Date 18-Oct-2014

Report

ON

CYBER SECURITY

SUBMITTED BY

Deepanshu Mangla, Kalpana Raj, Diksha S

BCA Students, Amity University, Gurgaon

ACKNOWLEDGEMENT

I take this opportunity to express our profound gratitude and deep regards to my guide, Prof. NK Goyal for his exemplary guidance, monitoring and constant encouragement throughout the course of this research. The blessing, help and guidance given by her time to time shall carry us a long way in the journey of life on which we are about to embark.

We are obliged to team members of this research , for the valuable information provided by them in their respective fields. We are grateful for their cooperation during the period of our research.

Lastly, we thank almighty, our parents, brother, sisters and friends for their constant encouragement without which this research would not be possible.

Deepanshu Mangla

Kalpana Raj

Diksha S

ABOUT CMAI

CMAI is the only integrated professional registered Association in India for ICT, Education, Cyber security, Communications, Multimedia, Manufacturing Industries and Infrastructure Sector having more than 48,500 stakeholders as its members. It is an apex premier body with more than 54 International and Domestic MOU partners and representatives all over the world. In Education field CMAI is known for Cyber Security, Vocational Courses, National and State Level Education Summit and Awards etc. CMAI has so far trained more than 10,000 delegates in Cyber security and CMAI interacts with more than 1, 00,000 Educational Institutes. CMAI is also known for CMAI ICT World Communication Awards, Global ICT Forum, training and formation of Cyber Security-Ethical Hacking and Safe Web Development.

Vision: To facilitate inclusive growth of the communications sector in India through participation of all stakeholders including Service providers , Operators , Infrastructure providers and Vendors.

Mission: To create a platform, where all stakeholders of Telecom/ IT Industry , Policy Makers and International Associations can work together in creating value for the Indian Telecom/IT Sector and in providing Quality yet Affordable Products and Services to the Indian consumers.

INDEX

INTRODUCTORY

Overview

The emergence of the Internet in the late 1980s led to the evolution of cyberspace as a fifth domain of human activity and in last two decades, Internet has grown exponentially worldwide. India too has witnessed significant rise in cyber space activities and usage of internet so much so that it has not only become one of the major IT destinations in the world but has also become the third largest number of Internet users after USA and China. Such phenomenal growth in access to information and connectivity has on the one hand empowered individuals and on the other posed new challenges to Governments and administrators of cyberspace.

Cyber space has unique characteristics *viz*. anonymity and difficulty of attribution, coupled with enormous potential for damage and mischief. This characteristics not only adds to the vulnerabilities but also makes cyber security a major concern across the globe since it is being exploited by criminals and terrorists alike to carry out identity theft and financial fraud, conduct espionage, disrupt critical infrastructures, facilitate terrorist activities, steal corporate information and plant malicious software (malware) and Trojans. The emergence of cloud and mobile technology has further complicated the cyber threat landscape. Moreover, with the advent of sophisticated and malicious cyber tools physical damage on critical infrastructure and systems are inflicted and systematically information from targeted systems are stolen. All this makes cyber security an issue of critical importance with profound implications for our economic development and national security. Given the growing threats to cyber assets and all pervasive inter-connected information systems, countries around the world are engaged in actions for ensuring security of their cyber space.

Cyber security, a complex issue, cuts across domains and national boundaries and makes it difficult to attribute the origin of cyber-attacks. It, therefore, calls for a strategic and holistic approach requiring multi-dimensional and multi-layered initiatives and responses. 2

Nature of Cyber Space

The Cyber Space comprises of computer systems, computer networks and Internet. The latter includes Local Area Networks and Wide Area Networks. The Internet is a network of networks spread across the globe. Commercially, these computer systems are called servers, desktops, laptops, Personal Digital Assistants (PDAs), mobile computing platforms etc.

Unlike physical space, cyber space is anonymous and borderless. Once anybody is on Internet he can access any system on Internet spread across the globe from anywhere. The cyber space offers virtual environment where anyone can hide his identity on the network and creates a pseudo name or can acquire some other identity. The security of the computer infrastructure is of greater importance under these conditions.

Cyber Space usage: World and Indian scenario

1.6 The Department of Electronics and Information Technology informed that the Internet is a powerful force for good. Within 20 years it has expanded from almost nothing to a key component of critical national infrastructure and a driver of innovation and economic growth. It facilitates the spread of information, news and culture. It underpins communications and social networks across the world. A return to a world without the Internet is now hardly conceivable. A list of top 20 countries with highest number of internet users is given at Annexure I. Interestingly, India is at 3rd position with an estimated 100 million internet users as on June, 2011.

1.7 The Committee were informed that India is among the top five countries in Web Hosting. The rankings in web hosting during the years 2011 and 2012 is as under:-

Country	**2011 Ranking**	**2011 Percentage**	**2012 Ranking**	**2012 Percentage**
United States	1	47	1	44
Greater China	2	7	2	9
South Korea	3	7	4	8.5
United Kingdom	4	5	5	7
Canada	5	5	6	5
India	14	0.82	12	1.5

1.8 A comparative usage of cyber space worldwide and in India during the years 2005 and 2012 is as under:-

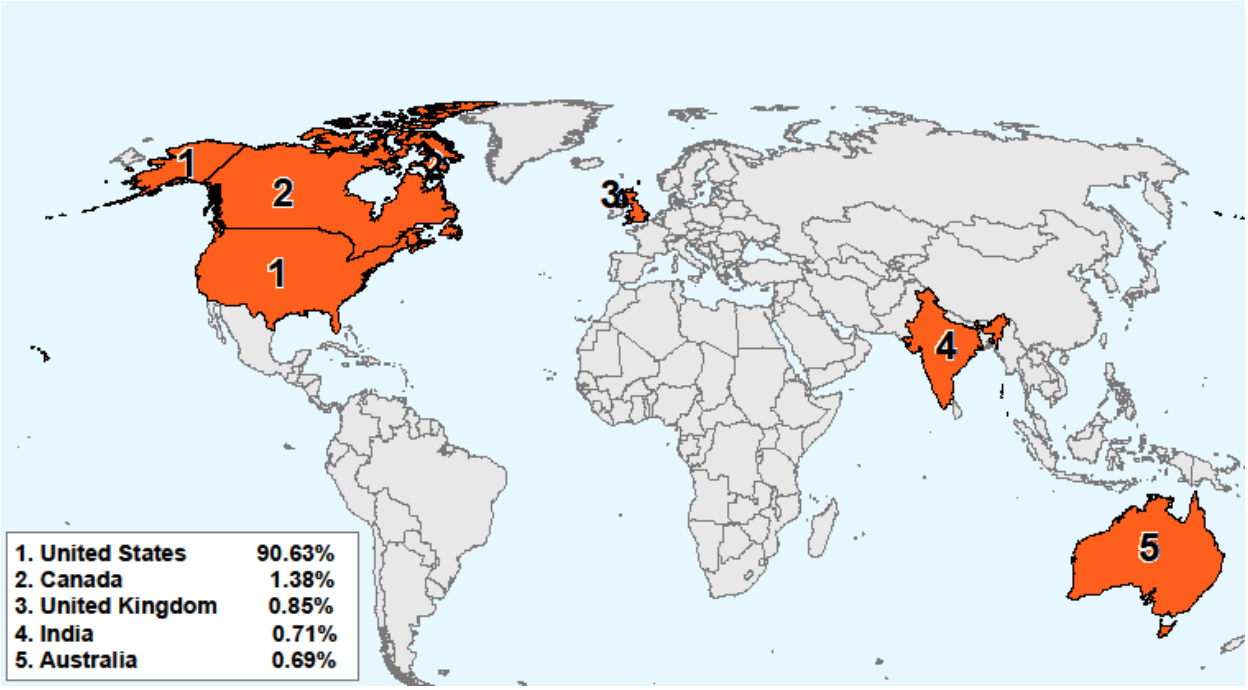
Cyber Space Usage	**World wide**		**India**	
	2005	**2012**	**2005**	**2012**
Total number of websites	7.5 million	698 million (registered) 209 million(active)	1.7 Lakhs	14 million 1.7 million '.in'(registered) 1 million '.in' (active)
Number of Internet users	720 million	2.41 billion	21 million	150 million
Number of email accounts	315 million	3.146 billion	11 million	180 million

