The State of Home Computer Security

Examensarbete utfört i Informationsteori
vid Tekniska Högskolan i Linköping
av

Ulf Frisk
Semir Drocić

Reg nr: LiTH-ISY-EX--04/3565--SE
Linköping 2004
The State of Home Computer Security

Examensarbete utfört i Informationsteori
vid Tekniska Högskolan i Linköping

av

Ulf Frisk
Semir Drocić

Reg nr: LiTH-ISY-EX--04/3565--SE

Supervisor: Viiveke Fåk
Examiner: Viiveke Fåk

**Title**: The State of Home Computer Security

**Author**: Ulf Frisk, Semir Drocic

**Abstract**: Hundreds of millions of people use their home computers every day for different purposes. Many of them are connected to the Internet. Most of them are unaware of the threats or do not know how to protect themselves. This unawareness is a major threat to global computer security. This master thesis starts by explaining some security related terms that might be unknown to the reader. It then goes on by addressing security vulnerabilities and flaws in the most popular home computer operating systems. The most important threats to home computer security are reviewed in the following chapter. These threats include worms, email worms, spyware and trojan horses. After this chapter some possible solutions for improving home computer security are presented. Finally this master thesis contains a short user survey to find out what the problems are in the real world and what can be done to improve the current situation.

**Keyword**: home computer security, worm, spyware, phishing, trojans
Abstract

Hundreds of millions of people use their home computers every day for different purposes. Many of them are connected to the Internet. Most of them are unaware of the threats or do not know how to protect themselves. This unawareness is a major threat to global computer security.

This master thesis starts by explaining some security related terms that might be unknown to the reader. It then goes on by addressing security vulnerabilities and flaws in the most popular home computer operating systems. The most important threats to home computer security are reviewed in the following chapter. These threats include worms, email worms, spyware and trojan horses. After this chapter some possible solutions for improving home computer security are presented. Finally this master thesis contains a short user survey to find out what the problems are in the real world and what can be done to improve the current situation.

Keywords:  home computer security, worm, spyware, phishing, trojans
Acknowledgment

We wish to thank our supervisor and examiner associate prof. Viiveke Fäk for smart advices and inspiring comments on our work. We improved our knowledge in the home computer security area a lot during this work. We believe that this area of computer science will become significantly more important in the future.

We also wish to thank the persons who took part in our small user survey. Their collaboration was very important for this thesis.
# Contents

1 Introduction ................................. 1
   1.1 Delimitations ................................ 2
   1.2 Methods and sources ....................... 2
   1.3 Glossary .................................. 2
   1.4 Notations ................................ 3

2 Security related terms ...................... 5
   2.1 Security related terms ................... 6
   2.2 Abbrevations ................................ 21

3 The Home Computer .............................. 23
   3.1 Relevant operating systems ................. 24
   3.2 Case study: Windows XP Home Edition .......... 25
      3.2.1 Initial vulnerabilities .................. 25
      3.2.2 Windows Update ......................... 25
      3.2.3 Access control .......................... 26
      3.2.4 Hidden file extensions .................. 27
      3.2.5 Email settings .......................... 27
      3.2.6 Internet Explorer ....................... 27
      3.2.7 Other services and aspects ............... 28
   3.3 Case study: Windows 98 Second Edition .......... 30
      3.3.1 Initial vulnerabilities .................. 30
      3.3.2 Windows Update ......................... 31
      3.3.3 Access control .......................... 31
      3.3.4 Hidden file extensions .................. 31
      3.3.5 Email settings .......................... 32
      3.3.6 Internet Explorer ....................... 32
      3.3.7 Other services and aspects ............... 32
   3.4 Recent vulnerabilities ..................... 32
      3.4.1 RPC-DCOM: one month from patch to attack 32
      3.4.2 The messenger service ................... 33
      3.4.3 Internet Explorer ....................... 34
      3.4.4 Application programs .................... 35
Chapter 1

Introduction

"If GM had kept up with the technology like the computer industry has, we would all be driving $25.00 cars that got 1,000 miles to the gallon." - Bill Gates, co-founder of Microsoft Corp.

When IBM introduced their first Personal Computer, PC, in the beginning of the eighties no one could believe that the development of computer technology would progress so fast as it has done in the past 20 years. No one thought that 20 years later there would be a PC in almost every home, and that they all would be interconnected. During these 20 years several big breakthroughs in computer technology helped ordinary people to change their opinion about computers. Graphical user interfaces, the Internet and web browsers helped change the public opinion that a computer was something sold by IBM that had to be serviced by an army of engineers in white smocks.

In the middle of the nineties personal computers had become easy enough to use for ordinary people thanks to new Windows versions. This together with frequent price cuts and the ever expanding Internet helped spark the interest of many ordinary people. In several countries tax cuts for home computers further helped to spark this interest. It became trendy to own a computer. Today there exists a computer in almost every home in developed countries, and even though the less developed world are still far behind computerization is increasing fast.

The huge amount of home computers and the massive Internet usage has improved the information flow in various ways. People now have access to the information they need around the clock and can electronically communicate with people around the world. It is hard to list all the benefits, but there are also some important problems that needs to be addressed. Ordinary people has basically unwillingly become system administrators of their own home computers. Most of them don’t have any basic knowledge on how to protect their computers from the ever increasing threats on the Internet. Malicious code writers use the Internet to launch various attacks on computer systems around the world. Organized crime uses the Internet to steal important information such as credit card numbers. Shady corporations install programs that monitor surfing patterns without
the knowledge of the users.

What is the state of home computer security today? Which are the most important threats against home computer users today? What can be done to improve the current situation? These are the questions that this thesis will try to answer.

1.1 Delimitations

This thesis will focus on the home computer users, security vulnerabilities in the most common operating systems and applications of today, different kinds of threats against the home computers such as worms and spyware. The thesis will also try to recommend some measures in order to improve home computer security in the future.

This thesis will not focus on issues related to physical security such as thefts and hardware failures, nor issues related to wireless connectivity, telecommuting and corporate laptops used at home. Security problems related to future not yet mainstream technology such as Internet connected consumer electronics has also been left out on purpose. One other important topic that won’t be addressed in this thesis is the spam problem.

1.2 Methods and sources

This area of computer security differs from the traditional science in that sense that results are often presented in non traditional ways. Scientific results in other areas are often presented in papers at scientific conferences. Computer security related results are often presented in a more informal way on the Internet. There are special sites and mailing lists for security professionals. The press is also interested in these issues because worm and virus attacks are interesting for a lot of people nowdays.

The basic knowledge needed to complete this thesis was acquired from associate prof. Viiveke Fäk’s courses in computer security and cryptology. Further on, the information needed was mainly to be found on the Internet. One of the organizations that offers a lot of security related information is CERT [3]. A short user survey was also conducted which produced several interesting results.

1.3 Glossary

The most important terms that might be unfamiliar to the readers are listed below, a more comprehensive list is found in Chapter 2.
1.4 Notations

Phishing
Phishing is the act of luring sensitive information, such as passwords and financial data, from a victim by masquerading as someone trustworthy with a real need for such information.

Spyware
A software that gathers information about a computer user without the user’s knowledge or informed consent, and then transmits this information to an external third party such as an organisation that expects to be able to profit from it in some way.

Virus
A self-replicating and propagating program, usually operating with some form of input from the user, although generally the user is unaware of the intent of the virus. Often considered to be a self-propagating trojan horse, composed of a mission component, a trigger component, and a self-propagating component.

Worm
A self-reproducing program which is distinguished from a virus by copying itself without being attached to a program file, or which spreads over computer networks, particularly via email.

1.4 Notations
The notations [MS0x-xxx] and [bid: xxxx] are commonly used throughout the thesis. The first notation denotes a Microsoft security patch id. For more information what these individual patches contain please visit Microsoft’s web site [6]. The second notation denotes a bugtraq id. Bugtraq is a database that contains information about known vulnerabilities, which can be found at SecurityFocus [20].
Introduction
Chapter 2

Security related terms

Home computer security is a very important topic for all computer users, but many complicated terms are used in texts when discussing this subject. This makes it very hard for the layman to understand the information published by various security vendors. For some people the published information becomes so complicated to read, because of all the unfamiliar terms, that they abstain from reading it altogether.

This chapter contains a list of important security related terms, terms that are used in the thesis and other terms that are important from a general point of view. This chapter also contains explanations of abbreviations commonly used throughout the thesis.
2.1 Security related terms

Abuse of Privilege
When a user performs an action that they should not have, according to organizational policy or law.

Access
The ability to enter a secured area. The process of interacting with a system. Used as either a verb or a noun.

Access Authorisation
Permission granted to users, programs or workstations.

Access Control
A set of procedures performed by hardware, software and administrators to monitor access, identify users requesting access, record access attempts, and grant or deny access.

Access Sharing
Permitting two or more users simultaneous access to file servers or devices.

Administrative Domain
An environment or context defined by a security policy, security model, or security architecture.

Administrator
An individual who:
* Oversees the operation of a network.
* Is responsible for installing programs on a network and configuring them for distribution to workstations.
* May also update security settings on workstations.

Alarm
A sound or visual signal triggered by an error condition.

Alert
An automatic notification that an event or error has occurred.

Alertable Event
Any event or member of an event set configured to trigger an alert.

Anti-virus
A software that is used to prevent and remove infections from a computer system.
2.1 Security related terms

Asset
A physical item, informational item, or capability required by an organization to maintain productivity. Examples include computer systems, customer databases, and assembly lines.

Asset Measure
A quantitative measurement of an asset. The asset measure is the confidentiality, integrity, and availability of an asset in relation to other assets in an organization.

Asset Value
The perceived or intrinsic worth of an asset.

Asymmetric encryption
A cryptographic system that uses two keys, a public key known to everyone and a private key known only to the recipient of the message. When Alice wants to send a secure message to Bob, she uses Bob’s public key to encrypt the message. Bob then uses his private key to decrypt it. An example of a commonly used algorithm is the RSA algorithm. Also see public key, private key.

Attack Signature
The features of network traffic, either in the heading of a packet or in the pattern of a group of packets, which distinguish attacks from legitimate traffic.

Audit
The independent collection of records to access their veracity and completeness.

Audit Trail
An audit trail may exist on paper or on disk. In computer security systems, a chronological record of when users log in, how long they were engaged in various activities, what they were doing and whether any actual or attempted security violations occurred.

Authentication
The process of establishing the legitimacy of a node or user before allowing access to requested information. During the process, the user enters a name or account number (identification) and password (authentication).

Authorisation
The process of determining what kind of activities are permitted. Usually, authorization is in the context of authentication. Once you have authenticated a user, the user may be authorized different kinds of access or activity.
Back Door
An entry point to a program or a system that is hidden or disguised, often created by the software’s author. A certain sequence of control characters permits access to the system manager account. If the back door becomes known, unauthorized users (or malicious software) can gain entry and cause damage.

Bastion Host
A system that has been hardened to resist attack at some critical point of entry, and which is installed on a network in such a way that it is expected to come under attack. Bastion hosts are often components of firewalls, or may be "outside" web servers or public access systems. Generally, a bastion host is running some form of general purpose operating system (e.g., Linux, VMS, Windows NT, etc.) rather than a ROM-based or firmware operating system.

Black Hat
Communities or individuals who either attempt to break into computer systems without prior authorization, or who explore security primarily from an attack perspective. The term originates from old American western genre movies where the "good guys" always wore white hats and the "bad guys" always wore black.

Bug
A programming error in a software program that can have unwanted side effects.

Callback
A security feature that lets a host disconnect a remote caller after a successful connection and then recall the remote computer, either for security verification or financial responsibility.

Certificate
Cryptographic systems use this file as proof of identity. It contains a user’s name and public key.

Certificate Authority
An office or bureau that issues security certificates.

Certificate Store
A database that contains security certificates.

Computer Security
Technological and managerial procedures applied to computer systems to ensure the availability, integrity and confidentiality of information managed by the computer system.
2.1 Security related terms

**Computer Security Audit**
An independent evaluation of the controls employed to ensure appropriate protection of an organization’s information assets.

**Content Filtering**
A subcategory of a security policy that pertains to the semantic meaning of words in text (such as email messages). It can also include URL filtering and other contents such as disturbing pictures and movies.

**Data Driven Attack**
A form of attack in which the attack is encoded in innocuous-seeming data which is executed by a user or other software to implement an attack. In the case of firewalls, a data driven attack is a concern since it may get through the firewall in data form and launch an attack against a system behind the firewall.

**Defence in Depth**
The security approach whereby each system on the network is secured to the greatest possible degree. May be used in conjunction with firewalls.

**Direct Action Virus**
A virus that immediately loads itself into memory, infects other files, and then unloads itself from memory.

**DNS Spoofing**
Assuming the Domain Name System (DNS) name of another system by either corrupting the name service cache of a victim system, or by compromising a domain name server for a valid domain.

**Dropper**
A program, not itself infected, that will install a virus on a computer system. Virus authors often use droppers to seed their creations in the wild, particularly in the case of boot sector infectors. The term injector may refer to a dropper that installs a virus only in memory.

**Email Bomb**
Code that when executed sends many messages to the same address for the purpose of using up disk space and/or overloading the email or web server.

**Encrypted Virus**
A virus using encryption to hide itself from virus scanners. That is, the encrypted virus jumbles up its program code to make it difficult to detect.
Encryption
A method of scrambling or encoding data to prevent unauthorized users from reading or tampering with the data. Only individuals with access to a password or key can decrypt and use the data. The data can include messages, files, folders, or disks.

Exploit
A program or technique that takes advantage of software vulnerabilities that can be used for breaking security, or otherwise attacking hosts over the network.

Exposure
An exposure is a state in a computing system (or set of systems) which is not a universal vulnerability, but either:
* Allows an attacker to conduct information gathering activities.
* Allows an attacker to hide activities.
* Includes a capability that behaves as expected, but can be easily compromised.
* Is a primary point of entry that an attacker may attempt to use to gain access to the system or data.
* Is considered a problem according to some reasonable security policy.

False Negative
False negative can be used in several different contexts. When used in biometrics it refers to when a user is denied access when the user should have been granted access. There are two types of false reports from anti-virus software. A false negative report is when an anti-virus software reports no viral activity or presence, when there is a virus present. References to false negatives are usually only made in technical reports. Most people simply refer to an anti-virus program "missing" a virus. A false negative is more generally known in the security community as a false acceptance (except for biometrics were it is known as a false rejection), or a Type II error.

False Positive
False positive can be used in several different contexts. When used in biometrics it refers to when a user is granted access when the user should have been denied access. The second kind of false report that an anti-virus software can make is to report the activity or presence of a virus when there is, in fact, no virus. False positive has come to be very widely used among those who know about viral and anti-virus programs. Very few use the analogous term, "false alarm." A false positive is more generally known in the security community as a false rejection (except for biometrics were it is known as a false acceptance), or a Type I error.

Firewall
A system or combination of systems that enforces a boundary between two or more networks.
2.1 Security related terms

Flooding Programs
Code which when executed will bombard the selected system with requests in an effort to slow down or shut down the system.

Front-end Security Filter
A security filter, which could be implemented in hardware or software, that is logically separated from the remainder of the system to protect the system’s integrity.

Gateway
A bridge between two networks.

Global Security
The ability of an access control package to permit protection across a variety of mainframe environments, providing users with a common security interface to all.

Guard
A processor that provides a filter between two disparate systems operating at different security levels or between a user terminal and a data base to filter out data that the user is not authorized to access.

Hack
Any software in which a significant portion of the code was originally another program.

Hacker
An individual who intends to enter an environment to which he or she is not entitled to enter. This can be done for various purposes (entertainment, profit, theft, prank, etc.).

Hijacking
An attack whereby an active, established, session is intercepted and used by an attacker.

Hoax
A chain letter that usually spreads a false virus warning. More information about hoaxes can be found in section 4.2.

Host-based Security
The technique of securing an individual system from attack. Host-based security is operating system and version dependent.

Hot Standby
A backup system configured in such a way that it may be used if the system goes down.
Hybrid Gateways
An unusual configuration with routers that maintain the complete state of the TCP/IP connections or examine the traffic to try to detect and prevent attack. Hybrid gateways are often complicated and are therefore hard to maintain and audit.

Identification
The process that enables recognition of an entity by a system, generally by the use of unique machine readable user names.

Insider Attack
An attack originating from inside a protected network. Insider attacks are usually performed by an employee.

Internet Worm
Also known as the UNIX Worm after the operating system it used, or the Morris Worm after the author, or, very specifically, the Internet/Morris/UNIX Worm, or sometimes simply the Worm, as the only one to be so capitalized. Launched in November of 1988, it spread to some three to four thousand machines connected to the Internet, wasting CPU cycles and clogging mail spools. It affected mail traffic on the Internet as a whole for a few days and is probably the most widely known worm to the general public prior to Melissa, Loveletter, Code Red, Blaster, Mydoom...

Intrusion Detection
Detection of break-ins or break-in attempts either manually or via software expert systems that operate on logs or other information available on the network.

IP Sniffing
The act of reading IP packets on the network not intended for the sniffer. This can be used to steal unencrypted passwords sent over the network.

IP Splicing
An attack whereby an active, established, session is intercepted and co-opted by the attacker. IP Splicing attacks may occur after an authentication has been made, permitting the attacker to assume the role of an already authorized user. Primary protections against IP Splicing rely on encryption at the session or network layer.

IP Spoofing
An attack whereby a system attempts to illicitly impersonate another system by using its IP network address.

Joke
A program with annoying or funny functionality. Jokes are not destructive.
2.1 Security related terms

Kerberos
A single sign-on system that uses symmetric key encryption via a ticket-oriented mechanism.

Key
Data used in cryptosystems to perform encryption. Sometimes called a cryptovariable.

