ANSWERS TO ASSIGNMENT NO. 6

(1) Cyber Attacks and Digital Terrorism – IS/IT strategies for organizations must provide adequate security from cyber attacks and digital terrorism. On that note, answer the following questions.
(Reference – The Good Book-1, Chapter 16, on the subject of Social, Ethical and Legal Issues)

a. List a few reasons why cyber attacks and digital terrorism occur.

ANSWER

There are just too many reasons why people launch cyber attacks or execute digital terrorism and they all share one common thing – to cause damage and destruction, with motivations that range from anything – personal, political, economic or all.

a. **Personal Anger** – psychologically angry at your organization, your company, your country, etc for whatever reason like being left out of promotions or layed-off the job. So you “plant” viruses into your company’s network or computers. You must be smart in doing this, less you will be easily caught. It can be anything with anger. It may not be your company that you “destroy”. You may be angry at your girlfriend (e.g. breaking up), and you are extremely jealous that some one now took her away from you, so you decided to attack the computers of her company. Ha.. ha.. ha.. anything can trigger an attack. This type of activity can be classified as a personal digital terrorism.

b. **Hired Service** – Somebody hired you to go into “another somebody’s” computer network and get (steal) important information and you get paid handsomely for it. Then the guy who hired you instructed you to “destroy” the computers to wipe off all digital trails. You can do it or you can double-cross and tell the targeted company “that you are hired to do so and so by so and so” and that you do not intend to execute it. So you still get paid for it, now being paid both ways. And like James Bond and all the exciting spy stories, you must show realism, so you planned with your targeted company to do “mock-up destruction” of the company’s computers. Everything went well. You think you are now rich and you got away with it scot-free and happy, until you realized later that the first guy that hired you is a “mobster or gangster” which means you are as good as “dead”. Ha ha ha. This type of activity can be classified as a professional digital terrorism.

c. **Ransom Money** – You need money, nobody wants to help you, the banks do not want to give you a loan, your wife left you, your family members do not want to help you, your father is dead, your mother has no money to help you but you are special. You are a true computer wizard. What is the way out? Ha ha ha. Tell the bank that you have planted a “logic bomb” into their network. It will activate at a certain time unless the bank puts in some cash money into a bag and drop it somewhere following some “smart scheme” you have devised. Once you have retrieved the money and feel safe, you will send the
bank with the code that will de-activate the logic bomb. This type of activity can be classified as a personal desperate digital terrorism.

d. **Political War** – There are some people who get politically angry because those in power do not agree with their views or wishes. They want to display their “people’s power” or dislike by conducting demonstrations etc. One way as a warning is planting “logic bombs” with a ransom note that says unless the demands are met then the logic bomb will go off. This is typical against governments or organization/union of governments like “The G8”, “APEC Summit”, “World Economic Forum” etc. This type of activity can be classified as a political group digital terrorism.

e. **Declared War** – There exist true terrorist organizations that have publicly declared their all out war against countries or organizations. They have named their sworn-out enemies. Conducting cyber attacks is one of their strategies to achieve their aims – everything is possible in war. Each side will try to “destroy” or “cripple” each others’ war machineries and capabilities. Ha ha ha – For example: In the UN against Iraqi War, the whole radar system of Iraq was “jammed by the US” during the early phases of the war. All electronic and computer communications infrastructure of Iraq were crippled. This type of activity can be classified as an expected “political digital war” tactics and “not really digital terrorism”.

b. **What are viruses, worms, Trojan horses, logic bombs and DOS attacks?**

**ANSWER**

A **virus** is a small unit of usually malicious code that invades a computer program or file. There are many types of viruses and many different mechanisms of virus attacks against computers. Viruses are being continuously created by “bad” people and anti-virus databases are constantly being updated to combat and prevent such attacks. For example, a virus attack mechanism may be like the following: When someone opens a file infected with a virus (normally unknowingly), or when a program with a virus already attached (hidden) is being executed, the virus will “take action to do whatever it is programmed to do”. The actions can range from simple things like just giving “Got cha!” screen messages, copying itself to other programs, slowing down performance of computers, spreading itself to other computers on the network or to the worst case of “wiping” everything on the computer making the system “dead”. Essentially, there is no limit to “whatever a virus can be programmed to do”.