Risks in Cyber Space

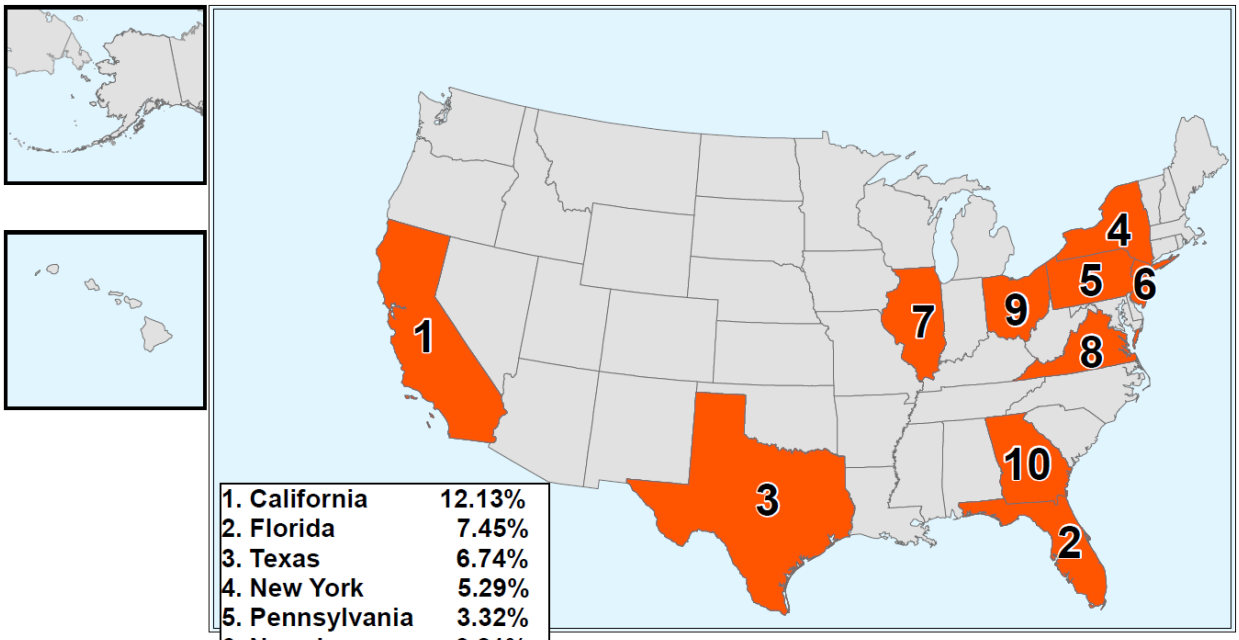
As per the Background Note furnished by the Department, the risks in cyber space are manifold. They threaten personal data security-that is to say, they may undermine the individual's ability to control the information that they have entered into or stored on connective devices such as PCs, mobile telephones, or databases operated by commercial organizations, Government agencies and others. Victims typically suffer financial loss through fraud, though in cases of identity theft they may also suffer loss of reputation, or, in extreme cases, may be accused of crimes they did not commit. Online risks may also impact upon personal safety – it means that they may lead to direct physical or psychological harm to the individual. One recent high-profile threat is the one posed to children by predatory pedophiles, which conceal their true identity whilst using the Internet to "groom" potential victims. Probably far more common is the online bullying of children by their peers, while even adults who injudiciously disclose personal information online have found that their personal physical safety has been compromised and abused. As of now, it can be said that the benefits, costs and dangers of the Internet, are poorly understood and appreciated by the general public. The current assumption that it is end users' responsibility for security bears little relation either to the capabilities of many individuals or to the changing nature of the technology and the risk. The key contributors to online risks for an individual can be summarized as follows:

- Lack of knowledge
- Carelessness
- Unintentional exposure of or by others
- Flaws in technology – for instance, in the services offered online
- Criminal acts.

Top Five Countries Ranked by the Total Number of Complaints Received by *Internet Crime Complaint Center* **(IC3) in 2013**



Top Ten States Ranked by the Total Number of Complaints Received by *Internet Crime Complaint Center* (IC3) in 2013



1. California	12.13%
2. Florida	7.45%
3. Texas	6.74%
4. New York	5.29%
5. Pennsylvania	3.32%
6. New Jersey	3.21%
7. Illinois	2.95%
8. Virginia	2.84%
9. Ohio	2.75%
10. Georgia	2.58%

Note: 10.09% of the complaints did not include location information

We many times listen in news that some hackers have hacked a website or had licked some confidential information in internet .

Did you really know what this term **“HACKER”** is .

- It is a term used in computing that can describe several types of persons

    - ***Hacker (computer security)***

someone who seeks and exploits weaknesses in a computer system or computer network

    - ***Hacker (hobbyist)***

who makes innovative customizations or combinations of retail electronic and computer equipment

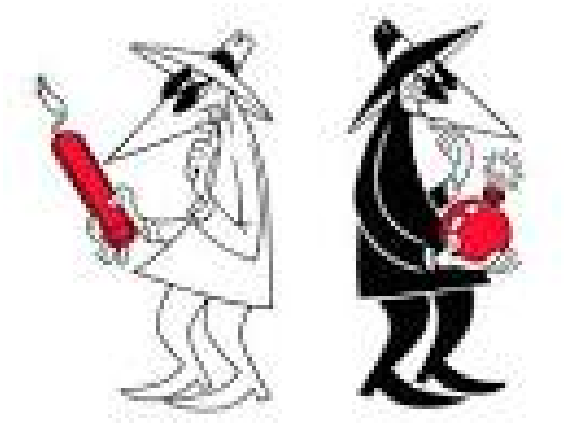
    - ***Hacker (programmer subculture)***

who combines excellence, playfulness, cleverness and exploration in performed activities

Types Of HACKERS

White hat

A white hat hacker breaks security for non-malicious reasons, perhaps to test their own security system or while working for a security company which makes security software. The term "white hat" in Internet slang refers to an **ethical hacker**. This classification also includes individuals who perform penetration tests and vulnerability assessments within a contractual agreement. The EC-Council, also known as the International Council of Electronic Commerce Consultants, is one of those organizations that have developed certifications, courseware, classes, and online training covering the diverse arena of Ethical Hacking.



