Security Dangers in Browsers

Introduction

- Web browsers are point of vulnerability
  - PCs are more secure due to
    - anti-virus softwares
    - Anti-spyware softwares
- Disadvantages of Internet Explorer
  - Ubiquity of browser
  - Directly connected to internet
  - Directly tied to Windows OS
  - Many security holes than other browsers
    - ActiveX Controls

How Hackers exploit browsers?

- Browser attacks target specific browsers (IE or Firefox)
- Buffer Overflow Attack
  - Data downloads automatically to buffer and then to nearby memory
  - This data copied to nearby memory may contain malicious code
    - Allow hacker to take control of PC
    - May download a Trojan on to PC

How Hackers exploit browsers?

- Drive-by download
  - May download similar to spyware
  - Can be a Trojan or a Spyware as well
  - Can be downloaded by clicking on Ads
- ActiveX
  - Allows software to download from Internet and run on the browser
  - Can create ActiveX controls that steal information

How to protect from Browser based Attacks?

- Avoid visiting sites which may be run by hackers
  - Avoid phishing attacks
- Use Firefox (safer) than Internet Explorer
- Run antivirus and anti-spyware regularly
- Keep antivirus and anti-spyware updated
- Avoid clicking pop-ups
- Disable ActiveX controls and JavaScript content

Working of Worms and Viruses

Introduction

- Malware are practically ubiquitous and no means of escaping them
- Viruses can delete data files, erase programs, destroy everything, flash annoying messages etc.
- Worms replicate to all machines which are connected to the network – internal or internet
- Use anti-virus and its components
  - Scanner
  - Eradication program

Working of Viruses

- One can get virus through an infected program, or opening a file infected by virus
- Virus hides inside a legitimate program, where it remains dormant until the infected program is run
- Sometimes, execution of virus may lead to infection in other programs
- Some viruses place *Virus Markers (v-markers)* inside programs that they infect
  - These messages help manage virus activities
- Viruses can corrupt program or data files

Working of Worms

- Worm is a generic program that spreads over a network
- Worms arrive to inbox like a normal file attachment
- When the user clicks the file, worm springs into action
- Worm checks the names of first 50 names in the inbox and attaches itself to the file and sends mails to them
- Each of these 50 recipients then open the file and fell as trap to the worms
- Also, this unrequired and undesired forwarding of mails overwhelm the mail servers

Working of Antivirus

- Scanners check for viruses and alert their presence
- Detection methods
  - Telltale virus makers using virus definitions
  - Check change in program’s file size
- Eradication programs disinfect or remove viruses from software