Palestine Polytechnic University
Department of Administrative Science and Informatics
Information Technology

Information Security

By:
Fadi Swate
Mohammad A. Amro
Mohammad M. Haddad
Rana Al-Natsheh
Somaya Al-Qwasmeh

Presented to:

Ms Ahlam Qura'

2004

Introduction

What is computer security?

Computer security is the process of preventing and detecting unauthorized use of your computer. Prevention measures help you to stop unauthorized users (also known as "intruders") from accessing any part of your computer system. Detection helps you to determine whether or not someone attempted to break into your system, if they were successful, and what they may have done.

What's before applying security ?

What resources are we trying to protect?

A hacker who compromises or impersonates a host will usually have access to all of its resources; like files, storage devices, phone lines .. etc. and from a practical perspective , some hackers are most interested in busing the identity of the host , not only to reach its dedicated resources but also to have an opportunity to make a link or some connection to other target ,possibly more interesting targets.
Other might actually be interested in the data on your machine , weather it is sensitive company material or government secrets.

Many enhanced techniques enable the entering your computer although you have a security system.

The strength of ones computer security defenses should be suitable to the threat outsiders.

So computer security is not a goal it’s a means toward a goal that is "Information Security".

The last question to be answered before deploying a security is:

How much security can be offered?

We can spilt the cost in two parts direct financial expenditures such as building a firewall.

so as a solution , machines with sensitive files may require extra level of passwords or file encryption , and we will talk about this later in this study.

The fact is one or every one wants to protect all such resources , here the obvious answer is to stop attackers at the front door or not let them into the computer system in the first place.

This leads us to our second major question :
Against whom must the computer system be defended?

Techniques that maybe enough against a teenager with a modem are quite useless against a major intelligence agency so they may use gateway

The other type is the in direct ones resulting from problems of convenience and productively and even moral problems.

Too much security can hurt as surly as too little can.

- Finding the proper balance is tricky but surly necessary
- One more point is worth mentioning . even if you do not believe you have valuable assets it is still worth keeping hackers out of your machine.

The Need For Data Security

Each major advance in information technology changes our ideas about data security. Consider the use of written messages to replace those carried in the memory of a messenger. Written messages are less prone to error, and since the courier need not know the message, but can destroy it in an emergency, there could be better security. Yet written messages can be concrete evidence of conspiracy or 'spying whereas a carrier of a spoken message might escape unsuspected. The need to hide the content of a written message must therefore have been realized very soon, and there is evidence that codes and ciphers appeared almost with the beginning of writing.

Such varied data security problems a from the more resent advances in information technology — large stores and microprocessors which give us processing wherever we need it. The microprocessor and the floppy disc create a new and urgent problem of safeguarding software. The requirements summed up by the phrase 'data security' do not stay the same; they change as the technology changes.
In order to avoid repeating the same phrases we will use conventional names for the actors in the security drama. The bad guys who are trying to do something with the system which

the designers would like to avoid will be called the enemy' 11 their activities will be called 'attacking' the system.

The advance of information technology has sparked off a public debate on the Subject of individual privacy. Like many public debates it expresses both rational
And irrational fears. Everyone is now alerted to the real dangers of inaccurate personal information and uncontrolled access to files. Most advanced countries have introduced laws to enforce a reasonable degree of individual data privacy and others have such laws in preparation. If we think of privacy as the legal concept, then security of data is one of the means by which the privacy can be obtained.
The implementation of these new laws is likely to produce applications for data security techniques.

Of the three operations carried out in information systems, storage, processing and transmission, it is undoubtedly data transmission that carries the greatest of security risks. A communication network consists of numbers of cables, radio links, switches and multiplexers in a variety of locations, all of these parts of the system being potential targets for 'line taps' or 'bugs'. It is impossible to make a widespread network physically secure, therefore security measures depend on information Techniques such as cryptography.

No data can be made secure without physical protection of some sort, of the equipment The effect of good design is to concentrate the need for physical security not to circumvent it entirely. In particular, processing of data usually (perhaps always) requires those data to be in clear form, not enciphered; therefore processors themselves must be protected from intrusion, such as the attachment of radio bugs. In many systems the data and operations needing the greater degree of security can be contained in one box of modest size, physically strong and designed to destroy its stored secrets when it is opened. This is called a tamper- resistant module and it is a central element of many systems which this book will describe

Security and people

The owners of a system depend for its security in the first place on the integrity
of the supplier which itself depends on the people who design build and maintain the system When it is in operation keys and passwords are introduced which protect it from enemies outside, including enemies in the ranks of the suppliers, unless software changes have subverted the protection. With good design, the security then depends on the people who operate the system and carry out its security –related procedures.

