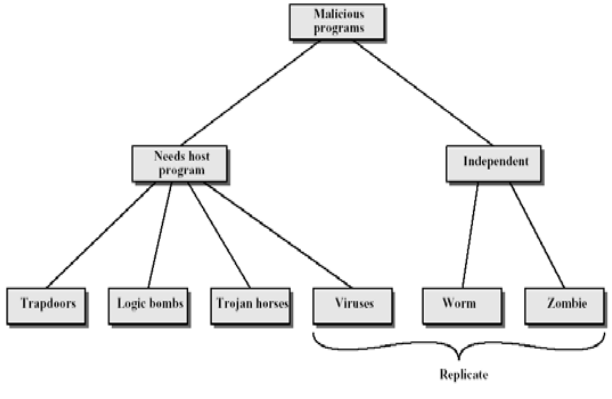
Malicious software. Attacks and countermeasures,I

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.

Taxonomy of malicious programs



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

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."

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 Time Lloyd: more than 10 millions dollars damage.

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.
- CBS example

Zombie

- A zombie is a program that secretly takes over another Internet-attached computer and then uses that computer to launch attacks that are difficult to trace to the zombie's creator.
- Zombies may be used in denial-of –service attacks, typically against targeted Web sites.

Viruses

- A virus is a program that can “infect” other programs by modifying then;
- 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.

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;

Theoretical analysis

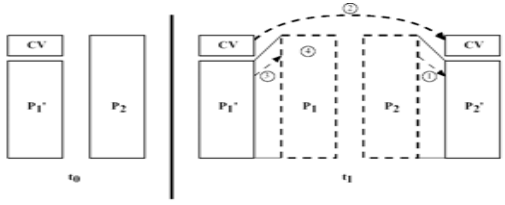
- **F. Cohen, 1980s-90s**: theoretical analyses of the viral mechanisms;
- First formal definition of computer viruses;
- **Undecidability theorem**:
  - In general, the problem of detection of viruses is undecidable;

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.

A compression virus



1. For uninfected file P2 the virus first compress P2 to make P2' which is shorter that original program by the size of the virus.
2. A copy of the virus is attached to the compressed program.
3. Original P1 is uncompressed.
4. P1 is executed.

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!

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.

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;

Worms

- Am 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 Massengers (MSN messenger, AOL messenger, etc).

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.”

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.