Internet Security

Er. Suruchi * Er. Shifali Mann ** and Er. Gurpreet Singh***
* Ludhiana College of Engineering & Technology/IT, Ludhiana, India
** Ludhiana College of Engineering & Technology/IT, Ludhiana, India
*** Ludhiana College of Engineering & Technology/CSE, Ludhiana, India

Abstract- In today's world, the internet is considered to be one of the most useful tools for people to communicate, find information and to buy goods and services. It is also a great tool to start your own online home based business. With the fast and relatively inexpensive data transfer that the internet provides, it makes sense to put it to use and to try and earn an income or just make life easier. However, with all the advantages of the internet, there are also some disadvantages. Because all financial dealings are made over the internet, it is estimated that billions or even trillions of dollars are being exchanged online everyday. This has spawned a new generation of criminals. These cyber criminals develop programs or software called spyware that invades your personal computer and starts gathering information such as your financial or personal details and sends it back to the person who developed the software. The thought of letting a stranger look at your personal and financial information without you knowing about it can definitely make you cringe in fear. Armed with this information, the cyber criminals may be able to steal money from you by committing a very serious crime called identity theft or identity fraud. In this paper various security threats and safety measures are discussed that affect internet security.
KEYWORDS: - Internet Security Threats, tools for security

I. INTRODUCTION

Since the internet has become popular, it is being used for many purposes. Through the help of the World Wide Web and websites, the internet has become very useful in many ways for the common man. Today internet has brought a globe in a single room. Right from news across the corner of the world, wealth of knowledge to shopping, purchasing the tickets of your favorite movie-everything is at your finger tips. Here is the list of some common uses of internet

Email: By using internet now we can communicate in a fraction of seconds with a person who is sitting in the other part of the world. Today for better communication, we can avail the facilities of e-mail. We can chat for hours with our loved ones. There are plenty messenger services and email services offering this service for free. With help of such services, it has become very easy to establish a kind of global friendship where you can share your thoughts, can explore other cultures of different ethnicity.

Information: The biggest advantage that internet offering is information. The internet and the World Wide Web has made it easy for anyone to access information, and it can be of any type, as the internet is flooded with information. The internet and the World Wide Web has made it easy for anyone to access information, and it can be of any type. Any kind of information on any topic is available on the Internet.

Business: World trade has seen a big boom with the help of the internet, as it has become easier for buyers and sellers to communicate and also to advertise their sites. Now a day's most of the people are using online classified sites to buy or sell or advertising their products or services. Classified sites saves you lot of money and time so this is chosen as medium by most of people to advertise their products.

Social Networking: Today social networking sites have become an important part of the online community. Almost all users are members use it for personal and business purposes. It is an awesome place to network with many entrepreneurs who come here to begin building their own personal and business brand.

Shopping: In today's busy life most of us are interested to shop online. Now a day's almost anything can be bought with the use of the internet. In countries like USA most of consumers prefer to shop from home. We have many shopping sites on internet like amazon.com, Dealsglobe.com etc. People also use the internet to auction goods. There are many auction sites online, where anything can be sold.

Entertainment: On internet we can find all forms of entertainment from watching films to playing games online. Almost anyone can find the right kind of entertainment for themselves. When people surf the Web, there are numerous things that can be found. Music, hobbies, news and more can be found and shared on the Internet. There are numerous games that may be downloaded from the Internet for free.

E-Commerce: Ecommerce is the concept used for any type of commercial maneuvering, or business deals that involves the transfer of information across the globe via internet. It has become a phenomenon associated with any kind of shopping, almost anything. It has got a real amazing and range of products from household needs, technology to entertainment.

Services: Many services are now provided on the internet such as online banking, job seeking, purchasing tickets for your favorite movies, and guidance services on array of topics in the every aspect of life, and hotel reservations and bills paying. Often these services are not available off-line and can cost you more.

Job Search: Internet makes life easy for both employers and job seekers as there are plenty of job sites which connect employers and job seekers.

