(Contributors, Timeline of Computer Viruses and Worms, 2014)OT5.4 – Uses of the Internet

# Elementary

1. The Internet is a cross platform network because it accessible from many platforms such as mobile devices, laptops and desktops, or OS wise, OSX, Windows, All Distributions of Linux, iOS, and Android. The Internet does not care what system you use to connect to it.
2. Four methods to connecting to the internet are:
   1. Dial-Up: Using traditional telephone lines/connections via a modem. Offers connection speeds up to 56 kilobits / second.
   2. Broadband: Faster than 2 megabits per second. A method of connection is via fibre optic cables.
   3. ISDN: This method provides a faster connection rate than a dial-up line and uses ‘multiplexing’, which allows the standard telephone line to carry more than one signal at a time.
   4. DSL: This method divides a regular copper telephone line into separate channels for telephone and for data. ADSL is a common form of DSL, which assumes that more information will be downloaded than uploaded, so the download speed is made much faster. An ADSL service divides a telephone line into three channels: one for receiving data, one for sending data and one for using the telephone. The service is limited by your computer’s distance from the ADSL modem at the telephone exchange, the quality of the telephone line and the number of users using the network at the same time.

# Basic

WWW: The World Wide Web (WWW) is the best known part of the internet and is a network of sites that can be searched and retrieved by the special protocol know as Hypertext Transfer Protocol.

VoIP: Services allowing telephone voice calls to be made over the internet instead of using regular telephone exchanges are know as Voice over Internet Protocol (VoIP).

On-line gaming: Many popular activities on the web involve playing games online. Early online adventure games, many of which are still popular, were known as MUDs. These games had their origins in the early days of computers as text-based adventure scenarios. With the arrival of faster broadband internet, Massively Multiplayer Online Games (MMOG), involving thousands of players playing a game simultaneously, have developed from these early MUD games.

# Sound

1. [jbloggs@sydneycollege.edu.au](mailto:jbloggs@sydneycollege.edu.au)
   1. jbloggs is the username and identifies the addressee
   2. The @ ‘at’ is a separator symbol which separates the username and the domain name.
   3. Sydneycollege is the domain name, which is the computer address, with full stops separating the parts.
   4. .edu.au is the suffix. The suffix ‘edu’ indicates that the domain name belongs to an academic institution and the ‘au’ tell us that is in in Australia.
   5. CC: stands for carbon copy and allows you to send a message to more than one email address at the same time.
   6. BCC: stands for blind carbon copy. Email addresses entered in this field are hidden from the receiver.
2. Sending an email involves many separate protocols all working together.
   1. SMTP: controls how the ordinary text of an email message is sent and received, as well as how the message is organized, with a header (including subject, sender, receiver addresses) and body (containing the message).
   2. Multipurpose Internet Mail Extensions (MIME): controls how attachments such as computer programs, graphics, or word-processed documents are encoded as files in binary code.
   3. Post Office Protocol (POP) controls how a mail server holds messages until they are downloaded and cleared.

# Competent

1. Netiquette (Etiquette in technology) governs what conduct is socially acceptable in online or digital situations.
2. Some of the general rules for correct netiquette are to not use your phone or other electronic devices where you are not supposed to, another is to treat others how you would like to be treated, to avoid using ALL CAPS OR SHOUTING, etc.

3.

|  |  |
| --- | --- |
| Emoticons |  |
| :) or :-) | Smile |
| ;) or ;-) | Wink |
| :D or :-D | Big Smile |
| |-) | Cool |
| B) or B-) | Evil Grin |
| :-> or >:> | Another Evil Grin |
| ~(\_:(1) | Homer Simpson |
| 888888888:-) | Marge Simpson |
| :[~ | Vampire |
| 8(:-) | Mickey Mouse |

# Extensive

## Viruses

A computer virus is a malware program that, when executed, replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be "infected". Viruses often perform some type of harmful activity on infected hosts, such as stealing hard disk space or CPU time, accessing private information, corrupting data, displaying political or humorous messages on the user's screen, spamming their contacts, or logging their keystrokes. However, not all viruses carry a destructive payload or attempt to hide themselves—the defining characteristic of viruses is that they are self-replicating computer programs which install themselves without the user's consent.

Viruses can spread via the Internet, removable storage media, and or other means of data transfer between computers. Antivirus software is often used to eliminate the virus from the ‘infected’ computer and thus preventing it from spread anymore from that computer.

## The Creeper Virus

The Creeper virus was first detected on ARPANET, the forerunner of the Internet, in the early 1970s. Creeper was an experimental self-replicating program written by Bob Thomas at BBN Technologies in 1971. Creeper used the ARPANET to infect DEC PDP-10 computers running the TENEX operating system. Creeper gained access via the ARPANET and copied itself to the remote system where the message, "I'm the creeper, catch me if you can!" was displayed. The Reaper program was created to delete Creeper.

