Viruses Part 4

How to Protect Against Viruses?

S-38.153 Security of Communication Protocols, Spring 2003

Vesa Vehkalahti

Prevention Measures (users)

- The easiest and the simplest way to avoid virus infections
- Good basis for protecting against viruses is to be well informed of different kind of viruses and how they work
- Common virus entry points should also be known to recognize threats and take the necessary precautions:
  - E-mail, WWW
  - Floppy disks and CDs

General Guidelines for Virus Prevention

- Acquire virus protection software and have it scan the hard-drive
- Anti-virus databases need to be updated often
- Backup important data files regularly
- Don't use pirated software
- Never use disks from an untrustworthy source and never download files from a site or person that you don't trust
- You should routinely test all software for viruses
- Freeware and shareware should be used with extreme care
- Always boot a system from the original write-protected and tested disk

General Guidelines for Virus Prevention

- Don't leave a disk in the floppy drive unless you are sure you want to boot from it
- Enter meaningful volume labels on all hard disks and diskettes
  - Routinely check volume labels and inspect the labels for changes
- Delete an E-mail with an attachment from an unknown source
  - Never open an email that looks unusual or suspicious
- Disable macros, if you don’t absolutely need them

Prevention Measures (companies)

Certain measures can be applied in companies and organizations and the following four-pronged strategy can be used:

- Form a group consisting of experts to deal with virus incidents
  - Responsible for education of users
  - Provides accurate information
  - Responds to reports of viruses
  - Deals with virus infections when they occur
- Each employee should know how to contact this group, if he or she suspects a virus infection

Prevention Measures (companies)

- Develop a plan to deal with viruses before there is a problem
  - □ Use anti-virus software to decrease the risk of an internal infection
  - □ Use a more general change detector on particularly critical systems
  - □ Put mechanisms in place to detect virus infections quickly
  - □ Know how to recover from a virus infection
- Test the plan periodically

Technical Protection Measures

- Firewalls are not very good protection measures against viruses
  - It only protects against viruses from the Internet

- A better way for technical protection is different kinds of anti-virus software

Anti-Virus Software Types

- Scanners
  - Most popular and effective
  - Contain detection / disinfection information for all known viruses
  - Alerts the computer user of the infection and displays the option to remove the virus
  - Frequent updates are needed
- Checksummers
  - Rely on detecting change
  - Don’t need updating
  - Complex programs and may sometimes display false warning messages
  - Findings need expert interpretation
  - Cannot be used to prevent an infection

Anti-Virus Software Types

- Heuristics
  - □ Detects viruses by using the characteristic structures of viruses defined on these programs
  - □ Doesn’t need updating
  - □ Main problem is that the virus writing community learns the rules used by heuristic software very quickly and starts writing viruses which can avoid them
    - Anti-virus companies can then reformulate the rules and reissue the software
  - □ Has a propensity to 'false-alarm‘
    - Because of this, heuristics have to be tempered effectively, in order that they are not over-sensitive

Anti-Virus Software Deployment Points

- In companies and organizations there are three main points where it makes sense to deploy anti-virus software:
  - On the internet gateway
  - On the servers
  - On the desktop (this applies to users in companies and at home)

Anti-Virus Software Deployment Points

- Internet gateway
  - This is a good place to install anti-virus software where it will check incoming and outgoing e-mail attachments
  - Main advantage is that incoming infected attachments sent to multiple e-mail addresses generates a single virus alert instead of multiple ones
  - A problem is the increasing use of encryption
    - Viruses will be safely hidden inside the encryption envelope

Anti-Virus Software Deployment Points

- Servers
  - □ Using anti-virus software on servers to scan centrally held files has several advantages over trying to scan the servers from a workstation
    - Network traffic is minimised since the scanning processes runs locally on the server
    - Any virus stealth mechanisms are not effective since the virus is never 'active' on the server
  - □ Most organisations deploy anti-virus software to scan their servers at regular intervals

Anti-Virus Software Deployment Points

- Desktop
  - □ Probably the most important part of the three-point scanning strategy
  - □ If the virus penetrates the internet gateway or the server scanner, the desktop catches it before it is allowed to infect the system
  - □ Keeping desktop anti-virus software up-to-date is one of the hardest tasks
    - This is especially the case on the desktops not permanently connected, such as laptops with docking stations

Possible Indications of a Virus Infection

- System slows down
- Unusual error messages or displays on your monitor
- Unusual sounds or music played at random times
- Your system has less available memory than normally should
- The operating system or regular applications refuse to start or some of your files suddenly don't work properly
- A disk or volume name has been changed
- Programs or files are suddenly missing
- Unknown programs or files have been created
- Turned-on access lights on a system device, when there should be no activity

What to Do If You Have a Virus?

- First try to get the virus protection software to "clean" or "disinfect" the files. Sometimes you may need a certain patch or other utility that removes the virus
- If this doesn't work, delete these files from your system
- You may also need to reformat your hard drive, destroying all the data on it
- Reinstall your software and data, assuming you have the original software disks and clean backups of your files
- Contact all the people you've recently exchanged information with and let them know that your system has been infected and theirs may be infected as well