A **worm** is defined as a type of virus that has the ability to copy itself from machine to machine, normally over a network. The term "worm" was chosen to depict the transmission mechanism that behaves like a worm in a human body. Many years ago, in the underdeveloped countries, children with “ring worms” in their body spread these worms to other children in the community. The virus multiply in the body then spreads through the food chain, cleaning and drinking water, excretions, skin absorptions and through many other media transmissions. In the computer sense, this virus behaves like a worm, copying itself and spreading across the network through the infected computer. The 2 key differences between a virus and a worm are the “multiplying or copying effect” and the “spreading across to other computers”. A virus may not multiply (remained one) and may attack only just one
computer host (the infected computer). A worm is the extension of the virus with the 2 additional attributes mentioned above.

A **Trojan horse** is a security-breaking program that is introduced into a computer and serves as a way for an intruder to re-enter the computer in the future. It may be disguised as something innocent such as a screen saver or a game. The key term in the Trojan horse is the “entry in disguise”. Named for a giant wooden horse that was supposed to be a gift but was filled with the Greek army (inside the horse’s stomach), a Trojan horse program is a deceptive method of entry into an enemy’s territory. The story goes that the Greeks gave the Trojans a huge wooden horse as a peace offering. The citizens of Troy accepted the gift, brought the horse inside the city, threw a victory bash (a party), and then went to bed. It wasn’t until the Greek soldiers attacked them and had set the city on fire that they realized they’d been had (tricked). In the computer sense, a Trojan horse follows that deceptive method for entry into computers. It can damage, delete, or destroy important files, essentially do anything it is programmed to do. The key thing here is not in the type of damage but in how it enters a computer – i.e. “by a deceptive way”.

A **logic bomb** is a program that is introduced into a computer and set to take action at a certain time or when a specified event occurs. It can do anything it was programmed to do.

A **DOS (Denial of Service)** attack is an action being implemented by invading a large number of computers on the network (usually internet) and instructing the computers to simultaneously send repeated messages to a target computer, thus either overloading the computer’s input buffer or jamming the communication lines into the computer so badly that legitimate users cannot obtain access to the targeted computer. The key terms here are “jamming the target computer or computers” so that those targeted computers can no longer provide services (i.e. users are denied of the services). Some people refer to DOS attacks as the Ping of Death or the Teardrop. However, these 2 types of attacks are not exhaustive for the DOS categories. It can be anything as long as it does essentially the thing we call - “Bringing civilizations to its knees” with “civilizations” here referring to “targeted computers” as in the cartoon below.
**Computer Spoofing** is an action of misleading a computer user from a true website (targeted computer) to another fraudulent website, for some malicious purposes i.e. depending on what the programmer wants to achieve. A “spoof” is a “a hoax” or a deception.

A **phishing** activity is an on-line fraud. *I have used paypal for the last 3 years and have had no problems what so ever. My paypal transaction rating is 103 and rising. The only problem I have encountered is bogus links purporting to come from paypal (that don’t) wanting you to put your login details password etc into the site or "phissing". These are easy to spot as they look quite basic with bad wording and mistakes.*

**Warez** (pronounced like the word “wares”) is a derivative of the plural form of "software". It refers primarily to copyrighted material traded in violation of its copyright license. The term generally refers to releases by organized groups, as opposed to peer-to-peer file sharing between friends or large groups of people with similar interest. It usually does not refer to commercial for-profit software counterfeiting. This term was initially coined by members of the various computer underground circles, but has since become commonplace among Internet users and the media.

