A

Seminar report

On

Internet Security

Submitted in partial fulfillment of the requirement for the award of degree
Of MCA

SUBMITTED TO:
www.studymafia.org

SUBMITTED BY:
www.studymafia.org

Preface

I have made this report file on the topic **Internet Security**; I have tried my best to elucidate all the relevant detail to the topic to be included in the report. While in the beginning I have tried to give a general view about this topic.

My efforts and wholehearted co-corporation of each and everyone has ended on a successful note. I express my sincere gratitude to …………..who assisting me throughout the preparation of this topic. I thank him for providing me the reinforcement, confidence and most importantly the track for the topic whenever I needed it.

Acknowledgement

I would like to thank respected Mr…….. and Mr. ……..for giving me such a wonderful opportunity to expand my knowledge for my own branch and giving me guidelines to present a seminar report. It helped me a lot to realize of what we study for.

Secondly, I would like to thank my parents who patiently helped me as i went through my work and helped to modify and eliminate some of the irrelevant or un-necessary stuffs.

Thirdly, I would like to thank my friends who helped me to make my work more organized and well-stacked till the end.

Next, I would thank Microsoft for developing such a wonderful tool like MS Word. It helped my work a lot to remain error-free.

Last but clearly not the least, I would thank The Almighty for giving me strength to complete my report on time.

Contents: -

Introduction: -

The Internet is an interconnection of millions of computers belonging to various networks world over. However SAFETY OF DATA, INFORMATION AND PRIVACY IN SUCH AN ENVIRONMENT IS UNDER QUESTION. The most dangerous threats that web users face today are hacking and virus, which not only damage the web sites but corrupt and change the data stored even in the hard disk, thereby, causing downtime running into hours and weeks.

- **RISKS INVOLVED: -**

The risks of the Internet reflect its size: 50 million users, 30 thousand networks, 10+ million computers, and 137 countries. As capacity, connectivity and mobility increase, so does risk. Prominent sites are probed daily. Banks may get 50 or more probes a day. Successful attacks are automated and posted to electronic bulletin boards; attack methodologies quickly spread.

- **WHY IS INTERNET VULNERABLE?**

❖ Many early network protocols that now form part of the Internet infrastructure were designed without security in mind.

❖ Internet is an extremely dynamic environment, in terms of both topology and emerging technology.

❖ Because of the inherent openness of the Internet and the original design of the protocols, Internet attacks are quick, easy, and inexpensive and may be hard to detect or trace.

- **COST OF INSECURITY:**

Computer security attacks cost as much as $10 billion a year. An attack can damage data integrity, confidentiality or availability.Cyber-terrorism was responsible for a loss of nearly 400 million pounds from 1993 to 1995 to Great Britain only.

- **PITFALLS OF INSECURITY:**

A) LOSS OF CONFIDENTIALITY:

Important information like research data, medical and insurance records, new products speculations and corporate investment strategies can be read or copied by someone not authorized to do so.

B) LOSS OF INTEGRITY:

Modification of information in unexpected ways is known as loss of integrity. This is particularly harmful for financial data used for activities such as electronics funds transfers, air traffic control and financial accounting.

C) LOSS OF AVAILABILITY

Information can be erased or made inaccessible resulting in loss of availability. Authorized users are subject to denial of service. Availability
is often the most important attribute in service-oriented business that depend on information (e.g. airline schedule).

➢ FORMS OF ATTACK ON SECURITY:

