WEEK-9

ETHICS ON VIRUS AND ANTIVIRUS SOFTWARE DEVELOPMENT

(Virus, Antivirus, Hacking)

Dr Eric Opoku Osei

Ethical

Discuss the Ethical consideration in the development of computer virus and antivirus Within the industry

DEFINITION

- Viruses: A computer virus, much like a flu virus, is designed to spread from host to host and has the ability to replicate itself. Similarly, in the same way that flu viruses cannot reproduce without a host cell, computer viruses cannot reproduce and spread without programming such as a file or document.

- Worms: A computer worm is a standalone malware (MALICIOUS SOFTWARE) computer program that replicates itself in order to spread to other computers.[1] It often uses a computer network to spread itself, relying on security failures on the target computer to access it. It will use this machine as a host to scan and infect other computers.

- Trojan Horses: is any malware which misleads users of its true intent. The term is derived from the Ancient Greek story of the deceptive Trojan Horse that led to the fall of the city of Troy. Trojans are generally spread by some form of social engineering, for example where a user is duped into executing an email attachment disguised to appear not suspicious, (e.g., a routine form to be filled in), or by clicking on some fake advertisement on social media or anywhere else.

VIRUS

- Viruses
  - HOW VIRUSES WORK

    A virus is a piece of self-replicating code embedded within another program called the host.
  - When a user executes a host program infected with a virus, the virus code executes first.
  - The virus finds another executable program stored in the computer's file system and replaces the program with a virus-infected program.
  - After doing this, the virus allows the host program to execute, which is what the user expected to happen.
  - If the virus does its work quickly enough, the user may be unaware of the presence of the virus.

VIRUS

- Because a virus is attached to a host program, you may find viruses anywhere you can find program files:
  - hard disks,
  - floppy disks,
  - CD-ROMs,
  - email attachments, (executable programs, macros)

- Some viruses are fairly innocent; they simply replicate. These viruses occupy disk space and consume CPU time, but the harm they do is relatively minor.
- Other viruses are malicious and can cause significant damage to a person's file system.

VIRUS

- Well-known computer viruses
  - The Brain virus (c. 1986) was the first virus to move from one IBM PC to another. The virus was written by the owners of a Pakistani computer store called Brain Computer Services
  - The Michelangelo virus dates back to 1991. If a PC user executes a program infected with the virus on March 6, the birthday of Renaissance painter and sculptor Michelangelo, the virus overwrites critical records on the boot disk.
  - The Melissa virus (c. 1999) lurks inside a macro in a Word document attached to an email message. When a user activates the virus by opening the infected attachment, Melissa sends an email message with the attachment to the first 50 people in the user's address book.

VIRUS

- The Love Bug (c. 2000) is another virus lurking inside an email message. Unlike Melissa, which limits itself to the first 50 people in a victim's address book, the Love Bug creates email messages for everyone in the address book. It deletes some kind of media files stored on the user’s hard disk, and it also collects passwords and emails them to several different accounts in the Philippines.

- Commercial antivirus software packages allow computer users to detect and destroy viruses lurking on their computers. To be most effective, users must keep them up-to date by downloading programs corresponding to the latest viruses from the vendor's Web site

WORMS

- A worm is a self-contained program that spreads through a computer network by exploiting security holes in the computers connected to the network.

- In October 1989, NASA scientists prepared for a Space Shuttle mission that would launch a probe to Jupiter. The robot probe, named Galileo, was fueled with radioactive plutonium. Antinuclear protestors created a worm that infiltrated a NASA network.

- Those who logged onto an infected computer were greeted with a banner with the words: **W**orms **A**gainst **N**uclear **K**illers. "Your System has been officially WANKed"
- The WANK worm is an example of cyberterrorism: a politically motivated attack against the IT resources of a government or its people in order to inflict damage, disrupt services, or generate fear.

TROJAN HORSES

- A Trojan horse is a program with a benign capability that conceals another, sinister purpose. When the user executes a Trojan horse, the program performs the expected beneficial task.
- However, the program is also performing actions unknown to, and not in the best interests of, the user.

- A remote access Trojan (RAT) is a Trojan horse program that gives the attacker access to the victim's computer. Two well-known RATs are Back Orifice and SubSeven.
- SubSeven consists of a client program running on the attacker's computer, and a server program running on the victim's computer.
- The attacker is able to capture images from the victim's monitor, record keystrokes, read and write files, watch traffic on the victim's local area network, and even control the mouse.

REMOTE ACCESS TROJAN (RAT)

- In order to gain access to another person's computer, the attacker must trick that person into downloading the RAT server.

- The most popular way to do this is to hide it inside a file posted to a Usenet news group specializing in erotica.
- The attacker advertises the file as containing sexually explicit videos or photos.
- Those who download the file bring the RAT into their computer.

TROJAN HORSES

- Trojan horse programs may
  - open an Internet connection that allows an outsider to gain access to files on the user's computer;
  - logging the keystrokes of the user and storing them in a file that the attacker can examine to learn confidential information, such as passwords
  - look for passwords stored on the computer and emailing them to the attacker's address;
  - destroy files on the user's computer;
  - launch a denial-of-service attack on a Web site;
  - turning the user's computer into a proxy server that can be used to launch spam or stash information gained from illegal activities (such as stolen credit card numbers).

Defensive Measures One Can Take

- The ability of a computer network to withstand the attacks of viruses, worms, and Trojan horses depends to a great extent on the skill and dedication of its system administrators, as well as the cooperation of the network's users.
- Authorization and authentication mechanisms.
  - **Authorization** is the process of determining that a user has permission to perform a particular action.
  - **Authentication** is determining that a person is who he claims to be.
    - Knowledge-based authentication mechanism - password
    - identification card or smart card
    - biometric data, such as a fingerprint or retinal scan
- A sure-fire way to prevent a network from being attacked by an external virus or worm is to detach it from the Internet
  - Or installing a firewall (a computer, positioned between a local network and the Internet that monitors the packets flowing in and out.)
  - An important responsibility of the system administrator is to keep the operating system up-to-date with the latest patches.

THANK YOU