A **zombie computer** (abbreviated zombie) is a computer attached to the Internet that has been compromised by a cracker, a computer virus, or a trojan horse. Generally a compromised machine is only one of many in a "botnet", and will be used to perform malicious tasks of one sort or another, under remote direction. Most owners of zombie computers would be unaware that their system was being used in this way. Zombies have been used extensively to send e-mail spam. It is estimated that between 50 to 80 percent of all spam worldwide is now sent by zombie computers. This allows spammers to avoid detection of the source of spam, and presumably reduces their bandwidth costs, since the owners of zombies pay for their computers' use of bandwidth. For similar reasons, zombies are also used to commit click fraud against sites displaying pay per click advertising. Zombies have also conducted distributed denial of service attacks, such as the attack upon the SPEWS service in 2003.

**Black-hat hacking** is the act of compromising the security of a system without permission from an authorized party, usually with the intent of accessing computers connected to the network (the somewhat similar activity of defeating copy prevention devices in software - which may or may not be illegal depending on the laws of the given country - is actually **software cracking**).

The term **cracker** was coined by Richard Stallman (FSF/GNU - The Man) to provide an alternative to abusing the existing word **hacker** for this meaning. This term's use is limited (as well as "black hat") mostly to some areas of the computer and security field and even there is considered controversial. One group that refers to themselves as hackers consists of skilled computer enthusiasts. The other, and the common usage, refers to people who attempt to gain unauthorized access to computer systems. Many members of the first group attempt to convince people that intruders should be called crackers rather than hackers, but the common usage remains unchanged.
Spamming is the abuse of any electronic communications medium to send unsolicited messages in bulk. While its definition usually extends to any unsolicited bulk electronic communication, some exclude from the definition of the term "spam" messages considered by the receiver (or even just the sender) to be targeted, non-commercial, or wanted. In the popular eye, the most common form of spam is that delivered in e-mail as a form of commercial advertising. However, over the short history of electronic media, people have spammed for many purposes other than the commercial, and in many media other than e-mail. Spammers have developed a variety of spamming techniques, which vary by media: e-mail spam, instant messaging spam, Usenet newsgroup spam, Web search engines spam, weblogs spam, and mobile phone messaging spam. Spamming is economically viable because advertisers have effectively no operating costs beyond the management of their mailing lists. Because the barrier to entry is so low, the volume of unsolicited mail has produced other costs which are borne by the public (in terms of lost productivity and fraud) and by Internet service providers, which must add extra capacity to cope with the deluge. Spamming is widely reviled, and has been the subject of legislation in a number of jurisdictions.

Opt-in e-mail advertising or permission marketing is a method of advertising by electronic mail wherein the recipient of the advertisement has consented to receive it. It is one of several ways developed by marketers to eliminate the disadvantages of e-mail marketing. Opt-out is a method of requiring a targeted individual to explicitly respond to a solicitation in order to keep from receiving some service or "widget", usually used in marketing. The concepts of opt-in or opt-out is really about options that you can choose, for example when you register for a free software or service (like wruslan@gmail.com), you can choose to receive updates, notices, new products etc. If you choose yes it is opt-in, and if you choose no it is opt-out.

http://www.securitydocs.com/library/2742
http://www.cnn.com/TECH/specials/hackers/primer/
Examples of non-acceptable content or links on the internet:

- Pirated software
- Hacking programs or archives
- Phissing
- Warez
- Cracks
- Illegal MP3’s
- Spamming software or scripts
- Adult contents
- Racism, terrorism, violent and/or abusive contents
- No less than double opt-in mailing lists
- Any content that includes using of viruses, Trojans or in any other illegal contents

**c. What is information theft? What is identity theft? What are the differences and implications of information and identity theft in the digital world?**

**ANSWER**

Thieves are simply obtaining something (materials or non-materials) through illegal means. So “information theft” is obtaining information illegally, for example, without the owner’s permission. Publicly published information is legally “public” and therefore, having such information by whatever means is never considered stealing or “theft”.

“Identity theft” according to the US Federal Trade Commission (FTC) is “someone (somebody else) is appropriating your personal information without your knowledge to commit fraud or theft.” For example, an identity thief uses information about you, such your name, address, social security number, credit card number and/or other identifying information to impersonate you and obtain loans or purchase items under your credit.