- Hacking
- Viruses
- Cookies
- Cyber terrorism

- **HACKING: -**

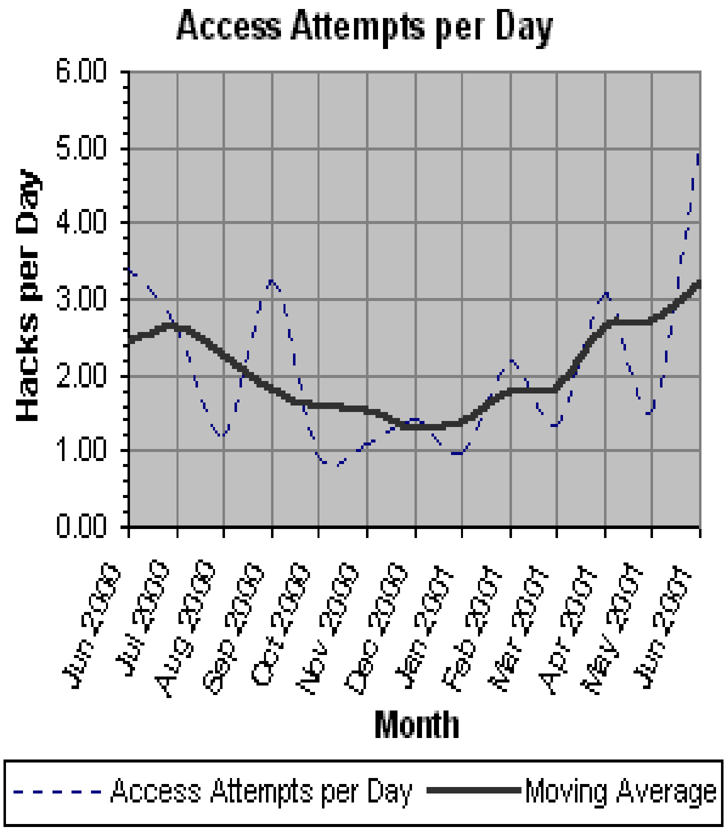
HACKING MEANS AN UNAUTHORIZED SURFER GETTING INTO A WEB SITE TO ALTER THE DATA AND INFORMATION STORED IN IT. This is normally done through the use of a 'backdoor' program installed on machine, which comes by opening an e-mail attachment. This program sends out more copies of itself to everyone in the user's address book, so it is possible for someone you know to unintentionally send you a malicious program.

❖ STATISTICS OF HACKING:

Various surveys conducted come up with interesting facts. These facts concern the types of hackers and trends in hacking.

[redacted]

As can be seen from above figure most of the hackers are amateurs who hack just for fun. Only a small percentage consists of professional hackers. A still smaller percentage consists of world-class cyber criminals



From the above graph it is clear that hacking attempts per day are on an increase. This has resulted in overall increase in hacking attempts.

❖ HOW TO REPORT HACKERS:

When an access attempt occurs, if alert popup are turned on, Zone alarm will tell the IP address of the hacker.

1. Make a note of all the information given by zone alarm. Select Start, Run... In the Run box, type in "WINIPCFG" and then click OK. This will tell what your IP address is (among other things). Write down that address.
2. Use an Internet tool like Sam Spade's address digger to look up which ISP uses this address.
3. This will return a lot of technical information. Some ISPs add remarks to this information telling you where to send abuse reports to. Make a note of any such E-mail addresses.
4. Now send e-mail to the abuse address (es).

• VIRUSES

Viruses are software programs containing malicious codes, which can affect the normal working of the computer by either altering or deleting the system information on the computer.

❖ FACTORS CAUSING VIRUSES:

1) Viruses were first seen in late 80's and the factor was spread of personal computers (PCs).

2) The second factor was use of bulletin board systems (BBS), where people could connect to BBS with modem and download software of any kind (games, office apps). BBS led to creation and use of so called Trojan Horses - the programs that reside in the computer, and based on any input like an action, computer time, disk capacity etc. usually do something really bad, like wiping the drive.

3) The third factor was creation of floppy disks, which were widely used at that time, as the hard drives were still expensive, and software usually fitted on a small capacity of floppy. Viruses often used a part of floppy data, which was preloaded and executed (boot sectors) to spread.

❖ MOTIVATION BEHIND CREATING VIRUSES:

1) Thrill of really well written code: many viruses, which mostly didn't do or didn't mean to do any damage were written simply, because coders had to write extremely efficient and small codes, to fit into boot sectors or computer memory.

2) It has got a lot with human psychology and society.

3) People love to see on T.V. talking about their virus, destroying whole of networks for the stronger kids laughed at them in kindergarten and they want to payback this time.