Key Length
Since most modern encryption algorithms are mathematically based, the length of keys is a major determining element in the strength of an algorithm, or the work factor involved in breaking a cryptographic system.

Key Management
The process of handling and controlling cryptographic keys and related material (such as initialization values) during their life cycle in a cryptographic system, including ordering, generating, distributing, storing, loading, escrowing, archiving, auditing and destroying the material.

Key Pair
In an asymmetric encryption system, a private, or confidential, key and its (mathematically) related public key. See also private key, public key.

Key Space
The range of possible values of a cryptographic key, or the number of distinct transformations supported by a particular cryptographic algorithm. Key space is actually a better determinant of cryptographic strength than simple key length.

Keyed Hash
A cryptographic hash or digest in which the mapping to a hash result is varied by a second input parameter that is a cryptographic key. If the input data object is changed, a new hash result cannot be correctly computed without knowledge of the secret key. Thus, the secret key protects the hash result so it can be used as a checksum even when there is a threat of an active attack on the data.

Kit
Usually used to refer to a program used to produce a virus from a menu or a list of characteristics. Use of a virus kit involves no skill on the part of the user. Fortunately, most virus kits produce easily identifiable code. Packages of anti-virus utilities are sometimes referred to as tool kits, occasionally leading to confusion of the terms.
Known-plaintext Attack
Cryptanalysis technique in which the analyst tries to determine the key from knowledge of some plaintext- ciphertext pairs, although the analyst may also have other clues, such as the knowing the cryptographic algorithm.

Least Privilege
Designing operational aspects of a system to operate with a minimum amount of system privilege. This reduces the authorization level at which various actions are performed and decreases the chance that a process or user with high privileges may be caused to perform unauthorized activity resulting in a security breach.

Logging
The process of storing information about events that occurred. Events that are usually logged are log-ins, session durations, break-in attempts, etc.

Logic Bomb
A resident computer program that triggers the perpetration of an unauthorized act when particular states of the system are realized. This may be a section of code, pre-programmed into a larger program, which waits for some trigger event to perform some damaging function. A virus may contain a logic bomb as a payload. Logic bombs which trigger on time events are sometimes known as time bombs.

Log Processing
How audit logs are processed, searched for key events, or summarized.

Loophole
An error of omission or oversight in software or hardware that permits circumventing the system security policy.

Macro Virus
A macro is a small piece of program code in a simple language, used to perform a simple, repetitive function. Microsoft’s VBA macro language can include macros in data files, and has sufficient functionality to write complete viruses. Macro viruses therefore broke the long-held belief that viruses only infected executable files, and that data files were safe. Script viruses are similar in that they contain their own source code, although a macro virus is embedded in the data file, and a script virus is generally a standalone object.

Malware
Malware (contraction of "malicious software") is software developed for the purpose of doing harm. Such software includes but is not limited to: worms, spyware and trojans.
2.1 Security related terms

**Memory Resident Virus**
A virus that stays in memory after it executes and infects other files when certain conditions are met. In contrast, non-memory resident viruses, called direct action, are active only while an infected application runs.

**Multilevel Secure**
A class of systems containing information with different sensitivities that simultaneously permits access by users with different security clearances and needs-to-know. It prevents users from obtaining access to information for which they lack authorization.

**Network-Level Firewall**
A firewall in which traffic is examined at the network protocol packet level.

**Network Worm**
A program or command file that uses a computer network as a means for adversely affecting a system’s integrity, reliability or availability. A network worm may attack from one system to another by establishing a network connection. It is usually a self-contained program that does not need to attach itself to a host file to infiltrate network after network.

**Nonrepudiation**
A property of a system or service that provides protection against false denial of involvement in a communication.

**One-time Pad**
An encryption system based on a series of keys, each of which is used only once. Given certain limits on the length of the key in relation to the length of the message, and the use of a secure channel for transmission of the pad, one-time pads are considered unbreakable.

**One-time Password**
In network security, a password issued only once as a result of a challenge-response authentication process. Cannot be “stolen” or reused for unauthorized access.

**Operating system**
The layer of software that sits between a computer and an application, such as an accounting system or email program. Examples of common operating systems are Microsoft Windows and Linux.

**Orange Book**
The Department of Defense trusted computer system evaluation criteria. It provides information to classify computer systems, defining the degree of trust that may be placed in them.
Password
A secret code assigned to a user as known by the computer system. Knowledge of the password associated with the user ID is considered proof of authorization.

Perimeter-based Security
The technique of securing a network by controlling access to all entry and exit points of the network.

PIN
In computer security, a personal identification number used during the authentication process. Known only to the user.

Policy
Organizational-level rules governing acceptable use of computing resources, security practices, and operational procedures.

Polymorphic
Pertaining to techniques that use some system of changing the form of a virus on each infection to try to avoid detection by signature scanning software.

Port Scan
An attack that sends client requests to a range of server port addresses on a host, with the goal of finding an active port and exploiting a known vulnerability of that service.

Private Key
In encryption a two-key system in which the key used to unlock data that has been encrypted with the public key. Also see asymmetric encryption, public key.

Proxy
1) A method of replacing the code for service applications with an improved version that is more security aware. Preferred method is by "service communities", i.e. Oracle, rather than individual applications. Evolved from socket implementations. 2) A software agent that acts on behalf of a user. Typical proxies accept a connection from a user, make a decision as to whether or not the user or client IP address is permitted to use the proxy, perhaps does additional authentication, and then completes a connection on behalf of the user to a remote destination.

Public Key
In encryption a two-key system in which the key used to lock data is made public, so everyone can "lock." A second private key is used to unlock or decrypt. Also see asymmetric encryption, private key.
2.1 Security related terms

Reference Monitor
An access control concept that refers to an abstract machine that mediates all accesses to objects by subjects.

Risk Analysis
The analysis of an organization's information resources, existing controls and computer system vulnerabilities. It establishes a potential level of damage in dollars and/or other assets.

Rogue Program
Any program intended to damage programs or data. Encompasses malicious trojan horses.

RSA
A public key cryptosystem named by its inventors, Rivest, Shamir and Adelman, who held the patent.

Sandbox
A security model providing that code or programs from untrusted sources can be run in an environment that restricts potentially dangerous activities and functions. Originally arising from and applied to the Java language applet system, it may now refer also to the general concept.

Scanner
1) A program which reads the contents of a file looking for code known to exist in specific virus programs. 2) In network situations, a program which examines computers and network systems examining configurations and looking for security vulnerabilities. This type of program can be used by both defenders and attackers. SATAN (Security Administrators Tool for Analysing Networks) is an example of this type of scanner.

Screened Host Gateway
A host on a network behind a screening router. The degree to which a screened host may be accessed depends on the screening rules in the router.

Screened Subnet
An isolated subnet created behind a screening router to protect the private network. The degree to which the subnet may be accessed depends on the screening rules in the router.

Screening Router
A router configured to permit or deny traffic using filtering techniques; based on a set of permission rules installed by the administrator. A component of many firewalls usually used to block traffic between the network and specific hosts on an IP port level. Not very secure; used when "speed" is the only decision criteria.
Security by Obscurity
A term used, usually perjoratively, to refer to the practice of attempting to secure a system by failing to publish information about it. This is done in the hope that nobody will be able to figure out how it works.

Smart Card
A device with embedded microelectronics circuitry for storing information about an individual. This is not a key or token, as used in the remote access authentication process.

Social Engineering
An attack based on deceiving users or administrators at the target site. Social engineering attacks can be carried out by telephoning users or operators and pretending to be an authorized user, to attempt to gain illicit access to systems. More information about social engineering can be found in Kevin Mitnick’s book [19].

Spam
Indiscriminately sent unsolicited, unwanted, irrelevant, or inappropriate messages, especially commercial advertising in mass quantities. In sufficient volume, spam can cause denial of service.

Spim
Spim is to Instant Messaging (IM) what spam is to emailing. Unsolicited advertisements, usually sent in bulk to IM users.

Stealth Virus
A virus that hides itself by intercepting disk access requests. When an anti-virus program tries to read files or boot sectors to find the virus, the stealth virus feeds the anti-virus program a clean image of file or boot sector.

Symmetric Encryption
A cryptographic system that uses one key. This single cryptographic key is used both to encrypt and decrypt the message. Also known as secret-key encryption and single-key encryption. Examples of symmetric encryption algorithms are the DES and AES algorithms.

Technical Vulnerability
A hardware, firmware, communication, or software flaw that leaves a computer system open for potential exploitation, either externally or internally, thereby resulting in risk for the owner, user, or manager of the system.
2.1 Security related terms

**Trojan Horse**
1) Any program designed to do things that the user of the program did not intend to it do or a program that disguises its harmful intent.
2) A program that installs itself while the user is making an authorized entry and then is used to break-in and exploit the system.
More information about trojan horses can be found in section 4.5.

**Two-Factor Authentication**
Authentication based on at least two of the three types: something a user knows, is, or has. In order to access a system the user must demonstrate both factors.

**Untrusted Process**
A process that has not been evaluated or examined for adherence to the security policy. It may include incorrect or malicious code that attempts to circumvent the security mechanisms.

**User**
Person or process accessing a system either by direct connections (i.e., via terminals), or indirect connections (i.e., prepared input data or receive output that is not reviewed for content or classification by a responsible individual). Considered by many experts to be the entity responsible for the greatest range of security problems.

**User ID**
A unique symbol or character string that is used by a system to identify a specific user.

**User Profile**
Patterns of a user’s activity that can be used to detect changes in normal routines.

**Virtual Private Network (VPN)**
A restricted-use, logical (i.e., artificial or simulated) computer network that is constructed from the system resources of a relatively public, physical network such as the Internet. VPNs are often constructed using encryption (located at hosts or gateways) and often by tunneling links of the virtual network across the real network.

**Virus**
A self-replicating and propagating program, usually operating with some form of input from the user, although generally the user is unaware of the intent of the virus. Often considered to be a self-propagating trojan horse, composed of a mission component, a trigger component, and a self-propagating component.
Vulnerability
A weakness in system security procedures, system design, implementation, internal controls, and so forth, that could be exploited to violate the system security policy; the possibility of an exploit or exposure to a threat, specific to a given platform.

Vulnerability Analysis
The systematic examination of systems in order to determine the adequacy of security measures, identify security deficiencies, and provide data from which to predict the effectiveness of proposed security measures.

Vulnerability Assessment
A measurement of vulnerability which includes the susceptibility of a particular system to a specific attack and the opportunities available to a threat agent to mount that attack.

Windows Script Host (WSH)
A language similar to Visual Basic for Application (VBA) and Visual Basic Script (VBScript) that will run scripts on certain Windows systems. The LoveLetter worm was a Windows script worm that used WSH.

White Hat
In an attempt to avoid debates about "good" hackers versus "bad" hackers versus "crackers" versus phone phreaks versus virus writers versus vxers, the security community has taken to describing those who attempt to explore security solely from the perspective of defence as the "white hats." The term originates from old American western genre movies where the "good guys" always wore white hats.

Worm
A self-reproducing program which is distinguished from a virus by copying itself without being attached to a program file, or which spreads over computer networks, particularly via email. More information about worms can be found in section 4.1.

Zombie
A specialized type of backdoor or remote access program designed as the agent, or client (middle layer) component of a DDoS (Distributed Denial of Service) network. Once a zombie is installed on a computer, it identifies itself to a master computer, and then waits for instructions from the master computer. Upon receipt of instructions from the master computer, a number of zombie machines will send attack packets to a target computer. Zombie may refer to the control program run to control one of the middle layer computers, or it may refer to a computer so controlled.
Zoo
Jargon reference to a set of virus programs of known characteristics used to test anti-virus software.

2.2 Abbreviations

CERT
Computer Emergency Response Team (CERT) — an organization created by DARPA after the Morris Internet worm that deals with computer security. CERT is a part of the Carnegie Mellon University. CERT is not to be confused with US-CERT which is part of the Department of Homeland Security. US-CERT stands for Computer Emergency Readiness Team. The two organisations work closely together and cross reference each other.

DCOM
Distributed Component Model (DCOM) — a protocol used in Microsoft Windows to enable software components to communicate over the network.

DDoS
Distributed Denial of Service (DDoS).

DoS
Denial of Service (DoS).

FBI
Federal Bureau of Investigation (FBI) — the United States federal bureau of investigation.

ICF
Internet Connection Firewall (ICF) — the built in firewall in Microsoft Windows XP.

ISP
Internet Service Provider (ISP).

IIS
Internet Information Server (IIS) — A web server made by Microsoft.

LSASS
Local Security Authority Subsystem Service (LSASS).
NetBIOS
Network Basic Input Output System (NetBIOS) – an API that arguments the DOS BIOS by adding special functions for local area networks.

NSA
National Security Agency (NSA) — the United States national security agency.

P2P
Peer to Peer (P2P) — a technique in which no distinction is made between clients and servers, all participants are somewhat equal peers. This is different from the traditional client – server model.

RPC
Remote Procedure Call (RPC) — a protocol that one program can use to request a service from a program located in another computer without having to understand network details.

SSN
Social Security Number (SSN).

VBS
Visual Basic Script (VBS).
Chapter 3

The Home Computer

The growing use of broadband connections gives home computer users faster and "always on" access to the Internet. These home computer users are often unaware of how to protect themselves from getting successfully attacked. Broadband and "always on" connections together with security unaware users has made home computer users the prime target for recent virus and worm attacks; however it doesn’t stop with that, home computer users are also the prime target of scammers and companies with shady business practices.

This chapter will focus on the technical aspects of home computer security. It will not focus on the pure "social engineering" aspect when a user is tricked into installing a malicious program; however it is important to know that design flaws, bugs and too lax default settings is often used by attackers to trick the user into running such malicious code.

Microsoft Windows, the preferred choice of operating system among home computer users, can be configured in secure ways, but default installations are often very insecure due to bugs and lax default security settings. Home computer users without enough knowledge and interest in computers are unlikely to change default settings in Windows in order to improve their computer security. This chapter will show how such lax default security settings is the main problem from a technical point of view today.
3.1 Relevant operating systems

Figure 3.1 visualizes the ratios between operating systems used when performing searches on the Google search engine according to Google Zeitgeist [13].

A few noteworthy things are found in this statistics:

- Windows 98 is still very popular.
- Windows XP is the most popular operating system.
- Alternatives to Microsoft Windows mainly Linux and MacOS have got a very small market cap. Despite all the press Linux recently got it makes up for only 1% of the searches on Google.

The Google statistics visualizes the ratios between different operating systems used when searching on Google, not the ratios between operating systems used at home. The statistics still provides a rough estimate on which operating systems was the most popular ones at the time of writing.

The Google statistics includes both corporate users and home users. Windows 2000 was aimed primarily at the corporate market while Windows 98 was primarily aimed at the consumer market. Windows XP targets both the corporate and the consumer market. One other important observation is that Windows 98 is more often used on older computers than Windows XP. An old computer is less likely to be connected to the Internet than a new one. This leads to the conclusion that Windows 98 actually had a larger market cap than 24% when studying home computers only, while Windows 2000 had a smaller market cap than the one in Figure 3.1.

This chapter will focus on the two most common operating systems: Windows XP Home Edition and Windows 98. Windows 2000 will not be treated primarily due to the similarities with Windows XP and the corporate profile. MacOS and Linux will not be covered because of their low market cap.
3.2 Case study: Windows XP Home Edition

Windows XP Home Edition is the most popular operating system used by home computer users today. Its importance is expected to grow as old computers that are running Windows 98 are upgraded or replaced by new ones. This case study will focus on the default settings of the operating system and their importance from a user—security perspective. The reason for focusing on the default settings is that most default settings are unlikely to be changed by the end user and that they affect security maybe more than anything else.

A clean copy of Windows XP Home Edition was installed and used in this case study to examine what is good and what is not so good out of a security—user perspective.

3.2.1 Initial vulnerabilities

Windows XP Home Edition contains several remotely exploitable vulnerabilities [MS03-026, MS03-039, MS03-043, MS04-011] in its initial state. Vulnerabilities that allow an attacker to take control of the computer as soon as it is connected to the Internet or any other infected network unless special precautions are taken.

Some of these initial vulnerabilities has successfully been exploited by the Blaster and Sasser worms and their variants. The Blaster worm and its variations exploited vulnerabilities in the RPC-DCOM service [MS03-026, MS03-039] and the Sasser worm exploited a vulnerability in the LSASS service [MS04-011]. More information about the Blaster and Sasser worms can be found in section 4.1.4. The Blaster and Sasser worms are still active on the Internet. This makes Windows hard to update without getting infected since the preferred way of updating Windows is to connect to the Internet and run Windows Update.

Windows XP Home Edition also contains numerous other vulnerabilities that allow attackers to take control of the computer if the user can be tricked into visiting a specially crafted web page, or by receiving a malicious email, or by playing an audio file, or by opening a help file...

3.2.2 Windows Update

No information was given to the user that Windows needed to be updated after the installation. The user gets notifications about registering Windows and about registering a passport account for MSN Messenger, but not any security notifications. The Windows Update icon is not found in the main start menu. The user has to click on the programs submenu to find the Windows Update icon.

Windows is set to automatically download new patches from Windows Update and prompt the user when they are ready to be installed. Windows does not automatically download new patches before Service Pack 1 is installed. Service Pack 1 has to be downloaded and installed manually through Windows Update. At first the service pack was installed and the computer was restarted. No indication that there were more available patches to download were initially given, but after a
while windows had found them and reminded the user that there were new available
updates to install.

3.2.3 Access control

Windows XP and other Windows NT based operating systems utilizes Access Con-
trol Lists, ACLs to restrict or allow access to objects in the operating system. Pro-
cesses, user accounts, resources, files, directories, etc., are all objects of a certain
type according to [10]. This security model is very flexible and allows Windows
XP Professional to be configured in very secure ways.