Information theft is simply about “stealing information” for whatever use the thief wants it for, whereas “identity theft” is the extension of information theft with the user wanting to “impersonate you” or “be identified as you” using that stolen identification information to be used for many things, good and mostly bad.

A thief can use the stolen identification information for criminal activities including validating against computer software systems: - the banks identification system (to steal your money in the bank), the credit card system (to use your credit card to buy things), the immigration system (to run out of the country) and many more. It all looks like it is actually you performing those activities and not the thief.

A thief who is also a hacker can do more, for example, penetrate - the records registry system (to hack and change your date of birth, your gender status, your parents names, etc), the police crime database system (to hack and say that you committed a crime which you never did), the university records system (to hack and change your grades from A to F, to change your major degrees etc ), the White House Security System (to visit and say hello to the most powerful man in the world), the FBI and CIA computer systems etc.
(2) Securing applications from hackers – Mini Case for Assignment 6 Question 2.

This document about web application attacks was written by a security analyst working for an important government organization in Malaysia, NISER (National ICT Security and Emergency Response) Center.

The correct IS/IT strategies for an organization must include sufficient protection from computer hackers. Read the short case study provided at the end of this assignment document and answer the following questions:

a. What are the mechanisms of the following 3 types of hacker attacks?

- **Source Code Disclosure**
- **SQL query positioning**
- **Session hijacking**

**ANSWER**

**Source code disclosure:**

The attacker uses this technique by injecting external codes (either through client-side code injection or server-side code injection) to attack a website. The objectives are to obtain the source code of the server-side script such as active server page (ASP), Java server page (JSP) and PHP hypertext preprocessor (PHP) files, and also to get information on the Web application logic such as database structure, source code comments and parameters.

**SQL query positioning**

The attacker uses this technique by injecting or embedding SQL commands inside the query parameters (i.e. text boxes for inputs) on a web page to attack a website. Normally, Web applications send query strings and their parameters to the database server to get the requested data from the database. Attackers may take advantage of this because they can embed SQL commands inside these parameters, and this is called SQL query poisoning. This kind of attack may lead to back-end database compromise.

**Session hijacking**

The attacker uses this technique by intercepting the HTTP connection and alters the cookie’s value from a web page to attack a website. This is called session hijacking. When the attackers successfully hijack a session, they can access all of the user's data on the website (e.g. names, addresses, credit card numbers etc).

b. The term Intrusion Detection System (IDS) is a very important topic that every computer security personnel must know. What is it and how does it work? (Please go and find out through your own resources to answer this question).
**ANSWER**

**What is IDS** - An Intrusion Detection System (or IDS) generally detects unwanted manipulations (entries or intrusions) to systems that normally go through as "unknown and bad" data traffic in the computer network. There are a lot of different types of IDS. The manipulations may take the form of attacks by skilled malicious hackers, or Script kiddies using automated tools.

**Purpose** - An IDS is required to detect all types of malicious network traffic and computer usage that can't be detected by a conventional firewall. This includes network attacks against vulnerable services, data driven attacks on applications, host based attacks such as privilege escalation, unauthorized logins and access to sensitive files, and malware (viruses, trojan horses, and worms).

**Components of IDS** - An IDS is composed of several components: Sensors which generate security events, a Console to monitor events and alerts and control the sensors, and a central Engine that records events logged by the sensors in a database and uses a system of rules to generate alerts from security events received. There are several ways to categorise an IDS depending on the type and location of the sensors and the methodology used by the engine to generate alerts. In many simple IDS implementations all three components are combined in a single device or appliance.

Examples of types of IDS:

A **Signature-Based Intrusion Detection System** identifies intrusions by watching for patterns of traffic or application data presumed to be malicious.

An **Anomaly-Based Intrusion Detection System** identifies intrusions by notifying operators of traffic or application content presumed to be different from 'normal' activity on the network or host.

