since attackers and malicious code often takes advantage of known vulnerabilities. This includes not only the operating system but also software like the web-browser, e-mail reader and firewall etc. Some software have automatic update features while others require manual downloads of patches. Manual downloads are very user demanding and a better solution is a patch management system that allows for central control.

Encryption

For laptops that contain sensitive data and are used in environments where the risk for theft is high, an encryption mechanism should be used. The EFS feature built-into the operating system is one possibility. This will require some configuration by the IT department and the user will have to do some extra work when booting the system. If it is sensitive data then it might be worth this extra effort to protect it.

10.2.2 VPN configuration

VPN protocol

Since PPTP is not considered a secure VPN protocol, an IPSec based solution should be used. Not only does it provide superior security for transmitted data, device authentication will make sure that only approved PCs can connect from remote locations.

User authentication

Static passwords is an old authentication method associated with many problems. Because of this a modern strong authentication method should be used. The two-factor scheme based on an authentication token that generates one-time passwords does not require much work by the user. An attacker that picks up this password will not have any use for it, the same goes for the save password feature in the login dialog.

10.3 Recommended non-technical actions

The following sections contain recommendations for non-technical actions that should be taken by the company. Just like for the recommended technical actions, these recommendations are the result of considering the requirements presented in Chapter 2, the issues described throughout this report and the possible mitigation actions presented in Table 10.1.

10.3.1 Security policy

A security policy that states which rules apply to to the remote access solution should be created. A remote PC that is connected through VPN can in many ways be considered equal to a PC directly connected to the corporate network. Because of this there is no reason why the rules that apply to a PC at the office should not apply to a remote PC. The goal of having these rules is to make sure that the security issues related to the remote access solution are handled in a way that is consistent with the overall security policy for the company.

These rules should be documented and made available to to everybody who take advantage of the remote access solution. This document should not be longer than two pages, and address the following issues:

- The purpose of allowing remote access. What the PC may be used for and which applications may be installed.
- Any special concerns regarding the configuration of the security mechanisms, e.g. the firewall and anti-virus software.
- Routines regarding backup of data for the remote PC.
- Which private activities that are allowed to use the PC for and who may use the PC.

10.3.2 Increased user awareness

As we have seen technical mechanisms only provide a solution for some of the security problems. A large part of the problems can only be solved if users are aware of the risks. It is not easy to avoid being infected by a virus without knowledge of how viruses work. This is similar to real world viruses that centuries ago spread wildly because people took actions that helped viruses without even knowing it. Some form of education is probably the only way to remedy this situation. In practice this is a real challenge since many employees are naturally more interested in solving the task at hand instead of learning about things that do not interest them, i.e. IT security.

The previous chapter contains information about good IT security practice that users should be aware of. It also includes some recommendations of web-sites and mailing-lists that can be useful for employees who want to keep themselves informed in this area.

IT security is not something that is achieved through a single one time action. It is a continuous process that should be a present as a small part of the day-to-day corporate operation. Just like locking the door to the apartment and handling the wallet with care is part of day-to-day life.

10.3.3 Routines

There must be established routines sanctioned by the management to handle the following issues:

- Who is responsible for authorizing an employee to use the remote access solution.
- Who is responsible for looking over the security policy once or twice a year to make sure that it is in line with the overall corporate security policy. Changes in user behavior as new technologies are introduced will have to be considered. A modified security policy must be communicated to all users.
- How should a PC be handled when it is not used for remote access anymore. Sensitive information should be removed before it is sold or thrown away.

10.4 Private PCs

The nature of a private PC will introduce new problems that are not an issue for corporate owned PCs. These are used for private things which usually means:

- Non-employees are using the PC, e.g. family members and friends.
- Non work related applications are installed, e.g. games and P2P file sharing applications.

This can increase the security risks and is not acceptable. All PCs which connect to the corporate network should be subject to the same security policy.

A private PC could of course be used if the owner agrees to follow this security policy. In practice this can be hard to achieve since it will probably limit the employee's private usage of the computer. Another issue is support of the PC when there are problems, should the employee or the company be responsible for this. For employees that need the ability to work from remote locations a laptop or a desktop PC owned by the company is the preferred solution.