In a well-designed system it should be clear who is being trusted and to what extent, but there is no way to make the system proof against, unlimited deceit.

The Law

the 1986 act contains terms that are not defined Law, for that matter, even within the country, is not much help The Internet should be available to everyone even hackers The internet provides many new opportunities, but these cannot be accessed if you have a fortress-under-siege mentality. Still there are risks associated with opining up your system .

In the aftermath of the worm, question have been raised about how the virus spread how it was contained and what steps if any are needed to increase Internet security. These questions have been the meetings and reports prepared by government agencies and university researchers. A GAO report filed on the request of the government reported the main vulnerabilities The 1dentified vulnerabilities included the lack of a focal point for addressing internet wide security problems security weaknesses at some host sites and problems in developing distributing and installing systems software fixes and inept or ill-trained administrators ten years down the road new and emerging web security problem still can be broadly traced back to these underlying problems

Security in Web-based s stems is a fundamental question where much could have been learned from failures in earliend to the basic t access points to the enterprise network from remote locations. In addition, organizations need to provide security for:

1. Network and system administrators accessing network equipment and connected devices.
2. . Laptop computers used by mobile professionals and telecommuters.
3. Specific websites within the corporate intranet or extranet.
4. E-mail messages transported over private or public networks.
5. Several aspects of the organization's information assets' security ties in very tightly with its web server security, starting with the publicly accessible site, the intranet. The main focus throughout this book, however, is on the Web-connected systems.

Intruders and Networks

Hacking

Why Hack?

Intruders (hackers, attackers, or crackers) may not care about your identity. Often they want to gain control of your computer so they can use it to launch attacks on other computer systems.

Having control of your computer gives them the ability to hide their true location as they launch attacks, often against high-profile computer systems such as government or financial systems.

Intruders may be able to watch all your actions on the computer, or cause damage to your computer by reformatting your hard drive or changing your data.

How easy is it to break into my computer?

Unfortunately, intruders are always discovering new holes to exploit in computer software. The complexity of software makes it increasingly difficult to thoroughly test the security of computer systems.

When holes are discovered, computer vendors will usually develop patches to address the problem. However, it is up to you.

Networks Security against intruders

In this section we will mentioned first some technological terms user in networks after that how intruders may use.

Technology used in Networks

This section provides a basic introduction to the technologies that provide a short overview of each topic.

What does broadband mean?

Broadband is the general term used to refer to high-speed network connections. In this context, Internet connections via cable modem and Digital Subscriber Line (DSL) are frequently referred to as broadband Internet connections

Bandwidth is the term used to describe the relative speed of a network connection, for example, most current dial-up modems can support a bandwidth of 56 kbps

What is cable modem access?

A cable modem allows a single computer (or network of computers) to connect to the Internet via the cable TV network. The cable modem usually has a LAN (Local Area Network) connection to the computer.

What is DSL ?

Digital Subscriber Line (DSL) Internet connectivity, unlike cable modem-based service, provides the user with dedicated bandwidth. However, the maximum bandwidth available to DSL users is usually lower than the maximum cable modem rate because of differences in their respective network technologies. Also, the "dedicated bandwidth" is only dedicated between your home and the DSL provider's central office ; the providers offer little or no guarantee of bandwidth all the way across the Internet.

How are broadband services different from traditional dial-up services?

Traditional dial-up Internet services are sometimes referred to as "dial-on-demand" services. That is, computer only connects to the Internet when it has something to send, such as email or a request to load a web page. Once there is no more data to be sent, or after a certain amount of idle time, the computer disconnects the call. Also, in most cases each call connects to a pool of modems at the ISP, and since the modem IP addresses are dynamically assigned, computer is usually assigned a different IP address on each call. As a result, it is more difficult for an attacker to take advantage of vulnerable network services to take control of your computer.

Broadband services are referred to as "always-on" services because there is no call setup when your computer has something to send. The computer is always on the network, ready to send or receive data through its network interface card (NIC). Since the connection is always up, your computer’s IP address will change less frequently , thus making it more of a fixed target for attack.

Many broadband service providers use well-known IP addresses for home users. So while an attacker may not be able to single out your specific computer as belonging to you, they may at least be able to know that your service providers' broadband customers are within a certain address range, thereby making your computer a more likely target than it might have been otherwise.

The table below shows a brief comparison of traditional dial-up and broadband services.