Black hat

A "black hat" hacker is a hacker who "violates computer security for little reason beyond maliciousness or for personal gain" (Moore, 2005). Black hat hackers form the stereotypical, illegal hacking groups often portrayed in popular culture, and are "the epitome of all that the public fears in a computer criminal". Black hat hackers break into secure networks to destroy data or make the network unusable for those who are authorized to use the network. Black hat hackers are also referred to as the "**crackers"** within the security industry and by modern programmers. Crackers keep the awareness of the vulnerabilities to themselves and do not notify the general public or manufacturer for patches to be applied. Individual freedom and accessibility is promoted over privacy and security. Once they have gained control over a system, they may apply patches or fixes to the system only to keep their reigning control. Richard Stallman invented the definition to express the maliciousness of a criminal hacker versus a white hat hacker who performs hacking duties to identify places to repair.

Grey hat

A grey hat hacker is a combination of a black hat and a white hat hacker. A grey hat hacker may surf the internet and hack into a computer system for the sole purpose of notifying the administrator that their system has a security defect, for example. They may then offer to correct the defect for a fee.

Elite hacker

A social status among hackers, *elite* is used to describe the most skilled. Newly discovered exploits circulate among these hackers. Elite groups such as Masters of Deception conferred a kind of credibility on their members.

Script kiddie

A script kiddie (also known as a *skid* or *skiddie*) is a non-expert who breaks into computer systems by using pre-packaged automated tools written by others, hence the term script (i.e. a prearranged plan or set of activities) kiddie (i.e. kid, child—an individual lacking knowledge and experience, immature) usually with little understanding of the underlying concept.

Neophyte

A neophyte, "n00b", or "newbie" is someone who is new to hacking or phreaking and has almost no knowledge or experience of the workings of technology and hacking.

Blue hat

A blue hat hacker is someone outside computer security consulting firms who is used to bug-test a system prior to its launch, looking for exploits so they can be closed. Microsoft also uses the term *BlueHat* to represent a series of security briefing events.

Hacktivist

A hacktivist is a hacker who utilizes technology to publicize a social, ideological, religious or political message.

Hactivism can be divided into two main groups:

- Cyberterrorism - Activities involving website defacement or denial-of-service attacks.
- Freedom of information - Making information that is not public, or is public in non-machine-readable formats, accessible to the public.

Nation state

Intelligence agencies and cyberwarfare operatives of nation states.

Organized criminal gangs

Groups of hackers that carry out organized criminal activities for profit.

Most famous hacking groups

1. Anonymous - "We are Anonymous. We are Legion. We do not forgive. We do not forget. Expect us."

2. Milw0rm

3. Masters of Deception

4. LulzSec - "Laughing at your security since 2011."

5. Network Crack Program Hacker Group

Some Famous Hackers

- ***Kevin Mitnick*** does not like being called a hacker. He instead claims to be a social engineer, who has broken into the systems of Nokia, Fujitsu and Motorola. He was arrested in 1995 and served five years in jail. He now runs his own computer security consultancy company.
- ***Kevin Poulsen*** started out with an amusing hack into the phone lines of a radio station that allowed him to be the 102nd caller, which made him win a Porsche. He also broke into the phone system to reactivate old numbers. Poulsen was able to hack into the federal investigation database.
- ***Robert Tappan Morris*** creating the Morris worm. The worm ended up affecting 6,000 major Unix machines, practically shutting them down and causing millions of dollars in damage. It was probably the first worm of its kind

- ***Michael Calce*** was able to cause the temporary shutdown of sites like Yahoo, Amazon and eBay. Using the name of MafiaBoy, Calce hacked to the large commercial sites that led to denial-of-service attacks across 75 computers in 52 networks

Methodologies

The goal of any hacker is to compromise the intended target or application. Hackers begin with little or no information about the intended target, but by the end of their analysis, they have accessed the network and have begun to compromise their target. Their approach is usually careful and methodical, not rushed and reckless. The seven-step process that follows is a good representation of the methods that hackers use:

- **Step 1.** Perform footprint analysis (reconnaissance).
- **Step 2.** Enumerate applications and operating systems.
- **Step 3.** Manipulate users to gain access.
- **Step 4.** Escalate privileges.
- **Step 5.** Gather additional passwords and secrets.
- **Step 6.** Install back doors.
- **Step 7.** Leverage the compromised system.

Types of Cyber crime/attack

IP Spoofing Attacks

The prime goal of an IP spoofing attack is to establish a connection that allows the attacker to gain root access to the host and to create a backdoor entry path into the target system.

IP spoofing is a technique used to gain unauthorized access to computers whereby the intruder sends messages to a computer with an IP address that indicates the message is coming from a trusted host. The attacker learns the IP address of a trusted host and modifies the packet headers so that it appears that the packets are coming from that trusted host.

At a high level, the concept of IP spoofing is easy to comprehend. Routers determine the best route between distant computers by examining the destination address, and ignore the source address. In a spoofing attack, an attacker outside your network pretends to be a trusted computer by using a trusted internal or external IP address.

If an attacker manages to change the routing tables to divert network packets to the spoofed IP address, the attacker can receive all the network packets addressed to the spoofed address and reply just as any trusted user can.

IP spoofing can also provide access to user accounts and passwords. For example, an attacker can emulate one of your internal users in ways that prove embarrassing for your organization. The attacker could send email messages to business partners that appear to have originated from someone within your organization. Such attacks are easier to perpetrate when an attacker has a user account and password, but they are also possible when attackers combine simple spoofing attacks with their knowledge of messaging protocols.

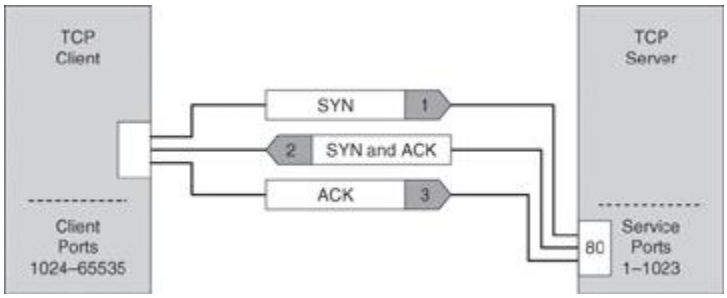
A rudimentary use of IP spoofing also involves bombarding a site with IP packets or ping requests, spoofing a source, a third-party registered public address. When the destination host receives the requests, it responds to what appears to be a legitimate request. If multiple hosts are attacked with spoofed requests, their collective replies to the third-party spoofed IP address create an unsupportable flood of packets, thus creating a DoS attack.