A cheap solution that can be used instead of having one private and one corporate PC is to use a removable hard drive. This makes it possible to insert a corporate hard drive when the PC is used for business purposes and a private hard drive when the PC is used for private purposes. This is virtually the same as having two PCs, except that they can not be used at the same time.

10.5 Summary

These recommended actions should provide sufficient protection to reduce the highest risks to an acceptable level. The technical actions will provide a basic level of centrally controlled protection for each remote PC. This relieves users from configuration issues which increases user friendliness. At the same time it is possible to monitor that the security policy is enforced. The non-technical actions provide clear rules and routines, which is something that was requested by all involved parties; users, IT staff and management.

Chapter 11

Conclusions

The survey conducted among remote access users at this company shows that it is still common to use dial-up modems to connect to the Internet. This was expected as a way of connecting during business trips etc. but not as a primary way of connecting. In theory this is not something that prevents these employees from using the VPN based solution but because of the properties of dial-up connections it is in practice often only used for shorter durations to download or upload files etc. The full power of the VPN technology is not taken advantage of.

The interest in using VPN is high and most employees give the limited bandwidth as the main reason for not using it more. Broadband technologies are growing fast and the number of Swedish homes that take advantage of them are increasing [PTS03a]. When new technologies are introduced security is usually not the main consideration. This is the case for many companies that are introducing or have introduced remote access solutions.

The presented security recommendations are based on a risk analysis which show that the risk for attackers actively trying to hack into the corporate network is not considered very likely. The main threats come instead from user mistakes and from malicious code like viruses and worms which spread without targeting specific systems. These recommendations, which include a documented policy that clearly states which rules that apply, are very important. Partly because the number of employees who want to take advantage of the remote access solution probably will increase, but also because a single compromised remote PC is all that is necessary to cause problems.

Private PCs should only be used if the corporate security policy can still be enforced. This is usually hard since popular private activities are often not in line with the policy. It can be a problem for the IT department since the corporate network, which is their responsibility, will include PCs that are not owed by the company hence not completely under their control.

The main thing to remember though, is that the importace of user awareness can not be ignored, even if sofisticated technical security measures are implemented.

This project has been conducted for a limited period of time. The area is very wide and it has been necessary to limit the scope of it to be able to finish during this period. It would probably have have been possible to do a complete thesis on just one of the subjects that were addressed here, like risk analysis, user authentication or intrusion detection.

Further studies that would be interesting to do include the implementation of an IDS. This can make it possible to see if the result of the risk analysis is correct, i.e. attack attempts that target this particular system is low. At the same time this can be used to verify that implemented security mechanisms are actually working.

Another interesting project would be to look at the possibilities to replace the VPN based solution with an application server based solution. As more employees begin using always-on broadband connections this is a solution which may become more attractive.

Appendix A

Glossary

3DES	Triple DES.
ADSL	Asymmetric Digital Subscriber Line. Communications protocol designed to allow high speed data communication over existing telephone lines.
AES	Advanced Encryption Standard.
AH	Authentication Header. A security protocol that is used in the IPSec architecture.
CA	Certificate Authority.
CERT	Computer Emergency Response Team.
CHAP	Challenge Handshake Authentication Protocol.
DDoS	Distributed Denial-of-Service.
DES	Data Encryption Standard.
DMZ	Demilitarized Zone. A network, which is located between a trusted network and an untrusted network, usually between a corporate network and the Internet.
DoS	Denial-of-Service.
Dumpster-diving	Going through a person's or a company's garbage to find some information that may be used to attack a system.
ESP	Encapsulation Security Payload. A security protocol that is used in the IPSec architecture.
GRE	Generic Routing Encapsulation.

Hardening When steps are taken to make a system as secure as possible, e.g. by disabling services that are not needed, activating security features etc.

HIDS Host-based Intrusion Detection System.

HTTP Hyptertext Transfer Protocol. The protocol used when browsing the World Wide Web.

HTTPS HTTP over SSL.

ICF Internet Connection Firewall. Personal firewall included in Microsoft's Windows XP operating system.

ICMP Internet Control Message Protocol. A protocol operating as an integral part of the Internet Protocol to provide infrormation about for example errors in Internet Protocol transmissions.

IDS Intrusion Detection System.

IETF Internet Engineering Task Force. An open community concerned with the evolution of the Internet architecture.

IIS Internet Information Server. Microsoft's web server.

IKE Internet Key Exchange.