4) Someone writes a virus to trash a network that has offered some kind of insult (real or imagined) and due to careless thinking.

❖ TYPES OF VIRUSES:

1) Virus
2) Trojan horses
3) Worms

1) VIRUS:

a) THE BOOT SECTOR VIRUS:

Virus resides in a portion of a computer drive that is only read when the computer is booted up; at which time the virus is loaded into memory. This cripples down the system to an extent that the hard disk may have to be formatted.

e.g. Michelangelo virus

b) THE POLYMARIC VIRUS

It changes slightly each time it is executed and thus, can defeat anti-virus which search for certain strings of code to identify viruses.

e.g. Vienna by Mark Washburn

c) THE MACRO VIRUS:

It affects the word processing and spreadsheet documents that use macros. Macros can often perform system operations such as creating or deleting

files, or writing into already existing files and thus have the potential to cause a great deal of damage.
e.g. Concept

2) TROJAN HORSES:

Trojans are less deadly and generally considered sleeping viruses and do not cause extreme damages like crashing down the computer. Trojan horse is basically a program in which malicious or harmful code is contained inside apparently harmless program or data in such a way that it can get control and do its chosen form of damage, such as ruining the file allocation table on your hard disk.

3) WORMS:

Worms are spread over computer networks, and are distinct from viruses in that they do not have a host file. Often there is an attachment to the e-mail, and when the user opens the attachment, the worm is executed. Worms commonly attempt to send copies of themselves to everyone in the user's address bookworms generally use security holes in operating systems to gain access.
e.g. Internet worm

• RECENT VIRUSES DETECTED:

❖ THE LOVE BUG:

Detected on May 4, 2000 the most destructive computer worm of all times was predicted to have done billions of dollars in damage. Carrying the phrase "I LOVE YOU" in the subject line of e-mail, forced the network administrators to shut down e-mail systems.

❖ CODE RED:

Detected on June 18,2001 by eye, a computer security firm, the worm is designed to perform three basic functions:
(i) Propagate it
(ii) Deface the web page of the victim
(iii) Start a distributed denial of service attack on http\\www.whitehouse.org, the official Whitehouse website.

- **SIRCAM**

  Detected in July 2001,SIRCAM is an e-mail worm that has spread to users in 50 countries. The worm can delete files from hard drive. Experts define this worm as self-propagating worm written in English and Spanish language.

- **ANNA KOURNIKOVA**

  Detected in February 2001, this worm spreads via e-mail. The hoax e-mail carried an attachment that was identified as a picture of Russian tennis star. Once opened, it spread around the world, slowing down e-mail systems and shutting down servers.

- **MELISSA**

  Detected in April 1999, this worm is known as queen of e-mail viruses. This worm spreads through infected computer's Microsoft Outlook e-mail address book. It can delete files from hard drive.

- **NIMDA**

  Detected in September 2001,this worm spreads by sending infected e-mails that carry an attachment labeled "readme.exe". Its target is personal computers and Microsoft computer servers.

- **<u>COOKIES: -</u>**

Cookies are software that gets stored automatically in a computer, as soon as one surfs a particular site or home page of the ISP. Through this important data related to the location of user computer, his browser, name of computer, user name, ISP no. And those who plant cookies on the computer know name. Though there may not be any damage to hardware or software in this case, but it has financial implications. Developed by Netscape, this otherwise useful software for market research is now being misused more, by several websites and portals.

Some dummy e-commerce sites are specially created to attract consumers to buy product, online thereby storing relevant information about them, like age, address, and credit card no. And telephone number. Also information related to web pages visited by a surfer is stored, so that a marketer gets to know about buying habits of a potential buyer. These user profiles are utilized for market research and advertisement by the unscrupulous Web site companies who also sell data to other marketing companies, without the consent of the surfer.

❖ INCIDENTS:

PROBE

A probe is characterized by unusual attempts to gain access to system or to discover information about the system.

SCAN

A scan is simply a large number of probes done using an automated tool.