A **Network Intrusion Detection System** is an independent platform which identifies intrusions by examining network traffic and monitors multiple hosts. Network Intrusion Detection Systems gain access to network traffic by connecting to a hub, network switch configured for port mirroring, or network tap. An example of a NIDS is Snort.

A **Host-based Intrusion Detection System** consists of an agent on a host which identifies intrusions by analyzing system calls, application logs, file-system modifications (binaries, password files, capability/acl databases) and other host activities and state.

A **Hybrid Intrusion Detection System** combines both approaches. Host agent data is combined with network information to form a comprehensive view of the network. An example of a Hybrid IDS is Prelude.

In a **passive system**, the IDS sensor detects a potential security breach, logs the information and signals an alert on the console.
In a **reactive system**, the IDS system responds to the suspicious activity by logging off a user or by reprogramming the firewall to block network traffic from the suspected malicious source, either autonomously or at the command of an operator.

(3) **Computer Security** – Computer security is a never-ending and ongoing problem for organizations with IS/IT assets.

List down and describe the responsibilities of the individual user in maintaining the security of the organization’s computers.

*(Reference – The Good Book-1, Chapter 16, on the subject of Social, Ethical and Legal Issues, Review Question No. 5)*

**ANSWER**

It is the responsibility of every individual in an organization to protect and maintain the security of the organization’s computer resources. As an individual user the responsibilities include, but is not limited to:

1. **strictly abiding by the policies and procedures laid down by the organization regarding the use of computers and network resources**
2. **not using unauthorized programs and software (untested and may contain malicious codes) that may compromise the security of the network**
3. **using good password techniques, changing passwords regularly, keeping passwords safe and not disclosing them to unauthorized parties**
4. **ensuring that the workstations in use have anti-virus software installed, and regularly updating virus definition files**
5. **installing operating system updates and application patches and fixes regularly**
6. **ensuring that important business information are regularly backed-up and stored away safely**
7. **knowing how to handle suspicious mails especially those with attachments and mails from unknown senders**
8. **when working on sensitive and confidential company’s information, not to leave the computer display on when unattended**
9. **not abusing computer resources like sending out spam mail, hate-mails or visiting pornographic sites as these sites are full of “unwanted and unsafe elements” like viruses, Trojans, worms, time or logic bombs, spywares, etc.**
10. **ensuring that applications in use are configured at the correct security levels,**
11. **implementing security protections that come built-in with the applications**
(12) turning on automatic updates for anti-virus, fixes and patches downloads, where possible

(13) when in doubt, asking someone in the organization who knows

(4) Software Licensing and Use - Today the adoption of open source software applications is increasingly being considered by many IS/IT Managers in both profit-making and non-profit making organizations.

(Reference – The Good Book-1, Chapter 16, on the subject of Social, Ethical and Legal Issues)

a. Explain the difference(s) between a copyright and a patent on a computer program.

**ANSWER**

Software developers own the software they create. The ownership rights of the computer programs or software they produce are protected by both copyrights and patents.

A copyright is a registration with the relevant bodies (with enforcement powers) that provides effective protection against software piracy (i.e. illegal copying, production and distribution of software). Essentially, it protects against copying because the “right to copy” is with the creator. For software copyright, we must seek permission, approval or authorization from the creator to do any copying of the “copyrighted” material. In the case of the creator being the employee of a company, the copyright owner is usually the company but authorship is with the creator (inventor).

In general, for most computer programs or software the copyright owner does not sell the software itself, but only the right to use it under certain specified conditions. This is exactly the case when we purchase software, like buying Microsoft Windows XP or Microsoft Office XP. We are licensed by Microsoft as a user of the software and we do not own the software. If the user violates the conditions of purchase to use the software, then the purchaser is deemed to have violated the copyright.

A patent is also a registration with the relevant bodies but of an invention or a process that gives its creator the exclusive right to the manufacture and use of a new design, new process or new method for a limited period of time. Similarly, in the case of the inventor being the employee of a company, the patent owner is usually the company.

