CGS 3763: Operating System Concepts
Spring 2006

Security – Part 2

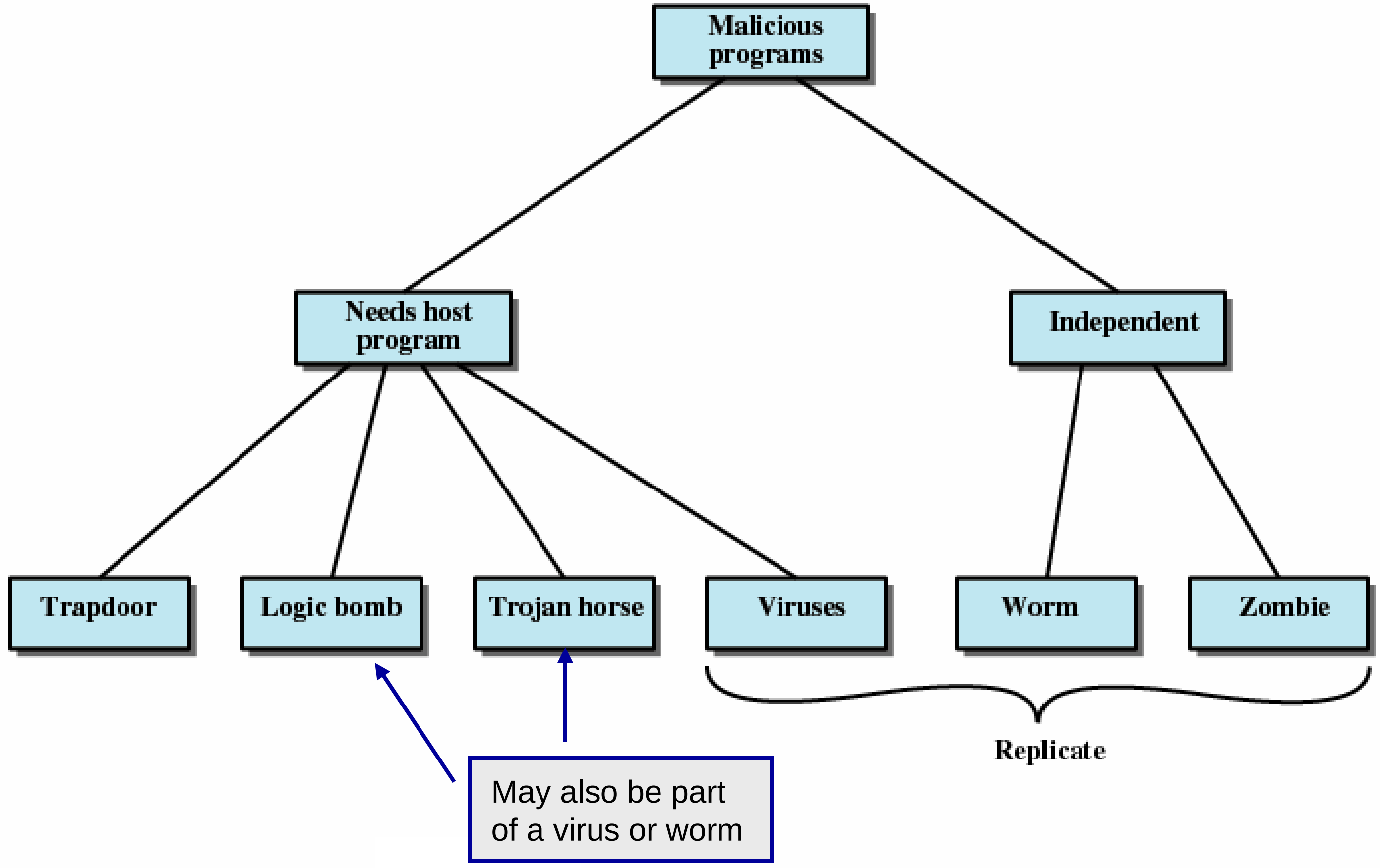
Instructor : Mark Llewellyn
markl@cs.ucf.edu
CSB 242, 823-2790
http://www.cs.ucf.edu/courses/cgs3763/spr2006

School of Electrical Engineering and Computer Science
University of Central Florida

Malicious Programs (Malware)

- Those that need a host program
  - Fragments of programs that cannot exist independently of some application program, utility, or system program.
- Independent
  - Self-contained programs that can be scheduled and run by the operating system.

Malicious Programs (Malware) (cont.)



May also be part of a virus or worm

Taxonomy of Malicious Programs

Trapdoor

- Entry point into a program that allows someone who is aware of trapdoor to gain access.
- Used by programmers to debug and test programs.
  - Avoids necessary setup and authentication.
  - Method to activate program if something goes wrong with authentication procedure.
  - Typically activated via a special sequence of input or is triggered by being run from a certain user ID.
  - Remember the movie “War Games”?