Internet security is a branch of computer security specifically related to the Internet, often involving browser security but also network security on a more general level as it applies to other applications or operating systems on a whole. Its objective is to establish rules and measures to use against attacks over the Internet. The Internet represents an insecure channel for exchanging information leading to a high risk of intrusion or fraud, such as phishing. When we access internet computer sends a message over the web that uniquely identifies the computer along with its location. It allows the information to return which is requested for. With the rapid explosion of e-commerce and the Internet as a serious business tool, a lot of attention has been given to "information security." Helping businesses securely manage information has become a multi-billion dollar industry. Companies such as Verisign®, Microsoft®, Cisco®, Oracle® and SUN Microsystems®, to name a few, all spend a significant amount of time and money developing their services with security in mind. There are many facets of Internet security and there are many ways you need to protect yourself when using the Internet, whether it'd be browsing on web pages or the email or using the email. There are viruses that are out there that can be distributed through websites that can be distributed through email, even valid attachments to email can have viruses embedded in them and automatically execute when they open on your computer; so you need anti-virus software for that. Over two hundred and fifty new viruses are discovered each month. When you're browsing web pages, there could be malicious code on the web pages such as adware, spyware or even, malicious, you know very bad things like viruses that can go into your computer and delete things or send your passwords and personal information from your computer out to other users. A lot of times people will use phishing through email to try and get you to submit info, personal information or senses of information and they'll use that for the purposes of identity theft. So, why do we need the Internet security? Anytime you use the Internet you could be at risk and your information and your personal finances or even your family. So, protect yourself and make sure you know what you're doing on the Internet and that you're doing it securely. We need security so that third party cannot enter the organization and gain physical or virtual access to private information, to prevent unauthorized information from leaving the premises, monitor and control internal employees access to information and systems.

II. TYPES OF INTERNET THREATS

We are living in a digital world, were computers are not just an ordinary thing anymore but a "necessity" to our everyday lives. Most of us only knew a little about computer security threats, the most common were "virus" and "worm". There are many types of threats for internet. Some of threats are discussed below:

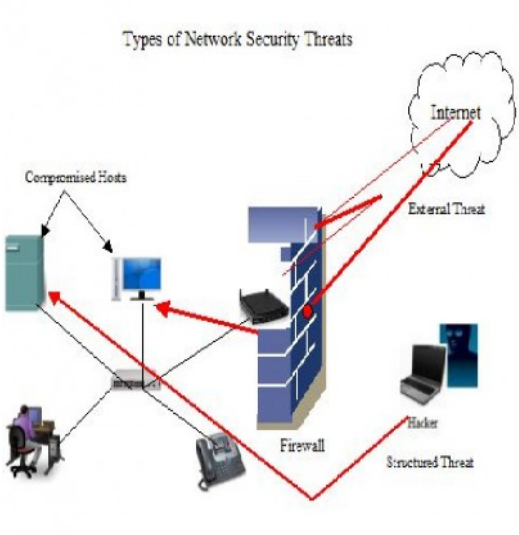

Figure 1: Types of Network Security Threats

Image Spam: Image-based SPAM has increased in the past year, and a higher percentage is making it past SPAM filters. The reason this happens is the images are varied each time a message is sent out. SPAM images are just slightly changed each time the message is sent. The difference may be a change in the border, or the variance of one pixel, but the change is enough to get past traditional content and signature-scanning filters. These SPAM messages are compared to snowflakes, because each one looks similar, but is different. Every image is in fact unique, but from a distance it will look identical.

Phishing: You receive an email that is made to look as though it comes from a legitimate company you normally do business with. The email, for example, might tell you that some sort of service normally provided to you is due to expire soon. The email directs you to a phony Web site made to look like the site of the company you do business with. Once there, you are asked to provide personal information -- such as a credit card or Social Security number -- so that your service can be continued.

E-mail Spoofing: E-mail Spoofing is when an email message appears to have originated from one source when it actually was sent from another source. E-mail spoofing is often an attempt to trick the user into making a damaging statement or releasing sensitive information (such as passwords). Spoofed e-mail can range from harmless pranks to social engineering ploys. Examples of the latter include:

E-mail claiming to be from a system administrator requesting users to change their passwords to a specified string and threatening to suspend their account if they do not comply. E-mail claiming to be from a person in authority requesting users to send them a copy of a password file or other sensitive information. Windstream, as well as most legitimate businesses, WILL NEVER ask for any sensitive information in an e-mail.

E-mail Borne Viruses: Viruses and other types of malicious code are often spread as attachments to e-mail 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. Also, malicious code might be distributed in amusing or enticing programs. Never run a program unless you know it to be authored by a person or company that you trust. Also, don't send programs of unknown origin to your friends or co-workers simply because they are amusing -- they might contain a Trojan horse program.

Chat Clients: Internet chat applications, such as instant messaging applications and Internet Relay Chat (IRC) networks, provide a mechanism for information to be transmitted bi-directionally between computers on the Internet. Chat clients provide groups of individuals with the means to exchange dialog, web URLs, and in many cases, files of any type.Because many chat clients allow for the exchange of executable code, they present risks similar to those of email clients. As with e-mail clients, care should be taken to limit the chat client’s ability to execute downloaded files. As always, you should be wary of exchanging files with unknown parties.