IP Internet Protocol.

IPSec Internet Protocol Security. A security architecture that is used to provide security for both IP version 4 and IP version 6.

ISDN Integrated Services Digital Network.

ISP Internet Service Provider.

Kerberos An authentication scheme that relies on a trusted server to perform key management functions.

L2TP Layer 2 Tunneling Protocol.

MAC address Media Access Control address. The hardware address of a device connected to a shared network.

MD5 Message Digest 5. A commonly used hash function.

MPPE Microsoft Point-to-Point Encryption.

NAPT Network Address Port Translation. Also called traditonal NAT and sometimes referred to as PAT. A technology for one-to-many mapping of IP addresses, allowing several hosts to share a single IP address on the Internet while having different IP addresses on the local network.

NAT Network Address Translation. Also called basic NAT. A technology for performing a one-to-one mapping of IP adresses to allow a host to have different IP addresses on different subnets.

NIDS Network-based Intrusion Detection System.

NIST National Institue of Standards and Technology.

Non-repudiation The concept of ensuring that parties involved in an transcation can not later deny that the transaction has occurred.

OSI model Open Systems Interconnection 7-layer reference model for network architecture defined by the International Organization for Standardization (ISO).

OWA Outlook Web Access.

PAP Password Authentication Protocol. Clear text authentication protocol that may be used with PPP.

PAT Port Address Translation. See NAPT.

Patch A software update that corrects an error.

POP3 Post Office Protocol version 3. The most common protocol for receiving e-mail.

PPP Point-to-Point Protocol.

PPTP Point-to-Point Tunneling Protocol.

PSTN Public Switched Telephone Network.

PTS Post- och telestyrelsen. The Swedish National Post and Telecom Agency.

RSA Rivest-Shamir-Adleman. A public-key cryptosystem invented by Ronald Rivest, Adi Shamir and Leonard Adleman.

SA Security Association. An agreement between two communicating parties about which security services should be used.

SAM Security Accounts Manager.

SHA1 Secure Hash Algoritm 1. A commonly used hash function.

SMTP Simple Mail Transfer Protocol. The most common protocol for sending e-mail.

Social-engineering Using social skills to get access to information that should not be revealed.

Spam Unsolicited bulk e-mail.

SSL Secure Sockets Layer. A protcol designed to support encrypted communication on the Internet.

TCP Transmission Control Protocol. A connection-oriented reliable communication service built on top of IP.

UDP User Datagram Protocol. A connectionless unreliable datagram service built on top of IP.

VDSL Very high bit-rate Digital Subscriber Line. Communications protocol designed to allow high speed data communication over existing telephone lines.

VPN Virtual Private Network.

Wardriving Driving around with a laptop computer and a wireless network interface card in order to detect wireless Access Points.

WEP Wired Equivalent Privacy.

Appendix B

OSI reference model

The Open Systems Interconnection 7-layer reference model is a model for network architecture defined by the International Organization for Standardization (ISO). Although this model and its associated concepts are very useful for discussions about network architecture, it is not widely used for actual implementations. The Internet is based on the TCP/IP protocol suite. Figure B.1 shows the OSI layers in relation to the TCP/IP suite along with some common protocols.

