

## Malicious software. Attacks and countermeasures,I

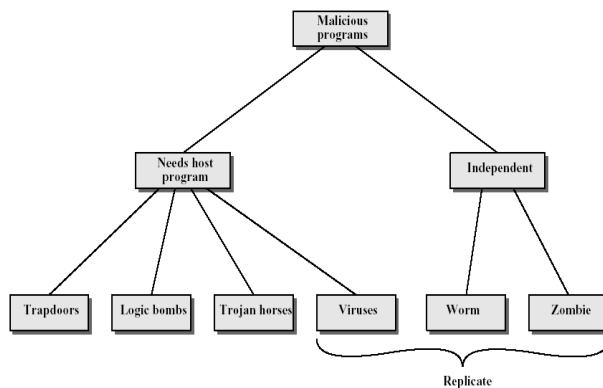
COMP 522

## Malicious programs

- Software threats to computer systems:
  - malicious programs that exploit vulnerabilities in computer systems to launch attacks on security and privacy;
  - continuous development new types of malicious programs and countermeasures;
  - vulnerabilities in computer systems are almost inevitable due to their immense complexity.

COMP 522

## Taxonomy of malicious programs



COMP 522

## Trap doors

- Trap door is a secret entry point into a program that allows someone that is aware of the trapdoor to gain access without going through the usual security access procedures;
- Trap doors may be used legitimately during debugging and testing programs;
- Trap doors become threats when they are used to gain unauthorized access

COMP 522

## Trap door

---

- Ken Thompson, in his Turing Award Lecture, 1984: an example of trap door is discussed: modifying a C compiler can make a trap door which is almost impossible to find;
- “Moral is obvious. You can't trust code that you did not totally create yourself.”

---

COMP 522

## Logic Bomb

---

- The logic bomb is code embedded in some legitimate program that is set to explode when certain conditions are met:
  - Presence or absence of certain files;
  - Particular day of the week or data
  - Particular user running the application
- Once triggered, a bomb may alter or delete data, cause machine halt, etc.
- The case of Tim Lloyd: more than 10 millions dollars damage.

---

COMP 522

## Trojan Horses

---

- A Trojan Horse is a useful (or apparently) useful program containing hidden code that, when invoked, performs some unwanted or harmful function.
- Thompson example: a compiler is a Trojan Horse – very difficult to discover.
- Very Recent Zeus trojan, 2007- now: millions computers are infected

---

COMP 522

## Zombies and Botnets

---

- A zombie is a program that secretly takes over another Internet-attached computer and then uses that computer to launch attacks and propagate itself
- Zombies may be used in denial-of –service attacks, or sending spam messages.
- Large orchestrated collections of zombies usually referred to as botnets
- Example: Bredolab botnet (2009-2010) >30 million computers infected

---

COMP 522

## Viruses

- A virus is a program that can “infect” other programs by modifying them;
- The modification includes a copy of the virus program, which can then go on to infect other programs;
- A virus attaches itself to another program and executes secretly when the host program is run.

COMP 522

## Typical virus phases

- **Dormant phase:** the virus is idle;
- **Propagation phase:** the virus places an identical copy of itself into other programs or into some system areas on the disk ;
- **Triggering phase:** the virus is activated to perform the function for which it was intended;
- **Execution phase:** the function is performed;

COMP 522

## Theoretical analysis

- **F. Cohen, 1980s-90s:** theoretical analyses of the viral mechanisms;
- First formal definition of computer viruses;
- **Undecidability theorem:**
  - In general, the problem of detection of viruses is undecidable;

COMP 522

## Simple Virus (after F.Cohen)

```
program V :=
{goto main;
 1234567;

  subroutine infect-executable :=
  {loop;
   file := get-random-executable-file;
   if (first-line-of-file = 1234567)
   then goto loop
   else prepend V to file; }

  subroutine do-damage :=
  {whatever damage is to be done}

  subroutine trigger-pulled :=
  {return true if some condition holds}

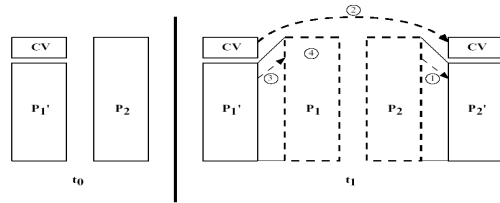
main:  main-program :=
       {infect-executable;
        if trigger-pulled then do-damage;
        goto next;}

next:
}
```

Easy to detect: it increases the size of infected programs.

COMP 522

## A compression virus



1. For uninfected file  $P_2$  the virus first compress  $P_2$  to make  $P_2'$  which is shorter than original program by the size of the virus.
2. A copy of the virus is attached to the compressed program.
3. Original  $P_1$  is uncompressed.
4.  $P_1$  is executed.

COMP 522

## Types of viruses

- **Parasitic virus:** most common for of virus. It attaches itself to executable files and replicates, when the infected program is executed.
- **Memory-resident virus:** lodges in main memory as part of resident system program. From that point on, the virus infects every program that executes.
- **Boot sector virus:** infect a boot record and spreads when a system is booted from the disk containing the virus.
- **Stealth virus:** a form of virus designed to hide itself from detection
- **Polymorphic virus:** a virus that mutates with every infection, making detection by the “signature” impossible

These types are not mutually exclusive!

COMP 522

## Macro viruses and e-mail viruses

- Macro viruses take advantage of a **macro** feature found in Word and other office applications;
- A macro is executable program embedded in a word processing document, or other type of file;
- Autoexecuting macro, that is automatically invoked (say,when opening or closing a file) , without explicit user input ,makes it possible to create a macro virus;
- Macro viruses are easily spread. A common method is by electronic mail.

COMP 522

## Infamous Melissa virus

- Typical example of macro virus spread via e-mail;
- It makes use of MS Word macro embedded in an attachment;
- If recipient opens the e-mail attachment, th Word macro is activated and
  - The virus sends itself to everyone on the mailing list in the user's e-mail application;
  - The virus does local damage;

COMP 522

## Worms

---

- An e-mail virus propagates itself from system to system with a “help” of human, who opens some attachments, etc;
- Network **worm** programs actively use network connections to spread from systems to systems without any user participation:
- Typically worms use:
  - Electronic mail facility;
  - Remote execution capability;
  - Remote login capability;
  - 2005: worms propagating via Instant Messengers (MSN messenger, AOL messenger, etc).

---

COMP 522

## Computer Business Review (Security survey 2005)

---

- “It is clear that the biggest, most successful, malware threats have been the network worms, which remotely exploit vulnerabilities in software, compromising machines and spreading very quickly.”

---

COMP 522

## From the CBR survey

---

**August 2003**, the worm Blaster and its Nachi variant :

- caused Air Canada to delay flights while it cleaned its check-in desk computers;
- CSX's 23,000-mile rail network, the third-largest in North America, halted;
- The administrators of The New York Times had to turn off their network while they sorted the issue out.
- In government and military, Edwards Air Force Base in California conceded part of its network to Blaster;
- Overall cost of damages: many millions of dollars.

---

COMP 522