The fine grained security model of Windows XP Professional has been sim-
plified in Windows XP Home Edition. There exists two different levels of rights
available for users: computer administrator and limited. An account with adminis-
trator privileges has access to the whole computer. An account with administrator
privileges can create and delete user accounts, install programs and delete files be-
longing to any user. A limited account can’t install most programs, can’t access
some files on the computer, can’t create and change settings in the computer that
would affect other users. By default new users are given administrator privileges.

![Figure 3.2. Available user privileges in Windows XP Home Edition.](image)

A default user is created during the installation. This default user is given
administrator privileges and is automatically logged on to the system. It is easier to
run as an administrator, since the user then has got full access to everything. This
also means that potential attackers that successfully gain access to the computer
through a program the user is running automatically gets administrator privileges.
The preferred way from a security point of view would be to give the default user
limited privileges only, but this will make things more complicated for the user.
3.2 Case study: Windows XP Home Edition

This illustrates one of the main problems of computer security today: in order to get a secure system the user has to be restricted, but if the user is restricted too much the computer isn’t usable anymore.

3.2.4 Hidden file extensions

Windows XP Home Edition hides extensions for known file types by default to make things easier for the user. This is not completely transparent to the user since the user still has to deal with file extensions in some application programs.

This weakness is often used by email worms to trick the user into opening an executable attachment. The user might receive an email containing a file with a double file extension, e.g. ILOVEYOU.TXT.VBS but will only see ILOVEYOU.TXT and open it, because text files are harmless and contain no worms... This technique of using double file extensions is commonly used by today’s email worms. The ILOVEYOU.TXT.VBS is a real example of a worm called I Love You described more in detail in section 4.1.3.

Show file extensions

It is possible for the user to enable file extensions by changing a setting in Windows Explorer. However some file extensions remain hidden even after changing this setting according to the U.S. National Security Agency (NSA) [21]. Some of these hidden file extensions might masque malicious code. These hidden file extensions are mainly different types of links including shortcuts .lnk and Internet shortcuts .url.

3.2.5 Email settings

This case study will focus on the built in email program, Outlook Express 6.0. This Outlook version offers the options: "Warn me when other applications try to send as me" and "Do not allow attachments to be saved or opened that could potentially be a virus". Both these options are enabled by default.

The first option warns the user when a program or potential worm accesses the address book or tries to send email messages through Outlook Express. Many recent email worms come with their own email engine and utilizes other sources than the address book to gather email addresses, i.e. scan the file system for email addresses.

The second option blocks potentially harmful attachments. It is best to have both these options enabled out of a security perspective. But the option to block potentially harmful attachments is pretty draconian according to the NSA [21] and they suggest that it’s possible to disable this setting and rely on perimeter defense, e.g. virus scans at the Internet Service Provider (ISP) and local anti-virus software.

Outlook Express 6.0 also uses the Internet Explorer Security Zones to determine what should be allowed to run in the emails. The default zone used by Outlook Express is the Restricted Sites Zone. The default settings in this zone is
already very conservative from a security perspective; however the NSA suggests some alterations to these settings [21]. Changing the settings according to NSA’s suggestions will counter known attacks that use active content contained within the body of the received email messages.

3.2.6 Internet Explorer

A common vector of attack is to trick the user into opening a web page that contain malicious code. In some cases when legitimate sites have been hacked it’s not even necessary to trick the user into visiting the pages. The malicious code on the web pages is then loaded on to the user’s computer using some known or unknown Internet Explorer vulnerability.

More vulnerabilities are related to Internet Explorer than any other Windows component. Chances are that Internet Explorer will contain several newfound vulnerabilities if Windows hasn’t been updated for a month or two.

It is also important to remember that Internet Explorer might open a helper program if it encounters a special file, for example Internet Explorer might open Microsoft Word inside the current window if a word file is encountered. Word might contain vulnerabilities unless it is updated. This means that an attacker can gain access to a computer if the computer user clicks on a specially crafted word file on the web.

Security holes in Internet Explorer are often used to install a special class of programs called spyware. A spyware program might report surfing habits to the program creator, serve ads the user doesn’t want to see, act as an ad-server serving ads to other users on other computers, or change the phone number on the Internet connection (if dialup is used) to an expensive pay number. More information about spyware can be found in section 4.4. Another disturbing trend is that trojans stealing information such as credit card numbers, SSNs and online banking passwords is becoming increasingly popular to install this way. More information about trojans can be found in section 4.5.

3.2.7 Other services and aspects

Windows XP Home Edition has a lot of services enabled by default. Some of them can be accessed from the network and therefore pose as a potential security threat. Some of these services make sense to have enabled in a corporate environment, but why are they enabled by default in the home edition? The Internet Connection Firewall (ICF) can block external access to these services if it is enabled. Figure 3.3 illustrates the open network ports in Windows XP Home Edition. The most targeted port by worms is port 445 (microsoft-ds in the figure), which is the entry point for both the Sasser and Blaster worms.
The Internet Connection Firewall

Windows XP Home Edition comes with a built in firewall called “Internet Connection Firewall” also known as “ICF”. This is a basic firewall that blocks incoming traffic not initiated by the computer. It successfully shields the computer against worms exploiting the RPC-DCOM and LSASS vulnerabilities; however this firewall is not enabled by default. The user has to manually enable the firewall. The firewall doesn’t protect against potentially malicious web pages that exploit security holes in Internet Explorer.

The ICF runs as a normal Windows service which means that it’s disabled during startups and shutdowns. This allows worms that use the RPC-DCOM or LSASS vulnerabilities to infect vulnerable computers when they are starting up even if the firewall setting is enabled! The firewall is enabled some time after the desktop is presented to the user.

Remote Procedure Call, RPC

Remote Procedure Call (RPC) is a protocol that programs can use to request a service from another program on the network. RPC helps with interoperability because the program using RPC does not have to understand the underlying network protocols. The RPC service is enabled by default in Windows XP Home Edition.

The RPC service in its unpatched state contains several vulnerabilities that can be used to execute malicious code. These vulnerabilities are used by the Blaster and Sasser worms described in section 4.1.4.
Messenger

The messenger service in Windows is not to be confused with MSN Messenger. The messenger service is enabled by default and allows administrators to send messages to the users using the computers.

The messenger service is vulnerable for an attack in its unpatched state that could result in a full system compromise. A patch [MS03-043] is available. More information about the messenger service is found in section 3.4.2.

System Restore Service

The system restore service backs up selected system and program files so that the system can later be restored into a previous state if something should go wrong. This is usually a desirable service, but it might back up viruses if the computer has been infected. Windows prevents external programs from accessing system restore files including anti-virus programs. Symantec recommend restarting the system restore service after a virus infection. Restarting the service will result in the deletion of old backups that might be infected. Instructions how to do this can be found on Symantec's web site [5].

3.3 Case study: Windows 98 Second Edition

Windows 98 was released on June 25, 1998\(^1\). It is a hybrid 16-bit/32-bit product just like Windows 95. Although Windows 98 was substantially larger and somewhat slower than Windows 95 it became a big success. Windows 98 SE (Second Edition) was released on June 10, 1999\(^2\). It included many minor fixes for issues in the first edition and an upgraded version of Internet Explorer.

Microsoft originally planned to stop supporting Windows 98 as early as January 16, 2004 but because of its popularity Microsoft decided to keep support running until June 30, 2006. Windows 98 accounted for 24% of the searches on Google in January, 2004. And even though its popularity is dropping due to upgrades to Windows XP, Windows 98 will continue to be one of the most popular operating systems for a long time.

In this case study a clean copy of Windows 98 SE was installed and used to examine what is good and what is not so good out of a security – user perspective.

3.3.1 Initial vulnerabilities

Windows 98 is initially vulnerable against a remote Denial of Service (DoS) attack [MS00-029]. This attack involves sending fragmented IP packets to the computer. Windows 98 does not contain any vulnerable services that can be exploited remotely to run malicious code without any user interaction.

\(^1\)U.S. release date.
\(^2\)U.S. release date.
Windows 98 contains numerous initial vulnerabilities in various parts of the operating system. These vulnerabilities can be used to execute malicious code on the computer if the user is tricked into visiting a specially crafted web page, receives an email worm or simply by opening the wrong file on a network share.

3.3.2 Windows Update

Windows Update was mentioned in some of the screens during the installation. No additional information is given after the installation that an update is needed for security reasons. Many programs and Windows components are quite old and require an upgrade. If the user chooses to upgrade to Internet Explorer 6.0 and the most recent DirectX chances are that the user will run Windows Update to upgrade these applications and components.

Windows Update needs to be run three times initially. The first run will upgrade Internet Explorer to version 6.0 and restart the computer, the second run will upgrade DirectX and restart the computer and the last run will download and apply various security fixes and restart the computer. No information is given after a restart notifying the user that the update sequence is not yet finished. The total amount of data that is downloaded is approximately 40MB.

Windows Update is not set to run automatically, and there is no setting to make it run automatically. If you use the built in scheduler to schedule a Windows Update task it merely opens up the Windows Update web site and waits for the user to click through it. There are currently no settings in Windows 98 to enable auto download and auto install of security patches. Security patches have to be downloaded by manually visiting Windows Update.

3.3.3 Access control

Windows 98 doesn’t support different levels of user privileges like Windows XP. All users and programs run with the equivalent of Windows XP’s administrator privileges. Users on the same local computer can access each others files and change settings in the operating system. Windows 98 uses the FAT and FAT32 file systems, neither of these file systems provide any security at all unlike Windows XP’s preferred file system NTFS.

3.3.4 Hidden file extensions

Windows 98 hides extensions for known file types by default to the user. This is done to make things easier for the user, just like in Windows XP Home Edition. This is discussed in the Windows XP Home Edition case study in section 3.2.4. Approximately the same things that apply to Windows XP applies to Windows 98 in this case.
3.3.5 Email settings

The built-in email client in Windows 98, Outlook Express 6.0 works in approximately the same way as the email client in Windows XP Home Edition described in section 3.2.5.

3.3.6 Internet Explorer

After running Windows update the Internet Explorer version is upgraded to version 6.0 just as in Windows XP Home Edition. Most of the problems in the Windows XP version in section 3.2.6 applies to the Windows 98 version as well, the main difference is that malicious code loaded on to the computer might do more harm to the system in Windows 98 due to the lack of security in the operating system.

3.3.7 Other services and aspects

By default, netbios is enabled on all TCP/IP connections, over the network or over dialup modems. This service has no use for the end user initially, but it listens on port 139 and poses as a potential security threat. There is no way of easily disabling netbios over TCP/IP in Windows 98.

Direct hardware access

Windows 98 allows programs to directly access the computer hardware without going through the operating system. This allows for some compatibility with old legacy MS-DOS applications but it also has undesirable side effects. This lack of protection can destabilize the operating system and be exploited by viruses destroying computer hardware. One example of this is the CIH/Cernobyl virus that attacks the flash BIOS successfully forcing the user to take the computer to a computer technician.

3.4 Recent vulnerabilities

This section will address some recent security vulnerabilities in both the Windows operating systems and in some commonly used application programs. Only recent vulnerabilities are addressed, that is vulnerabilities discovered or exploited after July 1st 2003.

3.4.1 RPC-DCOM: one month from patch to attack

Microsoft released a security bulletin and a patch [MS03-026] on July 16, 2003 to fix a vulnerability in the RPC interface that would allow an attacker to execute arbitrary code on the victims computer. This vulnerability affected all NT based operating systems including Windows 2000 and Windows XP and was remotely exploitable.
3.4 Recent vulnerabilities

The largest Swedish tabloid Aftonbladet [1] had an article about "Experts warn for hacker attack" on August 1, 2003. The article warned the readers that hackers could enter almost any computer running Microsoft Windows and that they could steal data, destroy files and spy on email messages. The article suggests that the readers should visit www.windowsupdate.com and update Windows. The article also mentions that the readers ought to have a firewall installed. This article is interesting because it shows that the public was given information about this vulnerability before the Blaster worm was released.

Shortly after the Blaster worm started to spread on August 11, 2003 it was front page news on the newspapers all over the world. On August 13 Aftonbladet had a poll on their Internet page asking whether the readers had been infected or not by the Blaster virus\(^3\). As much as 23% of the 50,000 readers that answered, answered that their computer had been infected by the Blaster virus.

The patch had been available for almost a month and 23% of the readers of Aftonbladet said they had been infected, despite the fact that major newspapers had warned about this earlier!

**The reasons for this include but are not limited to:**
1. This happened in the middle of the summer holidays.
2. The warnings in mainstream press never made it to the front page.
3. The warnings in mainstream press talked about hackers stealing information. Home computer users that don’t have any sensitive information on their computers don’t understand why a hacker would want to target their computer.
4. The default settings in Windows are not set to automatically download and install new security patches.
5. The built in firewall in Windows XP is disabled by default.

Shortly after the Blaster worm was released yet another vulnerability in the RPC-DCOM interface was discovered. A more detailed description of the actual Blaster worm and its variants can be found in section 4.1.4.

3.4.2 The messenger service

The messenger service in Windows is not to be confused with MSN Messenger. The messenger service is enabled by default and allows administrators and software to send messages to the users using the computers. It is not normally of any use for the home computer user.

The messenger service is vulnerable for an attack in its unpatched state that could result in a full system compromise. A patch is available [MS03-043]. This vulnerability is remotely exploitable like the RPC-DCOM vulnerability the Blaster worm uses.

This service has also been targeted by spammers since it allows them to send text advertisements to Windows NT, 2000 and XP systems. There are commercial

---

\(^3\)The Blaster worm is technically not a virus, that term is used here because Aftonbladet chose to use the term virus.
programs available that will allow mass messaging a large number of computer users. A user might be tricked into giving away passwords or visiting a specially crafted web page containing malicious code since this message looks and behaves like a system message. Microsoft recommends enabling the ICF and disabling the messenger service http://www.microsoft.com/windowsxp/pro/using/howto/communicate/stopspam.asp.

3.4.3 Internet Explorer

Microsoft’s Internet Explorer is the most popular browser today. Figure 3.4 clearly illustrates this. The three most popular browsers are all different versions of Internet Explorer according to Google Zeitgeist [13].

![Figure 3.4. Browsers accessing Google.](image)

Internet Explorer has shown that it’s prone to different vulnerabilities in the past. Internet Explorer has been the Windows application/component in the past with most vulnerabilities, and the list of vulnerabilities would be too long to list here together with descriptions of each vulnerability. Some of these vulnerabilities are less dangerous and might lead to a DoS attack crashing the browser, while others have been more serious – allowing execution of malicious code. Shady companies haven’t been late to exploit these Internet Explorer bugs to install spyware programs or dialers without the user’s knowledge on computers running an unpatched version of Internet Explorer.

Some recent vulnerabilities in Internet Explorer have also been exploited by scammers to trick users to give up their passwords or credit card numbers by making the computer user believe they are visiting the real page, such as www.paypal.com
3.4 Recent vulnerabilities

or www.ebay.com. This type of attack is called phishing. More information about phishing attacks can be found in section 4.3.

It is important to understand that other browsers also contain vulnerabilities, but the combination of the most used browser and new fresh vulnerabilities makes Internet Explorer prone to attacks. If a computer user wishes to use Internet Explorer for web surfing it’s very important to keep Windows up-to-date with security patches. It is also important to keep in mind that multiple external applications use Internet Explorer and the built in Windows components to render HTML pages and HTML emails, so an Internet Explorer vulnerability might affect both the browser and the email program...

3.4.4 Application programs

It is common that home computer users know that they have to update Windows, and that they do so when they get reminders that new updates are available for installation. However it is not enough to simply keep the operating system up-to-date. The application programs installed might also contain vulnerabilities that can be exploited by an attacker to take control of the computer. The application programs are much less likely to be updated than Windows itself.

This is an important observation since Internet Explorer and other programs often invoke helper applications when displaying a file the application itself cannot understand. Examples of such helper applications that Internet Explorer use to display documents are Adobe Acrobat Reader and Microsoft Word.

This introduces a new vector of attack. A vulnerability in Adobe Acrobat Reader, Microsoft Word or any other commonly used helper application will result in a vulnerable Internet Explorer. If the user visits a web page containing a specially crafted file or document that is displayed with the help of a vulnerable helper application, the user’s computer could end up running malicious code.

The user could also be tricked into clicking on an email attachment containing a malicious document or follow a link to a malicious document. This could result in execution of malicious code. This thesis will only contain a brief overview of these problems for a few commonly used application programs in home computers.

Microsoft Office

Microsoft Office is by far the most popular office suite at the time of writing of this thesis. It’s widely used by both business users and home computer users. Microsoft Office contains several vulnerabilities [bid: 9010, 8835, 8761] in its unpatched state. It is unlikely to have been patched ever according to the user survey in chapter 6.

The result of this is that a potential attacker could execute malicious code on a user’s machine without the user’s authorization even if Windows is fully up-to-date with the most recent security patches. An attacker could send an email containing a word attachment or embed the word document in a malicious web page. Internet Explorer would then invoke Microsoft Word as a helper application to be able to show the malicious document to the user.
Security software

Security software such as firewalls and anti-virus programs are becoming increasingly popular due to recent worm outbreaks. Security software is meant to protect the computer from attacks, but it is important to remember that security software is just software... Software can contain vulnerabilities, security software is no exception.

The Witty worm is a recent example of what can happen when something goes really wrong. The Witty worm started to spread in March, 2003. It spread through Internet Security Systems Inc.’s BlackICE and RealSecure products exploiting a buffer overrun vulnerability [bid: 9913] in the firewall included in those products. The worm overwrote random sectors of the hard disk effectively corrupting data including the operating system until the computer crashed.

