



S J P N Trust's

**Hirasugar Institute of Technology, Nidasoshi.**

*Inculcating Values, Promoting Prosperity*

Approved by AICTE, Recognized by Govt. of Karnataka and Affiliated to VTU Belagavi

ECE Dept.

NS

VIII Sem

2017-18

**Department of Electronics & Communication Engg.**

**Course : Network Security**

**Sem.: 8<sup>th</sup> (2017-18 EVEN)**

**Course Coordinator:**

**Prof. Nyamatulla M Patel**

# CRYPTOGRAPHY AND NETWORK SECURITY

Unit-07

**Malicious Software**



# Malicious Software

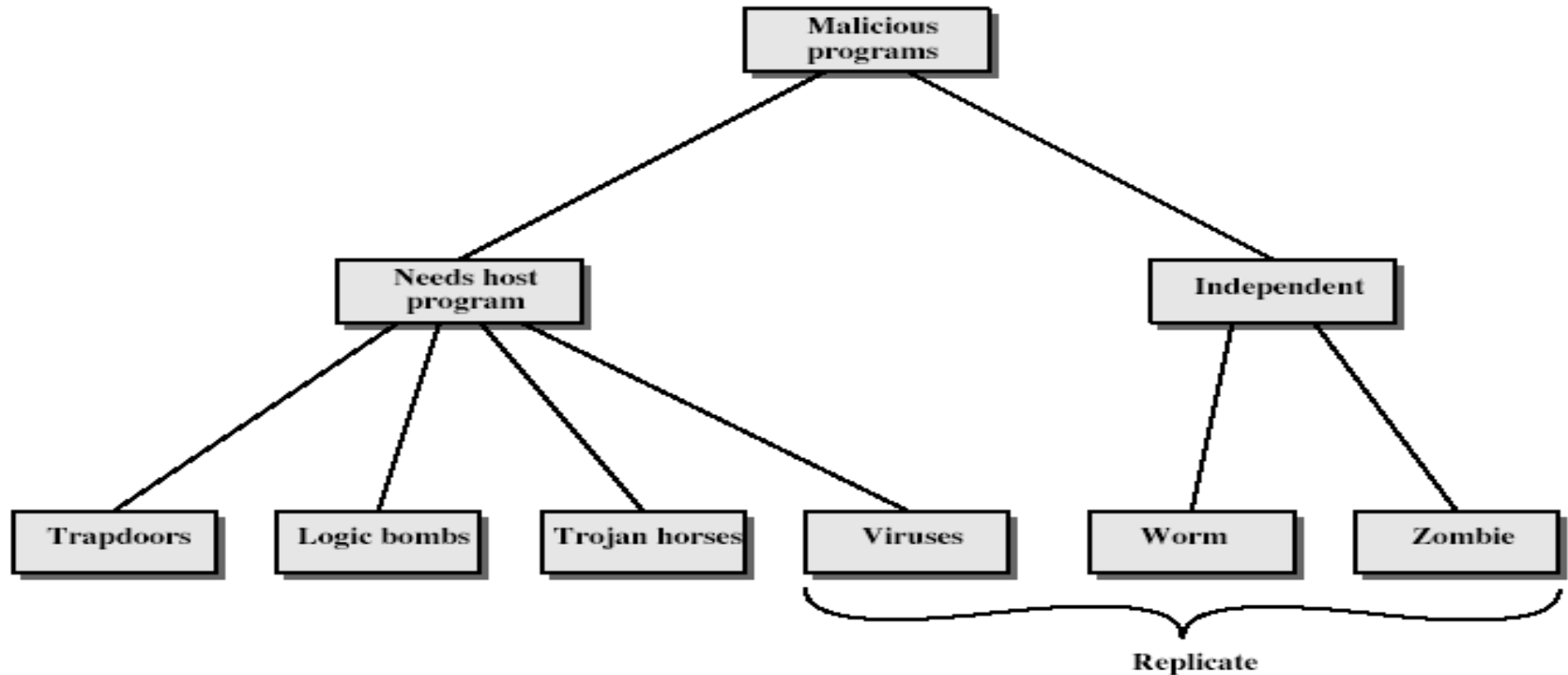
*What is the concept of defense: The parrying of a blow. What is its characteristic feature: Awaiting the blow.*

**—On War, Carl Von Clausewitz**

# Viruses and Other Malicious Content

- computer viruses have got a lot of publicity
- one of a family of **malicious software**
- effects usually obvious
- have figured in news reports, fiction, movies (often exaggerated)
- getting more attention than deserve
- are a concern though

# Malicious Software



# Trapdoors

- secret entry point into a program
- allows those who know access bypassing usual security procedures
- have been commonly used by developers
- a threat when left in production programs allowing exploited by attackers
- very hard to block in O/S
- requires good s/w development & update

# Logic Bomb

- one of oldest types of malicious software
- code embedded in legitimate program
- activated when specified conditions met
  - eg presence/absence of some file
  - particular date/time
  - particular user
- when triggered typically damage system
  - modify/delete files/disks



