Announcements

• HW 6 is online
  – due December 10th.

• Final exam:
  – Tuesday, Dec. 21
  – 11:00am-1:00pm
  – Towne 311
Resource for Malicious Code

• New Book: Exploiting Software
  – Greg Hoglund and Gary McGraw
Recap

• Malicious Programs
  – Viruses
  – Boot Viruses, Memory Resident, Macros

• Today:
  – Computer Virus Defenses
  – Computer Worms
Detecting Viruses

- Scanning
- Integrity checking
- Heuristic detection
Virus Signatures

• Viruses can’t be completely invisible:
  – Code must be stored somewhere
  – Virus must do something when it runs

• Fragments of the virus code itself
  – Strings: “kindly check the attached LOVELETTER”

• Effects on the computing environment
  – Changes to the Windows registry

• Propagation Behavior
  – Copying/modifying system files.
Virus Scanners

• Search the system for *virus signatures*
  – Signs that a virus is present
  – e.g. Registry entries, hidden files, e-mail headers, etc.

• What to scan?
  – Main memory
  – All files in file system
  – Should also check boot sector

• When to scan?
  – On access (when a program is run)
  – On demand (at user’s request, or scheduled)
  – When e-mail is received?
  – Before web content is displayed?
Virus Scanning: Pros & Cons

• Pros
  – Effectively detects *known* viruses before they can cause harm
  – Few false alarms

• Cons
  – Can detect only viruses with known signatures
  – Signature set must be kept up to date
  – Virus writers can easily change virus signatures
Integrity Checks

• Virus scanner computes hash or checksum of executable files
  – Assumed to be virus free!
  – Stores the hash information

• Verifies new hash vs. saved one during scan
Integrity Checks: Pros & Cons

• Pros
  – Can detect corruption of executables too
  – Reliable
  – Doesn’t require virus signatures

• Cons
  – False positives (i.e. recompilation)
  – Can’t use it on documents (they change too often)
  – Not supported by most vendors
Heuristic Detection

• Collection of ad hoc rules that identifies virus behavior or virus-like programs
  – Modification of system executables
  – Modification of “template documents” like normal.doc
  – Self-modifying and self-referential code
  – …
Heuristics: Pros & Cons

• Pros
  – Perhaps able to detect unknown viruses

• Cons
  – Heuristics are hard to develop
  – Too may false positives
Polymorphic Viruses

• Virus writers know that virus signatures are the most effective way to detect viruses

• Polymorphic viruses mutate themselves during replication to prevent detection
  – Virus should be capable of generating many different descendents
  – Simply embedding random numbers into virus code is not enough
Strategies for Polymorphic Viruses

• Change data:
  – Use different subject lines in e-mail

• Encrypt most of the virus with a random key
  – Virus first decrypts main body using random key
  – Jumps to the code it decrypted
  – When replicating, generate a new key and encrypt
    the main part of the replica

• Still possible to detect decryption portion of
  the virus using virus signatures
Advanced Polymorphic Viruses

- Randomly modify the decryption portion of the virus by:
  - Inserting no-op instructions: subtract 0, move value to itself
  - Reordering independent instructions
  - Using different variable/register names
  - Using equivalent instruction sequences
    \[ y = x + x \quad \text{vs.} \quad y = 2 \times x \]
CERT Advice 1

- Use virus protection software
- Use a firewall
- Don't open unknown email attachments
- Don't run programs of unknown origin
- Disable hidden filename extensions
- Keep all applications, including your operating system, patched
Cert Advice 2

- Turn off your computer or disconnect from the network when not in use
- Disable Java, JavaScript, and ActiveX if possible
- Disable scripting features in email programs
- Make regular backups of critical data
- Make a boot disk in case your computer is damaged or compromised