Technical Discussion of IP Spoofing

TCP/IP works at Layer 3 and Layer 4 of the Open Systems Interconnection (OSI) model, IP at Layer 3 and TCP at Layer 4. IP is a connectionless model, which means that packet headers do not contain information about the transaction state that is used to route packets on a network. There is no method in place to ensure proper delivery of a packet to the destination, since at Layer 3, there is no acknowledgement sent back to the source by the destination once it has received the packet.

The IP header contains the source and destination IP addresses. Using one of several tools, an attacker can easily modify the source address field. Note that in IP each datagram is independent of all others because of the stateless nature of IP. To engage in IP spoofing, hackers find the IP address of a trusted host and modify their own packet headers to appear as though packets are coming from that trusted host (source address).

TCP uses a connection-oriented design. This design means that the participants in a TCP session must first build a connection using the three-way handshake, as shown in Figure 1-4.



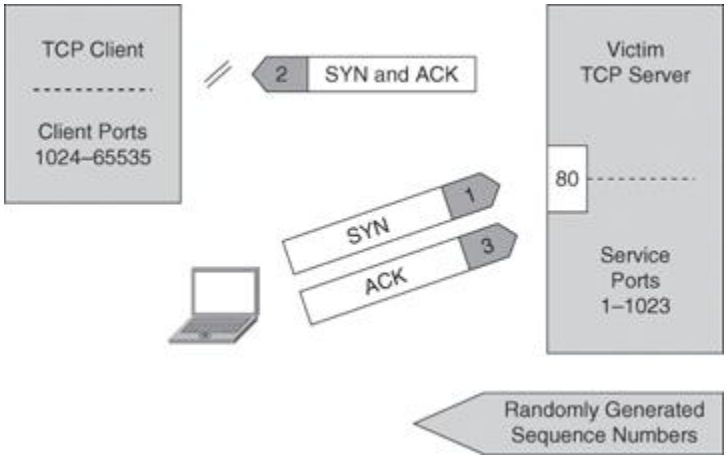
. TCP Three-Way Handshake

After the connection is established, TCP ensures data reliability by applying the same process to every packet as the two machines update one another on progress. The sequence and acknowledgments take place as follows:

1. The client selects and transmits an initial sequence number.
2. The server acknowledges the initial sequence number and sends its own sequence number.
3. The client acknowledges the server sequence number, and the connection is open to data transmission.

Sequence Prediction

The basis of IP spoofing during a TCP communication lies in an inherent security weakness known as sequence prediction. Hackers can guess or predict the TCP sequence numbers that are used to construct a TCP packet without receiving any responses from the server. Their prediction allows them to spoof a trusted host on a local network. To mount an IP spoofing attack, the hacker listens to communications between two systems. The hacker sends packets to the target system with the source IP address of the trusted system, as shown in Figure 1-5.



. Sequence Number Prediction

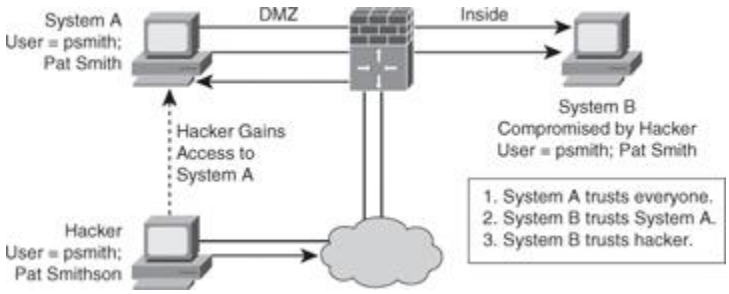
If the packets from the hacker have the sequence numbers that the target system is expecting, and if these packets arrive before the packets from the real, trusted system, the hacker becomes the trusted host.

To engage in IP spoofing, hackers must first use a variety of techniques to find an IP address of a trusted host and then modify their packet headers to appear as though packets are coming from that trusted host. Further, the attacker can engage other unsuspecting hosts to generate traffic that appears as though it too is coming from the trusted host, thus flooding the network.

Trust Exploitation

Trust exploitation refers to an individual taking advantage of a trust relationship within a network.

As an example of trust exploitation, consider the network shown in Figure 1-6, where system A is in the demilitarized zone (DMZ) of a firewall. System B, located in the inside of the firewall, trusts System A. When a hacker on the outside network compromises System A in the DMZ, the attacker can leverage the trust relationship it has to gain access to System A.



Trust Exploitation

A DMZ can be seen as a semi-secure segment of your network. A DMZ is typically used to provide to outside users access to corporate resources, because these users are not allowed to reach inside servers directly. However, a DMZ server might be allowed to reach inside resources directly. In a trust exploitation attack, a hacker could hack a DMZ server and use it as a springboard to reach the inside network.

Several trust models may exist in a network:

- Windows
  - Domains
  - Active Directory
- Linux and UNIX
  - Network File System (NFS)
  - Network Information Services Plus (NIS+)

Password Attacks

Password attacks can be implemented using several methods, including brute-force attacks, Trojan horse programs, IP spoofing, keyloggers, packet sniffers, and dictionary attacks. Although packet sniffers and IP spoofing can yield user accounts and passwords, password attacks usually refer to repeated attempts to identify a user account, password, or both. These repeated attempts are called *brute-force attacks*.

To execute a brute-force attack, an attacker can use a program that runs across the network and attempts to log in to a shared resource, such as a server. When an attacker gains access to a resource, the attacker has the same access rights as the rightful user. If this account has sufficient privileges, the attacker can create a back door for future access, without concern for any status and password changes to the compromised user account.

Just as with packet sniffers and IP spoofing attacks, a brute-force password attack can provide access to accounts that attackers then use to modify critical network files and services. For example, an attacker compromises your network integrity by modifying your network routing tables. This trick reroutes all network packets to the attacker before transmitting them to their final destination. In such a case, an attacker can monitor all network traffic, effectively becoming a man in the middle.

Passwords present a security risk if they are stored as plain text. Thus, passwords must be encrypted in order to avoid risks. On most systems, passwords are processed through an encryption algorithm that generates a one-way hash on passwords. You cannot reverse a one-way hash back to its original text. Most systems do not decrypt the stored password during authentication; they store the one-way hash. During the login process, you supply an account and password, and the password encryption algorithm generates a one-way hash. The algorithm compares this hash to the hash stored on the system. If the hashes are the same, the algorithm assumes that the user supplied the proper password.

Remember that passing the password through an algorithm results in a password hash. The hash is not the encrypted password, but rather a result of the algorithm. The strength of the hash is such that the hash value can be re-created only by using the original user and password information, and that it is impossible to retrieve the original information from the hash. This strength makes hashes perfect for encoding passwords for storage. In granting authorization, the hashes, rather than the plain-text password, are calculated and compared.

Hackers use many tools and techniques to crack passwords:

- **Word lists**: These programs use lists of words, phrases, or other combinations of letters, numbers, and symbols that computer users often use as passwords. Hackers enter word after word at high speed (called a *dictionary attack*) until they find a match.
- **Brute force**: This approach relies on power and repetition. It compares every possible combination and permutation of characters until it finds a match. Brute force eventually cracks any password, but it might take a long, long time. Brute force is an extremely slow process because it uses every conceivable character combination.
- **Hybrid crackers**: Some password crackers mix the two techniques. This combines the best of both methods and is highly effective against poorly constructed passwords.