	Dial-up	Broadband
Connection type	Dial on demand	Always on
IP address	Changes on each call	Static or infrequently changing
Relative connection speed	Low	High
Remote control potential	Computer must be dialed in to control remotely	Computer is always connected, so remote control can occur anytime
ISP-provided security	Little or none	Little or none
Table 1: Comparison of Dial-up and Broadband Services		

How is broadband access different from the network used at work?

Corporate and government networks are typically protected by many layers of security, ranging from network firewalls to encryption. In addition, they usually have support staff who maintain the security .

ISP is responsible for maintaining the services they provide to customer, customer probably won't have dedicated staff on hand to manage and operate the network. customer ultimately responsible for his own computers. As a result, it is up to him to take reasonable precautions to secure your computers

What is a protocol?

protocol is a well-defined specification that allows computers to communicate across a network.

What is IP?

IP stands for "Internet Protocol". It can be thought of as the common language of computers on the Internet. , it is important to know a few things about IP in order to understand how to secure the computer.

What is an IP address?

IP addresses are similar to telephone numbers , when we want to call someone on the telephone, we must first know their telephone number. Similarly, when a computer on the Internet needs to send data to another computer, it must first know its IP address.

IP addresses are typically shown as four numbers separated by decimal points, or “dots”. For example, 10.24.254.3 and 192.168.62.231 are IP addresses.

Every computer on the Internet has an IP address associated with it that uniquely identifies it. However, that address may change over time, especially if the computer is

- dialing into an Internet Service Provider (ISP)
- connected behind a network firewall
- connected to a broadband service using dynamic IP addressing.

What are static and dynamic addressing?

Static IP addressing occurs when an ISP permanently assigns one or more IP addresses for each user. These addresses do not change over time.

Dynamic IP addressing allows the ISP to efficiently utilize their address space. Using dynamic IP addressing, the IP addresses of individual user computers may change over time.

If a dynamic address is not in use, it can be automatically reassigned to another computer as needed.

What is NAT?

Network Address Translation (NAT) provides a way to hide the IP addresses of a private network from the Internet while still allowing computers on that network to access the Internet.

NAT can be used in many different ways, but one method frequently used by home users is called "masquerading".

Using NAT masquerading, one or more devices on a LAN can be made to appear as a single IP address to the outside Internet. This allows for multiple computers in a home network to use a single cable modem or DSL connection without requiring the ISP to provide more than one IP address to the user. Using this method, the ISP-assigned IP address can be either static or dynamic. Most network firewalls support NAT masquerading.

What are TCP and UDP Ports?

TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) are both protocols that use IP. Whereas IP allows two computers to talk to each other across the Internet, TCP and UDP allow individual applications on those computers to talk to each other.

In the same way that a telephone number or physical mail box might be associated with more than one person, a computer might have multiple applications running on the same IP address. Ports allow a computer to differentiate services such as email data from web data.

A port is simply a number associated with each application that uniquely identifies that service on that computer. Both TCP and UDP use ports to identify services.

Some common port numbers are 80 for web (HTTP), 25 for email (SMTP), and 53 for Domain Name System (DNS).

What is a firewall?
Firewalls is : a system or group of systems that enforces an access control policy between two networks. In the context of home networks, a firewall typically takes one of two forms:

- Software firewall - specialized software running on an individual computer.
- Network firewall - a dedicated device designed to protect one or more computers.

Both types of firewall allow the user to define access policies for inbound connections to the computers they are protecting. Many also provide the ability to control what services (ports) the protected computers are able to access on the Internet

The Risk

What is at risk?

As mentioned Information security is concerned with three main areas:

- Confidentiality :information should be available only to those who have rightfully have access to it

- Integrity : information should be modified only by those who are authorized to do so .

- Availability : information should be accessible to those who need it when they need it

These concepts apply to Internet users just as much as they would to any corporate or government network. users probably wouldn't let a stranger look through your important documents or any other thing personal Also, you should have some assurance that the information you enter into your computer remains intact and is available when you need it.

Some security risks arise from the intruders via the Internet.

The most known type of intruders are hackers :

Hacker, in computer science, originally, a computer phile—a person totally engrossed in computer programming and computer technology. In the 1980s, with the advent of personal computers and dial-up computer networks, hacker acquired a pejorative connotation, often referring to someone who secretively invades others' computers, inspecting or tampering with the programs or data stored on them. (More accurately, though, such a person would be called a “cracker.”) Hacker also means someone who, beyond mere programming, likes to take apart operating systems and programs to see what makes them tick.