Other examples of recent vulnerabilities are the vulnerabilities in Symantec’s popular Norton Internet Security software suite [bid: 9912, 9915, 10333, 10334, 10335, 10336]. All these vulnerabilities are related to the firewall included in Norton Internet Security. Some vulnerabilities allow an attacker to perform a DoS attack against the computer running the firewall, while others allow an attacker to execute malicious code on the vulnerable computer.

Instant messengers

Two of the most commonly used instant messaging programs today are Microsoft’s MSN Messenger and America Online’s ICQ. Both MSN Messenger and ICQ have a history of security vulnerabilities. Some vulnerabilities could be "used" to perform a DoS attack against the instant messaging program, while other vulnerabilities could be used to have a look at the local file system or/and steal information.

Instant messaging programs introduce yet another vector of attack that worms can use to spread. Spammers can also make use of instant messaging programs to deliver advertisements to the users. Instant messaging spam is called spim. The spam and spim problems are not treated in this thesis.

The most popular instant messaging networks are controlled by large corporations. This gives them some degree of control that they can make use of if a serious vulnerability is found. They can lock out old vulnerable clients and force the users to upgrade to a secure client. Recent instant messaging clients auto-update themselves in the background; often without the user’s knowledge.

Adobe Acrobat Reader

Adobe’s Acrobat Reader is the most commonly used program to read .pdf files. So far no serious exploits of Adobe’s Acrobat Reader have been reported. There have been .pdf viruses, but they haven’t affected Acrobat Reader. SecurityFocus.com has got a report of a buffer overflow vulnerability in Acrobat Reader 5.1 [bid: 9802], but it’s unknown if this buffer overflow vulnerability can be used to execute malicious code at the time of writing.
3.4 Recent vulnerabilities

Macromedia Flash Player

Macromedia Flash is a vector graphics based graphics animation program by Macromedia according to Wikipedia [25]. The files called "flash files" may be included in web pages to view in a web browser. The most common use is in animated ads on web pages. Macromedia Flash Player for Internet Explorer is included in Windows by default. Macromedia’s Flash Player has had several security vulnerabilities in the past, allowing an attacker to supply executable code in a flash animation or crash the user’s browser by supplying a malicious flash animation [bid: 5340, 10057]. Macromedia’s Flash Player is an interesting vector of attack because it is so popular in online advertisements. If malicious flash content could be inserted into an ad it would be possible to turn a legitimate site into a malicious site.

Winamp

Winamp is a popular media player. It is mostly used to play mp3s but it supports almost any format out there via plugins. Winamp has had several vulnerabilities in the past. Most of them are only exploitable if the attacker already has got access to the computer; however one serious security vulnerability was reported last year to bugtraq. This vulnerability [bid: 8567] could allow an attacker to run malicious code on the computer if the user is tricked into playing a specially crafted MIDI file in Winamp.

QuickTime

Apple’s QuickTime Player had very few vulnerabilities in the past. One recent vulnerability [bid: 7247] describes how QuickTime Player fails to properly handle some types of URLs. An attacker might be able to execute commands on the computer running QuickTime Player by supplying specially crafted URLs.

Real Player

Real Network’s Real Player is the main competitor of Microsoft’s Media Player together with Apple’s QuickTime. It is common that content providers on the web, such as newspapers and tv-stations publish streams for both Real Player and Microsoft’s Media Player. The various versions of Real Player contain several vulnerabilities. Several of these vulnerabilities [bid: 9579, 9378, 8453] would allow an attacker to execute malicious code if the user can be tricked into opening a malicious video clip or video stream.

KaZaA and P2P applications

KaZaA is the most popular peer-to-peer (P2P) application at the time of writing. KaZaA allows users to search and download music, documents, images, software, videos and movies. Some of the older versions of KaZaA Media Desktop contain
vulnerabilities [bid: 7680, 6747, 6543] that would allow an attacker to perform denial of service attacks or execute malicious code on the computers that are running the vulnerable KaZaA version.

KaZaA and other P2P applications are interesting because they introduce yet another vector of attack for malicious code such as worms and viruses. Several worms make use of P2P networks to spread. A common technique is to create a copy of the worm in a shared folder with an attractive name, such as a crack or keygenerator for popular applications, or as a media file using a double file extension e.g. britney-nude.avi.exe. A user searching for cracks, keygenerators or any other program might download the worm and execute it. Another interesting observation is that a peer in a peer-to-peer network is aware of its neighbour peers. This could allow for a worm that exploits a vulnerability in a commonly used P2P client to spread very fast.
Chapter 4

Threats

The Internet is a very powerful medium and communication via the Internet is an everyday thing for people all around the world. The Internet has become one of the most important communication channels on Earth. Some applications for Internet usage make it possible to communicate with people situated in different parts of the world in high speed, even in real time. The possibilities are enormous and the Internet has a huge impact on our way of communicating and living. In the near future the Internet will probably become even more important, because the number of users and tasks that can be performed with help of the Internet increase for every day.

But, there are also some aspects of the Internet that create huge problems for many users. Information security is one of the most important issues when discussing the future of the Internet. Malicious attackers use the Internet to scan target IP addresses, to harvest email addresses and sell them to spammers, to steal credit card numbers or money from bank accounts, to disable web pages, to generate DoS attacks and to do various attacks on computers connected to the Internet.

The aim of this chapter is to give an overview of the major threats of today and considerations of the threats in the near future.
4.1 Worms

The year 2003 got nicknamed "the year of the worm" in the computer security community, because of the enormous impact that some computer worms had on Internet traffic and computer security in different parts of the world. These worms caused huge waste of information and economic resources. They also created a kind of mass hysteria about computer security and malicious code writers. Worms are definitely one of the biggest threats to the Internet today.

One of the most popular applications used on the Internet is email. It is used by huge numbers of Internet users to send and receive various messages every day. Email is enormously important for many people. But, many don’t know that email is maybe the most vulnerable application in a company’s network. Email and other Internet applications are used by malicious users as a very fast and powerful tool to spread computer viruses, especially computer worms.

Computer worms are reproducing programs that run independently and travel across network connections. The main difference between viruses and worms is the method in which they reproduce and spread. A virus is dependent upon a host file or a boot sector, and the transfer of files between machines to spread, while a worm can run completely independently and spread of its own will through network connections. The name "worm" was taken from The Shockwave Rider, a 1970s science fiction novel by John Brunner. Researchers writing an early paper on experiments in distributed computing noted the similarities between their software and the program described by Brunner and adopted the name.

Computer worms can be sorted in different ways, but generally there are two types of worms: host computer worms and network worms. Host computer worms are entirely contained in the computer they run on and use network connections only to copy themselves to other computers. Network worms consist of multiple parts, each running on different machines and using the network for several communication purposes. Propagating a segment from one machine to another is only one of those purposes. Network worms that have one main segment which coordinates the work of the other segments are sometimes called "octopuses".

4.1.1 Worm segments

Worm writers are aware of how important small size and simple construction is for the worm’s ability to spread across the network. These two attributes make worms more effective and make possible very fast propagation. Generally, we can say that worms consist of three main segments: attack mechanism, payload and new target selection.

Every computer system has its specific vulnerabilities and worms usually exploit them first. Buffer overflow vulnerabilities are the major part of the security holes that worms exploit. The worm’s attack mechanism uses the vulnerabilities to copy itself onto the target system.

The payload is the part of the worm code that performs malicious actions against the infected host. The payload can be any type of program that perform
various harmful actions on the host’s computer system. A common payload for a worm is to install a backdoor in the infected computer. These backdoors are used by malicious individuals for sending junk email or to cloak a website’s address of the victim. Spammers, the people who create and distribute junk email, are willing to pay for the creation of such worms. They cooperate with worm writers and pay for lists of IP addresses of infected machines. Other malicious code writers try to blackmail companies with threatened Distributed Denial of Service (DDoS) attacks. The backdoors can also be exploited by other worms that spread using the backdoor opened by previous worms. There are also some simple worms that have no payload. They just spread themselves and generate huge network traffic.

When the worm’s code is executed, it attempts to spread again. A worm has to find new target computers that are vulnerable to its attack mechanism. The fact that worms can spread without human intervention and that they can use different techniques to spread makes them very successful in propagation. Worms can infect thousands of computers in a very short time period.

4.1.2 Spreading methods

Worms can use multiple methods of spreading. Hybrid worms can have several different ways of spreading at the same time. Some worms use file sharing programs to propagate, some use network connections and backdoors on computer systems. But, the most used method in the past one-year period is email in combination with social engineering, that showed frightening results causing damages for billions of dollars around the world.

When a potential victim receives a worm over email, it can be in the form of an attachment or it can be a part of the message. The attachment could claim to be anything from a Microsoft Word document to a picture of some celebrity. Clicking on the attachment to open it activates the worm, but in some older versions of Microsoft Outlook Express clicking on the attachment is not necessary to activate the worm if you have the program preview pane activated. Microsoft release security patches regularly to correct software problems, but not everyone keeps their computer up-to-date with the latest patches. Some worms spread with email messages without attachments meaning that it is enough to open a message to be infected.

After the worm has been activated, it searches for a new list of email addresses to send itself to. It goes through the files on the infected computer, such as the email program’s address book and the web pages the user has recently looked at, to find them. Once the worm has its list of email addresses it sends emails with copies of itself to all the addresses it found and the cycle starts again. Some worms use the victim’s email program to spread themselves through email, but many worms include a mail server within their code, so the victim’s email program doesn’t even have to be open in order for the worm to spread. This kind of worms is very aggressive and they produce thousands of copies causing huge network traffic. This process can lead to congestion problems on the Internet and even to server breakdowns at some Internet locations.
4.1.3 Famous worms in the computing history

The first program that could reasonably be called a worm was written in 1971 by Bob Thomas. This program was in response to the needs of air traffic controllers and would help to notify operators of when control of a certain airplane moved from one computer to another. This program did not reproduce itself. After this several other programmers tried their hands at similar programs, but the idea gradually died out in a couple of months. In the early 1980’s, a team of Xerox’s Palo Alto Research Center began experimenting with worm programs. They developed 5 worms, each of which were designed to perform helpful tasks around the network. Some worms were quite simple, such as the Town Crier worm, which simply traveled throughout the network posting announcements. Other worms were quite clever and complex, such as the ”Vampire” worm. This worm was idle during the day, but at night, it would take advantage of the largely idle computers and apply them to complex tasks which needed the extra processing power. At dawn, it would save the work it had done so far, and then become idle, waiting for the next evening.

These programs were very useful, but it became apparent that worm could be dangerous tools if incorrectly used. This was demonstrated amply when one of Xerox’s worms malfunctioned during the night. When people arrived at work the next day, they found that computers throughout the research center had crashed. Moreover, when they tried to restart the machines, the malfunctioning worm immediately crashed them again. A new patch had to be written to prevent the worm from crashing the systems. During 1987 a fast-spreading worm called the IBM Christmas Worm hit IBM mainframes and caused significant damage for many computer users.

Worms are a very interesting phenomenon, that caused many problems for computer users during the past couple of decades. Worm writers change strategy often and create more and more sophisticated worms. It is not possible to describe all the worms that have been active in the wild in the computer history in this thesis due to space limitations. Only specially interesting worms, that caught the attention of the computer users around the world and became famous have been included.

Morris worm

The first worm to attract wide attention was written by Robert Tappan Morris, Jr., a graduate student in computer science at Cornell University. It was released on November 2, 1988 (from MIT, to disguise the fact that it came from Cornell), and quickly infected a great many computers on the Internet at the time. The worm was written just to spread, not to cause damage. Unfortunately, some bugs in the code made the worm dangerous. Target computers could be infected many times and each additional process would slow down the machine until it became unusable. The worm propagated through a number of bugs in BSD Unix and its derivatives. Morris’s worm received vast amount of media attention, becoming front page news for over a week after the occurrence. The media jumped on the story of the program that had single handedly crashed the Internet and caused a
huge problems for the Internet community. The Computer Emergency Response Team (CERT) was created in order to try preventing future problems.

**Melissa**

Melissa was detected in the wild in March 1999. It is a worm/macrovirus that executes a macro in a document attached to an email. The worm forwards the document to the first 50 people in the user’s Outlook address book. This worm also infects other Word documents and subsequently mails them out as attachments. Melissa modifies the user’s documents by inserting quotes from the TV series "The Simpsons". Even worse, it can send out confidential information from the computer without first notifying the user. Melissa spread faster than any other previous worm/virus and infected hundreds of thousands of PCs.

**PrettyPark**

PrettyPark operates on three different levels: as a worm, as a password-stealing trojan horse, and as a backdoor to the victim’s computer. This worm was detected in the wild in June 1999. It spreads by email when an unsuspecting user receives a message with a file attachment PrettyPark.exe. Once the victim executes the attached file, the worm infects the system by copying itself to the system directory as a file named files32.vxd. It also modifies the registry, so that it will run whenever Windows runs an .exe program file. When this worm is detected the victim should first correct the registry and then delete the worm’s file. This is very important, because unless the registry is corrected, Windows will not be able to run other .exe files.

**Bubbleboy**

Bubbleboy is a demonstration Visual Basic Script (VBS) worm. It is the first malware known that can spread to a user’s PC without the need to open an attachment. This is possible because Bubbleboy’s script is included within the email message itself. Although Bubbleboy has the potential to spread among those using Windows 98/2000, IE5, and Outlook/Outlook Express, the fact is that it is merely a demonstration, sent to some anti-virus companies in November 1999. It was actually not in circulation but inaccurate news stories made many people believe it was, and therefore posed as an imminent threat. Even though Bubbleboy was no threat, there is a possibility that worms that use its techniques may become a danger in the future.

**KAK**

KAK is a JavaScript worm, based on Bubbleboy. KAK was detected in the wild in December 1999. It’s embedded in an email, in place of the user’s signature. If the recipient is running Windows 95/98, and Outlook Express 5.0 without a patch Microsoft made available, then the script can write a file to the Windows Startup
folder. Nothing else happens, and the file (kak.hta) can be deleted at that point, with no harm done. However, if kak.hta is still there the next time Windows starts up, it will run automatically, and will replace the contents of the autoexec.bat file with a command to delete itself when the PC is rebooted. More importantly, it will write a copy of the worm program to the Windows system folder, and modify the registry to run that program every time the system starts. The program then will use Outlook Express to spread, by replacing the user’s signature in outgoing emails with a hidden copy of the original script. KAK is something that scanners did not have to deal with previously, because it is not an “attachment”, but is a script embedded in the body of the email. If the scanner is an older version, it might not be checking the email bodies, thus allowing KAK to write its file to the hard disk, and detecting it only after the fact.

Chode/911

When it first appeared in April 2000, Chode, also called the 911 Worm, was considered enough of a threat to be the subject of an advisory from the FBI. Its claim to fame is that it is the first worm/virus that can travel by itself (no email needed) directly from one Windows PC to another via the Internet, by searching for, and exploiting, ”Windows sharing”. The worm has a dangerous payload routine. Depending on its random counter the worm either formats hard drives or dials '911', an emergency hotline number in the U.S., using a modem if one is installed on COM1- COM4 ports. One of the worm’s versions sends dial commands to all these ports regardless of modem presence in the infected system. The worm is able to spread itself only if Windows is installed in the directory named C:\WINDOWS\, so if this directory name is different or if Windows is installed on another drive, the worm fails to spread itself. The worm will not work under Windows NT as it has a different startup directory path.

Love Letter

Love Letter is a VBS worm that spread widely around the world in May 2000. Love Letter was able to spread so fast simply because people were too curious for their own good and opened an email attachment without knowing what was in it. In its original form the worm sent itself to users via email attachments. The message subject was ”ILOVEYOU” and the message text was: ”kindly check the attached LOVELETTER coming from me”. The attachment was called LOVE-LETTER-FOR-YOU.TXT.vbs (note the double extension). When clicked on the attachment would run (assuming Windows Scripting Host is installed) and the cycle would start again. The double extension is important for this worm as it tries to exploit an ease of use function described more in detail in sections 3.2.4 and 3.3.4. Email programs and directory programs are often set, by default, not to show file extensions. This is supposed to shield a user from the details of the computer’s operation. In this case, it made things worse since, if a user had that option set, the attachment would show up as LOVE-LETTER-FOR-YOU.TXT
and thus appear to be a harmless text file instead of a malicious executable script.

**Navidad**

Navidad (or Feliz Navidad, Spanish for Merry Christmas) is a worm with a new twist. If you send an email to someone whose computer is infected, it is designed to send you an automatic reply, with a file called navidad.exe attached. Clicking on that file will infect your PC, and it will spread after that by getting addresses from your unread emails, and sending itself out to people who write to you. The original version of Navidad was not able to get far, because it had a major design flaw, but it has been reported to be "in the wild" in September 2000. Since it modifies the registry incorrectly, it should simply cause an infected computer to stop functioning, and even prevent Navidad from functioning, if Windows is restarted. Even though the original version is defective, this worm is interesting because of its reply strategy that can be used to infect new computers.

**Code Red**

The Code Red worm became famous in mid 2001 because it attempted to launch a DoS attack against www.whitehouse.gov, the White House web site. Code Red operated in three stages: scanning, flooding and sleeping. During the scanning phase the worm searched for vulnerable IIS web servers and infected them. In the flooding phase the worm sent bogus data packets to the White House web site. The White House however changed their web site's IP address and was therefore able to avoid the attack. Experts believed the worm's final sleep phase could last indefinitely, and that even infected machines would not pose a threat to anyone else. The worm also replaced the web site texts with the phrase "Hacked By Chinese!" and installed a backdoor on the infected computers. At its peak, the worm infected 2,000 machines every minute, and infected 359,000 machines and cost $1.2 billion according to the BBC. The worm could have affected more computers, but because of a Code Red warning many people were able to protect their machines before getting infected.