Logic Bomb

- Code embedded in a legitimate program that is set to “explode” when certain conditions are met.
  - Presence or absence of certain files.
  - Particular day of the week.
  - Particular user running application.
- Once triggered, the bomb may alter or delete data or entire files, cause a machine to halt, or do some other damage.
- Case of Tim Lloyd, who was convicted of setting a logic bomb that cost his employer, Omega Engineering, more than $10 million, derailed its corporate growth, and eventually led to the layoff of 80 workers. He was ultimately convicted, sentenced to 41 months in prison and ordered to pay $2 million in restitution.

Trojan Horse

- A useful, or apparently useful, program that contains hidden code that when invoked performs some unwanted or harmful function.
- Can be used to accomplish functions indirectly that an unauthorized user could not accomplish directly.
  – For example, it may set file permission so everyone has access to any file.
  – Modify a compiler to insert additional code into certain programs as they are compiled, such as a system login program. The code creates a trap door in the login program that permits the author to log on to the system using a special password.

Virus

- Program that can “infect” other programs by modifying them; the modification includes a copy of the virus program, which can then go on to infect other programs.
- Lodged in a host computer, a typical virus takes temporary control of the computer’s disk operating system. Then, whenever the infected computer comes into contact with an uninfected piece of software, a fresh copy of the virus passes into the new program.
- Thus, the infection can be spread from computer to computer by unsuspecting users who either swap disks or send programs to one another over a network.

Worms

- Use network connections to spread from system to system. Once active in a system, a worm can behave as a virus , or it could implant Trojan horse programs.
- Electronic mail facility
  - A worm mails a copy of itself to other systems.
- Remote execution capability
  - A worm executes a copy of itself on another system.
- Remote log-in capability
  - A worm logs on to a remote system as a user and then uses commands to copy itself from one system to the other.

Zombie

- Program that secretly takes over another Internet-attached computer.
- It uses that computer to launch attacks that are difficult to trace to the zombie’s creator.
- Typically, zombies are used in denial-of-service attacks against a targeted website.
- The zombie is planted on hundreds of computers belonging to unsuspecting third parties, and then used to overwhelm the target by launching an overwhelming onslaught of traffic.

The Nature of Viruses

Stages of a virus:

- Dormant phase
  - Virus is idle. Not all viruses have this stage.
- Propagation phase
  - Virus places an identical copy of itself into other programs or into certain system areas on the disk.
- Triggering phase
  - Virus is activated to perform the function for which it was intended.
  - Caused by a variety of system events.
- Execution phase
  - Function is performed.

Types of Viruses

- Parasitic
  - Attaches itself to executable files and replicates.
  - When the infected program is executed, it looks for other executables to infect.
- Memory-resident
  - Lodges in main memory as part of a resident system program.
  - Once in memory, it infects every program that executes.

Types of Viruses (cont.)

- Boot sector
  - Infects boot record.
  - Spreads when system is booted from the disk containing the virus.
- Stealth
  - Specifically designed to hide itself from detection by antivirus software.
  - May use compression so that the infected program is exactly the same length as an uninfected version.

Types of Viruses

- Polymorphic
  - Creates copies during replication that are functionally equivalent but have distinctly different bit patterns.
  - Mutates with every infection, making detection by the "signature" of the virus impossible.
  - Mutation engine creates a random encryption key to encrypt the remainder of the virus.
    - The key is stored with the virus.

Macro Viruses

- In recent years, the number of viruses encountered at corporate sites has risen dramatically. Much of this increase is due to the proliferation of one of the macro viruses. Macro viruses are particularly threatening for a number of reasons:

1. Platform independent.
   – Most infect Microsoft Word documents.
2. Infect documents, not executable portions of code.
3. Easily spread. Commonly via email.

Macro Viruses (cont.)

- A macro is an executable program embedded in a word processing document or other type of file.
- Autoexecuting macros in Word
  - Autoexecute
    - Executes when Word is started
  - Automacro
    - Executes when defined event occurs such as opening or closing a document
  - Command macro
    - Executed when user invokes a command (e.g., File Save)

Antivirus Approaches

- The ideal solution to the threat of viruses is prevention: do not allow a virus to get into the system in the first place.
- This goal is, in general, impossible to achieve, although prevention can reduce the number of successful viral attacks.
- The next best approach is to be able to do the following:
  - Detection – once the infection has occurred, determine that it has occurred an locate the virus.
  - Identification – once detection has been achieved, identify the specific virus that has infected a program.
  - Removal – once the specific virus has been identified, remove all traces of the virus from the infected program and restore it to its original state.

Generic Decryption

- Since a polymorphic virus is typically encrypted, GD technology passes all executable files through a GD scanner, which includes the following elements:
  - CPU emulator
    - Instructions in an executable file are interpreted by the emulator rather than the processor.
  - Virus signature scanner
    - Scan target code looking for known virus signatures.
  - Emulation control module
    - Controls the execution of the target code .

