CS 3IS3 Fall 2007

07 Malicious Software

William M. Farmer

Department of Computing and Software
McMaster University

15 November 2007

Overview

- Malicious software is computer code that is intended to cause a security policy to be violated.
    - Also called malware.
    - Malicious software is not the same as faulty software.
- Malicious software includes:
    - Trojan horses.
    - Computer viruses.
    - Computer worms.
    - Computer bacteria.
    - Logic bombs.
    - Malicious mobile code.

Trojan Horses

- A Trojan horse is a program with an overt (documented or known) effect and a covert (undocumented or unexpected) effect.
  - Some Trojan horses can replicate themselves.
- One of the most common uses of a Trojan horse is to provide a back door to a program.
- A key aspect in a Trojan horse is how the illicit code is hidden.
  - Hidden in disguised form in the source code.
  - Present in the executable but not in the source code.
  - Hidden in a secondary program such as a compiler.

Computer Viruses

- A computer virus is a program that inserts itself in one or more files and then performs some (possibly null) action.
  - The first phase is called the insertion phase.
  - The second phase is called the execution phase.
- Examples:
  - Boot sector infector: The virus inserts itself into the boot section of a disk.
  - Executable infector: The virus inserts itself into an executable program.
- Viruses can insert either executable or interpretable code.
  - The former are usually machine dependent.
  - The latter (called macro viruses) can be machine independent.

Methods Viruses Use to Avoid Detection

- Prevent system data (such as file size and last modified date) from being changed.
- Avoid insertion into bait and anti-virus files.
- Intercept requests to the operating system (stealth virus).
- Encrypt the virus with a different key for each insertion (encrypted virus).
  - Decrypting routine is not encrypted.
- Encrypt the virus and modify the decrypting routine (polymorphic virus).
- Rewrite the virus each time it is inserted (metamorphic virus).
  - A metamorphic virus is usually large and complex.

Computer Worms and Bacteria

- A computer worm is a program that copies itself from one computer to another.
    - A worm's functionality may be entirely limited to replication and migration.
- A computer bacterium is a program that absorbs all of some class of resource.
    - A bacterium often exhausts a resource by means of rapid reproduction.
- Worms and bacteria are used to implement denial of service attacks.

Logic Bombs

- A logic bomb is a program that performs an action that violates a security policy when some external event occurs.
  - Many logic bombs are programmed to go off on certain dates.
- Logic bombs are sometimes planted by disgruntled employees who have insider access to information systems.

Mobile Code

- Mobile code is software that is intended to be moved from one computer to another.
- Mobile code paradigms:
  1. Code on demand: Software requested by a client and provided by a server. Examples: Java applets, Javascript in HTML files.
  2. Remote evaluation: Software that a client sends to a server for execution.
  3. Mobile agents: Software that migrates autonomously from computer to computer.
- The use of mobile code is dangerous because it effectively allows a foreign, and potentially malicious, program to execute on your own computer.

Defenses Against Malicious Software

- Do not allow executable files to be modified or data files to become executable without certification.
- Limit the services available to a user when executing a program by:
  - Restricting the distance of information flow.
  - Reducing the rights of the user.
  - Executing in a controlled sandbox.
  - Not being root.
- Inhibit sharing across domain boundaries.
- Check the integrity of files.
- Scan for specific viruses.
- Scan for statistical evidence of malicious alteration.
- Execute proof-carrying code when possible.