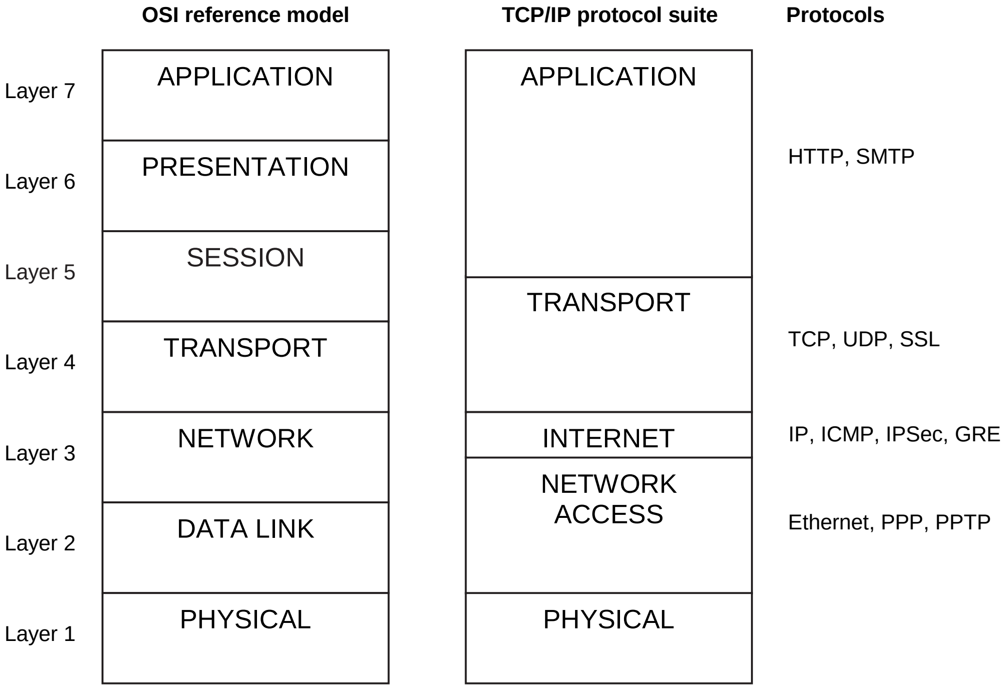


Figure B.1: The OSI reference model in relation to the TCP/IP protocol suite and some protocols commonly used on the Internet.

Appendix C

Cryptography

Cryptography is a good tool for achieving the properties and performing the processes that are necessary in a secure system. This includes:

- Authentication
- Confidentiality
- Integrity
- Non-repudiation

There are different forms of encryption algorithms that are useful in different ways to achieve these things. The following sections describe these forms as well as other common concepts related to cryptography, like digital signatures and certificates.

C.1 Symmetric encryption

Symmetric encryption is also called conventional encryption or private-key encryption. This form of encryption is based on a key that is used for both encryption and decryption, see Figure C.1. This key must be shared and kept secret by both the encrypting party and the decrypting party.

There are two main problems with this form of encryption. Firstly, it is hard for two parties to agree on a secret key before they have established a way to communicate securely. Secondly, when many parties want to be able to communicate securely with one another, one secret key have to be agreed on for each pair. This is acceptable if there is a limited number of parties but as more parties are introduced this solution does not scale very well.

The most well known symmetric encryption algorithm is the Data Encryption Standard (DES) which was developed in the 1970-ies and later adopted by the United Statues Government. This uses an encryption key of 56-bits.

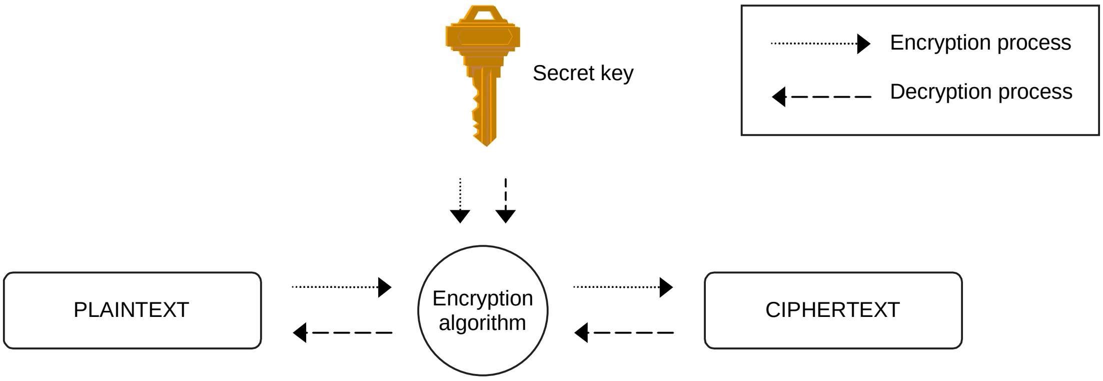


Figure C.1: Symmetric encryption algorithms makes use of a secret key both for encryption and decryption.

As techniques for cracking DES has improved the need for more secure algorithms have increased. A version of DES that allows for key lengths up to 168-bits is the Triple DES (3DES). Other common algorithms include the RC2 and RC4 algorithms from RSA Security, which are frequently used in Microsoft's products.