**Nimda**

Nimda is one of the more complex virus/worm constructs released. It started to spread in November 2001. This worm is a hybrid that has four different ways of spreading. It infects files, spreads itself via email, spreads via web sites, and spreads via local area network exploits. It infects different versions of Windows ranging from Windows 95 to Windows 2000 as well as Microsoft's Internet Information Server (IIS). Nimda is the first worm to infect .exe files by embedding them into itself as a resource. It also infects web pages so unsecured browsers will get infected upon viewing the web page. Nimda is also the first worm to use any user's computer to scan a network for vulnerable machines behind a firewall to attack (in the past only infected servers did that). This worm uses its own built in email server to send email messages. Compromised machines attack other machines on the Internet.
Nimda damages system and document files on infected computers and uses network resources. Huge email traffic caused by Nimda slows the network.

**Bugbear**

The Bugbear worm was first detected in the wild in October 2002. It infected users running Windows via a security hole in Microsoft Outlook, Microsoft Outlook Express and Internet Explorer. The worm copied itself to the hard drive and on to other computers that shared a network. The worm copied the passwords and credit card numbers a user typed. Then, it could send a file with the personal information collected to several email addresses. In its first week, 320,000 infected emails were sent. The worm spread easily because when it sent emails of an infected computer’s address book, the subject lines read, ”just a reminder,” ”bad news,” ”interesting” and other subjects that seemed innocent. In 2003 Bugbear reappeared, but in a far more damaging strain. In 24 hours the newer version, Bugbear.B, caused the same damage that it had taken the previous Bugbear three days to cause. Bugbear.B claimed its new victims quickly because a flaw [MS01-020] in Microsoft Outlook meant the program automatically opened email attachments.

**4.1.4 The latest worms in the wild**

The worms described in this section are some of the latest worms in the wild. These worms are some of the most famous and there are many other worms in the wild right now. According to wildlist.org there were almost 500 worms, viruses and trojan horses in the wild at the end of April 2004. Many worms build so called worm families, because new variants are being released regularly and different variants can be active at the same time. New behavior patterns are shown in the last few months when some of the worm families started fighting each other on the Internet. This war is still in progress at the time of writing this text. The worm families who are fighting are Mydoom, Netsky and Bagle. Some of these worm families will be described in general and readers who need deeper knowledge about particular variants are encouraged to search the Internet and available literature for more information. The main source for this section is F-Secure’s Computer Virus Information Center [9].

**Sobig**

Sobig is a worm that uses email and shared network folders for spreading. It infects computers running Microsoft Windows 95, 98, ME, NT, 2000 and XP. Sobig has its own SMTP engine, meaning that an infected machine’s email program does not even have to be active in order for the worm to spread. It uses a technique known as spoofing, pretending to be a message coming from some of known Internet addresses e.g. x@microsoft.com.

Many of the addresses are valid addresses that are being spoofed for malicious purposes. Message characteristics varies for different variants of the Sobig worm. When the attachment is run, the worm copies itself into the Windows folder and
4.1 Worms

The Sobig worm creates a new process by running its .exe file. The worm searches the local hard drive for files with the extensions .txt, .html, .eml, .htm, .wab and .dbx. The files that are found are used to extract a list of recipient email addresses that will be used by the worm to send infected emails. It also opens up a backdoor, making the computer vulnerable to hackers, who can plant dangerous trojans. These malicious programs often let unauthorized users remotely take over a system, steal important personal information or use the infected PC to send junk email. More information about trojans can be found in section 4.5.

Blaster

The Blaster worm, also known as Lovesan, wreaked havoc on Microsoft Windows 2000 and XP users in August 2003. The worm spread quickly, checking for vulnerable computers and then sending itself to those machines. Blaster exploits the RPC DCOM buffer overflow vulnerability [MS03-026]. This vulnerability allows attackers to gain full access and execute any code on target machines, leaving them compromised. The vulnerability affects unpatched systems running Windows NT, 2000, XP, and Server 2003. This worm can only propagate into systems running Windows 2000 or XP.

The worm can affect the functionality of infected computers in different ways. Some users found that their computers were sluggish, but otherwise may have been unaware that they had been infected. On other machines that were infected, the computer was forced to reboot after several minutes, according to Microsoft’s
Figure 4.2. The Blaster worm.

When the worm found a vulnerable computer it attempted to retrieve the file "msblast.exe". When the file was retrieved, the computer began to scan other systems to attack them in a similar manner. Additionally, the worm was designed to launch a DDoS attack against Microsoft’s Windows Update web site www.windowsupdate.com. However the primary update site was and still is windowsupdate.microsoft.com. Microsoft removed www.windowsupdate.com from the Internet and successfully avoided the DDoS attack. In November 2003, Microsoft announced it would offer $250,000 for the information leading to the arrest of Blaster’s creator. The money would come from a $5 million fund, which was created to catch virus writers responsible for the attacks on Microsoft’s operating systems.

Swen

Swen is a worm that spreads with the help of infected email attachments, the KaZaA file sharing network, IRC channels, and open network file shares. The worm was first detected on September 14th 2003, according to TechNewsWorld [16], but it was not seen as a priority, and the threat was not added to updated protection from leading anti-virus vendors. When propagating via email, Swen pretends to be a message from Microsoft’s Windows Update. When the victim double clicks on the attachment, the worm installs itself in the system and starts its propagation routine. The worm is very successful in blocking many anti-virus programs and firewalls. When launched for the first time, Swen imitates message boxes from a Microsoft Internet Update Pack and patch installation process.
When attempting to execute a new copy on the computer that is already infected, Swen displays following message:

The worm scans the computer for files with the following extensions: .dbx, .mdx, .eml, .wab, .html and .asp. It extracts all the email addresses it can find in the files described above and store them in a separate file. The worm attempt to connect to
one of the many predefined servers to send infected emails. If that is not possible, Swen requests the right address and SMTP server by displaying following error message:

![Swen's request](image)

**Figure 4.5.** Swen’s request.

Swen attempts to block anti-virus software and firewalls that exist on the infected system.

When the worm detects that the user is trying to execute a suspected anti-virus program the execution is halted and the following fake error message is displayed:

![Fake error message](image)

**Figure 4.6.** Swen’s fake error message.

Using a direct connection to an SMTP server the worm sends infected emails to all available addresses. The infected emails are sent in HTML format and the worms are found in the attachments.
The Swen worm has several interesting features. One of the most amazing is the worm's capability to communicate with the website that keeps track of how many computers have been successfully infected. According to TechNewsWorld [16] more than 1.5 million computers around the world were infected with the Swen worm at the end of September 2003.

**Bagle**

Bagle is a mass-mailing worm that spreads attached to infected emails. The worm is activated when the user clicks on the attachment's icon. Then the worm copies itself to the system directory and start searching disk drives for files with the...
extensions .wab, .txt, .htm and .html. The worm scans these files for email-like text strings, then sends infected messages to the email addresses found. The worm uses its own built in email server to send infected messages. Bagle also install a backdoor on the infected computer which will allow the attacker to take control over the computer at any time. The attacker can then steal information from the infected computer, execute commands and download files.

Mydoom
Mydoom, also known as Novarg, was one of the fastest spreading worms in the history of the Internet. The worm was detected in the wild on the 26th of January 2004, according to Symantec. Mydoom propagates in two different ways. It spreads as an attached file to infected email messages and via the file sharing network KaZaA. The message in Mydoom is sent as a binary attachment. It often arrives in a .zip archive, but could also arrive as a .bat, .cmd, .exe, .pif or as a .scr file. The attached file could be represented by a text icon in most cases even though it is an executable file, which are renowned for carrying viruses. The worm activates when the victim launches the infected file by double clicking on the attachment. The worm then installs itself on the system and starts its propagation routine.
4.1 Worms

Figure 4.9. The Mydoom worm.

Mydoom harvests email addresses from infected machines and targets files with the following extensions: .pl, .adb, .tbb, .dbx, .asp, .php, .sht, .htm and .txt. It also tries to bypass some commonly used anti-spam protections i.e., like replacing the @ character with at and several other combinations. When loaded, some versions of the worm launch Notepad and show garbage characters.

Figure 4.10. Notepad with garbage content opened by Mydoom.

At the same time as the worm replicates itself, it opens a backdoor that could allow hackers to break in. In some instances it installs a keystroke capture program that records everything being typed, including potential passwords and credit card numbers. The worm is also spreading via the popular Internet file sharing network KaZaA. It appears with names such as "Winamp5" and "ICQ2004-final" on the KaZaA network. The peak infection ratio, the measure of how fast the worm propagates on the Internet at a certain time period, of Mydoom was one in 12 emails, according to MessageLabs [17], a British security firm.
Sasser

Sasser is a network worm that spreads very fast using existing network connections. It does not spread via email and can infect computers connected to the Internet without any action from the user. The worm was detected in the wild the May 1st, 2004. Sasser exploits a buffer overrun vulnerability in the Local Security Authority Subsystem Service (LSASS). This will cause infected computers to display an error message and to repeatedly reboot when connected to the Internet. According to Microsoft [6] only systems running on Windows 2000 or Windows XP are affected by this worm. Computers with other Windows operating systems can also be a source of transmission when a malicious user runs the file containing the worm in any of these computers.

Sasser is easy to recognize, as it restarts Windows XP/2000 computers when it attempts to infect these computers by exploiting the LSASS vulnerability. When this action is carried out, the operating system displays the following message on screen:

![System Shutdown](image.png)

Information about the vulnerability and the patch for the flaw were made available by Microsoft on April 13th, 2004. The appearance of the worm just 18 days (in comparison with Blaster’s 30 days) after the vulnerability was made public confirms current trends in malicious software. The period between a vulnerability being discovered and malicious programs which target the vulnerability is becoming increasingly shorter.

4.1.5 Worms of the future - the digital armagedon?

One of the leading researchers in the computer worms area, Nicholas C Weaver from the University of California, Berkeley, believes that it is possible to construct hyper-virulent active worms that can infect all vulnerable hosts on the entire Internet in
less than one hour. Mr Weaver is arguing in his paper [24] that worms could be much faster and much more malicious in the future. He believes that what we have seen by now is just a small part of the worms potential to spread fast and cause huge damage. The potential is far worse, spreading faster than the computer community can respond and leaving a wake of damaged data and corrupted machines. By the time people understand what was happening, all damage would already be done and the Internet temporarily destroyed.

A good example for how fast worms can spread across the Internet is the Slammer worm that created panic around the globe at the end of January 2003. Slammer was the fastest computer worm in the history of computing. As it began spreading throughout the Internet, it doubled in size every 8.5 seconds. It infected more than 90 percent of vulnerable hosts within 10 minutes. Slammer, also called Sapphire, started spreading slightly before 05:30 UTC on January 25, 2003.

![Figure 4.12. The geographic spread of the Slammer worm 30 minutes after its release.](image)

Half an our later, almost 75,000 hosts were infected at different locations around the world. The diameter of each circle in figure 4.12. is a function of the logarithm of the number of infected machines. Large circles visually under-represent the
number of infected cases in order to minimize overlap with adjacent locations. Fortunately, Slammer did not contain a malicious payload, but its aggressive spreading caused considerable harm simply by overloading networks and taking database servers out of operation. If the worm had carried a malicious payload, had attacked a more widespread vulnerability, or had targeted a more popular service, the effects would likely have been far more severe.

The efficiency of finding new targets is very important for a worm’s ability to spread fast. Optimizing the scanning code can result in significant improvements in speed. Using hitlist scanning can give the greatest benefit to worms of the future. Before the worm is released, the worm author collects a list of huge numbers of potentially vulnerable computers with good network connections. The use of precompiled target lists during the initial spread and permutation scanning can enable malicious code writers to create worms able to infect most or all vulnerable computers in the first 15 minutes of release.

There are also some researchers who believe that it is possible to create a high speed worm that can infect the entire Internet in less than one minute. The method is similar to Weaver’s, but the hitlist consists of really huge numbers of addresses of potentially vulnerable computers. It is technically possible to scan the Internet and collect millions of addresses before a worm is released. This kind of Warhol worm could theoretically infect the entire Internet in less than 30 seconds!

Fortunately, there is a big gap between theory and praxis. Worm writers have to solve some very complex problems before they are able to create well-functioning Warhol worms. The Slammer worm was a warning that some of malicious code writers do have the knowledge to achieve spreading speed close to a Warhol worm. There is no doubt that worms are one of the major threats to today’s Internet. Using existing and evolving methods of propagation, worms of the future will become increasingly more powerful and harder to contain.

4.2 Virus hoaxes

Virus hoaxes are interesting because they take advantage of the only security vulnerability that is and will be impossible to remove – the user. A user might be tricked into harming his or her own system, simply by providing instructions how to do it. This is a pure social engineering attack. Social engineering is the art how to trick a person into doing things the person shouldn’t do. For more information and examples on social engineering please see Kevin Mitnick’s book “The Art of Deception” [19].

This thesis won’t address many of the issues related to various virus hoaxes, it will merely mention some of them and give an example of a common virus hoax.

A virus hoax often comes in the form of a chain letter email from a known person such as a friend. The email often tells the computer user that the computer might be infected by a virus. The computer user that has received such a bogus email is often asked to forward the email to the whole address book in case the user’s address book contacts have been infected too thus actively participating in
4.2 Virus hoaxes

spreading the hoax.

The hoax emails usually contain some bogus information in addition to the instructions how to forward the hoax email. What exactly this bogus information actually is of course varies depending on which hoax the user receives. An old hoax still going strong is the jdbgmgr.exe virus hoax that is asking the user to delete a certain Windows file, other hoaxes might warn the user to open certain emails with a certain subject.

4.2.1 The jdbgmgr.exe virus hoax

One of the most widespread virus hoaxes ever is the jdbgmgr.exe virus hoax. This virus hoax started early in April, 2002 among Spanish-speaking computer users. The hysteria spilled over to English-speaking computer users during mid April, 2002 according to Vmyths.com [23]. This virus hoax exists in many different forms, not only English and Spanish versions exists. There are Swedish versions of this virus hoax as well. An example of an English version of this virus hoax can be seen in Table 4.1.

<table>
<thead>
<tr>
<th>Dear Sirs:</th>
</tr>
</thead>
<tbody>
<tr>
<td>It is possible that a VIRUS could be sent to you because you were registered in our Outlook’s directory.</td>
</tr>
<tr>
<td>This VIRUS sends itself to all addresses registered in your Outlook’s Address Book (happens also with other e-mailing programs). If you find it please resend this email to all your email addresses.</td>
</tr>
<tr>
<td>How to erase it:</td>
</tr>
<tr>
<td>This virus is not found neither by Mc Afee, Norton, or any other AntiVirus programs.</td>
</tr>
<tr>
<td>How to erase it:</td>
</tr>
<tr>
<td>1) In the Start Menu go to &quot;Search Files&quot;, then search for jdbgmgr.exe or j*.exe</td>
</tr>
<tr>
<td>2) the Virus programs has a Teddy Bear as the Icon.</td>
</tr>
<tr>
<td>3) Once you found it, erase it.</td>
</tr>
<tr>
<td>4) go to the windows’ trash can and empty it or at least open it and then erase the file with the teddy bear icon.</td>
</tr>
<tr>
<td>5) resend this email to everybody on your mailing lists.</td>
</tr>
<tr>
<td>BYE, AND SHAME ON THE VIRUS DEVELOPERS! THEY HURT ALL BUSINESS, PEOPLE, AND OTHERS.</td>
</tr>
</tbody>
</table>

Table 4.1. The jdbgmgr.exe virus hoax.

A more detailed descripion of the various versions of the jdbgmgr.exe virus is found at F-Secure [14].
The targeted file, jdbgmgr.exe is a Windows system file. Removing this file has no affect at all in most cases. It is used by Visual J++, a since long discontinued Microsoft product. Some Java programs, created with Visual J++, might cease to function if this file is removed.

4.3 Phishing

According to Wikipedia [25] Phishing is the act of luring sensitive information, such as passwords and financial data, from a victim by masquerading as someone trustworthy with a real need for such information. The term *phishing* was coined in the mid nineties by crackers attempting to steal AOL accounts. *Phishing* is a variation of the word *fishing*: fishers (and phishers) set out hooks, knowing that although most of their prey won't take the bait, they might entice some to bite. Most of the information regarding Phishing in this section and all figures originates from the Anti-phishing Working Group [2] web site.

4.3.1 Phishing scams

The standard way of performing a phishing scam is to set up a bogus website imitating the look and feel of a legitimate website such as eBay, Citibank or PayPal. When the bogus website is brought online the phishers will send forged emails to a group of users. Sending these emails can be easily done by using a bulk emailer service or after buying a list of email addresses. These emails will look like a legitimate email from the company targeted by this specific phishing scam. The email will ask the user to visit the bogus website and will provide a link to it inside the email.

It is possible to perform a phishing scam using other vectors of delivery than email, for example using an Instant Messaging service like MSN or ICQ. The only difference from the email case is the vector of delivery. This thesis will only address the email part due to its commonality.

According to the U.S. Department of Justice [22] the phishing emails and websites associated with the phishing emails may appear completely legitimate at the first glance. What Internet users may not realize is that phishers can easily copy logos and other information from legitimate businesses’ websites and place them into phishing emails and websites.

