VIRUSES Part I

S-38.153 Security of Communication protocols, Spring 2003

Jarkko Kuisma

Introduction

- In the mid-eighties, the Amjad brothers of Pakistan ran a computer store. Frustrated by computer piracy, they wrote the first computer virus, a boot sector virus called Brain. From those simple beginnings, an entire counter-culture industry of virus creation and distribution emerged, leaving us today with several tens of thousands of viruses.

What is a Virus?

- Computer viruses are called viruses because they are in a certain way like biological viruses. A computer virus passes from computer to computer as biological virus passes from person to person.
- A biological virus is not a living thing. A virus is a fragment of DNA. Unlike a cell, a virus has no way to do anything or to reproduce by itself. Instead, a biological virus must inject its DNA into a cell.

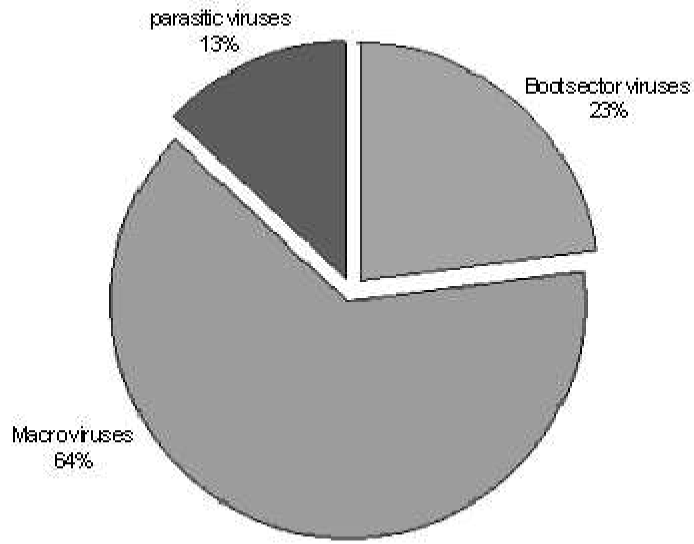
General Information about viruses

- A properly engineered virus can have a major effect on the worldwide Internet.
- Viruses are categorized in two sections: traditional viruses and the newer e-mail viruses.

Virus categories

- Boot viruses, Multipart viruses
- DOS file viruses, Windows viruses (Windows95/98/NT, Windows 3.x)
- Macro viruses
- Internet Worms/viruses (Email, etc.)
- Script, Java, WinHelp viruses (e.g. Visual Basic Script viruses, HTML file infectors)
- Malware: Trojans, Backdoors, etc.
- OS/2, Unix viruses
- Polymorphic Generators and Generator-based Viruses
- Virus Constructors, Joke programs
- Information on Computer Hoaxes

Three most common types



Types of Infection

The most common forms of electronic infections

- Viruses - a virus is a small piece of software that penetrate on programs. Each time the program runs, the virus runs too, and it has the chance to reproduce.
- E-Mail viruses - An e-mail virus moves around in e-mail messages, and usually replicates itself by automatically mailing itself to people in the victim's e-mail address book. Viruses are *generally* (almost always) OS (operating system)-specific. Meaning, viruses created for a DOS application can do no damage on a Macintosh, and vice-versa.

- Virus hoax messages: familiar to most email users. One of the main reasons for this is that they play on peoples ignorance - users are understandably concerned about viruses, and so consider it 'helpful' if, as suggested by the majority of hoaxes, they forward the message to all contacts in their address book.
- Such an action, all be it well-meaning, is *not* helpful. It may increase network load considerably.

- Worms - software that uses computer networks and security holes to replicate itself. A copy of the worm scans the network for another machine that has a specific security hole. It copies itself to the new machine using the security hole, and then starts replicating from there.
  - example: the **Code Red** worm replicated itself over 250,000 times in approximately nine hours on July 19, 2001.

- Trojan Horses - The program claims to do one thing (it may claim to be a game) but instead does damage when you run it (it may erase your hard disk). Trojan horses have no way to replicate automatically.
- In the future, viruses cross OS-boundries because Java, ActiveX programming languages break the typical "rules" of how a virus is OS-specific.