C.2 Asymmetric encryption

Asymmetric or public-key encryption is another form of encryption. This solves the problems with having to agree on a secret key and having a large number of keys that symmetric encryption suffer from. The solution is to use two keys instead of one, one key for encryption and another key for decryption, see Figure C.2. Each subject, e.g. a person or a server, that needs to be able to encrypt or decrypt information is assigned a key-pair consisting of one public and one private key. The public key should be published and given to other subjects which the subject wishes to share information with. The private key on the other hand must be kept secret and must not be revealed to anyone.

To communicate securely, the sending party simply encrypts the message with the receiving subject's public key, hence only the intended subject, with the corresponding private key, can decrypt the message.

Even though this scheme solves both main problems with symmetric encryption, it does not replace the need for symmetric encryption altogether. The reason for this is that it is much slower, a symmetric encryption algorithm can be 1000 times faster. This is a significant difference for many applications that require a fast encryption algorithm.

This form of encryption include the Advanced Encryption Standard (AES).

C.3 Hash functions

Another form of algorithms closely related to encryption are hash functions, these are functions that are considered mathematical irreversible, also called message digests or

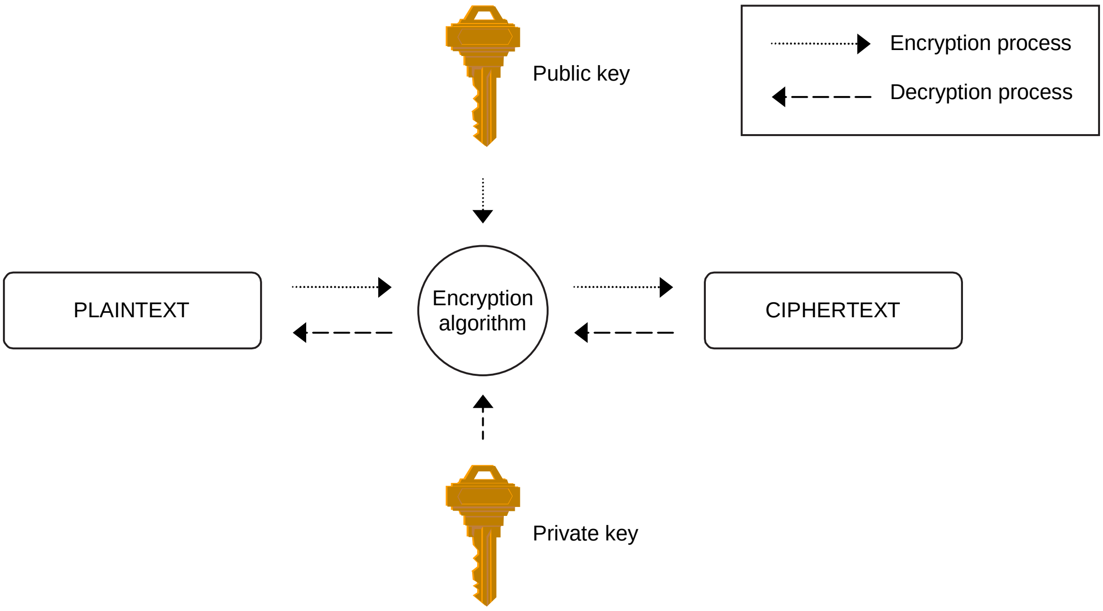


Figure C.2: Asymmetric encryption algorithms makes use of a two keys, one public, that is available to everybody, and one private, that is kept secret.

one-way functions.

A hash function takes some input data and produces a hash value of this input data, see Figure C.3. Two properties are important for a good hash function; different input data should produce different hash values and it should not be possible to deduce the input data even if the hash value is given. Common hash algorithms in use today include the Secure Hash Algorithm 1 (SHA1) and Message Digest 5 (MD5).

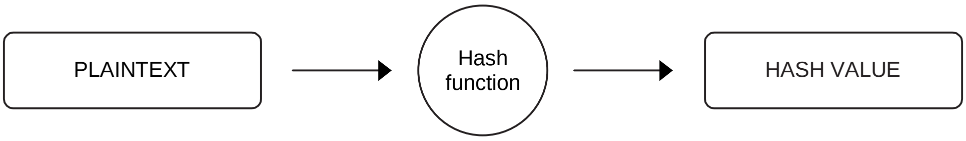


Figure C.3: Hash functions are irreversible functions that should not be possible to decrypt.