Overseas Money Transfer Scam: If an e-mail sounds too good to be true, then it is. You'll receive an e-mail from someone claiming to represent a foreign government or someone formerly involved with a foreign government. The person will claim that, through a change in leadership or death, he or she has been left with a large amount of money. They will ask your help getting the money out of the country, and if you help you can receive a large share of the money. The message will go on to ask you to respond to the e-mail with bank account information and other personal information to help set up the transfer. The best thing you can do is ignore the e-mail and hit the delete button.

Trojan Horse Programs: Trojan horse programs are a common way for intruders to trick you (sometimes referred to as social engineering) into installing back door programs. These can allow intruders easy access to your computer without your knowledge, change your system configurations, or infect your computer with a computer virus.

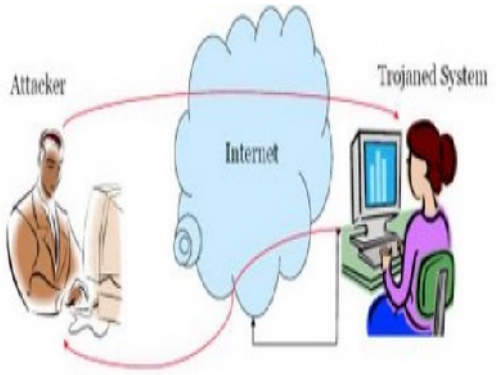

Figure 2: Trojan Horse

Denial of Service Attack (DOS Attack): Another form of attack is called a denial-of-service (DOS) attack. This type of attack causes your computer to crash or to become so busy processing data that you are unable to use it. In most cases, the latest patches will prevent the attack. It is important to note that in addition to being the target of a DOS attack, it is possible for your computer to be used as a participant in a denial-of-service attack on another system.

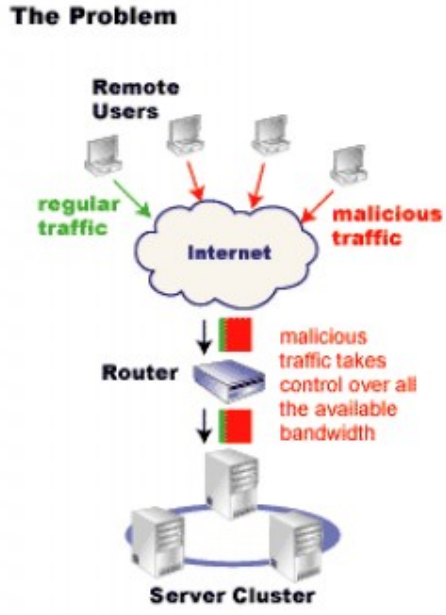

Figure 3: Denial of Service Attack

Being an Intermediary for Another Attack: Intruders will frequently use compromised computers as launching pads for attacking other systems. An example of this is how distributed denial-of-service tools are used. The intruders install an agent (frequently through a Trojan horse program) that runs on the compromised computer awaiting further instructions. Then, when a number of agents are running on different computers, a single handler can instruct all of them to launch a denial-of-service attack on another system. Thus, the end target of the attack is not your own computer, but someone else's -- your computer is just a convenient tool in a larger attack.

Modem Hijacking: This is perhaps one of the most prevalent scams on the Internet today. When you visit a web site, you'll often see pop-up ads that ask you various questions and offer you a variety of services. To receive them, all you have to do is select **yes** on one or more ads. If you haven't read the fine print, however, you can unwittingly be agreeing to have software downloaded to your modem, which then instructs your modem to make long distance calls to overseas pay-per-call services. These calls can result in hundreds of dollars in charges. This usually impacts dial-up customers, rather than broadband customers. Often you don't know this has happened until you receive your next phone bill.

Unprotected Windows Shares: Unprotected Windows networking shares can be exploited by intruders in an automated way to place tools on large numbers of Windows-based computers attached to the Internet. Because site security on the Internet is interdependent, a compromised computer not only creates problems for the computer's owner, but it is also a threat to other sites on the Internet. The greater immediate risk to the Internet community is the potentially large number of computers attached to the Internet with unprotected Windows networking shares combined with distributed attack tools. Another threat includes malicious and destructive code, such as viruses or worms, which leverage unprotected Windows networking shares to propagate. There is great potential for the emergence of other intruder tools that leverage unprotected Windows networking shares on a widespread basis.