Phishing emails usually include false statements intended to create the impression that there is an immediate threat or risk to the user’s accounts on the targeted businesses. Phishing emails have falsely claimed that the recipients’ Visa credit card has been used by another person, or that a recent credit card transaction has been declined. In other cases the receiver is promised a ”prize” or another special benefit. Although messages promising a ”prize” sounds attractive rather than threatening the object is the same: to trick the recipient into disclosing their financial and personal data.
4.3 Phishing

4.3.2 An example

The email found in table 4.2 is a hoax and will take the user to a forged Citibank web page when clicking the link. The email looks like a standard text email, but is in fact a html email. This is the reason why the url read citibank.com but will take the user to another page if the user clicks on the link. The web page found in figure 4.13 looks like a legitimate Citibank web page but but the entire address bar is spoofed. The spoofed address bar is scripted using HTA, HTML and javascript with images and text to deliver the bogus web page that could easily be mistaken for a genuine Citibank page.

Dear Citibank Member,

This email was sent by the Citibank server to verify your E-mail address. You must complete this process by clicking on the link below and entering in the small window your Citibank ATM/Debit Card number and PIN that you use on ATM.

This is done for your protection – because some of our members no longer have access to their email addresses and we must verify it.

To verify your E-mail address and access your bank account, click on the link below:

https://web.da-us.citibank.com/signin/citiifl/scripts/email_verify.jsp

Thank you for using Citibank

Table 4.2. Citibank spoof email.

4.3.3 Statistics and trends

In February, 2004, there were 282 new phishing attacks reported to the Anti-phishing Working Group [2]. This was a 60% increase compared to the number of unique attacks reported in January (176). The most targeted sector was financial services, and the most targeted companies was eBay, Citibank, PayPal and AOL. In February eBay was the most targeted company (104 unique attacks), followed by Citibank and PayPal with 58 and 42 unique attacks. The number of phishing scams targeting eBay has risen by more than 100% since December, 2003, and the

\[1\text{PayPal is owned by eBay.}\]
number of scams targeting PayPal has risen by 320% in two months! Figure 4.14 displays the number of unique phishing attacks from December, 2003 to February, 2004.

**Organized crime is getting interested in phishing**

Historically the first phishing scams were conducted by individuals that wanted to gain access to AOL accounts so that those individuals were able to surf the net for free. This was back when AOL and other ISPs charged per minute in the U.S. It is quite common that individuals still are behind Internet scams, but an increasingly large amount of phishing emails originates from eastern Europe and Russia. These international phishers are often more organized and are harder to trace than most individual phishers. Organized crime is getting interested in phishing, identity theft and stealing money from online banking services.
Phishing scams are becoming more technologically advanced

The Internet scams are increasingly becoming more technologically advanced, and are becoming harder to separate from the legitimate sites. A commonly used practice when trying to scam the users of an online service is to set up a copy of the site on a cousin url, e.g. paypal-secure.com if the goal is to scam PayPal users. Some recent phishing scams have stopped using this technique and started to script a copy of the entire address bar. Figure 4.13 is an example of this. An Internet Explorer window without the address bar is opened, and a javascript in that page will script a fake address bar. Phishers have also successfully exploited vulnerabilities in Internet Explorer in order to spoof the origin of the web site they display. This Internet Explorer vulnerability was well known and widely abused in December, 2003 and January, 2004 before Microsoft patched it.

4.4 Spyware

According to Wikipedia [25] spyware is defined as: a software that gathers information about a computer user without the user’s knowledge or informed consent, and then transmits this information to an external third party such as an organization that expects to be able to profit from it in some way.

Data-collecting programs installed with the user’s knowledge are not, properly speaking, spyware, if the user fully understands what data is being collected and with whom it is being shared.

More broadly, the term spyware is applied to a wide range of related malware
products which are not spyware in the strict sense. These products perform many
different functions, including the delivery of unrequested advertising, harvesting
private information, re-routing page requests to illegally claim commercial site
referral fees, and installing stealth phone dialers.

It is very common that home computers contain at least a couple of spyware
files today. This was confirmed in the user survey found in chapter 6. This section
will focus on spyware in its broad sense.

4.4.1 Adware

Adware also known as advertising supported software are software applications in
which advertisements are displayed while the program is running. Adware helps
recover programming and development costs, and helps to lower the price of the
application for the end user. Some adware gives the user the option to pay a small
fee in order to get rid of the ads.

The term adware is often used together with the term spyware. While it is true
that many adware products are also spyware products it is important to remember
that adware does not equal spyware. Examples of non spyware adwares are Eudora
– a popular email client and ICQ – a popular instant messaging client. An example
of an adware that has been criticized for being spyware is the popular KaZaA file
sharing application.

4.4.2 Spyware

An ordinary computer user, lets call him Joe has started to get a lot of spam in his
email inbox lately. Joe doesn’t enjoy reading about business ventures in Nigeria,
nor does he care about mortgages or about Viagra. Joe decides to get a spam filter!
Joe knows that he can buy spam filters at his local computer store, but he doesn’t
want to pay for one so he decides to download a free one off the net. Joe find this
great free spam filter, he clicks through the usual steps in the installation without
paying much attention, and all of the sudden all his spam are gone. Joe is happy
that the spam problem has been eliminated, but the next time he surfs the net he
swears about all the new popups he are getting, that the site owners are greedy
bastards. He never connects the sudden increase in popups to his brand new spam
filter...

The story above is purely fictional, but it clearly illustrates the core of the
spyware problem. The spam filter Joe downloaded was a spyware program. When
he installed it he agreed to the End User License Agreement (EULA) without
reading it. In the EULA it was clearly stated on lines 425-550 that Joe’s spam
filter also would act as an advertisement server providing new personalized popup
advertisements to him. In order to be able provide these personalized ads the
spyware program records Joe’s surfing patterns and transmits them to the company that
created the spam filter.

Spyware programs are often downloaded by the user. They usually provide a
useful service, such as removing spam, removing other spywares, keeping track of
4.4 Spyware

usernames and passwords, synchronizing the computer clock to a NTP server or providing access to a file sharing network.

In addition to spywares downloaded by the user there exist spywares that automatically install themselves onto the user’s system by exploiting known browser vulnerabilities. Some spywares might steal personal information such as SSN’s, Internet banking passwords and credit card numbers. It can be argued whether such applications are spywares or trojans. More information about trojans can be found in section 4.5.

4.4.3 Phone dialers

A phone dialer, or just dialer, is a piece of software installed on the computer that creates a connection to the Internet or another computer network over the phone line. Many ISPs offer installation CDs that contains dialers that are meant to simplify the process of setting up a proper Internet connection, an example of this is the AOL software.

However there exists another class of dialers, dialers that dial expensive foreign and pay numbers. The user is often tricked into installing the dialer software. When it’s installed, the dialer either changes the number of the current Internet connection to an expensive pay number – often a foreign number, or sets up a new connection to the Internet or to a private server.

Dialers are usually installed when the user clicks yes in an auto-install popup in their web browser. It is also possible to get a dialer installed even when clicking no in the auto-install popup or just by surfing around if the browser isn’t up-to-date.

Users with broadband connections are usually not affected. Dialers can still be downloaded and installed, but dialing a number is usually not possible. Dialup users that wish to protect themselves against dialers can take several actions. One action is to download a program called bluffstopparen from Konsumentverket [15] that acts as a guardian for the modem and only allows the computer to connect to numbers the user defined in advance. One other possible action is to order a service called telia kod from Telia2. This service blocks all pay- and foreign numbers, in order to dial such a number the user has to enter a code first. Dialers cannot possibly know this code and cannot dial the number.

An example

Date Regon is a dialer that has been distributed by several sites, including the popular swedish sites snyggast.com, snyggast.se and oldgames.se, all which are owned by the same group of companies: Harrys Expo Ltd, also known as HAR-EXP Ltd, Let To Phone AB, ScanBill, Internet-B, EzNet, Trom Brom Strom and GBR-Gruppen AB. An image of the Date Regon auto-install popup is found in figure 4.15.

Users that have installed this dialer has gotten bills from the companies mentioned, and if they refused to pay they got even more letters from different debt-

2The dominating telecommunications company in Sweden.
recovery companies finally even letter from the enforcement officers. The companies even took several users to court when they refused to pay according to Dagens Nyheter [8]. The company behind Date Regon lost in tingsrätten and was refused an appeal in a hovrätten.

Figure 4.15. The Date Regon dialer auto-install popup

4.4.4 Statistics and trends

According to Earthlink [12], a large American ISP, industry experts suggest that these types of programs may reside on up to 90 percent of all Internet connected computers. Earthlink has scanned approximately two million computers, and found over 54 million total instances of spyware, an average of 26.5 spyware instances per scanned computer.

The majority of the spyware instances found were adware cookies. A cookie is a file that web site owners can store on the local computer in order to keep track of users between visits. Large advertisement networks use this technique to keep track of users across different sites in order to be able to deliver more targeted advertisements. More than 44 million adware cookies were found on the scanned computers.

Even more disturbing was that Earthlink found over 11 million spyware adware programs installed, and almost 700,000 trojan like programs. More information about trojans can be found in section 4.5.
4.5 Trojan horses

One of the first tricks used by crackers to break into systems and take control of them derives from the ancient idea by Ulysses to conquer the city of Troy building a large, wooden statue of a horse. The statue was large enough to hide several warriors in it. The inhabitants brought themselves the horse containing the enemy warriors inside the city walls. The following night it was easy for the warriors to exit from the horse, kill the few guards at the main gate, and open the doors for the rest of the army. The city was then put to fire and destroyed by a surprise action.

Nowadays a computer trojan horse is a destructive program that masquerades as a benign application. Unlike worms, trojan horses do not replicate themselves but they can be just as destructive. One of the most insidious type of a trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer. Another good example is a web browser or a mail agent, that in addition to performing its normal function (so that the user is unsuspicious) sends secret information (for example passwords) to another user on another machine. Information that can subsequently be exploited to take control of the system. Trojan horses rely on users to install them, or they can be installed by intruders who have gained unauthorized access by other means. Then, an intruder attempting to subvert a system using a trojan horse relies on other users running the trojan horse to be successful.

4.5.1 Malicious actions

Trojan horses can do anything that the user executing the program has the privileges to do. They can delete files that the user can delete, transmit any file that the user can read to the intruder and change any file that the user can modify. Trojans can install other programs with the privileges of the user, such as programs that provide unauthorized network access. They can install viruses and other trojan horses, without notifying the user. They can execute privilege-elevation attacks, that is the trojan horse can attempt to exploit a vulnerability to increase the level of access beyond that of the user running the trojan horse. If this is successful, the trojan horse can operate with the increased privileges.

If the user has administrative access to the operating system, the trojan horse can do anything that an administrator can. The Unix "root" account, the Microsoft Windows NT "administrator" account, or any user on a single-user operating system has administrative access to the operating system. If the user uses one of these accounts, or a single-user operating system, the impact of a trojan horse can be devastating.

A compromise of any system on a network, including a compromise through trojan horses, may have consequences for the other systems on a network. Particularly vulnerable are systems that transmit authentication material, such as passwords, over shared networks in cleartext or in a trivially encrypted form. This is very common. If a system on such a network is compromised via a trojan horse (or
another method) the intruder may be able to install a network sniffer and record usernames, passwords and other sensitive information as it traverses the network. Additionally, a trojan horse, depending on the actions it takes, may implicate the user’s site as the source of an attack and may expose the user’s organization to liability.

4.5.2 Propagation

Users can be tricked into installing trojan horses by being enticed or frightened. For example, a trojan horse might arrive in email described as a computer game. When the user receives the email, they may be enticed by the description of the game to install it. Although it may in fact be a game, it may also be taking other actions that are not readily apparent to the user, such as deleting files or mailing sensitive information to the attacker. As another example, an intruder may forge an advisory from a security organization, such as the CERT, that instructs system administrators to obtain and install certain patches.

Other forms of “social engineering” can be used to trick users into installing or running trojan horses. For example, an intruder might telephone a system administrator and pose as a legitimate user of the system who needs assistance of some kind. The system administrator might then be tricked into running a program of the intruder’s design. Software distribution sites can be compromised by intruders who replace legitimate versions of software with trojan horse versions. If the distribution site is a central distribution site whose contents are mirrored by other distribution sites, the trojan horse may be downloaded by many sites and spread quickly throughout the Internet community.

Because the Domain Name System (DNS) does not provide strong authentication, users may be tricked into connecting to sites different than the ones they originally intended to connect to. This could be exploited by an intruder to cause users to download a trojan horse, or to cause users to expose confidential information.

Intruders may install trojan horse versions of system utilities after they have compromised a system. Often, collections of trojan horses are distributed in toolkits that an intruder can use to compromise a system and conceal their activity after the compromise, e.g., a toolkit might include a trojan horse version of ls which does not list files owned by the intruder. Once an intruder has gained administrative access to your systems, it is very difficult to establish trust in it again without rebuilding the system from known-good software. A trojan horse may be inserted into a program by a compiler that is itself a trojan horse.

Finally, a trojan horse may simply be placed on a web site to which the intruder entices victims. The trojan horse may be in the form of a Java applet, JavaScript, ActiveX control, or other form of executable content.
4.5.3 Protection

Trojan horses are very dangerous and it is not easy to protect computer systems from them. The major problem is not the technique for protection like firewalls and antivirus programs, but the human factor. There are many computer users who don’t care or don’t know anything about the threats of the Internet. This fact and social engineering skills of trojans writers makes anti-trojan protection very difficult. It is important to get computer users aware of the trojan problems and to teach them to be critical when surfing or using email. The tips on avoiding worms in section 5.1.1 are worth reading. These tips can help the user to avoid trojan horses as well.

4.6 Summary

The Internet offers many opportunities to improve communications between people. The Internet infrastructure makes it possible to communicate with people and remote computer systems situated in different parts of the world. The possibilities are enormous, but the Internet also offers huge possibilities for malicious users, worm writers and criminals. With the recent adaptation of broadband technology this development is further increased. This chapter has concentrated on the most important threats of today that are related to home computer security.

Worms are definitely one of the major threats to both home computer security and the Internet as a whole. The latest worm outbreaks, like Slammer, Blaster and Sasser, confirm this amply. These worms caused economical losses of several billions of dollars. Some worms like the Slammer worm spread very fast. The Slammer worm infected 75,000 hosts in less than half an hour, most of them in the first 10 minutes. Since the Slammer outbreak new ways to further increase the propagation speed has been discovered making it possible to infect most of the vulnerable Internet connected computers in a very short timespan before anyone can react to stop the process.

Another big threat to home computer security are email worms in combination with social engineering. This type of worms has been very successful in the past and still are, thanks to the low security awareness among ordinary computer users. These worms almost always contain an attachment and a text fooling the user to click on the attachment and activate the worm. For some of these worms it might be enough to open the email to get infected. Older worms used to send copies of itself to all addresses found in the address book of the infected computer. The more recent worms have their own built in email server, and harvests email addresses not only from the address book. Recent email worms like Netsky, Beagle and Mydoom all used some degree of social engineering to fool the computer users into clicking on the attachments.

Phishing attacks are increasing at an alarming rate. A phishing attack can be potentially very harmful because phishers target financial information and information that can be used for identity theft. A user might not notice the phishing attack before it is already too late, when the bank account is emptied.
Spyware is another problem that is increasing rapidly. Users are tricked into installing useful utility programs that are in fact only a front for an advertisement software that serves popups and harvests personal data sending it to the spyware vendor. Some spyware applications might even install itself automatically without the user noticing by exploiting security vulnerabilities in the browsers.

Different kinds of backdoors and trojan horses are often installed by various worms, allowing the worm writers to take control of the computer remotely and use it for various harmful purposes. The most common purposes are DDoS attacks and spam distribution. This clearly illustrates that all threats are related to each other and that different kinds of black hats are starting to work together. An example of this is that spammers are working together with worm writers to set up spam relays.
Chapter 5

Possible Solutions

This chapter will present some possible solutions to the problems presented in chapter 3 and 4. The problems related to home computer security are very complex, and there are no absolute truths or magic solutions that will solve everything. The computer security area is rapidly changing and new types of threats constantly emerge. The possible solutions presented are not a complete list of solutions. Most of these problems can be solved with alternative solutions as well.
5.1 Operating system security

Chapter 3 highlighted some weaknesses in the most popular home operating systems today. These weaknesses are often exploited by different malware programs, such as worms. This combination creates a huge threat to home computer security. This section will briefly present some possible solutions to these problems. Section 5.2 will also present some solutions to these problems that has already been included in Microsoft’s Service Pack 2 for Windows XP.

The installation

Windows XP and Windows 2000 are vulnerable to several types of remote attacks during the installation and before available patches are applied. It is very important to install Windows the right way to avoid getting infected by a worm that exploits the initial vulnerabilities. The Blaster and Sasser worms that target these vulnerabilities are still active on the Internet! A more detailed description of the Blaster and Sasser worms can be found in section 4.1.4.

1. Make sure the computer is physically disconnected from the network, i.e. make sure the network cable is not plugged in.
2. Install Windows.
3. Enable the Internet Connection Firewall.
4. Connect the computer to the network and start to download patches. When the computer asks whether it should be restarted now or later; disconnect the computer from the network. This is important because the ICF is disabled during startups and shutdowns, see section 3.2.7 for a more detailed description.
5. Restart the computer. Wait a while after the computer has been fully started to make sure the Internet Connection Firewall service has started, and connect the computer to the network. Repeat step 4 and 5 until all patches are applied.

Do not run as administrator

Malicious code runs in the same security context as in which it was launched. This usually means in the same security context as the user launching the code. If the user launching a piece of malicious code has got administrative privileges then the malicious code might cause severe harm to the system. Severe harm might also include the personal information of all users using that particular computer. If the user is launching a piece of malicious code with only user privileges then the malicious code can cause severe harm to that particular user’s files and spy on that particular user’s personal information. However it cannot cause severe harm to the system as a whole or spy on other users information.