Password cracking attacks any application or service that accepts user authentication, including the following:

- NetBIOS over TCP (TCP 139)
- Direct host (TCP 445)
- FTP (TCP 21)
- Telnet (TCP 23)
- Simple Network Management Protocol (SNMP) (UDP 161)
- Point-to-Point Tunneling Protocol (PPTP) (TCP 1723)
- Terminal services (TCP 3389)

NOTE

RainbowCrack is a compilation of hashes that provides crackers with a list that they can use to attempt to match hashes that they capture with sniffers.

Confidentiality and Integrity Attacks

Confidentiality breaches can occur when an attacker attempts to obtain access to read-sensitive data. These attacks can be extremely difficult to detect because the attacker can copy sensitive data without the knowledge of the owner and without leaving a trace.

A confidentiality breach can occur simply because of incorrect file protections. For instance, a sensitive file could mistakenly be given global read access. Unauthorized copying or examination of the file would probably be difficult to track without having some type of audit mechanism running that logs every file operation. If a user had no reason to suspect unwanted access, however, the audit file would probably never be examined.

In Figure 1-7, the attacker is able to compromise an exposed web server. Using this server as a beachhead, the attacker then gains full access to the database server from which customer data is downloaded. The attacker then uses information from the database, such as a username, password, and email address, to intercept and read sensitive email messages destined for a user in the branch office. This attack is difficult to detect because the attacker did not modify or delete any data. The data was only read and downloaded. Without some kind of auditing mechanism on the server, it is unlikely that this attack will be discovered.

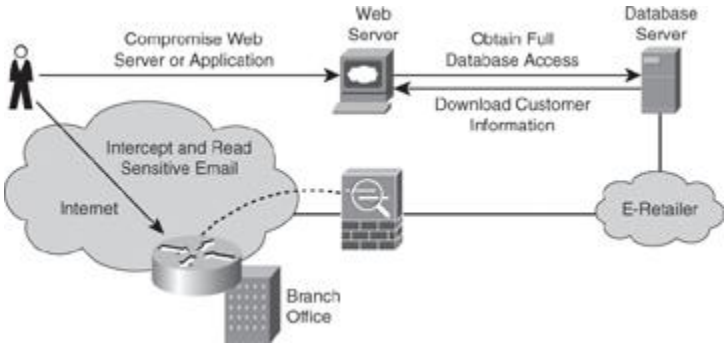


Figure 1-7. Breach of Confidentiality

Attackers can use many methods to compromise confidentiality, the most common of which are as follows:

- Ping sweeps and port scanning: Searching a network host for open ports.
- Packet sniffing: Intercepting and logging traffic that passes over a digital network or part of a network.
- Emanations capturing: Capturing electrical transmissions from the equipment of an organization to deduce information regarding the organization.
- Overt channels: Listening on obvious and visible communications. Overt channels can be used for covert communication.
- Covert channels: Hiding information within a transmission channel that is based on encoding data using another set of events.
- Wiretapping: Monitoring the telephone or Internet conversations of a third party, often covertly.
- Social engineering: Using social skills or relationships to manipulate people inside the network to provide the information needed to access the network.
- Dumpster diving: Searching through company dumpsters or trash cans looking for information, such as phone books, organization charts, manuals, memos, charts, and other documentation that can provide a valuable source of information for hackers.
- Phishing: Attempting to criminally acquire sensitive information, such as usernames and passwords, by masquerading as trustworthy entities.
- Pharming: Redirecting the traffic of a website to another, rogue website.

Many of these methods are used to compromise more than confidentiality. They are often elements of attacks on integrity and availability.

Man-in-the-Middle Attacks

A complex form of IP spoofing is called man-in-the-middle attack, where the hacker monitors the traffic that comes across the network and introduces himself as a stealth intermediary between the sender and the receiver, as shown in Figure 1-8.

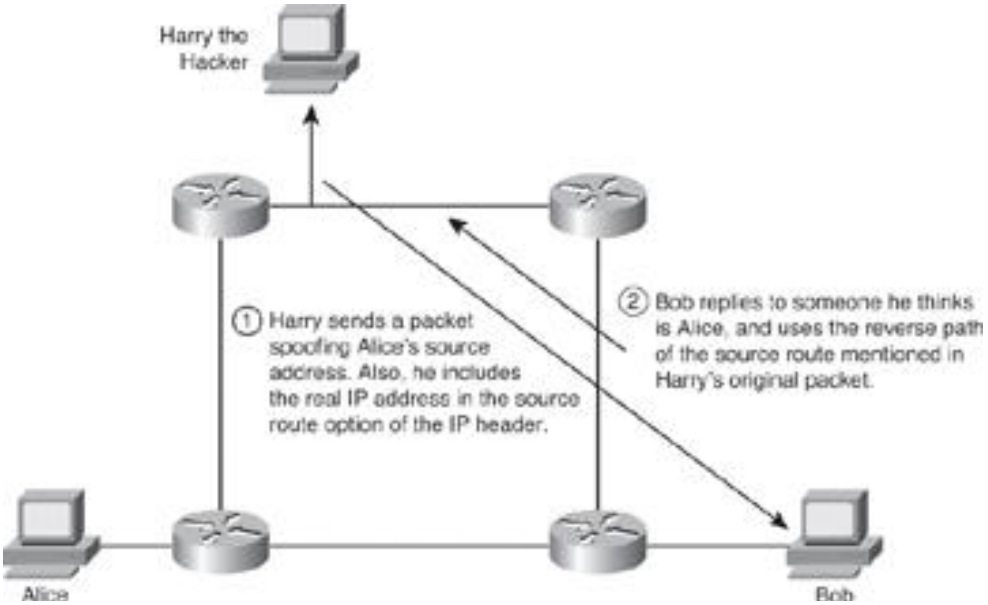


Figure 1-8. IP Source Routing Attack

Hackers use man-in-the-middle attacks to perform many security violations:

- Theft of information
- Hijacking of an ongoing session to gain access to your internal network resources
- Analysis of traffic to derive information about your network and its users
- DoS
- Corruption of transmitted data
- Introduction of new information into network sessions

Attacks are blind or nonblind. A blind attack interferes with a connection that takes place from outside, where sequence and acknowledgment numbers are unreachable. A nonblind attack interferes with connections that cross wiring used by the hacker. A good example of a blind attack can be found at http://wiki.cas.mcmaster.ca/index.php/The_Mitnick_attack.

TCP session hijacking is a common variant of the man-in-the-middle attack. The attacker sniffs to identify the client and server IP addresses and relative port numbers. The attacker modifies his or her packet headers to spoof TCP/IP packets from the client, and then waits to receive an ACK packet from the client communicating with the server. The ACK packet contains the sequence number of the next packet that the client is expecting. The attacker replies to the client using a modified packet with the source address of the server and the destination address of the client. This packet results in a reset that disconnects the legitimate client. The attacker takes over communications with the server by spoofing the expected sequence number from the ACK that was previously sent from the legitimate client to the server. (This could also be an attack against confidentiality.)