# Trojan Horse

- program with hidden side-effects
- which is usually superficially attractive
  - eg game, s/w upgrade etc
- when run performs some additional tasks
  - allows attacker to indirectly gain access they do not have directly
- often used to propagate a virus/worm or install a backdoor
- or simply to destroy data



# Zombie

- program which secretly takes over another networked computer
- then uses it to indirectly launch attacks
- often used to launch distributed denial of service (DDoS) attacks
- exploits known flaws in network systems

# Viruses

- a piece of self-replicating code attached to some other code
  - cf biological virus
- both propagates itself & carries a payload
  - carries code to make copies of itself
  - as well as code to perform some covert task

# Virus Operation

- virus phases:
  - dormant – waiting on trigger event
  - propagation – replicating to programs/disks
  - triggering – by event to execute payload
  - execution – of payload
- details usually machine/OS specific
  - exploiting features/weaknesses

# Virus Structure

```
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:  
}
```

# Types of Viruses

- can classify on basis of how they attack
- parasitic virus
- memory-resident virus
- boot sector virus
- stealth
- polymorphic virus
- macro virus

# Macro Virus

- **macro code** attached to some **data file**
- interpreted by program using file
  - eg Word/Excel macros
  - esp. using auto command & command macros
- code is now platform independent
- is a major source of new viral infections
- blurs distinction between data and program files making task of detection much harder
- classic trade-off: "ease of use" vs "security"

# Email Virus

- spread using email with attachment containing a macro virus
  - cf Melissa
- triggered when user opens attachment
- or worse even when mail viewed by using scripting features in mail agent
- usually targeted at Microsoft Outlook mail agent & Word/Excel documents



# Worms

- replicating but not infecting program
- typically spreads over a network
  - cf Morris Internet Worm in 1988
  - led to creation of CERTs
- using users distributed privileges or by exploiting system vulnerabilities
- widely used by hackers to create **zombie PC's**, subsequently used for further attacks, esp DoS
- major issue is lack of security of permanently connected systems, esp PC's

# Worm Operation

- worm phases like those of viruses:
  - dormant
  - propagation
    - search for other systems to infect
    - establish connection to target remote system
    - replicate self onto remote system
  - triggering
  - execution

# Morris Worm

- best known classic worm
- released by Robert Morris in 1988
- targeted Unix systems
- using several propagation techniques
  - simple password cracking of local pw file
  - exploit bug in finger daemon
  - exploit debug trapdoor in sendmail daemon
- if any attack succeeds then replicated self

# Recent Worm Attacks

- new spate of attacks from mid-2001
- **Code Red**
  - exploited bug in MS IIS to penetrate & spread
  - probes random IPs for systems running IIS
  - had trigger time for denial-of-service attack
  - 2<sup>nd</sup> wave infected 360000 servers in 14 hours
- **Code Red 2**
  - had backdoor installed to allow remote control
- **Nimda**
  - used multiple infection mechanisms
    - email, shares, web client, IIS, Code Red 2 backdoor

# Virus Countermeasures

- viral attacks exploit lack of integrity control on systems
- to defend need to add such controls
- typically by one or more of:
  - **prevention** - block virus infection mechanism
  - **detection** - of viruses in infected system
  - **reaction** - restoring system to clean state

# Anti-Virus Software

- **first-generation**
  - scanner uses virus signature to identify virus
  - or change in length of programs
- **second-generation**
  - uses heuristic rules to spot viral infection
  - or uses program checksums to spot changes
- **third-generation**
  - memory-resident programs identify virus by actions
- **fourth-generation**
  - packages with a variety of antivirus techniques
  - eg scanning & activity traps, access-controls



# Advanced Anti-Virus Techniques

- generic decryption
  - use CPU simulator to check program signature & behavior before actually running it
- digital immune system (IBM)
  - general purpose emulation & virus detection
  - any virus entering org is captured, analyzed, detection/shielding created for it, removed

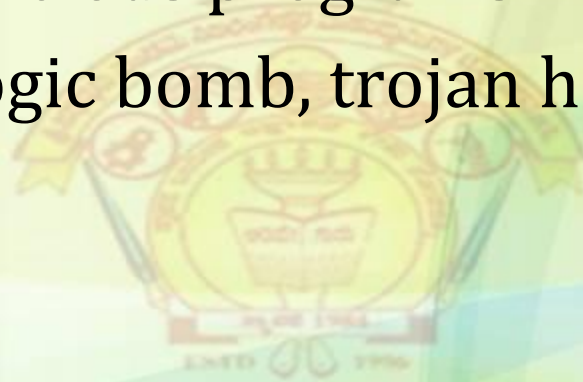


# Behavior-Blocking Software

- integrated with host O/S
- monitors program behavior in real-time
  - eg file access, disk format, executable mods, system settings changes, network access
- for possibly malicious actions
  - if detected can block, terminate, or seek ok
- has advantage over scanners
- but malicious code runs before detection

# Summary

- have considered:
  - various malicious programs
  - trapdoor, logic bomb, trojan horse, zombie
  - viruses
  - worms
  - countermeasures



# Queries ....?