Some Types of Risks

Intentional misuse of your computer

The most common methods used by intruders to gain control of home computers are briefly described below.

- Trojan horse programs
- Back door and remote administration programs
- Denial of service
- Being an intermediary for another attack
- Unprotected Windows shares
- Mobile code (Java, JavaScript, and ActiveX)
- Cross-site scripting
- Email spoofing
- Email-borne viruses
- Hidden file extensions
- Chat clients
- Packet sniffing
- Trojan horse programs

Trojan horse programs

are a common way for intruders to trick networks users into installing "back door" programs. These can allow intruders easy access the hacked computer without user knowledge, change the system configurations, or infect the computer with a computer virus.

Back door and remote administration programs

On Windows computers, three tools commonly used by intruders to gain remote access to user computer are BackOrifice, Netbus, and SubSeven. These back door or remote administration programs, once installed, allow other people to access and control user computer.

Denial of service

Another form of attack is called a denial-of-service (DoS) attack. This type of attack causes user computer to crash or to become so busy processing data that he is unable to use it. In most cases, the latest patches will prevent the attack.

Being an intermediary for another attack

Intruders will frequently use user computers for attacking other systems user computer is just a convenient tool in a larger attack.

Unprotected Windows shares

Unprotected Windows networking shares can be used by intruders in an automated way to place tools on Windows-based computers attached to the Internet.

Mobile code (Java/JavaScript/ActiveX)

There have been some problems with mobile code (e.g. Java, JavaScript, and ActiveX). These are programming languages that let web developers write code that is executed by your web browser. Although the code is generally useful, it can be used by intruders to gather information (such as which web sites you visit) or to run destructive code on your computer.

It is possible to disable Java, JavaScript, and ActiveX in your web browser. its recommend that you do so if user are browsing web sites that he are not familiar with or do not trust.

Chat clients

Internet chat applications, such as instant messaging applications, provide a mechanism for information to be transmitted bi-directionally between computers on the Internet.

Because many chat clients allow for the exchange of executable code, they present risks similar to those of email clients. As with email clients, care should be taken to limit the chat client's ability to execute downloaded files. As always, user should be wary of exchanging files with unknown parties.

Packet sniffing

packet sniffer is a program that captures data from information packets as they travel over the network. That data may include user names, passwords, and personal information that travels over the network in clear text.

Actions home users can take to protect their computer systems

We recommends the following practices to users:

- Consult your system support personnel if you work from home
- Use virus protection software
- Use a firewall
- Don't open unknown email attachments
- Don't run programs of unknown origin
- Disable hidden filename extensions
- Keep all applications (including your operating system) patched
- Turn off your computer or disconnect from the network when not in use
- Disable Java, JavaScript, and ActiveX if possible

Further discussion on each of these points is given below.

Recommendations

Consult your system support personnel if you work from home

If user use your broadband access to connect to network, your ISP may have policies or procedures relating to the security for user network.

Use a firewall

Its strongly recommend the use of some type of firewall product, such as a personal firewall software package. Network firewalls (software or hardware-based) can provide some degree of protection against these attacks. no firewall can detect or stop all attacks, so it's not sufficient to install a firewall and then ignore all other security measures.

Don't run programs of unknown origin

User must never run a program unless he knows it to be authored by a person or company that he trust. Also, don't send programs of unknown origin to your friends , simply because they are containing a Trojan horse program.

Keep all applications, including your operating system, patched

Vendors will usually release patches for their software when a problem or threat has been discovered. Most product documentation offers a method to get updates and patches. User should be able to obtain updates from the vendor's web site. Read the manuals or browse the vendor's web site for more information.

Some applications will automatically check for available updates, and many vendors offer automatic notification of updates via a mailing list. Look on your vendor's web site for information about automatic notification. If no mailing list or other automated notification mechanism is offered you may need to check periodically for updates.

"www.windowsupdate.com is an example for all files needed to patch for sasser worm."

Turn off your computer or disconnect from the network when not in use

Turn off your computer or disconnect its Ethernet interface when you are not using it. An intruder cannot attack your computer if it is powered off or otherwise completely disconnected from the network.

Disable Java, JavaScript, and ActiveX if possible

Be aware of the risks involved in the use of "mobile code" such as ActiveX, Java, and JavaScript. A malicious web developer may attach a script to something sent to a web site, such as a URL, an element in a form, or a database inquiry. Later, when the web site responds to you, the malicious script is transferred to your browser.