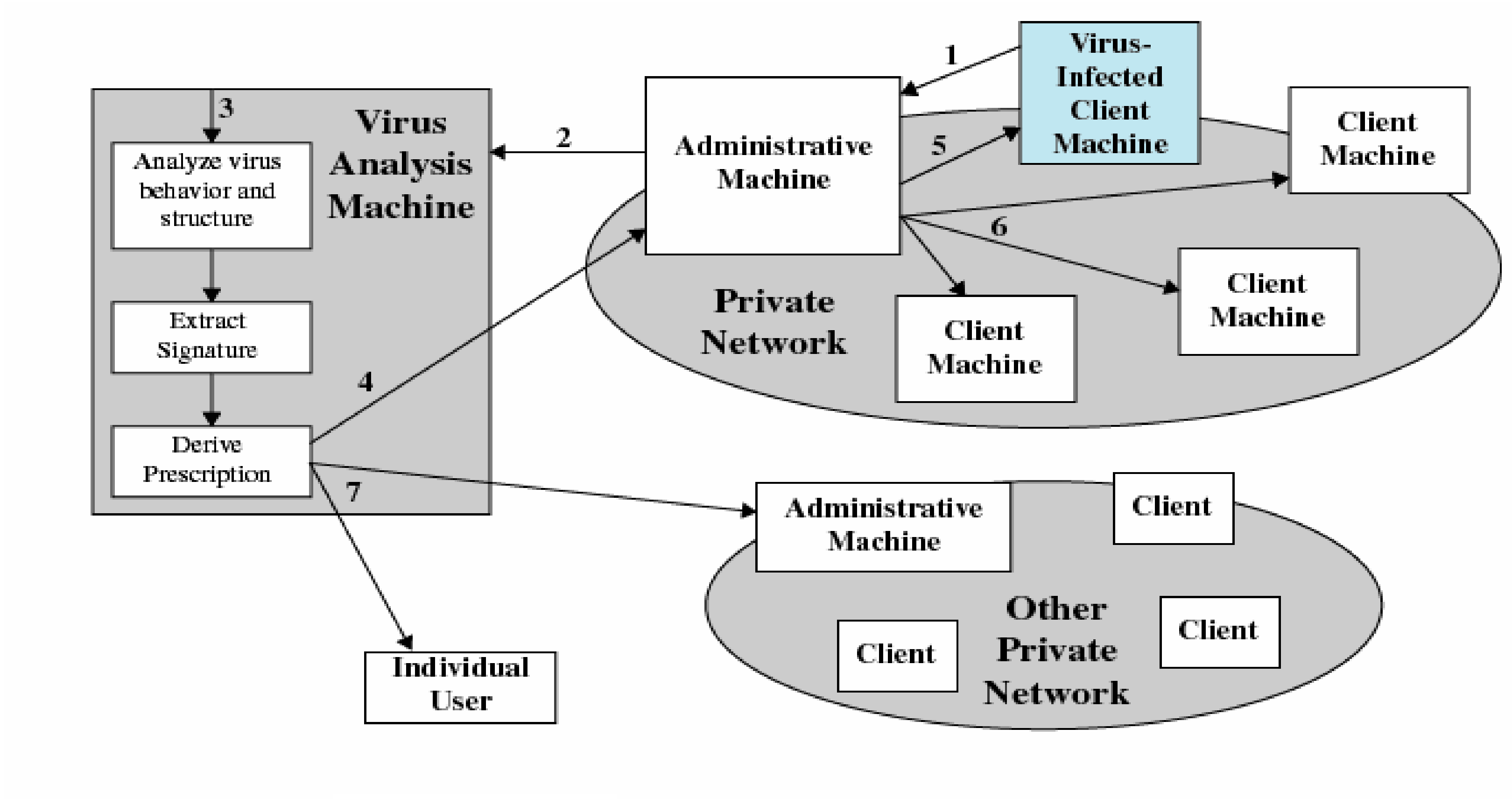
Digital Immune System

- A comprehensive approach to virus protected developed by IBM.
- Motivation has been the rising threat of Internet-based virus propagation
  - Integrated mail systems
  - Mobile-program system

Digital Immune System – How It Works

1. A monitoring program on each computer uses a variety of heuristics based on system behavior, suspicious changes to programs, or family signature to infer that a virus may be present. The monitoring program forwards a sample copy of any program thought to be infected to an administrative machine.
2. The administrative machine encrypts the sample and sends it to a central virus analysis machine.
3. This machine creates an environment in which the infected program can be run for analysis. The virus analysis machine then produces a prescription for identifying and removing the virus.
4. The resulting prescription is sent back to the administrative machine.
5. The administrative machine forwards the prescription to the infected client.
6. The prescription is also forwarded to other clients in the organization.
7. Subscribers around the world receive regular antivirus updates that protect them from the new virus.

Digital Immune System – How It Works (cont.)



Digital Immune System

E-mail Virus

- Activated when recipient opens the e-mail attachment.
- Activated by opening an e-mail that contains the virus.
- Uses Visual Basic scripting language.
- Propagates itself to all of the e-mail addresses known to the infected host.