Another cleaver man-in-the-middle attack is for the hacker to successfully introduce himself as the DHCP server on the network, providing its own IP address as the default gateway during the DHCP offer.

NOTE

At this point, having read about many different attacks, you might be concerned that the security of your network is insufficient. Do not despair: many of the attacks described here are mitigated by techniques explained in this book or in other Cisco Press security books, such as *CCNP Security SECURE 642-637 Official Cert Guide*.

Overt and Covert Channels

Overt and covert channels refer to the capability to hide information within or using other information:

- Overt channel: A transmission channel that is based on tunneling one protocol inside of another. It could be a clear-text transmission inserted inside another clear-text protocol header.
- Covert channel: A transmission channel that is based on encoding data using another set of events. The data is concealed.

There are numerous ways that Internet protocols and the data that is transferred over them can provide overt and covert channels. The bad news is that firewalls generally cannot detect these channels; therefore, attackers can use them to receive confidential information in an unauthorized manner.

With an overt channel, one protocol is tunneled within another to bypass the security policy; for example, Telnet over FTP, instant messaging over HTTP, and IP over Post Office Protocol version 3 (POP3). Another example of an overt channel is using watermarks in JPEG images to leak confidential information.

One common use of overt channel is for instant messaging (IM). Most organization firewalls allow outbound HTTP but block IM. A user on the inside of the network can leak confidential information using IM over an HTTP session.

In Figure 1-9, the firewall allows outbound HTTP while a user on the inside of the network is leaking confidential information using instant messaging over HTTP.

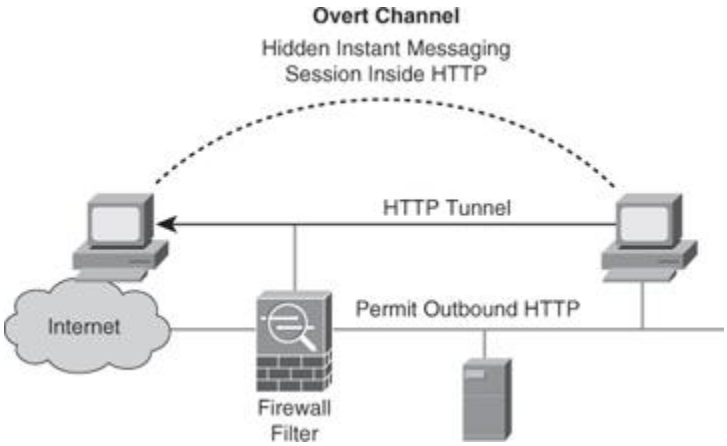


Figure 1-9. Overt Channel

NOTE

You can use the advanced protocol inspection in the Cisco IPS products and Cisco ASA 5500 series appliances to counter attacks such as a hidden IM session being sent inside HTTP.

Steganography is another example of an overt channel. Steganography (from the Greek word *steganos*, meaning “covered” or “secret”) literally means covered or secret writing. The combination of CPU power and interest in privacy has led to the development of techniques for hiding messages in digital pictures and digitized audio.

For example, certain bits of a digital graphic can be used to hide messages. The key to knowing which bits are special is shared between two parties that want to communicate privately. The private message typically has so few bits relative to the total number of bits in the image that changing them is not visually noticeable. Without a direct comparison of the original and the processed image, it is practically impossible to tell that anything has been changed. Still, it might be detected by statistical analysis that detects non-randomness. This non-randomness in a file indicates that information is being passed inside of the file.

NOTE

Steganography is very difficult to detect or prevent.

With a covert channel, information is encoded as another set of events. For example, an attacker could install a Trojan horse on a target host. The Trojan horse could be written to send binary information back to the server of the attacker. The client, infected with the Trojan horse, could return to the hacker’s server a ping status report in a binary format, where a 0 would represent a successful ping over a one-minute period, and a 1 would represent two successful pings over a one-minute period. The hacker could keep connectivity statistics for all the compromised clients he has around the world.

If ICMP is not permitted through a firewall, another tactic is to have the client visit the web page of the attacker. The Trojan horse software, now installed on the client, has a “call home” feature that automatically opens a connection to TCP port 80 at a specific IP address, the address of the hacker’s web server. All of this work is done so that the hacker can keep precise statistics of how many compromised workstations he possesses around the world. One visit per day would be represented by a 1, and no visits would be represented by a 0. As you might imagine, this technique is usually quite limited in bandwidth.

NOTE

Covert channels are very difficult to detect or prevent.

Phishing, Pharming, and Identity Theft

Identity theft continues to be a problem. In computing, phishing is an attempt to criminally acquire sensitive information, such as usernames, passwords, and credit card details, by masquerading as a trustworthy entity. Phishing is typically carried out by email or instant message (IM), although sometimes phone contact is attempted; the phisher often directs users to enter details at a website, as shown on the left in Figure 1-10. Phishing is an example of social engineering.

Figure 1-10. Phishing and Pharming Attacks

NOTE

A variation on phishing is spear phishing. In this case, a hacker sends an email that appears genuine to all the employees of an organization and hopes that a few get hooked. As an example, the email could say: “This is Christina, your HR director. The Automatic Payment organization which processes your pay is unable to do so this week. Please email me directly your banking information, and I will ensure that your pay is directly deposited in your bank account for Thursday morning.”

Pharming, also illustrated in Figure 1-10, is an attack aimed at redirecting the traffic of a website to another website. Pharming is conducted either by changing the hosts file on a victim computer or by exploiting a vulnerable Domain Name System (DNS) server. Pharming has become a major concern to businesses hosting e-commerce and online banking websites.

NOTE

Antivirus software and spyware-removal software cannot protect against pharming. Additional methods are needed such as server-side software, DNS protection, and web browser protection.

To protect against pharming, organizations implement “personalization” technologies, such as user-chosen images on the login page. Consider also supporting identified email initiatives such as DomainKeys Identified Mail (DKIM); these initiatives are beyond the scope of this book.

Availability Attacks

DoS attacks attempt to compromise the availability of a network, host, or application. They are considered a major risk because they can easily interrupt a business process and cause significant loss. These attacks are relatively simple to conduct, even by an unskilled attacker.

DoS attacks are usually the consequence of one of the following:

- The failure of a host or application to handle an unexpected condition, such as maliciously formatted input data or an unexpected interaction of system components.
- The inability of a network, host, or application to handle an enormous quantity of data, which crashes the system or brings it to a halt. Even if the firewall protects the corporate web server sitting on the DMZ from receiving a large amount of data and thus from crashing, the link connecting the corporation with its service provider will be totally clogged, and this bandwidth starvation will itself be a DoS.

Hackers can use many types of attacks to compromise availability:

- Botnets
- DoS
- DDoS
- SYN floods
- ICMP floods
- Electrical power
- Computer environment

NOTE

Many availability attacks can be used against confidentiality and integrity.

Botnets

Botnet is a term for a collection of software robots, or bots, that run autonomously and automatically. They run on groups of “zombie” computers controlled by crackers.