Turn off your computer or disconnect from the network when not in use

Turn off your computer or disconnect its Ethernet interface when you are not using it. An intruder cannot attack your computer if it is powered off or otherwise completely disconnected from the network.

Disable Java, JavaScript, and ActiveX if possible

Be aware of the risks involved in the use of "mobile code" such as ActiveX, Java, and JavaScript. A malicious web developer may attach a script to something sent to a web site, such as a URL, an element in a form, or a database inquiry. Later, when the web site responds to you, the malicious script is transferred to your browser.

The most significant impact of this vulnerability can be avoided by disabling all scripting languages. Turning off these options will keep you from being vulnerable to malicious scripts. However, it will limit the interaction you can have with some web sites.

Turn off your computer or disconnect from the network when not in use

Turn off your computer or disconnect its Ethernet interface when you are not using it. An intruder cannot attack your computer if it is powered off or otherwise completely disconnected from the network.

Disable Java, JavaScript, and ActiveX if possible

Be aware of the risks involved in the use of "mobile code" such as ActiveX, Java, and JavaScript. A malicious web developer may attach a script to something sent to a web site, such as a URL, an element in a form, or a database inquiry. Later, when the web site responds to you, the malicious script is transferred to your browser.

Turn off your computer or disconnect from the network when not in use

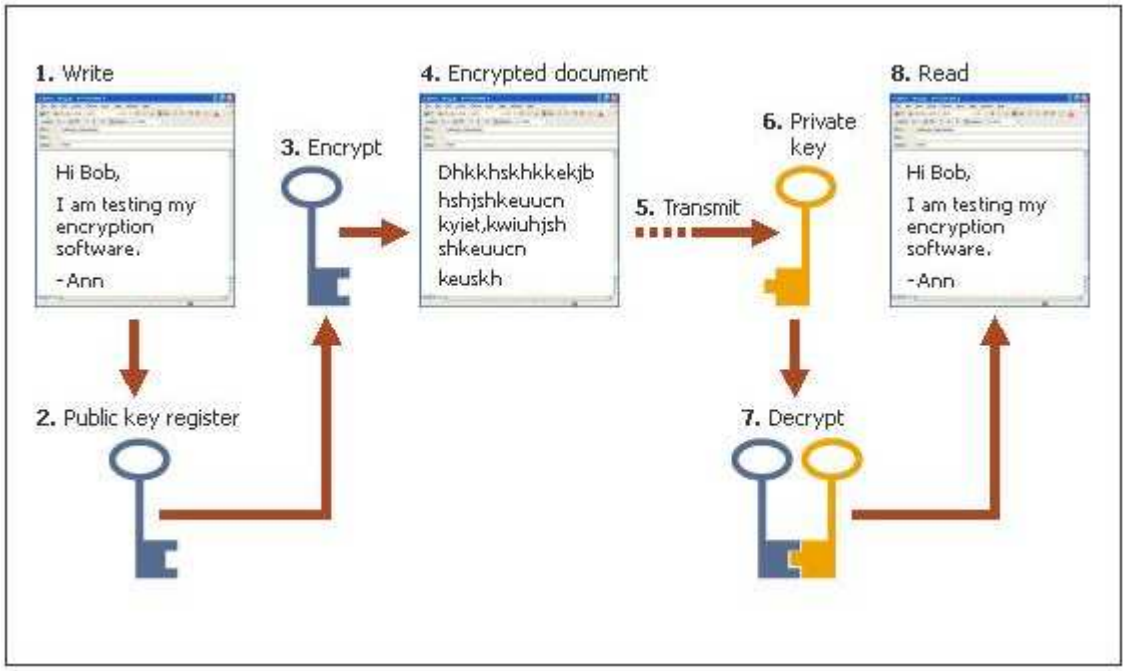
Turn off your computer or disconnect its Ethernet interface when you are not using it. An intruder cannot attack your computer if it is powered off or otherwise completely disconnected from the network.

Another methods used to secure the protocols like the TCP/IP

Encryption

Encryption is process of converting messages or data into a form that cannot be read without decrypting or deciphering it. The root of the word encryption—crypt—comes from the Greek word kryptos, meaning “hidden” or “secret.”

How Encryption Works



Encryption uses a step-by-step procedure called an algorithm to convert data or the text of an original message, known as plaintext, into ciphertext, its encrypted form. Cryptographic algorithms normally require a string of characters called a key to encrypt or decrypt data. Those who possess the key and the algorithm can encrypt the plaintext into ciphertext and then decrypt the ciphertext back into plaintext.

Popular Encryption Systems

Three of the most popular cryptography systems used are :

- the Data Encryption Standard (DES),
- Pretty Good Privacy (PGP).