Mobile Code (Java/JavaScript/ActiveX): There have been reports of problems with mobile code. 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 malicious code on your computer. It is possible to disable Java, JavaScript, and ActiveX in your web browser. We recommend that you do so if you are browsing web sites that you are not familiar with or do

not trust. Also, be aware of the risks involved in the use of mobile code within e-mail programs. Many e-mail programs use the same code as web browsers to display HTML. Thus, vulnerabilities that affect Java, JavaScript, and ActiveX are often applicable to e-mail as well as web pages.

Cross-Site Scripting: 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. You can potentially expose your web browser to malicious scripts by: Following links in web pages, email messages, or newsgroup postings without knowing what they link to. Using interactive forms on an untrustworthy site. Viewing online discussion groups, forums, or other dynamically generated pages where users can post text containing HTML tags.

Hidden File Extensions: Windows operating systems contain an option to Hide file extensions for known file types. The option is enabled by default, but a user may choose to disable this option in order to have file extensions displayed by Windows. Multiple e-mail borne viruses are known to exploit hidden file extensions. Other malicious programs have since incorporated similar naming schemes. The files attached to the e-mail messages sent by these viruses may appear to be harmless text (.txt), MPEG (.mpg), AVI (.avi) or other file types when in fact the file is a malicious script or executable (.vbs or .exe, for example).

Packet Sniffing: A 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 proprietary information that travels over the network in clear text. With perhaps hundreds or thousands of passwords captured by the packet sniffer, intruders can launch widespread attacks on systems.

III. TOOLS FOR INFORMATION SECURITY

We address Internet security concerns so that you can safely do online transactions with us. There are many ways to increase security while using the Internet. Some of the tools available are described below.

A. General computer security:

1. Anti-virus software
2. Firewalls

B. Web Browser Security:

1. Encryption
2. Updating your Web browser software
3. Clearing your cache

4. Cookies

C. Public Key Infrastructure (PKI):

1. Digital signatures

A. General Computer Security

Anti-Virus Software: Anti-virus software scans your computer and email messages for viruses. You have to regularly update your anti-virus software to be able to detect new viruses. Your anti-virus software helps protect the data on your computer software and your operating system.

Firewalls: A firewall acts as a barrier between internal and external computers in a network, controlling the flow of information between the two. When a computer outside the firewall tries to communicate with a computer inside, it must first communicate with the firewall, which drops, allows or denies requests before it passes them to the destination computer. This process protects the destination computer from unauthorized access.

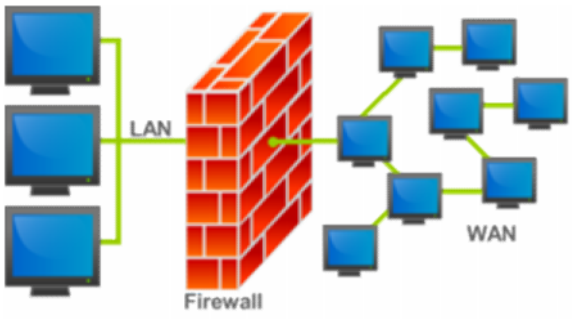

Figure 4: Firewalls

B. Web Browser Security

Encryption: Encryption has been used to transmit messages in various formats for hundreds of years; it is not a new concept created just for the Internet. As technology has evolved, so have the methods of encryption—from manually coding text to using complex computer programs. It uses a mathematical formula and an encryption key to scramble information so that an unauthorized person cannot understand the information. The scrambled information is decoded—or converted back—into the original format using the same mathematical formula and a decryption key so an authorized person can understand it. While the information is encrypted, it cannot be viewed. With **128-bit Secure Sockets Layer Version 3.0 (SSLV3)**

encryption, the privacy of information passing between your Web browser and our Web servers is ensured. Encrypting the information allows it to be transmitted and authenticated safely. Data cannot be compromised when SSL is in use. Through SSL the identity of the server computer can be verified. Although it is also possible to identify the user as well, CRA does not use this method of identification. When you send data using SSL encryption, the data is broken down into small, separate packages of information called blocks. SSL then encrypts each block. These encrypted blocks are sent over the Internet as individual network packets, and are individually addressed. Once all the packets have reached the safety of our secure Web server, they are reassembled and decrypted.

Updating Web Browser Software: If your browser does not meet our security requirement of 128-bit SSL Version 3.0 encryption, you will need to upgrade the one you have or download a new complete browser package.

Clearing Cache: When you visit a Web site, it is saved in your computer's memory and your browser's memory in an area called the cache. Your browser should display the Web site quicker the next time you visit because details about the contents, such as images and files, are stored in your cache. Your browser does not need to re-download all of the information about that Web site.