Use an Internet firewall

Install or enable an Internet firewall. Modern operating systems have many services, that can be accessed from the network, enabled by default. Please see figure
3.3 for an illustration of this. A firewall restricts access to these services. A more advanced firewall can also allow the user to define which programs should be able to access the Internet and therefore effectively block trojan horses, backdoors and spyware. The built in firewall that comes with Windows XP only block external computers that wish to access the home computer, not programs that wish to access the Internet.

An alternative to an installed personal firewall might be an external broadband router. These routers are not so expensive today. It is possible to buy a simple router for less than 50 USD. These routers allow multiple computers to share an Internet connection. A side effect of this is that the computers internal IP addresses are not directly accessible from the Internet. This offers the same degree of protection as a simple personal firewall as long as none of the possible other internal computers gets infected.

Use up-to-date anti-virus software

Most virus scanning software scan for known virus signatures only; therefore, they are ineffective against new types of viruses and worms. Update the anti-virus software regularly. If it is possible set it to update itself automatically. An anti-virus software that isn’t updated will give a false sense of security and can be worse than no anti-virus software at all.

Keep Windows up-to-date

Keep Windows up-to-date with recent patches from Microsoft. Set Windows to automatically download and automatically install new patches if this is possible.

Show file extensions

Windows hides known file types by default as described in section 3.2.4. Potentially malicious code can mask itself as a legit file by using double file extensions to fool the user. The National Security Agency recommends disabling this feature in the paper "Outlook E-mail Security in the Midst of Malicious Code Attacks" [21].

5.1.1 Tips on how to avoid computer worms

1. Most of the worms that use email to propagate use Microsoft Outlook or Outlook Express to spread. If you need to use Outlook, download and install the latest Outlook security patches from Microsoft. In general, keep your operating system and your applications up-to-date and apply the latest patches when they become available. Be sure to get the updates directly from the vendors.

2. When possible, avoid email attachments both when sending and receiving email.
3. Configure Windows to always show file extensions. This is done through Windows Explorer via the Tools menu: Tools/Folder Options/View - and uncheck ”Hide file extensions for known file types”. This makes it more difficult for a harmful file (such as an .exe or .vbs) to masquerade as a harmless file (such as .txt or .jpg).

4. Never open email attachments with the file extensions .vbs, .exe or .pif. These extensions are almost never used in normal attachments but they are frequently used by viruses and worms.

5. Never open attachments with double file extensions such as NAME.BMP.EXE or NAME.TXT.VBS.

6. Do not share your folders with other users unless necessary. If you do, make sure you do not share your full drive or your Windows directory.

7. Disconnect your network or modem cable when you’re not using your computer - or just power it down.

8. If you feel that an email you get from a friend is somewhat strange - if it is in a foreign language or if it just says odd things, double check with the friend before opening any attachments.

9. When you receive email advertisements or other unsolicited email. Do not open any attachments in them or follow any web links quoted in them.

10. Avoid attachments with sexual filenames. Email worms often use attachments with names like PORNO.EXE or PAMELA_NUDE.VBS to lure users into executing them.

11. Do not trust the icons of an attachment file. Worms often send executable files which have icons resembling icons of pictures, texts or archive files - to fool the user.

12. Never accept attachments from strangers in online chat systems such as IRC, ICQ or MSN Messenger.

13. Avoid downloading files from public newsgroups (Usenet news). These are often used by virus writers to distribute their new viruses.

5.2 Windows XP Service Pack 2

According to Microsoft the major goal of Windows XP Service Pack 2 is to reduce common openings for attack of the Windows operating system. It reduces
most common attack vectors in four ways: it better shields the network, enhances protection of memory, handles email more safely, and browses the Internet more securely, all this according to Microsoft. This section will address all issues except memory protection. The enhanced memory protection will be addressed in section 5.3.

Figure 5.1. Windows Security Center is included in Windows XP Service Pack 2. It presents relevant security information in an easily accessible way to the users.

Network Protection

Network protection is one of the largest areas of improvement in Service Pack 2. The Internet Connection Firewall (ICF) has been improved and renamed to Windows Firewall. The new firewall is enabled for all network interfaces by default. This ought to better shield home computer users that do not know about firewalls from attacks.

Windows Firewall is more advanced than ICF. It contains more settings than the basic ICF. Microsoft also has a new approach to the RPC and DCOM services. These services might be needed by some programs, services and remote computers, especially in corporate contexts. When active ICF blocks all access to these services
Possible Solutions

by default, Windows Firewall will allow, or deny access to these services depending on in which security context the service or program requesting the services is running in. For more information please see Microsoft’s Windows XP Service Pack 2 Overview [4].

The Alerter and Messenger services have been disabled by default. The Messenger service has been targeted heavily by advertisers that used it to deliver text advertisements to unprotected computer users in the past. The home computer user probably won’t notice these disabled services in any other ways than when it comes to reduced advertisements.

Internet browsing and email

Recent events including the outbursts of the Netsky, Mydoom and Bagle worms have shown that most viruses and worms still spread by email. Users are tricked into clicking on unsafe attachments. To help thwart this problem Microsoft will include a service called Attachment Execution Services (AES) that Outlook Express will use in order to determine whether an attachment is safe or not. The user will be denied access to unsafe attachments such as executable files.

Outlook Express will also block some HTML content in email messages such as images loaded from external servers. Images in emails are commonly used by spammers to identify whether an email address is working or not. The spammers do so by embedding a unique id in the image url. When the email program loads the image from the spammers web server in order to display it in the email the spammers will know that the email address is active. Outlook Express will allow the user to disable the blocking.

In the past different add-ons to Internet Explorer have been the source of many problems and crashes in the past. Service Pack 2 will include an add-on manager and crash detection that will attempt to detect crashes in Internet Explorer related to add-ons and give the user the opportunity to disable the faulty add-on. Internet Explorer will also include a popup blocker that will block most of the unwanted popup windows from appearing.

Improved computer maintenance

Windows XP Service Pack 2 will use a new version of the Windows Update web site. The new Windows Update service allows users to scan for the most critical updates and download only them if they wish. The automatic patch installer has also been improved. It now only downloads patches that need to be downloaded, and supports new compression technology that will make the patch sizes smaller. Large patches has been the main reason why dial-up users are generally not as up-to-date with Windows as broadband users as seen in the user survey in chapter 6.
5.3 Memory protection

Buffer overruns\(^1\) attacks are among the most common vectors of attack against today’s computers. Buffer overflows exist mainly due to weaknesses in the popular C and C++ programming languages and have been around since the seventies! The attacker usually sends a long string to an input stream – longer than the memory buffer allocated to hold it. Parts of the memory past the buffer boundaries are then overwritten by the attack code contained in the supplied string, resulting in a buffer overrun attack. Depending on the conditions the attacker might be able to execute arbitrary code supplied in the attack string, or merely crash the computer or the computer program.

Buffer overrun attacks can be very serious. If a buffer overrun vulnerability exists in a network service not protected by a firewall, worms can use the vulnerability to gain control of the vulnerable computer. Famous worms like The Morris Internet Worm, Code Red, Slammer, Blaster and Sasser have all abused known buffer overrun vulnerabilities. More information about these worms can be found in sections 4.1.3 and 4.1.4.

Protection against buffer overrun attacks has been around for a very long time. The protection methods range from automated code checks to detect buffer overrun vulnerabilities in source code to special compilation techniques that incorporate additional security measures in the compiled code. The problem with these techniques is that it takes a lot of time and effort and thus money to check the code for vulnerabilities. The code compiled with special protection techniques is also slower than unprotected code.

**Execution Protection (NX)**

On the 64-bit AMD K8 and Intel Itanium processor families, the CPU can mark memory with an attribute that indicates that code should not be executed from that memory\(^2\). This technology called execution protection (NX) functions on a per-virtual memory page basis, most often changing a bit in the page table entry to mark the memory page as non-executable (NX).

The Linux operating system already includes support for AMD’s NX technology and Microsoft will include support for it in Windows XP Service Pack 2. When an attempt is made to run code from a marked data page the processor hardware will raise an exception and prevent the code from executing. The NX technology would have stopped the Blaster worm dead in its tracks if it had been available and widely adopted back in 2003.

Currently support for this feature is limited to 64-bit processors, but Microsoft expects future 32-bit processors to contain execution protection as well \([4]\). Consumers are also expected to upgrade their 32-bit computers to 64-bit computers in due time.

---

\(^1\)Also known as buffer overflow.

\(^2\)There exist other non x86 processors that can mark pages as non-executable too.
Sandboxing

To help thwart buffer overrun attacks on 32-bit processors that lack the NX functionality Microsoft will add software checks in Service Pack 2 for Windows XP that will include checks of the two types of memory used by native code, the heap and the stack. The protection added to these two kinds of memory structures is called sandboxing according to Microsoft [4]. All binaries in the system have been recompiled with the new protective measures. For a more in-depth description please read Microsoft’s white paper on Service Pack 2 for Windows XP [4]. Because this is a software measure the system will take a small performance hit. There exists similar technology for other operating systems such as Linux.

5.4 Possible phishing solutions

In this section a few suggestions will be made on how to improve the current situation, not to eliminate the problem entirely. It is impossible to stop all online fraud, but it is possible to make it harder to commit fraud online or at the very least make it harder to get away with it.

Spam filters

Most phishing emails target big well known companies such as eBay and PayPal. The emails are sent as bulk email also known as spam to the receivers, with a forged sender address. Spam filters could mark emails with eBay as the sender as spam or delete them unless the sender IP-address is a well known eBay email server. The same thing could be done for all of the most popular phishing targets. Phishers would be forced to adapt their business model and target smaller companies, and fewer persons would be hurt.

Spam filters will continue to develop and capture more fraudulent emails. Important to notice is that many computer users recovered the fraudulent emails from their bulk email folder because they thought the spam filter made a mistake according to MillerSmiles [18]. A solution to this problem would be to move such emails to a fraud folder or mark them as frauds.

Identification tokens

The financial services targeted such as eBay and PayPal use usernames and passwords to identify the users. There exists three different main types of identification listed below in table 5.1.

The first group something you know typically means that the user knows a secret such as a password. This is what the most popular sites targeted by phishers use. The second group something you are typically means that the user possesses some human attribute, a biometric feature that can be scanned such as a fingerprint or retinal scan. The problem with biometrics is that it is still quite expensive and that some users find it intrusive. The third group something you have typically means
5.4 Possible phishing solutions

1. Something you know.
2. Something you are.
3. Something you have.

Table 5.1. The main methods of identification.

that the user has got a particular physical device that can be used to authenticate
the user. This physical device or security token is typically a smart card. Smart
cards are fairly cheap, but they are more expensive than passwords.

For a service like PayPal or eBay that most users use to transfer small amounts
of money a smart card solution would become too expensive. However a possible
security improvement would be to give all users that reach above a certain threshold
a security token for free, and offer lesser users to buy one.

Internet infrastructure

A standard practice by phishers is to register a site at a cousin url, e.g. ebay-
billing.com if they wish to scam eBay users. It would help if the domain name
registrars refused to register such addresses. The problem is that such a system
probably would require manual review of suspected cousin domain names and that
some legitimate sites such as paypalsucks.com would be hurt.

One of the worst flaws in todays Internet infrastructure is the email system.
The email system contains no authentication system that verifies that the sender
is who he or she claims to be. It is very easy to send emails with forged sender
addresses. A solution to this problem would be very helpful when it comes to
combat spam and phishing, but this thesis will not deal with this problem.

Anti-fraud software

Several of the most targeted companies are releasing anti-phishing software. This
anti-phishing software is most often released in the form of toolbars that can be
installed in Internet Explorer. eBay and PayPal offer the eBay toolbar with the
"Account Guard" feature.

The eBay toolbar [7] warns the user when visiting a potentially fraudulent (spoof)
website by displaying a red light, and by displaying a green light on the eBay and
PayPal websites. The toolbar also lets the user report spoof web sites and warns
the user whenever the user enters their eBay or PayPal password on a non eBay
web site.

PayPalSucks.com is a legitimate consumer complaints site for unhappy PayPal users.
User education

Knowledge and common sense is very important when it comes to preventing phishing, fraud and identity theft. The users needs to be made aware of these issues. They need to know that the from email address can be falsified, they need to learn how to separate an authentic url from a "cousin-url" and they need to learn never to trust emails asking for personal details. A good start is to stop clicking on the links in emails from various financial firms and go to the site directly by using a bookmark or typing the address manually.

5.5 Backups

There is no such thing as being 100% protected against the different threats described in chapter 4 while being connected to the Internet. It is important to keep backups so that the system can be restored to a previous state if a destructive worm or other malware program infects the computer. Backups can also help recover from many non computer security related problems.

According to Gollmann [10] there exists three main aspects of computer security. These three aspects are listed below in table 5.2.

1. Confidentiality.
2. Integrity.
3. Availability.

<table>
<thead>
<tr>
<th>Table 5.2. The main aspects of computer security.</th>
</tr>
</thead>
</table>
| Worms, trojans and other malware might target all three main aspects, while other threats might target only one or two of the main aspects. Phishing is an example of an attack that usually targets the victim’s confidential financial data only. It is important to understand that backups do not protect against attacks targeting confidential data. However backups can help recover from an attack that corrupted files (integrity) that might result in an operating system crash (availability).

Disk space price is continuously dropping, and there is no indication that this drop will stop. Today it makes sense for almost everyone to take backups, even if no data that are considered important exists on the computer. The cost of taking backups today are often negligible when compared to the inconvenience an operating system crash as a result of an attack might cause.

Today there exists several programs that can backup a whole system to a hidden partition on the disk drive, or to DVD discs. These backup programs can then do incremental backups in order to preserve disk space and keep the backup up-to-date. Two such programs are Symantec’s Norton Ghost™ and IBM’s Rapid Restore™. Both programs exist as easy-to-use versions for home computer users.
Chapter 6

User Survey

A common opinion among today's IT security professionals is that the average home computer user is normally not aware of the threats against their home computers. That many of them don't care, or don't know, about computer security at all, their computers is just another piece of consumer electronics like a TV-set or a DVD-player. Because of their lack of interest, or knowledge, about computer security issues they miss important information provided by the different security and software vendors. As long as their computer functions normally in their opinion they are not interested in computer security issues. They only react when something disrupts their normal pattern of use. Then it is usually already too late.

This user survey is an attempt to find out what some real world users think about computer security, and whether they are aware of the current security threats or not. This survey is also an attempt to investigate what their current state of security is, and if they are up-to-date with the latest software patches.

The survey focuses on the security habits of some real world users with different backgrounds. Ten participants took part in the survey and it was never meant to be a huge statistical investigation.
6.1 Background

The interview was meant to give answers to several questions raised earlier in the thesis regarding home computer security. It was important to get feedback from real world users, not just computer security professionals and white papers, in order to avoid the usual stereotype of a home computer user as a person that know little or nothing about computer security.

The most important security issues raised earlier in the thesis are all related to different kinds of vulnerabilities. One main class of vulnerabilities is weaknesses and security holes in the operating systems. It was important to find out how well the home computer users were protected against attacks exploiting these vulnerabilities. Did the users run Windows Update regularly to update their systems? Did the users update their application programs to avoid any security issues related to them?

It was also important to find out how well protected the computers were against virus and worm infections, and other malware such as spyware and dialers. Had the users installed an anti-virus program to protect their computers against viruses and worms, was the anti-virus software up-to-date, and how often was the anti-virus software updated? Did the users know what a firewall was, and were their computers protected by one. Were the users aware of the dangers of spyware, dialers and other malware, if they were aware of the dangers did they protect themselves by running an anti-spyware program regularly?

Another major threat to home computer security is the user. Did the users know how to behave on the Internet? Did they know how to use email without getting infected?

When interviewing persons it is very important that the interviewers opinions don’t influence the answers of the interviewed person. One way to achieve this was to use a well constructed questionnaire that the interviewed persons were asked to complete without any interference of the interviewer. Another significant aspect of using a questionnaire is that all persons that took part in the interview answered the same questions.

It was very important to keep the questionnaire fairly short, to keep the interviewed persons interested, to avoid any ticks in the wrong boxes. It was decided that the questionnaire shouldn’t be longer than one page. SecurityFocus has got a security checklist [11] for home computer users that was used as a template for the questionnaire. The most relevant points in the checklist were transformed into questions in the questionnaire, in addition to this some relevant questions were added that had no corresponding point in the checklist. An introduction to the survey was also added, to provide some instructions on how to complete the questionnaire, that they could explain their answers to specific questions by writing down an explanation at the other side of the questionnaire. Of course all the persons interviewed were anonymous, this is also clearly stated on the questionnaire. The resulting questionnaire can be found in appendix A.
6.2 Results

The results of the survey are presented in this section. The sections below correspond to the sections in the questionnaire that was used in this survey. The questionnaire can be found in appendix A.

6.2.1 Windows

Some interesting observations were that many users didn’t know what it meant to run a computer as an administrator. Even if the users knew what it meant, they still didn’t know whether they ran Windows as an administrator or not (4/10). Most users in this survey are running Windows XP (8/10). The default access level in Windows XP is administrator, and most users never changed this setting and were effectively running as administrators (6/8). An interesting observation was that even advanced users, the computer science master student, didn’t know whether they ran Windows as an administrator or not.

The most common password was no password at all (4/10), this is also the default setting in Windows XP. Some users actually had a good knowledge about how to choose a good password, and they used it in practice (4/10). One user also thought he picked a good password, but when the interviewer asked whether the password was a dictionary word or not, he became unsure about the password proof.