- Rivest, Shamir, Adleman (RSA) system.

DES uses a single key for both encrypting and decrypting. It was developed by International Business Machines Corporation (IBM) and approved by the United States National Institute of Standards and Technology in 1976.

The Rivest, Shamir, Adleman (RSA) algorithm is a popular encryption method that uses two keys. It was developed for general use in 1977 and was named for the three computer scientists—Ronald L. Rivest, Adi Shamir, and Leonard Adleman—who originated it.

The RSA Data Security Company has been highly successful in licensing its algorithm for others to use.

PGP is an encryption system that also uses two keys. It is based on the RSA algorithm. PGP was invented by software developer Philip Zimmerman and is one of the most common cryptosystems used on the Internet because it is effective, free, and simple to use

Other Cryptosystems

This part is the most important for us because its used in networks and generally in the internet

Secure Sockets Layer (SSL), a protocol developed by Netscape Communications Corporation for transmitting private documents via the Internet

Secure Hypertext Transfer Protocol (S-HTTP), designed to transmit individual messages, also use encryption methods.

Email Security

Email, Or Electronic Mail, Is Becoming More And More Popular As People Learn To Communicate Again With Written Words. For Many Purposes It Is Superior To A Phone Call Because You Don't Have To Catch The Person In And You Can Get Straight To The Point. No Time Is Wasted On Casual Conversation. It Also Leaves A Written Record To Refer Back To For A Response Or If You Forget Who Said What. Email Is Superior To The Traditional Office Memo Because It Uses No Paper (Save The Trees!!) And It Can Be Sent To A Whole List Of People Instantly.

Purpose: Transmitting Messages Between Computer Users

Major Advantage: Speed For Communication And The Lower Cost .

Major Disadvantage: You Don't Know If The Receiver Actually Reads It, Though You Can Find Out If They Received It. Of Course In A Phone Conversation You Don't Really Know If The Person Is Actually Listening Either!

With No Body Language Or Vocal Intonations It Is Difficult To Convey The Emotional Tone You Want.
Introduction to Email Security

Today email is so widely used that it has become the default means of communication where the correspondents feel that they can discuss matters that can be kept between them. We analyze below how this might be a dangerous illusion, especially when discussing matters with legal, business or political content and I but may comment to use email safety .

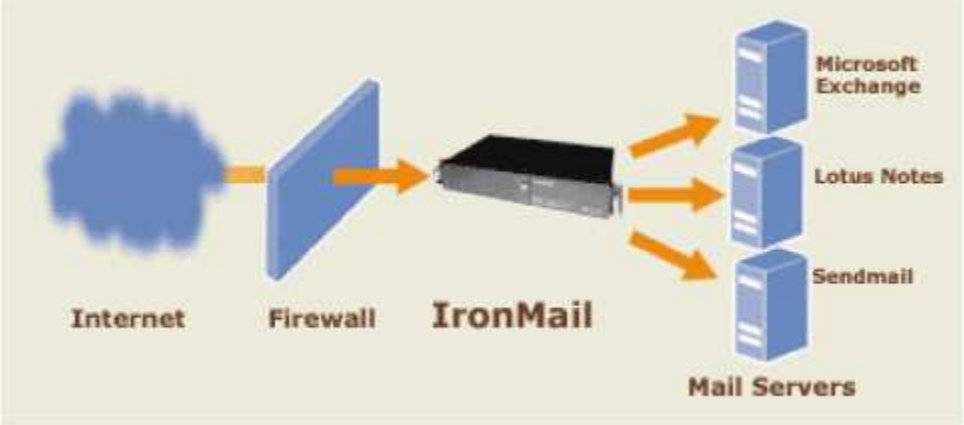
Email borne viruses

Viruses and other types of malicious code are often spread as attachments to email messages. Before opening any attachments, be sure you know the source of the attachment. It is not enough that the mail originated from an address you recognize. The Melissa virus spread precisely because it originated from a familiar address. Also, malicious code might be distributed in amusing or enticing programs.

Secure Your Communications email

Once your gateway is secure, the next step is securing your communications beyond the gateway to include your external users, partners, clients and others.
IronMail achieves this with our Mail-VPN feature.

Mail-VPN secures messages while they are in transit over the Internet, with no client interaction, using SSL technology. Mail-VPN can create secure tunnels to other mail servers or other IronMail units as well as end-users such as remote employees and telecommuters. Mail-VPN capabilities include:



The Only Comprehensive Security Solution For Email Systems
IronMail, an all-inclusive email security appliance, sits at the mail gateway between your network firewall and mail servers. Every connection to your mail server(s) passes through IronMail.
IronMail is the first product designed to provide application-level security for email.