ACCOUNT COMPROMISE

This is the unauthorized use of computer account by someone other than the account owner, without involving system level or root level privileges. An account compromise might expose the victims to serious data loss and data theft.

PACKET SNIFFER

It is a program that captures data from information packets as they travel over network. The data may include user names, passwords and proprietary information that travels over the network in clear text.

DENIAL OF SERVICE

In this form of attack, attackers 'flood' a network with large volumes of data or consume a scarce resource. Disrupting connections between machines prevents access to service.

• CYBER-TERRORISM:

Unlawful manipulation of information technology for illegal purposes is called cyber-terrorism. Computer crime or cyber-terrorism comprises all possible cases where a computer or network can play a role.

1) A Cyber Terrorist will remotely access the processing control systems of a cereal manufacturer, change the levels of iron supplement, and sicken and kill the children of a nation enjoying their food.
2) A Cyber Terrorist will place a number of computerized bombs around a city, all simultaneously transmitting unique numeric patterns, each bomb receiving each other's pattern
3) A Cyber Terrorist will disrupt the banks, the international financial transactions, and the stock exchanges. The key: the people of a country will lose all confidence in the economic system.

4) A Cyber Terrorist will attack the next generation of air traffic control systems, and collide two large civilian aircraft. This is a realistic scenario, since the Cyber Terrorist will also crack the aircraft's in-cockpit sensors. Much of the same can be done to the rail lines.
5) A Cyber Terrorist will remotely alter the formulas of medication at pharmaceutical manufacturers. The potential loss of life is unfathomable.

❖ TERRORISM CAN BE CLASSIFIED: --

1) BY CAUSE
2) BY ACTION

1) CLASSIFICATION BY CAUSE:

- ❖ *RELIGION:* The religious groups seek the most damaging level, as it is consistent with their indiscriminate application of violence.
- ❖ *NEW AGE*: New Age or single issue terrorists, such as the Animal Liberation Front, pose the most immediate threat, however, such groups are likely to accept disruption as a substitute for destruction.
- ❖ *ETHNO-NATIONALISM AND REVOLUTION*:
  Both the revolutionary and ethno-nationalist separatists are likely to seek an advanced-structured capability.
- ❖ *FAR-RIGHT EXTERISM:* These groups are likely to settle for a simple-unstructured capability, as cyber terror offers neither the intimacy nor cathartic effects that are central to the psychology of far-right terror.
- ❖ *INTERNATIONAL DIPLOMACY*: Some attacks are conducted in furtherance of political and social objectives.e.g.During the Kosovo conflict in 1999; NATO computers were blasted with the e-mail bombs and hit with denial-of -service attacks by hactivists protesting the NATO bombings.

2) CLASSIFICATION BY ACTION:

- ❖ *Simple-Unstructured:* The capability to conduct basic hacks against individual systems using tools created by someone else the organization possesses little target analysis, command control or learning capability.

- ❖ *Advanced-Structured:* The capability to conduct more sophisticated attacks against multiple systems or networks and possibly, to modify or create, basic hacking tools. The organization possesses an elementary target analysis command and control, and learning capability.

- *Complex-Coordinated:* The capability for a coordinated attacks capable of causing mass disruption against integrated, heterogeneous defenses (including cryptography). Ability to create sophisticated hacking tools. Highly capable target analysis, command and control, and organization capability

➢ ***Different web site, which provide help against cyber crime: -***

Government web site: -

Commodity futures trading commission
Consumer.gov
Computer crime and intellectual property section, criminal division, U.S. department of justice
Federal bureau of investigation
Federal trade commission
Internet fraud complaint center
Securities and exchange commission
U. S. customs service
U. S. postal inspection service
U. S. secret service
U. S. sentencing commission
Washington state attorney general

Nongovernmental web site: -

American association of retired person
Better business bureau
B B B on line
Internet fraud council
Internet fraud watch
Internet scam busters
National association of attorneys general
National association of securities Dealers regulation
National consumers league
National fraud information center
North American securities administrators association