When it comes to Windows Update the interviewed users can be split into two groups. The group that do update Windows (7/10), and the group that never update Windows (3/10). There was a strong connection between not updating Windows and the use of dial up modems (3/3). There was also a strong connection between updating Windows and broadband usage (6/7). In the group that do update Windows auto-updates are fairly uncommon (1/7). The main reason for this is that the users don’t feel comfortable with auto-updating, and they are used to update manually. One user even felt so uncomfortable with Windows Update

<table>
<thead>
<tr>
<th>Occupation</th>
<th>Age</th>
</tr>
</thead>
<tbody>
<tr>
<td>High school student</td>
<td>20</td>
</tr>
<tr>
<td>Biology student</td>
<td>23</td>
</tr>
<tr>
<td>Comp. Sci. master student</td>
<td>25</td>
</tr>
<tr>
<td>Clerk</td>
<td>30</td>
</tr>
<tr>
<td>Nursing student</td>
<td>33</td>
</tr>
<tr>
<td>Teacher</td>
<td>37</td>
</tr>
<tr>
<td>Aerobic instructor</td>
<td>44</td>
</tr>
<tr>
<td>Engineer</td>
<td>47</td>
</tr>
<tr>
<td>Farmer</td>
<td>57</td>
</tr>
<tr>
<td>IT Professional</td>
<td>61</td>
</tr>
</tbody>
</table>

Table 6.1. Occupation and age of interviewed persons.
so that he always updated his anti-virus software prior to updating Windows. The reasons for not updating Windows at all varied. Most users in this group said that they had nothing important on their computers (2/3), and didn’t understand why someone would like to attack their computers. Some users ignored Windows Update completely, depending on lack of knowledge or interest (3/10). The Windows XP users either disabled the automatic downloading of new patches, or didn’t know what the reminder about the new patches that had been downloaded meant.

The users that didn’t update Windows didn’t update Microsoft Office either. Among the persons that did update Windows most updated Microsoft Office, but only sporadically (4/7).

6.2.2 Security software

All persons interviewed knew what a computer virus or worm was in that sense that it is "something evil that can infect and harm the computer in various ways". Most users had an anti-virus program installed (8/10), but some of the anti-virus programs were not set to update themselves automatically. This resulted in that several of the interviewed persons thought they were protected against viruses, when in fact the anti-virus program never had been updated. Two other interesting observations were made. One of the more advanced users didn’t have an anti-virus program installed. One person thought he had an anti-virus program installed when in fact there were no anti-virus program installed. The reason for this was that he got a Norton anti-virus CD when he bought the computer so he thought the program was already installed.

The majority of the interviewed persons knew, or thought they knew what a firewall is (6/10), but not all of them actually had a firewall installed and enabled. The most popular firewall was Windows XP’s built in firewall ICF. One interviewed person answered that he didn’t have a firewall installed, but after inspection it was obvious that he actually had Windows XP’s built in firewall enabled. One of the more advanced users in this survey had tried a more sophisticated firewall that asked for permission for every single application or service that wished to access the Internet. After some time it became an irritating moment to answer yes or no, so he uninstalled the entire firewall, instead of lowering the security settings. He was running his computer entirely unprotected.

Most of the people that were familiar with the term spyware did have anti-spyware programs installed (3/5). The people with anti-spyware software used to find spyware installed when they scanned their computers. In most cases the anti-spyware software found only cookies belonging to spyware sites, but on some occasions spyware advertisement software had been found. None of the users that used anti-spyware programs updated them automatically. Several of the users without anti-spyware software didn’t know what spyware was, but several of them had spyware installed on their computers. They got extra popups containing advertisement messages for various companies, even on sites like Microsoft’s Windows Update. One dialup user without any anti-spyware software installed even said that he once got a porn dialer installed, even after clicking no on the Internet Explorer.
auto-install prompt.

6.2.3 Internet and email

Half of the users in the survey thought they knew how to use email attachments in a secure way (5/10). Some of them were still unsure; because they knew about viruses that can be activated without clicking on an attachment. All persons in the interview ignored spam, and didn’t unsubscribe to them. They also ignored ads telling them that their computer might be infected by virus.

Several persons use to do online shopping; however most of them only trust well known companies and would never buy something from an unknown or smaller company using their credit card number. The level of trust is larger when buying something with a COD\textsuperscript{1} system. The interviewed persons were generally quite unaware of the importance of secure web pages when buying stuff online.

6.3 Summary

The main reason why many ordinary users don’t worry about computer security is that they think there is nothing important on their computers, so why would someone want to attack their computer. Ordinary users don’t read security bulletins, they get their information from mainstream press, if they get it at all. As seen in section 3.4.1 mainstream press writes about hackers attacking computers in order to steal information. Articles like that further strengthens the opinion that virus writers and hackers only want important information, and that there is no need to protect the home computer.

Both interest and knowledge are important factors that affect home computer security. Interest in home computer security leads to better protection of the home computer, and a better knowledge about security related issues. Knowledge about security related issues often leads to a better computer security, but the survey showed that there are exceptions. Some users are well aware of the threats, but still don’t care to protect their computers.

Windows Update is not made for dialup users. The patches and service packs are large, and take a very long time to download. Several hours is not uncommon. Errors are likely to occur during this download process. The user survey clearly showed a strong connection between dialup usage and the lack of up-to-date operating systems.

The survey shows that many users don’t feel comfortable with automatically updating their software, such as anti-virus programs and operating systems. Most users prefer to manually update their software. The users feel that they will lose control over their own computer when allowing auto-updates. Some users don’t trust Microsoft’s Windows Update service, and prefer to update their anti-virus programs prior to updating Windows.

\footnotesize{\textsuperscript{1}Cash on delivery.}
Security products, such as firewalls, with too many advanced features can be counter productive. If the security product asks too many questions in order to achieve the desired level of security it quickly becomes irritating. The user might uninstall the whole security product altogether instead of lowering the security settings.

The presence of spyware applications are very common in today's home computers. The survey confirmed this, several users had spyware applications installed without their knowledge. They thought it was normal with all the popups, e.g. that Microsoft served popup ads on their Windows Update service. Most users were completely unaware about the dangers of spyware.

The survey showed that the average level of awareness among ordinary home computer users is relatively low, and will probably remain relatively low in the near future. In order to raise the general level of awareness it is important to make use of mainstream media, to reach out to the majority of users with the right information in the right time. It is important to get the journalists interested and educated in these issues, so that they report about this in right way. One other possible way to reach out to the general public could be to run advertisement campaigns.
Chapter 7

Conclusions per threat category

Home computer security is one of the most important areas in computer security in general. This is a previously forgotten area that has become increasingly more important lately and probably will become even more important in the future. The number of people with computers at home are still increasing, and the number of interconnected computers each person has is increasing. TV-sets, game consoles, mobile phones and other consumer electronics will soon all be connected to the Internet. All these processes raise concerns about security issues and how to protect the assets from being corrupted in different ways. This thesis has focused on the current state of home computer security, and how it might be possible to improve it.
7.1 Default settings

Chapter 3 has shown that the most common operating systems have very lax default security settings. The user survey in chapter 6 found out that less advanced computer users, that make up the bulk of the computer users today, are unlikely to change these default security settings. An example of this is that the most common operating system among home computer users, Windows XP Home Edition has services enabled that listens on multiple network ports as shown in figure 3.3. Most of these services have no use at all for the ordinary home computer users. Other problematic default settings that affect computer security are the hide file extensions for known file types, the default behavior for patch downloads and the firewall that is disabled by default. If Windows had shown the file extensions by default a lesser number of users would have been fooled by virus emails with double extensions attachments. If the firewall had been enabled by default it would have prevented or at least slowed down the spread of the Blaster and Sasser worms.

Service Pack 2 for Windows XP will address many of the issues discussed above. Important to remember is that Service Pack 2 will only be released for Windows XP, and that many persons still run older Windows versions at home. Another observation is that it is not the first time Microsoft has released patches that address security issues. Patches in the past has strengthened the default security settings in Outlook Express, but virus and worm authors found new ways to get into the computer. They will probably find new ways to get into the computer even after Service Pack 2 has been installed, if it is installed at all.

7.2 Security holes

This thesis has pointed out that security holes in the software is to blame for many of the problems the average home computer user faces. There is not much the average user can do about these security holes, except updating the software on a regular basis. Many programs today offers auto-updating functionality, but as shown in the user survey in chapter 6 most users feel uncomfortable with auto-updating their software.

A lot of the security holes today are related to various types of buffer overflow attacks. Buffer overflow attacks are an ancient form of attacks that has been around since the seventies, and it’s mostly due to weaknesses in the C and C++ programming languages. There has been technology available for quite some time to help prevent these buffer overflow vulnerabilities, but that technology has either resulted in higher software development costs, or worse performance of the running programs. Recently PC processor manufacturers such as AMD and Intel started to add hardware support to their processors to help prevent buffer overflow attacks without any slowdowns. AMD has added this technology called NX to their 64-bit processors. It will take some time to replace older processors, but in the future the impact of buffer overflow vulnerabilities can be expected to decrease due to this.
7.3 Windows Update

The user survey in chapter 6 clearly shows there is a strong connection between dialup usage and not updating Windows. Updating Windows via Windows Update can be a very tedious task for most dialup users. The main problem is that the patches can be quite big and they take a long time to download. There are several ways to ease this problem, one way is better compression technology, another way is to only download the patches needed, e.g. why download the Sasser patch when the firewall is enabled? Microsoft will add better compression technology and smarter patch download in Service Pack 2 for Windows XP; however the problem will remain for Windows 98 users.

7.4 Automated worms

In recent years fast spreading fully automated worms like Code Red, Slammer, Blaster and Sasser created huge problems throughout the world. By using different spreading techniques these worms are able to infect a huge number of vulnerable hosts in a relatively short time. Fortunately none of these worms was harmful in the sense that they destroyed important data such as files on the computers; however they all generated a huge amount of network traffic that caused congestion on the local network, and the Internet. It is only a matter of time until much more malicious worms will be found in the wild. To decrease the possibility of being infected by such worms it is recommended to have a firewall enabled, and to keep both the operating system and the anti-virus software updated.

All these worms have one thing in common, they all use different kinds of buffer overflow vulnerabilities to propagate. The recent addition of Execution Protection (NX) to the new 64-bit processors is an attempt to address this issue. When these NX processors are used together with operating systems that supports NX, such as Linux or Windows XP’s 64-bit Edition, the infection processes will be completely blocked.

The conclusion is that worms like this will continue to be one of the worst threats to global computer security for some time, but the problem will gradually diminish when old computers are phased out, and will eventually go away entirely.

7.5 Email worms

Worms using email as the main medium for propagation have become one of the most common type of worms. Older email worms often had embedded scripts that Outlook Express automatically executed when the user looked at the email, either in the preview pane or as a whole, and as a result of this infected the computer. Microsoft has since then released patches that tightened the security in Outlook Express. This forced email worm creators to rely upon social engineering techniques to trick the user into executing the virus. Microsoft will further tighten the security in Service Pack 2 for Windows XP 5.2; however the worm creators have found ways
around this in the past and probably will find it this time as well. Email worms have already started to use alternative ways of propagation, such as file sharing programs as KaZaA and public network shares.

### 7.6 Spyware

Spyware is a relatively new threat against home computer security and there are many indications that it is also a growing problem. Most users are still completely unaware of what spyware is and this was confirmed in the user survey in chapter 6. It was also confirmed that many users had spyware installed on their computers without their knowledge. The users lack of knowledge about spyware is the main reason why they don’t use any anti-spyware programs to protect their computers and their privacy. The spyware problem is expected to grow in the near future. One reason for this is that anti-virus vendors cannot add full support for spyware detection into their products because it is sometimes hard to separate a legitimate program from a spyware. This might leave the anti-virus vendors open for lawsuits from the spyware vendors.

### 7.7 Phishing

This thesis has shown, in section 4.3, that phishing is becoming increasingly popular. This problem is also expected to grow in the near future because the number of ordinary users are increasing for every day, and there are many indications that organized crime is getting interested in phishing and other scams such as the infamous Nigeria letters. These problems are mainly social engineering problems. Technical solutions might improve the situation somewhat, but in order to stop or at least decrease this problems the awareness of ordinary users have to be raised in some way.

### 7.8 The users

The level of knowledge among ordinary users about the different threats varies a lot. Almost every user knows about viruses and worms, and that it is good to have an anti-virus program installed. At the same time almost no one is aware of the spyware problem. Most users either are completely unaware or uninterested of the security issues. One of the main reasons for this uninterest is that a lot of people think that they don’t have anything important on their computers, so why would anyone try to target their computer.

If it was possible to increase the general awareness of the security related issues among the ordinary users this would result in huge gains in home computer security. The problem is to reach out with the important information to the general public. Mainstream media often write about the latest worms and how to protect the computers against them. The problem is that journalists often write about it in
such a way that the user’s view that they don’t have anything important on their computer is confirmed. Many users also simply ignore information like this because they are completely uninterested.

Improvements in home computer security would lead to an increased level of security in other sectors too, e.g. increased home computer security would make it harder to pull off DDoS attacks against businesses.
Chapter 8

Summary

Home computer security is a very problematic area today, and it will continue to be a problematic area in the future. The main problem is that most home computer users are not aware of the threats and how to protect themselves. Many ordinary users are also completely uninterested in these issues.

Worms that use buffer overflow vulnerabilities to infect computers is a serious threat to global computer security today. Techniques like hitlist scanning further increases this threat, while firewall adaptation decreases it somewhat. The NX technology introduced in new mainstream processors will stop worms like this. The threat from these worms will slowly diminish as older computers are replaced with newer computers that support the NX technology, but this will take time. However, this will not stop worms that use other methods of propagation. Tighter default security settings in the operating systems is an attempt to decrease the spread of such worms, but there are already indications that these worms will find alternative methods of propagation such as file sharing programs.

New threats against home computer security are also emerging. An example of a relatively new threat that will continue to grow in importance in the near future is spyware programs. There are also many indications that organized crime is getting interested in making money by targeting home computer users and their computers. Phishing is one of the methods that can be used to gain access to the users bank accounts and credit cards.

The conclusion is that some major threats of today will slowly diminish over time, only to get gradually replaced by new threats, threats that will rely more on social engineering techniques.

The most important thing is to raise the security awareness among ordinary people, but this is at the same time the hardest thing to do. How do you get someone that don’t care interested?
Bibliography


Appendix A

Questionnaire

This appendix contains the questionnaire that the persons interviewed were asked to complete before the interview started. In addition to the two page questionnaire this appendix contains some short instructions to the interviewer how to carry out the interview. Not all questions asked are covered in the questionnaire and the interview instructions, but these are the questions used to start and steer the discussion in order to get the information needed for this thesis.
Thank you for participating in this survey. Try to answer the questions as best as you can by checking one check box per question. If you do not know the answer to a question please check don't know instead of guessing. You will be anonymous, your name will not be mentioned in the final thesis. If you wish to clarify your answer on a specific question please do so by writing down the number of the question and the clarification on next page.

### Windows
1. Do you run Windows as an administrator?  
2. Did you pick a good password to log on to Windows?  
3. Is Windows Update set to automatically download and install updates from Microsoft?  
4. Do you run Windows Update manually to download and install updates from Microsoft? If the answer is yes: how often do you run Windows Update?  
5. If you run Microsoft Office: how often do you check Office Update for updates?

### Security software
6. Do you know what a computer virus or worm is? If the answer is yes:  
   Do you have an anti-virus program installed?  
   What is the name of your anti-virus program?  
   Does your anti-virus program automatically update itself?  
7. Do you know what a firewall is? If the answer is yes:  
   Do you have a personal firewall installed and running?  
   Do you use default settings or personalized settings?  
8. Are you familiar with the term “spyware”? If the answer is yes:  
   Do you have an anti-spyware program installed?  
   Does your anti-spyware program automatically update itself?

### Internet and email
9. Do you know how to use email attachments securely?  
10. Do you respond to spam, even to “unsubscribe”?  
11. Do you ignore ads that tell you that your computer has been hacked?  
12. If you buy online do you make sure that sensitive information is only entered on secure web pages (https)?
If you wish to clarify an answer in the questionnaire please do so by writing down the number of the question together with your clarification on this page.

________________________________________________________________________________

________________________________________________________________________________

________________________________________________________________________________

________________________________________________________________________________

________________________________________________________________________________

________________________________________________________________________________

________________________________________________________________________________

________________________________________________________________________________

________________________________________________________________________________

________________________________________________________________________________
Questions to ask

1. Point out to the user that he or she will be anonymous, that their name will not be mentioned in the thesis. Also point out that the purpose of this survey is to get a better picture of what the state of home computer security is today. That it is not meant to find any errors in the users computer security.

2. Ask whether the user has something to tell about about his or her computer security before starting to ask questions.

3. Ask the user to fill out the questionnaire.

4. Ask some more in-depth questions based on the questions in the questionnaire.

5. Ask whether the user's computer has been infected by a virus, worm, trojan horse or spyware in the past. If the answer is yes, which worms and viruses?

6. If the user agrees, check how secure the users computer is. How long ago was Windows updated?, how many uninstalled windows patches were there? Office? Is there an anti-virus program installed, how long ago was it updated? Do the user have a firewall installed, is it enabled? Spyware, -- if the user agrees, check for spyware on the computer, which spywares were installed?
In English

The publishers will keep this document online on the Internet - or its possible replacement - for a considerable time from the date of publication barring exceptional circumstances.

The online availability of the document implies a permanent permission for anyone to read, to download, to print out single copies for your own use and to use it unchanged for any non-commercial research and educational purpose. Subsequent transfers of copyright cannot revoke this permission. All other uses of the document are conditional on the consent of the copyright owner. The publisher has taken technical and administrative measures to assure authenticity, security and accessibility.

According to intellectual property law the author has the right to be mentioned when his/her work is accessed as described above and to be protected against infringement.

For additional information about the Linköping University Electronic Press and its procedures for publication and for assurance of document integrity, please refer to its WWW home page: http://www.ep.liu.se/

© Ulf Frisk, Semir Droicic