What does this mean? It means that IronMail will not allow exploitation of vulnerabilities in your email systems or allow your email system to be used as a delivery vehicle for attacks.
Securing Email Using SSL
SSL is widely known as the technology that allows companies like E*Trade to conduct millions of dollars a day in transactions securely over the Internet However, SSL is not specifically tied to web traffic (HTTP).

SSL is a transport-layer protocol developed to secure TCP/IP-based protocols such as Internet Message Access Protocol (IMAP), Post Office Protocol (POP), and, of course, HTTP.
By applying SSL technology to email, secure email becomes as easy to secure as web browsing.

Email Security Guidelines

1) Receiving Email With Attachments

a) Unsafe File Types. Never Open Any Email Attachment With Any Of The Following File Extensions:

File .Bat .
File.Com.
File.Exe .
File.Vbs.

b) Unknown File Types. Never Open Any Email Attachment Or Internal Email Link With A File-Type Extension You Do Not Recognize.

c) Microsoft Document Types. Never Open Any Email Attachment Or Internal Email Link With A Recognized Microsoft Document Type (E.G., .Doc, .Xls, .Ppt) Even From Someone You Know And Trust Without First Running An Updated Virus Scan Program On It.

d) Ask For Plain Text. If You Receive A .Doc, .Wpd, .Xls Or Or Other Unsafe File Type As An Attachment, Even From Someone You Know, Ask Them If They Will Convert It To .Rtf, .Txt Or .Cvs And Then Resend It To You. Then Delete The Original Email And Attachment.

e) Apparently Safe File Types. Apparently Safe File Types Include:

- .Gif, .Jpg, .Tif, .Bmp, .Mpg, .Mp3, .Avi And Other Recognized Multimedia File Formats
- .Txt, .Pdf, .Rtf

f) Delete Attachments. Make Sure To Configure Your Email Client So That It Always Deletes Email Attachments When You Delete The Email It Came With. Also, Make Sure That If Mail Attachments Are Automatically Moved To A 'Trash' Folder When The Email Is Deleted, That The Folder Is 'Emptied' Each Time You Quit The Program. Otherwise Dangerous Files May Be Left Stored Indefinitely In Your Email Attachments Directory Or And/Or Your Trash Directory.

g) Disable Email 'Executables'. In Eudora, Under Tools / Options / Viewing Mail, Make Sure To Disable (Unclick) "Allow Executables In Html Content."

2) Sending Email With Attachments:

a) Avoid Sending Attachments If The Same Information Can Be Sent As Plain Text Or Rtf.

b) Rather Than Sending A .Doc File As An Attachment, It's Often Best To Cut And Paste The .Doc Content Into Your Email As Text.

c) You Can Also Convert .Xls Files To .Csv (Comma-Delimited Format) Before Sending, Thus Minimizing The Risk Of Spreadsheet Macro And Script Viruses.

d) Only If It Is Essential To Retain Document Formatting, Embedded Objects, Etc., Should You Or Your Correspondents Send Unsafe File Types -- And Then Only If You Have Recently Run An Updated Virus Scanning Program That Includes Protection From Macro Viruses.

e) If You Need To Share Formatted Documents With A Group Or Committee, Consider Converting Them To Html And Posting Them To An Appropriate Location In Swift Or web.

3) Getting security information up to date abut email .

4) Other noting of scurity:

a) Don't run programs of unknown origin

b) Turn off your computer or disconnect from the network when not in use

Turn off your computer or disconnect its Ethernet interface when you are not using it. An intruder cannot attack your computer if it is powered off or otherwise completely disconnected from the network

Finally for email security I will remember all to follow the Email Security Guidelines because you don’t know what kind of information will be in you computer and the important of it and don’t know who want the get information for your computer and who will used it.

The business on the internet

The internet has become a marketplace , with millions of customers from around the world able to enter an electronic store and make purchases at any hour of the day . the type of commerce that can be conducted is extensive and demand new technologies to make transactions easier to conduct and to prevent electronic crime.

We have already covered one business application of internet technology :an internet. However , an intranet does not need to use the internet just its technology . In this section we will look at how the internet is used to conduct business with the public . In a later section we will discuss the special features that need to be added to allow people to conduct internet business safely .