Senior net
U.S. news & world report online- citizen’s toolbox

➢ *LEVELS OF SECURITY:*

Security can be provided at three levels:
a) Client side
b) Application side
c) Network level/router level

➢ *PROTECTION MEASURES:*

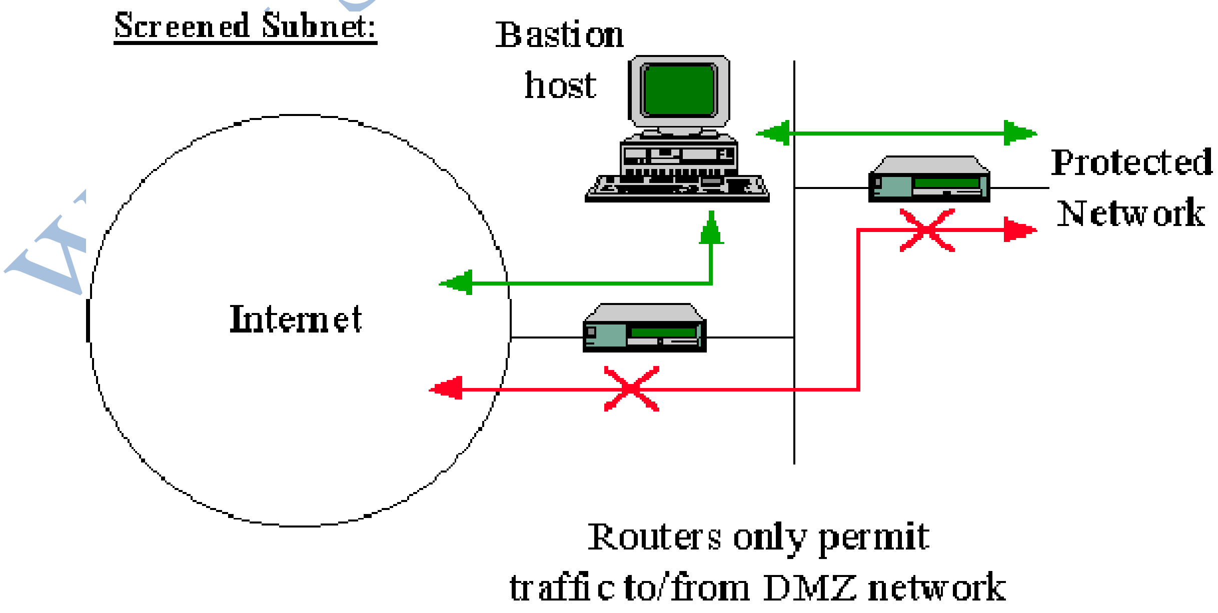
- Firewalls
- Anti-virus software
- Anti-cookie software
- Legislation

- *FIREWALLS*

TYPES OF FIREWALLS: --

A) NETWORK LAYER:

A network layer firewall called a ``screened host firewall" is represented. In a screened host firewall, access to and from a single host is controlled by means of a router operating at a network layer. The single host is a bastion host; a highly