## Trojans

A Trojan Horse is full of as much trickery as the mythological Trojan Horse it was named after. The Trojan Horse, at first glance will appear to be useful software but will actually do damage once installed or run on your computer. Those on the receiving end of a Trojan Horse are usually tricked into opening them because they appear to be receiving legitimate software or files from a legitimate source. When a Trojan is activated on your computer, the results can vary. Some Trojans are designed to be more annoying than malicious (like changing your desktop, adding silly active desktop icons) or they can cause serious damage by deleting files and destroying information on your system. Trojans are also known to create a backdoor on your computer that gives malicious users access to your system, possibly allowing confidential or personal information to be compromised. Unlike viruses and worms, Trojans do not reproduce by infecting other files nor do they self-replicate.

## The ANIMAL Trojan

ANIMAL is written by John Walker for the UNIVAC 1108. ANIMAL asked a number of questions of the user in an attempt to guess the type of animal that the user was thinking of, while the related program PERVADE would create a copy of itself and ANIMAL in every directory to which the current user had access. It spread across the multi-user UNIVACs when users with overlapping permissions discovered the game, and to other computers when tapes were shared. The program was carefully written to avoid damage to existing file or directory structures, and not to copy itself if permissions did not exist or if damage could result. Its spread was therefore halted by an OS upgrade which changed the format of the file status tables that PERVADE used for safe copying. Though non-malicious, "Pervading Animal" represents the first Trojan "in the wild".

## Worms

A worm is similar to a virus by design and is considered to be a sub-class of a virus. Worms spread from computer to computer, but unlike a virus, it has the capability to travel without any human action. A worm takes advantage of file or information transport features on your system, which is what allows it to travel unaided.

The biggest danger with a worm is its capability to replicate itself on your system, so rather than your computer sending out a single worm, it could send out hundreds or thousands of copies of itself, creating a huge devastating effect. One example would be for a worm to send a copy of itself to everyone listed in your e-mail address book. Then, the worm replicates and sends itself out to everyone listed in each of the receiver's address book, and the manifest continues on down the line.

Due to the copying nature of a worm and its capability to travel across networks the end result in most cases is that the worm consumes too much system memory (or network bandwidth), causing Web servers, network servers and individual computers to stop responding. In recent worm attacks such as the much-talked-about Blaster Worm, the worm has been designed to tunnel into your system and allow malicious users to control your computer remotely.

## The Morris Worm

The Morris Worm one of the first computer programs distributed via the Internet. Morris Worm was considered the first worm and infected about 10% of the Internet. It launched on November 2 1988 and caught wide spread media attention. It also resulted in the first conviction in the US under the 1986 Computer Fraud and Abuse Act. It was written by a student at Cornell University, Robert Tappan Morris, and launched on November 2, 1988 from MIT. At the time it was released it was estimated that the Internet was made up of about 60,000 computers, so about 6,000 computers had been infected. Although the worm was meant to be harmless, a mistake in the code meant that multiple copies of it could be installed and run on one computer, slowing it down eventually to being unusable.

# Bibliography

Beal, V. (2004, October 28). *The Difference Between a Computer Virus, Worm and Trojan Horse*. Retrieved August 14, 2014, from Webopedia: http://www.webopedia.com/DidYouKnow/Internet/virus.asp

Chiles, D. P. (2014, August 14). *Internet Etiquette*. Retrieved August 14, 2014, from Netiquette: http://www.networketiquette.net/internet/internet\_etiquette.html

Contributors, W. (2014, October 20). *Computer Virus*. Retrieved October 23, 2014, from Wikipedia: http://en.wikipedia.org/wiki/Computer\_virus#The\_first\_computer\_viruses

Contributors, W. (2014, August 11). *Etiquette in technology - Wikipedia*. Retrieved August 14, 2014, from Wikipedia: http://en.wikipedia.org/wiki/Etiquette\_in\_technology

Contributors, W. (2014, July 12). *Morris Worm - Wikipedia*. Retrieved August 14, 2014, from Wikipedia: http://en.wikipedia.org/wiki/Morris\_Worm

Contributors, W. (2014, October 23). *Timeline of Computer Viruses and Worms*. Retrieved October 23, 2014, from Wikipedia: http://en.wikipedia.org/wiki/Timeline\_of\_computer\_viruses\_and\_worms

Grover, D., Knights, H., & Gormley, E. (2011). *Information & Software Technology.* Melbourne: Pearson Australia.