A patent is not applicable or acceptable for natural processes or environmental processes because it belongs to God and so to all mankind. An example of a valid patent would be the “flap-cover design” of the cell phone held by Motorola for 15 years. After it expired, every other company produces models of flap-covered cell phones.
A patent for software or a computer program is however, controversial. Programs are algorithms or "ideas" just like mathematical algorithms and so most people believe cannot and should not be patented. It was argued that "even if you have not discovered the 'idea', somebody sometime in the future would eventually discover it". So "such ideas" should fall under the ownership of God, and rightly to all mankind. In the opinion of the US courts some years ago, copyright is acceptable for software ("ideas") but patenting is not. The judgment changes when Amazon.com was issued patents for its "one-click ordering" on the internet on the basis of a "computer-implemented process". The issue of patents remains controversial as different countries define and interpret "patent laws" differently.

b. What is copyleft? Hint: It has to do with the open source GPL (GNU General Public License). Go to the internet to find out about it and answer this question.

**ANSWER**

In a non-legal sense, copyleft is the **opposite** of copyright.

Copyleft describes a group of licenses applied to works such as software, documents, music, and art. Where copyright law is seen by the original proponents of copyleft as a way to restrict the right to make and redistribute copies of a particular work, a copyleft license uses copyright law in order to ensure that every person who receives a copy or derived version of a work, can use, modify, and also redistribute both the work, and derived versions of the work.
c. The open source software and free software usually share the same licenses, but according to the Free Software Foundation (FSF), the open source movement is philosophically different from the free software movement. What are the differences? Go to the internet to find out about it and answer this question.

ANSWER

FREE SOFTWARE (according to FSF)

Free software is a matter of liberty, not price. To understand the concept, you should think of free as in free speech, not as in free beer.'

Free software is a matter of the users' freedom to run, copy, distribute, study, change and improve the software. More precisely, it refers to four kinds of freedom, for the users of the software:

- The freedom to run the program, for any purpose (freedom 0).
- The freedom to study how the program works, and adapt it to your needs (freedom 1). Access to the source code is a precondition for this.
- The freedom to redistribute copies so you can help your neighbor (freedom 2).
- The freedom to improve the program, and release your improvements to the public, so that the whole community benefits (freedom 3). Access to the source code is a precondition for this.

A program is free software if users have all of the 4 freedoms described above.

Thus, you should be free to redistribute copies, either with or without modifications, either gratis or charging a fee for distribution, to anyone anywhere. Being free to do these things means (among other things) that you do not have to ask or pay for permission.

OPEN SOURCE SOFTWARE

Simply said, any software with the source code provided is termed as open source software.

(1) Most open source software is free software (we can do everything as defined with 4 freedoms stated by FSF above).

(2) Some open source software is NOT free software. The software and source code are given but the software portion only is free, the source code is not free. Ha ha ha

(3) Some open source software is NOT free software. The software and source code are given and the software portion is not free, only the source code is free. Ha ha ha

(4) Some open source software is given free (both software and source code) but is not to be modified, distributed or sold to others.
And there many more conditions or business models that people create to this effect. It can be confusing to a beginner. So you can actually create your software, put up on the internet and define whatever business models or terms of use you like.

OTHER IMPORTANT TERMS

A non-disclosure agreement (NDA), also called a confidential disclosure agreement (CDA), confidentiality agreement or secrecy agreement, is a legal contract between at least two parties which outlines confidential materials the parties wish to share with one another for certain purposes, but wish to restrict from generalized use. In other words, it is a contract through which the parties agree not to disclose information covered by the agreement. A NDA creates a confidential relationship between the parties. The NDA can be applied to anything including software.

Shared source is a type of licensing program that allows controlled access to full or limited amounts of product source code. It is not a particular license, as there are several different shared source programs, each with their own license and varying restrictions.

The term is typically used to refer to Microsoft's Shared Source Initiative, though the use as a generic licensing term is growing more widespread. Shared source licensing is also used by other projects and companies, such as Hewlett-Packard and Sun Microsystems.

