Lecture 11:

Malware: Viruses and Worms

4th Year- Course, CCSIT, UoA

Lecture Goals

To highlight:

1. Attributes of a virus
2. Attributes of a worm
3. Good traditions and practices against viruses and worms

Viruses

- A *computer virus* is a malicious piece of executable code that propagates typically by attaching itself to a ***host*** document — usually an executable piece of code — just as a biological virus needs a host, a living cell, that it inserts itself into for propagation.
- Any operating system that allows third-party programs to run can support viruses.
- Computer viruses need to know if a potential host is already infected, since otherwise the size of an infected file could grow without bounds through repeated infection. Viruses typically place a ***signature*** (such as a string that is an impossible date) at a specific location in the file for this purpose.

Typical hosts for computer viruses

1. Executable files (such as the '.exe' files in Windows machines), usually sent around as email attachments
2. Boot sectors of disk partitions
3. Script files for system administration (such as the batch files in Windows machines, shell script files in Unix, etc.)
4. Documents that are allowed to contain macros (such as Microsoft Word documents, Excel spreadsheets, Access database files, etc.)

Viruses and Unix

- Because of the way permissions work in Unix systems, it is more difficult for a virus to wreak havoc on a Unix machine.
- Let's say that a virus embedded itself into one of your script files. The virus code will execute only with the permissions that are assigned to you.
- For example, if you do not have the permission to read or modify a certain system file, the virus code will, in general, be constrained by the same restriction.

Virus Duplication

- At the least, a virus will duplicate itself when it attaches itself to another host document, that is, to another executable file.
- But the important thing to note that this copy does not have to be an exact replica of itself.
- In order to make more difficult the detection by pattern matching, the virus may alter itself when it propagates from host to host.
- In most cases, the changes made to the viral code are simple, such as rearrangement of the order independent instructions, etc.
- Viruses that are capable of changing themselves are called ***mutating viruses***.

More on Viruses

- Most commonly, the execution of a particular instance of a virus (in a specific host file) will come to an end when the host file has finished execution. However, it is possible for a more vicious virus to create a continuously running program in the background.

- To escape detection, the more sophisticated viruses ***encrypt themselves*** with keys that change with each infection. What stays constant in such viruses is the decryption routine.

- The payload part of a virus is that portion of the code that is not related to propagation or concealment.

The Anatomy of a Virus

A computer virus has three parts:

1. Infection mechanism: The means by which a virus spreads, enabling it to replicate. The mechanism is also referred to as the infection vector.
2. Trigger: The event or condition that determines when the payload is activated or delivered.
3. Payload: What the virus does, besides spreading. The payload may involve damage or may involve benign but noticeable activity.

Virus Lifetime (1)

During its lifetime, a typical virus goes through the following ***four phases***:

1. Dormant phase: The virus is idle. The virus will eventually be activated by some event, such as a date or the presence of another program or file. Not all viruses have this stage.
2. Propagation phase: The virus places a copy of itself into other programs or into certain system areas on the disk. The copy may not be identical to the propagating version; viruses often morph to evade detection.

Virus Lifetime (2)

3. Triggering phase: The virus is activated to perform the function for which it was intended. As with the dormant phase, the triggering phase can be caused by a variety of system events, including a count of the number of times that this copy of the virus has made copies of itself.

4. Execution phase: The function is performed. The function may be harmless, such as a message on the screen, or damaging, such as the destruction of programs and data files.