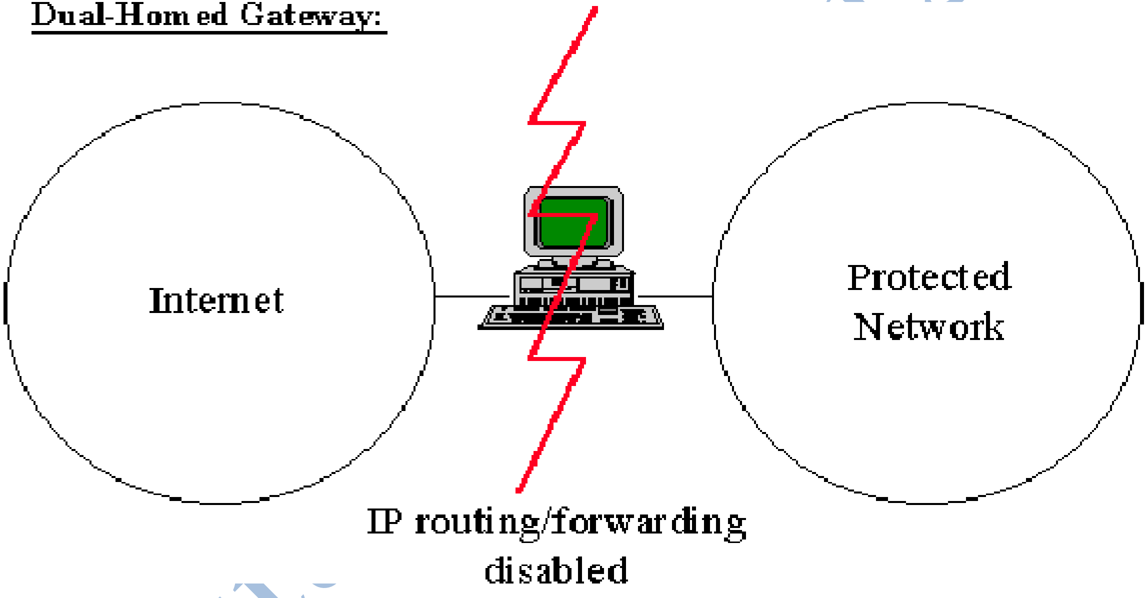
defended and secured strong point that (hopefully) can resist attack.

B) APPLICATION LAYER

An application layer firewall called a ``dual homed gateway'' is represented. A dual homed gateway is a highly secured host that runs proxy software. It has two network interfaces, one on each network, and blocks all traffic passing through it.

- ## ANTI-VIRUS SOFTWARE

Dual-Homed Gateway:



❖ PROTECTION FROM VIRUSES

A latest virus scanner should be run through the system on periodic bases.

Latest anti viruses available are: --

A) NORTON ANTIVIRUS 2003
B) McAfee VIRUSCAN 7.0
C) PC-Cillin 2003 VIRUS PROTECTION
D) Dr. SOLOMON Anti-Virus
E) SYMANTIC ANTIVIRUS 2003

• ANTI COOKIE SOFTWARE:--

1) Pretty Good privacy (PGP): encryption designer offer a program called PGP cookie cutter that will use filters to " either block or allow cookies at a user's command".
2) Luck man's anonymous cookie software disables all cookies or cookie file and allows you to browse World Wide Web with anonymity".
3) Cookie crusher software that automatically deletes the Magic-cookie and cookies. Text files at each start up.

Other anti cookie software available is:

a) Cookie Pal
b) ZDNet's cookie master
c) Cookie Crusher v2.6
d) BuZoff
e) IEClean
f) History kill

• LEGISLATION:

In addition to check the cyber-crime on technical fronts, legislation is an absolute necessity and deterrent for discouraging the cyber-terrorists. Government agencies need more teeth to effectively handle the cyber criminals. Judicial courts are to be vested with more powers for inflicting heavy penalties and punishments on such criminals.

The cyber-crimes are serious and must be addressed through legislation. In so doing, we will be in a better position to prevent and respond to cyber-terrorism if and when the threat becomes more serious.

In managing online security, it must be remembered that process is key." People have thrown technology at the problem, but the solution it requires is not strictly technical."

Because the technology is constantly changing and intruders continue to develop new tools and techniques, solutions do not remain effective indefinitely. It is necessary for companies, organizations and governments to regularly update and introduce newer security measures as often as possible.

➢ Conclusion: -

The Internet is an interconnection of millions of computers belonging to various networks world over .The most dangerous threats that web users face today are hacking and virus, which not only damage the web sites but corrupt and change the data stored even in the hard disk. There are different web sites that provide helps against cyber crime. The protections are also provides as anti-virus software, anti-cookies software, firewalls and legislation. The technology is constantly changing and intruders continue to develop new tools and techniques, solutions do not remain effective indefinitely. It is necessary for companies, organizations and governments to regularly update and introduce newer security measures as often as possible.

References: -

http://www.google.com
http://www.wikipedia.com
http://www.howstuffworks.com
www.studymafia.org