Though shared source licensing allows for source code access, it is not open source according to the Open Source Definition, because none of the license programs allows for commercial use of modified code. Most programs restrict code access to particular groups, institutions, or partners.

Some programs, such as the Shared Source Common Language Infrastructure, allow non-commercial modification and redistribution of code by any users. However, Enterprise Source Licensing allows only government institutions to view (but not modify or redistribute) the code.

d. What are the issues of internet file sharing? Are there any resolutions to the issues? Describe what you know of the current status on the subject.

ANSWER

Internet file sharing is the practice of making files available to other users for download over the Internet. Usually file sharing follows the peer-to-peer (P2P) model, where the files are stored on and served by personal computers of the users.

Most people who engage in file sharing are also downloading files that other users share. Sometimes these two activities are linked together. File sharing is distinct from file trading in that downloading files from a P2P network does not require uploading, although some networks either provide incentives for uploading such as credits or force the sharing of files being currently downloaded.
Internet file sharing is very different from downloading of files (e.g. software applications, etc) from ftp or http sites like for stuff like “freeware”, “shareware”, “pay-ware”, “rent-ware” etc. There are many business models for software availability on the internet, too many to mention. The key term to notice for “internet file sharing” is the word “sharing”.

This “sharing” concept comes from the actions of “What’s wrong with me paying for the original stuff (files on the internet, especially and historically music files like MP3) and then share with my friends, just like I normally do when I buy a music CD and my friends borrowed the CD to listen to the music? Similarly, I also borrowed music CDs from my friends to listen to the songs. Now and then I share money with my friends to buy music files on the internet. What’s wrong with it? And my friends are far-away friends and we are only connected by the internet.” Ha ha ha. This is the crux of the internet file sharing issue. I know that there is no problem with file sharing on the LAN or local intranet, music or non-music. Am I right or am I wrong? Ha ha ha.

A famous example of internet file sharing is Napster. Originally a centralized file system, Napster was the first major file-sharing tool and popularized file sharing for the masses. Napster was a localized index for MP3 files shared by the users logged into the system. Napster was sued for copyright violations in the US federal court and was finally shut down by legal attacks from the music industry.

Next comes Sharman Networks with a little twist to the internet file sharing mechanism. It developed the P2P file sharing software which does the same service Napster does. Sharman then started the Kazaa service to distribute the file-sharing software. This software is not a centralized file system (central directory), instead it is made up of many local directories on computers of users with fast connections, called supernodes. So to get the software, dial direct to the supernodes and wallah, you get your music software if that is what you wished. Ha ha ha. So again the major labels in the music industry sued Sharman Networks for copyright violations. The case is still pending.

http://news.com.com/Judge+Kazaa+can+be+sued+in+U.S./2100-1023_3-980274.html

Will the story of internet file sharing end? I personally do not think so as other technologies will spring up in the future. I believe that the RIAA (Recording Industry Association of America) going for the few big volume internet-file-sharing sites (i.e. on copyrighted materials) as the right thing to do. It is right to publicize these lawsuits as a scare tactic and thereby reduce the amount of copyrighted materials being downloaded and not paying fees or royalties. This discussion can go on forever, like they say until “the cows go home”. Ha ha ha
Mini Case for Assignment 6 Question 2

By Norhazimah Abdul Malik
Reproduced from NST, Computimes – C14
November 28, 2005

MOST companies today use the Web to do business with customers, employees, suppliers and others. This is because it is easier to maintain a Web-based application than a Windows-based one. But how can we be sure that a Web-based application is secured? Or that data is being shared only by the authorised users?

The Gartner Group estimates that 75 per cent of cyber attacks today are at the application level. And about 97 per cent of over 300 Web sites audited are vulnerable to Web application attacks.

The US Federal Bureau of Investigation also reveals that 95 per cent of the companies are hacked from Web applications, and only five per cent of them are aware of the attacks (http://conference.hackinthebox.org/hitbsecconf2005kl/materials/TT-Shreeraj-Shah-Webhacking-Kungfu.pdf)

From the figures, we can deduce that most company Web sites are prone to cyber attacks, and some of these companies are not aware that their Web applications have vulnerabilities that can be exploited by hackers.