How do the viruses spread?

- Early viruses were pieces of code attached to a common program like a popular game or a popular word processor. They spread by
  - Downloading
  - Floppy disk
- A virus like this is a small piece of code embedded in a larger, often legitimate program. Virus is designed to run first **when the legitimate program gets executed**. The virus loads itself into memory and looks around to see if it can find any other programs on the disk. If it can find one, it modifies it to add the virus's code to the unsuspecting program.

- Secondly: The virus launches the "real program." **The user really has no way to know that the virus ever ran.**
- The Virus has now reproduced itself, so two programs are infected. The next time either of those programs gets executed, they infect other programs, and the cycle continues.
- If the infected programs is given to another person on a floppy disk (or other media), then other programs could get infected.
- Most viruses also have some sort of destructive **attack** phase where they do some damage.

- A trigger activates the attack phase, and the virus will then "do something"
  - printing a silly message on the screen
  - erasing all of your data!

- The trigger might be a specific date, or the number of times the virus has been replicated, or something similar.
- Virus creators learned new tricks.
  - One important trick: the ability to load viruses into memory so they could keep running in the background as long as the computer remained on. This gave viruses a much more effective way to replicate themselves.
  - Another trick was the ability to infect the **boot sector** on floppy disks and hard disks.

- The boot sector is a small program that is the first part of the operating system that the computer loads.
- The boot sector contains a tiny program that tells the computer how to load the rest of the operating system.
- By putting its code in the boot sector, a virus can **guarantee it gets executed**. It can load itself into memory immediately, and it is able to run whenever the computer is on.
- Boot sector viruses can infect the boot sector of any floppy disk inserted in the machine, and on college campuses (example HUT) where lots of people share machines they spread like wildfire.

- In general, both executable and boot sector viruses are not very threatening any more. The first reason for the decline has been the huge size of today's programs. Nearly every program you buy today comes on a compact disc.
- Original compact discs cannot be modified and that makes viral infection of a CD impossible.
- However the CDR and CDRW-media are vulnerable against viruses because they can be used as ”floppies” for storing data.
- New BIOS-systems allow booting from CD for example

- The programs are so big that the ”only” easy way to move them around is to buy the CD. People certainly can't carry applications around on a floppy disk (like it was in the 1980s). Boot sector viruses have also declined because operating systems now protect the boot sector.
- Both boot sector viruses and executable viruses are still possible, but they are a lot harder now and they don't spread nearly as quickly as they once could.

- The environment of floppy disks, small programs and weak operating systems made these viruses possible in the 1980s, but that has been largely eliminated by huge executables, unchangeable CDs and better operating system safeguards.

Who Creates viruses and why?

- first category: students and schoolchildren (?)
- The second group consists of young people (often students), who are not experts in programming yet, but have already decided to devote themselves to creating and spreading.
- third category: "professional" viruses. These are very thoroughly thought out and debugged programs created by often by talented professional programmers. Such viruses implement original algorithms, undocumented system calls and unknown methods of incorporating into system data areas.

How to punish?

- The USA's largest group of defence lawyers (the National Association of Criminal Defense Lawyers) has backed a report claiming that sentences for computer-related crimes are too harsh.
- sentences that have been awarded for computer-related crimes were criticised for being tougher than those for comparable, non-computer-related crimes.
- the calculations of losses both unreliable and open to exaggeration.

- The loss estimation for identical offences can vary widely depending on factors such as the actions taken by the victim
  - (example: one victim may simply restore the hard drive from backup, while another spends large amounts of money hiring consultants to assess the damage)
- and the nature of the victim
  - (example: the losses resulting from a compromised system within a small business with a low turnover will be lower than those resulting from a similar attack on a thriving business).

the sentencing by US courts of Melissa author David Smith

- provoked considerable discussion within the anti-virus community. Some considered Smith's 20-month prison sentence a fitting penalty while others were disappointed by the shortness of the sentence.

how about Europe?

- Reuters: new laws approved by European Union justice ministers will mean that, in Europe, virus writers could be imprisoned for up to five years.