Information stored in the browser’s cache is not encrypted, so clearing the cache helps to ensure the security of your information. After you complete a secure session, you should close and reopen your browser to clear your browser’s cache of session cookies. If you are using Internet Explorer, you should also delete your temporary Internet files, before you close and reopen your browser

Cookies: A cookie is a computer text file sent to a visitor's Web browser (the software used to access the Internet such as Internet Explorer and Netscape) by a Web server (the computer that hosts the Web site) in order to remember certain pieces of information. This can useful for both Web site visitors and Web site operators because it can reduce the amount of time needed to input and process the same information each time a Web site is used.Only the Web server that originally sent the cookie can read information stored within it. Cookies can store only data that is provided by the server or that is generated by an explicit action by a visitor. They cannot read information from a visitor's hard drive.

C. Public Key Infrastructure(PKI)

PKI is a combination of policy and technology that establishes a secure working environment, allowing Internet users to conduct secure electronic transactions. PKI operates using public key cryptography and digital certificates held by each party transmitting over the Internet. This ensures that private information is kept protected from tampering and that the identities of the participants can be guaranteed. Unlike traditional cryptography that uses an identical key to encrypt and decrypt the message, public key cryptography uses one mathematical formula or algorithm—also called a key—to encrypt data and a second, related mathematical key to decrypt it. A PKI user has two keys: a public key openly accessible to anyone and tied to the digital certificate, and a private key kept secret by its holder. A message that is encrypted with a public key can only be decrypted with the corresponding private key. Using this key system ensures that no one else can view the private key holder's encrypted messages. In the Government of Canada PKI, once you have obtained your key, all you need to remember (and keep secret) is your user ID and password.

Digital Signatures: A digital signature is a type of electronic identification that can confirm the identity of the sender of a message, whether the message is encrypted or not. Digital signatures can only be generated by the signer. They can be verified, are tamperproof, cannot be forged or repudiated, and ensure that the information contained in the message is not changed during transmission.

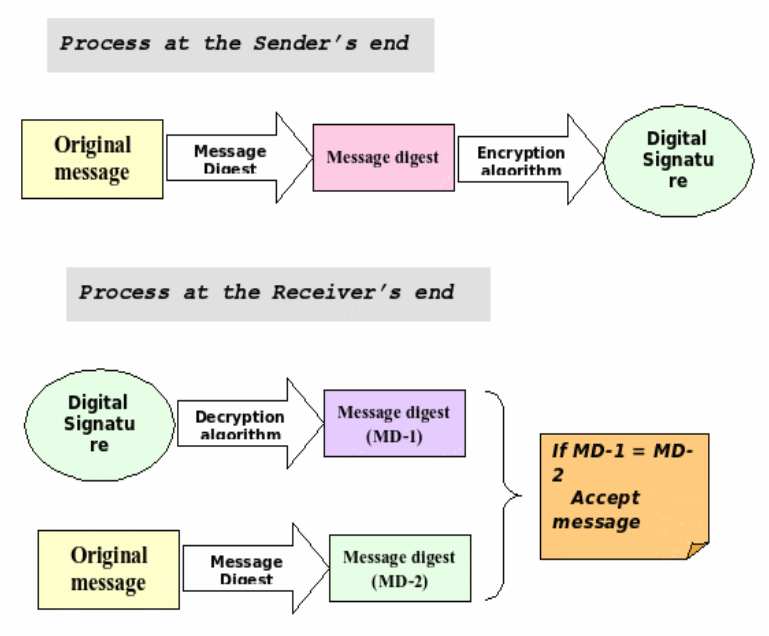

Figure 5: Digital Signatures

IV. CONCLUSION

After taking a look at many tools and options available for security, there are a lot of similarities between a security policy and Linus' security blanket. The fiber that makes up the blanket consists of the many tools and services used in a security policy; the firewalls, biometrics; passwords, access controls and documentation all are combined to cover the assets of the company. Along with the fiber that makes up a blanket, there also is a border that holds it all together, making it easy to unfold and use. For a security program, the border consists of common sense, a return on the security investment and diligence in implementing and operating the security program. Programs that are bound too tight or are created in a convoluted manner actually might end up being a detriment to the company. Security plans should be reviewed regularly, easy to use and enforceable throughout the organization.

References

[1] http://www.cra-arc.gc.ca/ntcs/scrty_tls-eng.html http://db.cs.sfu.ca/DBMiner .

[2]Ethical Hacking in Delhi www.net-hub.in/Ethical Hacking.

[3]http://xtream.online.fr/project/security.htm[4]http://ezineArticles.com/388245

[5]Network Security Threats and Solutions, Colin Daly, February, 2009.