“An inefficient virus kills its host. A clever virus stays with it.”

James Lovelock
Goals of Malware

- Steal user information
- Steal corporate information
- Ransomware
- Host files or perform calculations
- Create a botnet
- Install software
- Click fraud
- Break physical systems
Trojan Horses

• A Trojan horse is a program that does something malicious in addition to the expected function
• The author of the program intentionally adds code to do something in addition to what the user expects
• Often seen in “greeting card” programs
Animal Program

• The textbook mentions the animal program as an early Trojan horse
• When executed, the animal program copied itself into any directory that was writable
• The program was benign, but did consume disk space
Computer Viruses

- A computer virus is malicious software that propagates itself by adding its machine language to other executables.
- A virus is very similar to a Trojan horse, except that the malicious code is added after the program is written.
Virus Propagation

- A virus adds its machine language to the end of an executable.
Antivirus Software

• Antivirus software helps to detect malware
  – Pattern matchers that scan files for known viruses
  – Watch for suspicious activity, such as writing to an executable file
• Virus scanners can only look for known viruses
• Virus scanners are big string match programs looking for machine language known to be in a virus
• New virus signatures are created frequently and distributed by vendors
Hiding Viruses

• Viruses can hide through encrypting themselves
• The initial code of the virus decrypts the instructions and then executes the main portion of the virus
  – Encryption with different keys makes the encrypted instructions different and difficult to detect
• A polymorphic virus change the code in a random like manner to avoid scanners
Macro Viruses

• Some file types support macros, such as Microsoft office
• Macros allow programmers to add functionality to the documents
• The functionality can be malicious
• When an Office document is downloaded, Microsoft flags it as potentially dangerous
How can you defend against viruses?

• Antivirus software is on defense
• Works with the people around you to come up with another
Defense Against Virus Propagation

• Adding a digital signature to an executable file allows detection of any modification by a virus

• Disable writing to an existing executable file
  – A virus might create a new file and then change the name
  – Developers create new executables

• Software installation should make the entire directory read-only
Virus History

• Programmers for Apple II wrote some
  – Not called viruses; very experimental
• Fred Cohen
  – Graduate student who described them
  – Teacher (Adleman) named it “computer virus”
  – Tested idea on UNIX systems and UNIVAC 1108 system
Cohen’s Experiments

• UNIX systems: goal was to get superuser privileges
  – Max time 60m, min time 5m, average 30m
  – Virus small, so no degrading of response time
  – Virus tagged, so it could be removed quickly

• UNIVAC 1108 system: goal was to spread
  – As writing not inhibited, viruses spread easily
First Reports

• Brain (Pakistani) virus (1986)
  – Written for IBM PCs
  – Alters boot sectors of floppies, spreads to other floppies

• MacMag Peace virus (1987)
  – Written for Macintosh
  – Prints “universal message of peace” on March 2, 1988 and deletes itself
More Reports

• Duff’s experiments (1987)
  – Small virus placed on UNIX system, spread to 46 systems in 8 days
  – Wrote a Bourne shell script virus

• Highland’s Lotus 1-2-3 virus (1989)
  – Stored as a set of commands in a spreadsheet and loaded when spreadsheet opened
  – Changed a value in a specific row, column and spread to other files
Computer Worms

• A computer worm is a program that propagates itself without modifying other programs
• Some worms are transported by email and will automatically send themselves to everyone on the victims address book
Example: The Great Internet Worm

- The 99 line program was created by Robert Morris on November 2, 1988
- Targeted Berkeley, Sun UNIX systems
  - Used virus-like attack to inject instructions into running program and run them
  - To recover, had to disconnect system from Internet and reboot
  - To prevent re-infection, several critical programs had to be patched, recompiled, and reinstalled
- Analysts had to disassemble it to uncover function
- Disabled several thousand systems in 6 or so hours
- According to its creator, the Morris worm was not written to cause damage, but to gauge the size of the Internet
- Robert Morris was sentenced to three years probation, 400 hours of community service, and a fine of $10,050 plus costs
Rabbits

• Rabbits are programs that wastefully consume resources
• These create denial of service attacks

• The following will create an endless number of processes preventing needed processes from starting

```c
while (true) fork();
```
Create a Rabbit

• With the students around you, write a rabbit program that will stop a system
Logic Bombs

• A logic bomb is like a Trojan horse. It is created intentionally by the programmer
• Usually a logic bomb waits for a particular situation and then does something malicious
• A classical logic bomb was written by a programmer in the payroll department. If his ID number did not appear when printing paychecks (*indicating he was fired*), the program erased the payroll database
Tusting Trust

• Please read “Reflections on Trusting Trust” by Ken Thompson, Communications of the ACM, vol. 27, no. 8, August 1984
• Available on Blackboard under Course Materials
• It is a classic paper in Computer Science
• There are important concepts about source code inspection

• It is only 3 pages long