Electronic commerce

Electronic Commerce or e-commerce, the exchange of goods and services by means of the Internet or other computer networks. E-commerce follows the same basic principles as traditional commerce—that is, buyers and sellers come together to exchange goods for money. But rather than conducting business in the traditional way—in stores and other "brick and mortar" buildings or through mail order catalogs and telephone operators—in e-commerce buyers and sellers transact business over networked computers.

Types of e-commerce:-

- ✓ Product transaction
- ✓ Service transaction
- ✓ Auctions
- ✓ Business to Business

Transaction requirements

A business transaction requires the exchange of goods for equivalent value . the equivalent value is usually money or a representation thereof , such as accredit card number . Therefore , Internet transaction must provide a mechanism for such transfer . The following are desirable characteristics of Internet transaction :

>> payment:-

In the beginning of the internet business era , access to information was mostly free . information that was not free was usually made available through subscription and was protected by an access code . Goods that were sold were high-dollar items .

Internet information proprietors have begun to realize that giving away valuable information is not profitable . For example , a user who accesses a magazine article online could be charged for reading that article.

- >> Smartcards:-

Smartcard are similar to cards , but there is a major distinction between the two: Smartcards have an embedded computer chip that is capable of storing and updating data . Using a smartcard for internet trading will require a card reader/writer attached to the computer. A smartcard user would open an account with an institution that provides smartcard , such as a bank or perhaps an ISP.

Secure socket layer (SSl)/HTTP (S-HTTP)

Two of the most commonly used protocols for securing electronic transactions . SSL is supported by Netscape and Microsoft browsers and S-HTTP was developed by enterprise integration technologies and is used by spyglass, Open market , and several other software companies. It is possible to use both SSL and S-HTTP . The functional difference between the two is slight , so we shall discuss SSl as the example.

SSL is implemented at the presentation layer of the OSI reference model . It encrypts the Uniform Resource locator (URL) and the message , including the credit card number.

The SSL protocol is implemented in Web browsers and business software .Information exchanged between the customer and business is automatically encrypted before being transmitted and unencrypted by the recipient. As with all encryption methods, someone who intercepts the information can decrypt the messages, given sufficient time and energy. SSL use a public key encryption algorithm .

Secure Electronic Transaction (SET)

Another standard ,Secure Electronic Transaction (SET) ,has been jointly developed by Visa , MasterCard ,Netscape , Microsoft ,IBM, and another companies .Like SSL ,SET uses encryption to provide secure credit card transaction over the internet it includes features that ensure

>> Integrity(the packets being transmitted cannot be modified en route)

>> Confidentiality (a party to the transaction is assured of the identity of the other part)

>> Nonrepudiation (neither party can deny that the transaction took place)

In an SET transaction , the merchant dose not have access to the credit card number because it is encrypted .The merchant forwards the encrypted credit card number to an authorization center , where it is decrypted and the purchase is authorized.

This differs from the SSL approach, in the which the merchant has access to the credit card number.

Security in e-commerce:-

Established encryption methods such as Secure Sockets Layer (SSL), a protocol developed by Netscape Communications Corporation, encode credit card numbers and other information to foil would-be thieves. Shoppers can determine if the site they are using is secure by noting the "secure" icon at the bottom of their browser window. Also, the address bar of Internet browsers will carry the "https" prefix instead of the standard "http" prefix when the site is secured. Nevertheless, some consumers are reluctant to divulge credit card information over the Internet, and this reluctance has hindered the growth of e-commerce.

An alternative to credit card information is digital cash, or e-cash. In this arrangement, shoppers pay for a number of virtual credits through a single source, then use those credits as dollars when shopping. After checkout, the online retailer ships the goods to the buyer and adds shipping costs to the purchase price. Few e-commerce sites, however, offer e-cash.

Privacy :-

In addition to credit card security, many shoppers worry about privacy. To put them at ease, many Internet stores post "privacy statements" that explain their policy of sharing or not sharing customer information with other businesses. This privacy policy may include refusing to give the customer's name and e-mail address to companies that send unsolicited and unwanted commercial e-mail messages, often known as junk mail or spam. The U.S. Congress is considering legislation to force online companies to safeguard the privacy of online shoppers.

References

- Amrit Tiwana , Web Security , Digital Press , 1999.
- D.W Davies and W.L Rvice , Security for computer Networks , John Wiely & Sons lts , 1999.
- Businesses Data Communications second edition ,1999
- Tiffay Taylor , security Complete , Neil Edde 2002.
- William R. cnewick & steven M. Belliovin , Firewalls and Internet Security , Addison Wesely ,1994.

Index on The web