According to statistics published by the National ICT Security and Emergency Response Centre, there have been significant increases in Web defacement incidents. In the first quarter of this year, there were 256 Web defacements involving both public and private Web sites, compared to the previous quarter which recorded 42 of such incidents.

To have a secure Web application, developers of the application must know each attribute such as query string, form, cookie, script, etc, because they are vulnerable. These attributes can be exploited by an attacker and expose sensitive company information if they are not used securely.

Web application attacks. There are two types of Web application attacks: automated and manual. Automated attacks can be used to exploit a Web application using automated Web application attack tools such as wget, curl, black widow and teleport pro. Using these automated tools, crawling and attacks can be done shortly. This type of attack can be avoided by setting "honey traps" using HTTP Module (used in pre/post-processing of requests). The attacker can be put into an infinite loop using defence trick once it is trapped. To launch manual attacks, hackers must conduct information gathering such as address identification, port scanning, social engineering and vulnerability scanning to find out vulnerabilities that can be exploited.

Common Web application hacking methods include:

**Source code disclosure:**

The attacker uses this technique to obtain the source code of the server-side script such as active server page (ASP), Java server page (JSP) and PHP hypertext preprocessor (PHP) files, to get information on the Web application logic such as database structure, source code comments and parameters.

There are two types of malicious code injections which may allow the source code disclosure technique to be used: client-side code injection and server-side code injection.

An example of client-side code injection is cross-site scripting attacks that occur when the attackers embed malicious code such as script into a hyperlink. When the user clicks on the hyperlink, the malicious code will be executed at the Web server, which creates an output page containing the malicious content that can lead to internal data disclosure.
An example of server-side code injection is remote command execution that occurs when the attacker injects PHP/ASP code which can cause arbitrary command execution on the server.

This problem occurs because of poor design and written applications. Web developers should include exception handling in the programming so errors can be handled within the code. The errors should be logged and not displayed at the Web browser.

All inputs such as data types, buffer sizes and meta-characters should be sanitised and validated before being passed to the internal application logic. To ensure that a Web application is secured from this kind of attack, the developer should follow the secure coding practices to make sure that no "active code" is injected as data contents.

**SQL query poisoning:**

Normally, Web applications send query strings and their parameters to the database server to get the requested data from the database. Attackers may take advantage of this because they can embed SQL commands inside these parameters, and this is called SQL query poisoning. This kind of attack may lead to back-end database compromise.

SQL query poisoning attacks occur because there is no input validation for all inputs from the client. This is a result of bad programming practice.

A database should be configured correctly to eliminate unnecessary database users and stored procedures. Using alternative SQL query constructions such as stored procedures and prepared statements will overcome SQL query poisoning problems because the SQL string cannot be altered.

**Session hijacking:**

Hypertext transfer protocol (HTTP) connections are stateless. To keep track of an application's state when the application runs, an HTTP cookie is used. Cookies will be destroyed when the user logs out from the system.

Nowadays, there are tools that can be used to intercept HTTP connections and alter the cookies' value, and this is called session hijacking. If the attackers successfully hijack a session, they can gain access to all of the user's data.

Session identifiers, which are unique and generated randomly, can be used to prevent such attacks. These identifiers are transmitted between the client and the server. To secure session identifiers, make sure that they are not stored in the hidden field, and encrypt them to prevent captured, brute-forced or reverse-engineered exploitation.

**Conclusion:**

Web application attacks are increasing drastically because there is a lack of knowledge in securing the applications, especially during the development and deployment stages of the applications. To control or avoid this menace, we must ensure that security is being implemented not only during the coding stage, but also the deployment stage.

The operations of a Web application must be monitored by the administrator so any exploits can be detected earlier and damages can be minimised or avoided such as using an intrusion detection system to monitor and filter Web traffic. It is also recommended for all organisations to conduct a security audit assessment to ensure that an application is secured before it is published to the public.