C.4 Digital signatures

Digital signatures are the digital equivalence to written signatures. By using the private key, the sender of a message can sign a hash value of that message, this digital signature is then sent together with the message. The receiver can verify the identity of the sender by comparing the hash value of the message with the value of the digital signature decrypted with the senders public key.

This technique is used to verify the author of e-mails but also to verify other information like programs and certificates.

C.5 Certificates

A digital certificate is a piece of information that is certified by a trusted party using a digital signature. On the Internet the most common certificate standard is called X.509. This kind of certificate contains three things:

- The information that should be certified, e.g. the name of a server or the e-mail address of a person. Including the period for which the certificate is valid.
- The public key for the subject being certified.
- A digital signature of the trusted party, i.e. the Certificate Authority (CA).

The information stated in the certificate should be trusted by the receiver of the certificate if the CA is trusted.

Certificates are useful when two parties want to be able to communicate securely. By exchanging certificates they receive each others public keys and even if they do not know each other they can trust the information in the certificate if they trust the CA which signed the certificate. In the Internet community VeriSign and Thwate are two well known CAs.

Appendix D

Malicious code

Malicious code is computer code written just like any other computer program, but with the exception that it is done with malicious intent. Malicious code is usually categorized as a virus, worm or trojan horse. These are described in the following sections.

D.1 Viruses

A computer virus is a piece of code the attaches itself to, i.e. infects, program files. When an infected program file is executed the attached virus code is run. The virus can infect other program files and spread. Viruses usually require human intervention to spread, since the program file must be executed. The actions taken by the virus can be anything, including destruction of data, system performance degradation etc. The only limit is the imagination of the virus creator.

D.2 Worms

Like many other things in the history of computer science the first worm was developed at the XEROX Palo Alto Research Center in 1978 [Hil99]. It was a program used in a network experiment. The program was supposed to copy itself to hosts on the network to take advantage of unused computing power. An error in the program resulted in that the systems crashed.

Today the term worm is used to refer to a malicious program that spread from system to system. Usually it takes advantage of known software vulnerabilities and does not rely on human intervention to spread. Just like viruses worms can be created to cause various problems.

D.3 Trojan horses

A trojan horse is a disguised malicious computer program. It deceives the user by pretending to perform a useful function, but is actually performing some malicious task in the background. This may include collecting data about the user; like passwords and credit card information.

D.4 Blended threats

A blended threat is malicious code which takes advantage of the different characteristics described for viruses, worms and trojan horses. It is powerful since it takes advantage of different technologies and uses multiple methods to spread.

Bibliography

[And01] Ross J. Anderson. *Security Engineering - A Guide to Building Dependable Distributed Systems.* John Wiley & Sons, Inc., USA, 2001. ISBN: 0-471-38922-6.

[ats03] @stake LC 4 - The Password Recovery and Auditing Application, 2003. http://www.atstake.com/products/lc/.

[BBC00] BBC News - EU probes Echelon, July 2000. http://news.bbc.co.uk/1/hi/world/europe/820352.stm.

[Bel99] Steven M. Bellovin. Distributed firewalls. *Login Magazine*, pages 37–39, November 1999. http://www.research.att.com/~smb/papers/distfw.html.

[CBR03] William R. Cheswick, Steven M. Bellovin, and Aviel D. Rubin. *Firewalls and Internet Security - Repelling the Wily Hacker.* Addison-Wesley, USA, second edition, 2003. ISBN: 0-201-63466-X.

[CER03a] CERT Advisory CA-2003-21 W32/Blaster worm, August 2003. http://www.cert.org/advisories/CA-2003-20.html.

[CER03b] CERT/CC. *Overview Incident and Vulnerability Trends*, May 2003. http://www.cert.org/present/cert-overview-trends/.

[cir03] Default passwords, 2003. http://www.cirt.net/cgi-bin/passwd.pl.

[Cis03a] VPN IPSec virtual private networks in depth, 2003. Cisco Systems SAFE White paper, http://www.cisco.com/go/safe.

[Cis03b] Wireless LAN Security in Depth, 2003. Cisco Systems SAFE White paper, http://www.cisco.com/go/safe.

[Eco03] Ecora Patch Manager, 2003. http://www.ecora.com/ecora/products/patchmanager.asp.

[eth03] The Ethereal Network Analyzer, December 2003. http://www.ethereal.com.

