Recap

• Program Security
  – Buffer Overflows

• Today:
  – Computer Viruses
Buffer Overrun in the News

• From Slashdot
  – “There is an unchecked buffer in Microsoft Data Access Components (MDAC) prior to version 2.7, the company said. MDAC is a "ubiquitous" technology used in Internet Explorer and the IIS web server. The buffer can be overrun with a malformed HTTP request, allowing arbitrary code to be executed on the target machine.”

  – http://www.theregister.co.uk/content/55/28215.html
The Consequences

• From Microsoft
  – “An attacker who successfully exploited it could gain complete control over an affected system, thereby gaining the ability to take any action that the legitimate user could take.”

Certificate Revocation Problems

- “A malicious attacker would be able to reintroduce the vulnerable control with just a specially [constructed] HTML document.”

- “the company recommends removing "Microsoft" from IE's Trusted Publisher list”
  - Doing so will cause a warning to appear when doing an update
Viruses

• A computer virus is a (malicious) program
  – Creates (possibly modified) copies of itself
  – Attaches to a host program or data
  – Often has other effects (deleting files, “jokes”, messages)
Virus Attachment: Append

- Simplest case: insert copy at the beginning of an executable file
- Runs before other code of the program
- Most common program virus
Virus Attachment: Surround

- Runs before & after original program
- Virus can clean up after itself
Virus Attachment: Replace

- Doesn’t change the size of the program
- Virus writer must know structure of original program
- Not as common, user more likely to detect.
Virus Writer’s Goals

- Hard to detect
- Hard to destroy or deactivate
- Spreads infection widely/quickly
- Can reinfect a host
- Easy to create
- Machine/OS independent
Kinds of Viruses

- Boot Sector Viruses
- Memory Resident Viruses
- Macro Viruses
Bootstrap Viruses

- **Bootstrap Process:**
  - Firmware (ROM) copies MBR (master boot record) to memory, jumps to that program

- **MBR (or Boot Sector):**
  - Fixed position on disk
  - “Chained” boot sectors permit longer Bootstrap Loaders
Bootstrap Viruses

- Virus breaks the chain
- Inserts virus code
- Reconnects chain afterwards
Why the Bootstrap?

• Automatically executed \textit{before} OS is running
  – Also before detection tools are running
• OS hides boot sector information from users
  – Hard to discover that the virus is there
  – Harder to fix

• Any good virus scanning software scans the boot sectors
Other Homes for Viruses

• System Software
  – IO.sys, NTLDR, NTDETECT.COM
  – autoexec.bat, config.sys, command.com

• Memory resident software
  – Task manager
  – Window manager
  – Winamp
  – RealPlayer
  – ...

Macro Viruses

• Macros are just programs
• Word processors & Spreadsheets
  – Startup macro
  – Macros turned on by default
• Visual Basic Script (VBScript)
Melissa Virus

• Transmission Rate
  – The first confirmed reports of Melissa were received on Friday, March 26, 1999.
  – By Monday, March 29, it had reached more than 100,000 computers.
  – One site got 32,000 infected messages in 45 minutes.

• Damage
  – Denial of service: mail systems off-line.
  – Could have been much worse
Melissa Macro Virus

• Implementation
  – VBA (Visual Basic for Applications) code associated with the "document.open" method of Word

• Strategy
  – Email message containing an infected Word document as an attachment
  – Opening Word document triggers virus if macros are enabled
  – Under certain conditions included attached documents created by the victim
Melissa Macro Virus: Behavior

• Setup
  – lowers the macro security settings
  – permit all macros to run without warning
  – Checks registry for key value “… by Kwyjibo”
  – `HKEY_Current_User\Software\Microsoft\Office\Melissa`?

• Propagation
  – sends email message to the first 50 entries in every Microsoft Outlook MAPI address book readable by the user executing the macro
Melissa Macro Virus: Behavior

• Propagation Continued
  – Infects Normal.dot template file
  – Normal.dot is used by all Word documents

• “Joke”
  – If minute matches the day of the month, the macro inserts message “Twenty-two points, plus triple-word-score, plus fifty points for using all my letters. Game's over. I'm outta here.”
Melissa: Remedy

- Filter mail for virus signature (macro in .doc files)
- Clean Normal.doc
“I Love You” Virus/Worm

• Infection Rate
  – At 5:00 pm EDT (GMT-4) May 8, 2000, CERT had received reports from more than 650 sites
  – > 500,000 individual systems

• VBScript

• Propagation
  – Email, Windows file sharing, IRC, USENET news
Love Bug

• Signature
  – An attachment named "LOVE-LETTER-FOR-YOU.TXT.VBS"
  – A subject of "ILOVEYOU"
  – Message body: "kindly check the attached LOVELETTER coming from me."
Love Bug Behavior

• Replaced certain files with copies of itself
  – Based on file extension (e.g. .vbs, .js, .hta, etc)

• Changed Internet Explorer start page
  – Pointed the browser to infected web pages

• Mailed copies of itself

• Changed registry keys