Although the term *botnet* can be used to refer to any group of bots, it is generally used to refer to a collection of compromised systems running worms, Trojan horses, or back doors, under a common command and control infrastructure. The originator of a botnet controls the group of computers remotely, usually through a means such as Internet Relay Chat (IRC).

Often, the command and control takes place via an IRC server or a specific channel on a public IRC network. A bot typically runs hidden. Generally, the attacker has compromised a large number of systems using various methods, such as exploits, buffer overflows, and so on. Newer bots automatically scan their environment and propagate using detected vulnerabilities and weak passwords. Sometimes a controller will hide an IRC server installation on an educational or corporate site, where high-speed connections can support a large number of other bots.

Several botnets have been found and removed from the Internet. The Dutch police found a 1.5-million node botnet (http://www.wisegeek.com/what-is-a-botnet.htm), and the Norwegian ISP Telenor disbanded a 10,000-node botnet. Large, coordinated international efforts to shut down botnets have also been initiated. Some estimates indicate that up to 25 percent of all personal computers are part of a botnet (http://everything.explained.at/Botnet/).

DoS and DDoS Attacks

DoS attacks are the most publicized form of attack. They are also among the most difficult to eliminate. A DoS attack on a server sends an extremely large volume of requests over a network or the Internet. These large volumes of requests cause the attacked server to slow down dramatically. Consequently, the attacked server becomes unavailable for legitimate access and use.

DoS attacks differ from most other attacks because DoS attacks do not try to gain access to your network or the information on your network. These attacks focus on making a service unavailable for normal use. Attackers typically accomplish this by exhausting some resource limitation on the network or within an operating system or application. These attacks typically require little effort to execute because they either take advantage of protocol weaknesses or use traffic normally allowed into a network. DoS attacks are among the most difficult to completely eliminate because of the way they use protocol weaknesses and accepted traffic to attack a network. Some hackers regard DoS attacks as trivial and in bad form because they require so little effort to execute. Still, because of their ease of implementation and potentially significant damage, DoS attacks deserve special attention from security administrators.

System administrators can install software fixes to limit the damage caused by all known DoS attacks. However, as with viruses, hackers constantly develop new DoS attacks.

A DDoS attack generates much higher levels of flooding traffic by using the combined bandwidth of multiple machines to target a single machine or network. The DDoS attack enlists a network of compromised machines that contain a remotely controlled agent, or zombie, attack program. A master control mechanism provides direction and control. When the zombies receive instructions from the master agent, they each begin generating malicious traffic aimed at the victim.

DDoS attacks are the “next generation” of DoS attacks on the Internet. This type of attack is not new. UDP and TCP SYN flooding, ICMP echo-request floods, and ICMP directed broadcasts (also known as Smurf attacks) are similar to DDoS attacks; however, the scope of the attack is new. Victims of DDoS attacks experience packet flooding from many different sources, possibly spoofed IP source addresses, which brings their network connectivity to a grinding halt. In the past, the typical DoS attack involved a single attempt to flood a target host with packets. With DDoS tools, an attacker can conduct the same attack using thousands of systems.

Figure 1-11 shows the process of a DDoS attack:

1. The hacker uses a host to scan for systems to hack.
2. After the hacker accesses handler systems, the hacker installs zombie software on them to scan, compromise, and infect agent systems.
3. Remote control attack software is loaded on agent systems.
4. When the hacker issues instructions to handlers on how to carry out the DDoS attack.

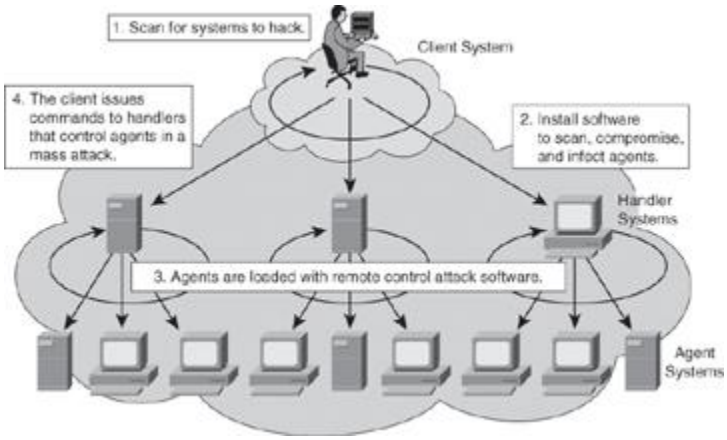


Figure 1-11. DDoS Attack

NOTE

Stacheldracht, which means “barbed-wire” in German, is a well-known tool used to conduct DDoS.

Blended Threats

The actual breach and vulnerability exploit is often accomplished using a combination of malware that infects, propagates, and delivers its payload following different techniques associated with traditional malware. Known as blended threats, these attack mechanisms combine the characteristics of viruses, worms, Trojan horses, spyware, and other malware.

A blended threat will exploit a vulnerability such as a buffer overflow or lack of HTTP input validation. Such attacks can spread without human intervention by scanning for other hosts to infect, embedding code in HTML, or by spamming, to name a few methods.

Blended threats plant Trojans and back doors. They are often part of botnet attacks, which try to raise privilege levels, create network shares, and steal data.

Most blended attacks are considered “zero day,” meaning that they have not been previously identified. Blended attacks are ever-evolving and pretested by cybercriminals on common antivirus products before they are released. These threats easily breach firewalls and open channels, and they represent a challenge to detect and mitigate.

Offline Versus Online Password Cracking

Password cracking techniques can be classified as offline or online. Offline password cracking involves having the hashed result of the original password. At its own pace, the hacker could try hashing different combinations of characters until one of the hash results matches the hash of the original password. Online password cracking involves, as an example, different combinations of password on a live system. It is more difficult to achieve success with this method because most login pages lock after a certain number of unsuccessful login attempts.

Principles of Secure Network Design

In planning an overall strategy for security architecture design, sound principles are needed to accomplish an effective security posture. The selective combination of these principles provides the fundamentals for threat mitigation within the context of a security policy and risk management.

- **Defense in depth:** This is an umbrella term that encompasses many of the other guidelines in this list. It is defined by architectures based on end-to-end security, using a layered approach. The objective is to create security domains and separate them by different types of security controls. The concept also defines redundancy of controls, where the failure of one layer is mitigated by the existence of other layers of controls.
- **Compartmentalization:** Creating security domains is crucial. Different assets with different values should reside in different security domains, be it physically

or logically. Granular trust relationships between compartments would mitigate attacks that try to gain a foothold in lower-security domains to exploit high-value assets in higher-security domains.