[EUR03] EUROPOL, Hague, Netherlands. *2003 EU Organised Crime Report - Open Version*, October 2003. File number: 2530-132, http://www.poliziadistato.it/pds/primapagina/europol/english_version.pdf.

[F-S03a] F-Secure Computer Virus Information Pages: Bugbear.B, June 2003. http://www.f-secure.com/v-descs/bugbear_b.shtml.

[F-S03b] F-Secure Computer Virus Information Pages: Deloder, March 2003. http://www.f-secure.com/v-descs/deloader.shtml.

[FE97] B. Fraser Ed. *Site Security Handbook*, September 1997. RFC 2196.

[Fed04] Federal Computer Incident Response Center. *Incident-related Statistics*, 2004. http://www.fedcirc.gov/incidentAnalysis/incidentStatistics.html.

[Hil99] Michael A. Hiltzik. *Dealers of Lightning - XEROX Parc and the Dawn of the Computer Age*. Harper Business, New York, USA, 1999. ISBN: 0-88730-989-5.

[HPV$^+$99] K. Hamzeh, G. Pall, W. Verthein, J. Taarud, W. Little, and G. Zorn. *Point-to-Point Tunneling Protocol (PPTP)*, July 1999. RFC 2637.

[IBM99] Layer 2 Tunneling Protocol (L2TP) Overview, 1999. http://www-1.ibm.com/servers/eserver/iseries/tcpip/vpn/redbooks/l2tppres/pdf/l2tppres.pdf.

[IEE04] IEEE Standards "Get IEEE 802"(TM): Wireless (IEEE 802.11), January 2004. http://standards.ieee.org/getieee802/802.11.html.

[IET04] IP security protocol (ipsec) charter, February 2004. http://www.ietf.org/html.charters/ipsec-charter.html.

[KA98a] S. Kent and R. Atkinson. *IP Encapsulating Security Payload (ESP)*, November 1998. RFC 2406.

[KA98b] S. Kent and R. Atkinson. *Security Architecture for the Internet Protocol*, November 1998. RFC 2401.

[key03] Ghost Keylogger, 2003. http://www.keylogger.net.

[Mai03] Søren Maigaard. Undersøgelse af datasikkerhed i forbindelse med hjemmearbejdspladser i danmark. Master's thesis, Technical University of Denmark, Lyngby, Denmark, 2003. IMM-THESIS-2003-41, ISSN 1601-233X, http://www.imm.dtu.dk/pubdb/views/publication_details.php?id=2529.

[Mic99] Virtual Private Networking in Windows 2000: An Overview, 1999. Microsoft Corporation White paper, http://www.microsoft.com/windows2000/docs/VPNoverview.doc.

[Mic03a] How to Enable NTLM 2 Authentication, May 2003. KB239869, http://support.microsoft.com/default.aspx?scid=kb;en-us;239869.

[Mic03b] How to Prevent Windows from Storing a LAN Manager Hash of Your Password in Active Directory and Local SAM Databases, October 2003. KB299656, http://support.microsoft.com/default.aspx?scid=kb;en-us;299656.

[Mic03c] L2TP/IPSec NAT-T Update for Windows XP and Windows 2000, February 2003. http://support.microsoft.com/default.aspx?scid=kb;en-us;818043.

[Mic03d] Microsoft Baseline Security Analyzer V1.2, 2003. http://www.microsoft.com/technet/security/tools/mbsahome.asp.

[Mic03e] Microsoft Security Bulletin MS03-026, July 2003. http://www.microsoft.com/technet/security/bulletin/MS03-026.asp.

[Mic03f] Trustworthy Computing, September 2003. Microsoft Corporation White paper, http://www.microsoft.com/mscorp/innovation/twc/twc_whitepaper.asp.

[Mic03g] Virtual Private Networking with Windows Server 2003: Overview, 2003. Microsoft Corporation White paper, http://www.microsoft.com/windowsserver2003/techinfo/overview/vpnover.mspx.

[mon01] Dsniff, 2001. http://monkey.org/˜dugsong/dsniff/.

[MSK03] Stuart McClure, Joel Scambray, and George Kurtz. *Hacking Exposed - Network Security Secrets & Solutions*. McGraw-Hill/Osborne, USA, fourth edition, 2003. ISBN: 0-07-222742-7.

[NBC03] Risks and Security: Security from External Threats. TV, 2003. CNBC Europe: Advantage Technology - Programme 6.

[Net96] Netscape Communications Corporation. *SSL 3.0 Specification*, November 1996. http://www.netscape.com/eng/ssl3/.

[NIS03a] National ICT Security and Emergency Response Centre. *Incident Statistics 2003*, December 2003. http://www.niser.org.my/statistics.html.

[NIS03b] National Institute of Standards and Technology. *ICAT Vulnerability Statistics*, September 2003. http://icat.nist.gov/icat.cfm?function=statistics.

[phe03] Default password list, December 2003. http://www.phenoelit.de/dpl/dpl.html.

[Pos81] J. Postel. *Internet Control Message Protocol*, September 1981. RFC 792.

[Pow00] Richard Power. *Tangled Web - Tales of Digital Crime from the Shadows of Cyberspace*. Que Corporation, USA, 2000. ISBN: 0-7897-2443-X.

[PTS03a] Post- och telestyrelsen. *Bredband i Sverige, 2003 - Tillgänglighet till IT-infrastruktur med hög överföringskapacitet*, August 2003. PTS-ER-2003:27, ISSN 1650-9862, http://www.pts.se/Archive/Documents/SE/BredbandiSverige2003_27.pdf.

[PTS03b] Post- och telestyrelsen. *Uppkopplad Nr 2/2003*, 2003. http://www.pts.se/internetsakerhet/Archive/Documents/SE/Uppkopplad_2_2003.pdf.

[RMK+96] Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, and E. Lear. *Address allocation for private internets*, February 1996. RFC 1918.

[SAN03] SANS Institute. *The Twenty Most Critical Internet Security Vulnerabilities*, October 2003. Version 4.0, http://www.sans.org/top20/top20.pdf.

[SE94] W. Simpson Ed. *The Point-to-Point Protocol (PPP)*, July 1994. RFC 1661.

[SE01] P. Srisuresh and K. Egevang. *Traditional IP Network Address Translator (Traditional NAT)*, January 2001. RFC 3022.

[SGF02] Gary Stoneburner, Alice Goguen, and Alexis Feringa. *Risk Management Guide for Information Technology Systems.* National Institute of Standards and Technology, 2002. Special publication 800-30.

[SM98] B. Schneier and Mudge. Cryptanalysis of Microsoft's Point-to-Point Tunneling Protocol (PPTP). In *Procceedings of the 5th ACM Conference on Communications and Computer Security*, pages 132–141. ACM Press, November 1998. http://www.schneier.com/paper-pptp.html.

[SM01] Joel Scambray and Stuart McClure. *Hacking Exposed Windows 2000 - Network Security Secrets & Solutions.* McGraw-Hill/Osborne, USA, 2001. ISBN: 0-07-219262-3.

[SMW99] Bruce Schneier, Munge, and David Wagner. *Cryptanalysis of Microsoft's PPTP Authentication Extensions (MS-CHAPv2)*, 1999. http://www.schneier.com/paper-pptpv2.html.

[sno04] SNORT - The Open Source Network Intrusion Detection System, 2004. http://www.snort.org/.

[Sto88] Clifford Stoll. Stalking the wily hacker. In *Communications of the ACM*, volume 31, issue 5, pages 484–497, New York, USA, May 1988. ACM Press. ISSN: 0001-0782.

[Sto00] Clifford Stoll. *The Cuckoo's Egg - Tracking a Spy Through the Maze of Computer Espionage.* Pocket Books, USA, 2000. ISBN: 0-7434-1146-3.

[Tel03] Telia blockerar datorer som skickar spam, November 2003. http://presstjanst.telia.se/press/pressrelease_print.jsp?article=3696.

[Tri04] Tripwire, 2004. http://www.tripwire.com.

[Wat03] WatchGuard VPN guide - WatchGuard Firebox system, 2003. http://www.watchguard.com/help/docs/v62VPNGuide.pdf.

[WCP02] John Wack, Ken Cutler, and Jamie Pole. *Guidelines on Firewalls and Firewall Policy.* National Institute of Standards and Technology, 2002. Special publication 800-41.

[zon04] Zone Labs, January 2004. http://www.zonelabs.com/store/content/home.jsp.