- **Least privilege:** This principle applies a need-to-know approach to trust relationships between security domains. The idea, which originated in military and intelligence operations, is that if fewer people know about certain information, the risk of unauthorized access is diminished. In network security, this results in restrictive policies, where access to and from a security domain is allowed only for the required users, application, or network traffic. Everything else is denied by default.
- **Weakest link:** This is a fundamental concept—a security system is as effective as its weakest link. A layered approach to security, with weaker or less protected assets residing in separated security domains, mitigates the necessary existence of these weakest links. Humans are often considered to be the weakest link in information security architectures.
- **Separation and rotation of duties:** This is the concept of developing systems where more than one individual is required to complete a certain task. The principle is that this requirement can mitigate fraud and error. This applies to information security controls, and it applies to both technical controls and human procedures to manage those controls.
- **Hierarchically trusted components and protection:** This principle applies a hierarchical approach to the compartmentalization and least privilege ideas, aiming at providing a more structured approach to data classification and security controls. The concept assumes that the hierarchy will be easier to implement and manage, resulting in similarly manageable and compartmentalized security controls.
- **Mediated access:** This principle is based on centralizing security controls to protect groups of assets or security domains. In that sense, firewalls, proxies, and other security controls act on behalf of the assets they are designed to protect, and mediate the trust relationships between security domains. Special considerations should be in place to prevent the mediation component from becoming a single point of failure.
- **Accountability and traceability:** This concept implies the existence of risk and the ability to manage and mitigate it, and not necessarily avoid or remove it. Information security architectures should provide mechanisms to track activity of users, attackers, and even security administrators. They should include provisions for accountability and nonrepudiation. This principle translates into specific functions, such as security audits, event management and monitoring, forensics, and others.

Cybercrime Prevention

STRATEGIES

Cyber criminals are no different than traditional criminals in that they want to make their money as quickly and easily as possible. Cybercrime prevention can be achieved fairly quickly and in a cost-effective manner. When armed with a little technical advice and common sense, many cybercrime attacks can be avoided. Similar to target hardening for a residence or a business (e.g., lights, locks, and alarms), the more difficult it is for a cyber criminal to successfully attack a target, the more likely he or she is to leave it alone and move on to an easier target.

The following ten tips are basic ways that cybercrime can be prevented.

- Keep the computer system up to date—

Cyber criminals will use software flaws to attack computer systems frequently and anonymously. Most Windows-based systems can be configured to download software patches and updates automatically. By doing this, cyber criminals who exploit flaws in software packages may be thwarted. This will also deter a number of automated and simple attacks criminals use to break into your system.

- Secure configuration of the system—

It is important that computers are configured to the security level that is appropriate and comfortable for the user. Too much security can have the adverse effect of frustrating the user and possibly preventing them from accessing certain web content. Using the“help” feature of the operating system can often address many of the questions in this area.

- Choose a strong password and protect it—

Usernames, passwords, and personal identification numbers (PIN) are used for almost every online transaction today. A strong password should be at least eight characters in length with a mixture of letters and numbers.

Using the same password for various sites or systems increases the risk of discovery and possible exploitation. It is never a good practice to write a password down and leave it near the system it is intended to be used on.

Changing a password every 90 days is a good practice to limit the amount of time it can be used to access sensitive information.

- Keep your firewall turned on—

A firewall helps to protect your computer from hackers who might try to gain access to crash it, delete information, or steal passwords and other sensitive information. Software firewalls are widely recommended for single computers. The software is prepackaged on some operating systems or can be purchased for individual computers. For multiple networked computers, hardware routers typically provide firewall protection. (www.fbi.gov/scams-safety/, How to Protect Your Computer, www.fbi.gov/scams-safety/computer_protect)

- Install or update your antivirus software—

Antivirus software is designed to prevent malicious software programs from embedding on your computer. If
it detects malicious code, like a virus or a worm, it works to disarm or remove it. Viruses can infect computers without the users' knowledge. Most types of antivirus software can be set up to update automatically (www.fbi.gov/scams-safety/, How to Protect Your Computer, www.fbi.gov/scams-safety/computer_protect.) Nearly 100 percent of the computers sold in the United States today come with some form of antivirus software. Failure to keep this software current is where a majority of the issues arise. The firewall monitors all data flowing in and out of the computer to the Internet, often blocking attacks from reaching the system. Antivirus software is the next line of defense, monitoring all online activity with the intent to protect the system from viruses, other malicious programs, and can be upgraded to protect against spyware and adware. To be safe on the Internet, the antivirus software should be configured to update itself every time the system connects to the Internet.

- Protect your personal information—

Using many of the online services today involves sharing basic personal information to include name, home address, phone number, and email address. Using common sense is the best way to protect against and prevent cybercrime. Do not respond to email messages that contain misspellings, poor grammar, odd phrases, or web sites with strange extensions. When in doubt about responding to an email, consider a telephone call to the organization to verify authenticity. Type the address for the website in the browser instead of clicking on a link. Any financial transaction website should have an "s" after the letters "http" (e.g., https://www.mystore.com not http://www.mystore.com). The "s" stands for secure and should appear when you are in an area requesting you to login or provide other sensitive data. Another sign that you have a secure connection is the small lock icon in the bottom of your web browser (usually the right-hand corner.)

- Read the fine print on website privacy policies—

On many social networking and photo sharing sites, there is wording on the privacy policies that allow the website to keep information and photos posted to the site, sometimes indefinitely, even after the original has been deleted by the user. While this may not discourage one from posting images or messages, awareness that this can be later retrieved and disseminated may be a consideration as to what information or photos are posted. What today may seem to be a harmless prank can have a devastating effect on one's reputation several years later when applying for a job or other opportunity.

- Review financial statements regularly—

Reviewing credit card and bank statements regularly will often reduce the impact of identity theft and credit fraud by discovering the problem shortly after the data has been stolen or when the first use of the information is attempted. Credit card protection services can often alert a person when there is unusual activity occurring on his or her account, for example, purchases in a geographically distant location or a high volume.of purchases. These alerts should not be taken lightly and could be the first indicator that a victim receives that something is wrong.

- If it seems too good to be true, it is—

No one is going to receive a large sum of money from a dead Nigerian politician, win a huge lottery from being "randomly selected from a database of email addresses," or make big money from "passive residual income a few hours each day working out of your home." Many of these crimes go unreported because the victim is too embarrassed to admit to law enforcement that they were duped.

- Turn off your computer—

With the growth of high-speed Internet connections, many opt to leave their computers on and ready for action. The downside is that being "always on" renders computers more susceptible. Beyond firewall protection, which is designed to fend off unwanted attacks, turning the computer off effectively severs an attacker's connection—be it spyware or a botnet that employs your computer's resources to reach out to other unwitting users. (FBI Website -Scams and Safety, How to Protect Your Computer: www.fbi.gov/scams-safety/computer_protect) The bottom line is for every preventative measure that you take, you limit your chances for becoming a victim of cybercrime.

Resources

- Federal Bureau of Investigation (FBI) for cybercrime information CybeRCRimes
www.fbi.gov/about-us/investigate/cyber/cyber
- Federal Bureau of Investigation (FBI) for tips to avoid Internet fraud
www.fbi.gov/scams-safety/fraud/Internet_fraud
- Internet Crime Complaint Center
www.ic3.gov
- Department of Justice- Computer Crime and Intellectual Property Section
www.cybercrime.gov
- Federal Trade Commission Consumer Information
www.ftc.gov/bcp
- National Crime Prevention Council
www.ncpc.org