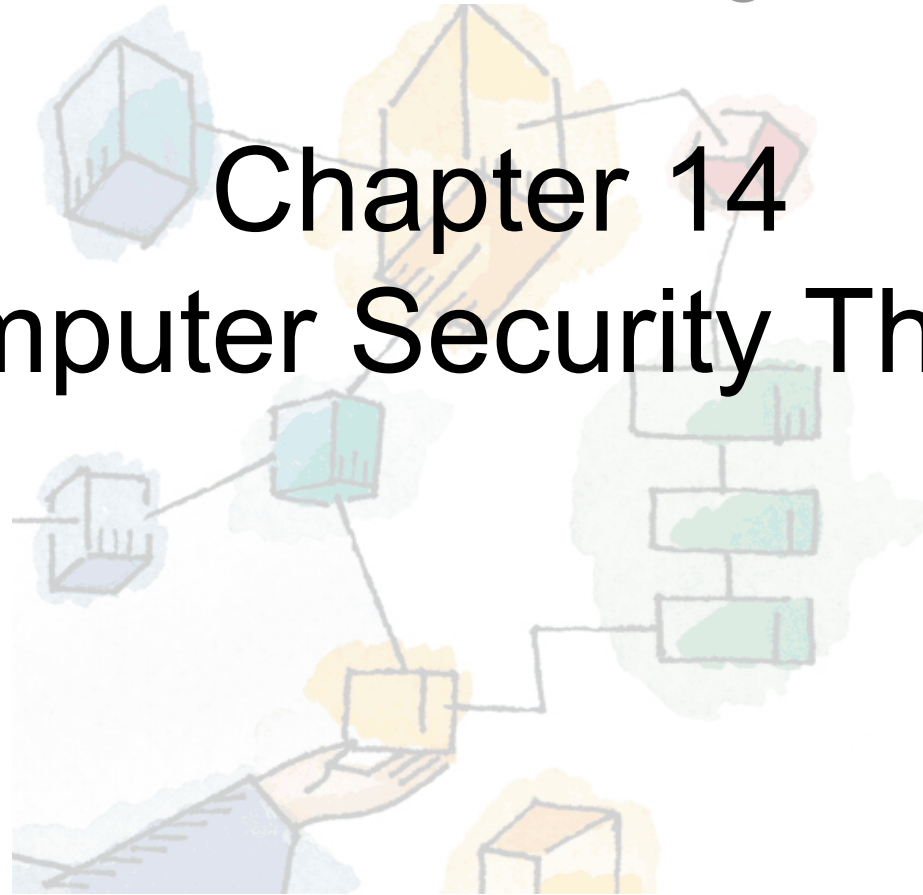
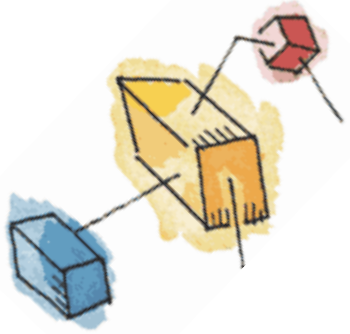


*Operating Systems:
Internals and Design Principles, 6/E*
William Stallings

Chapter 14
Computer Security Threats

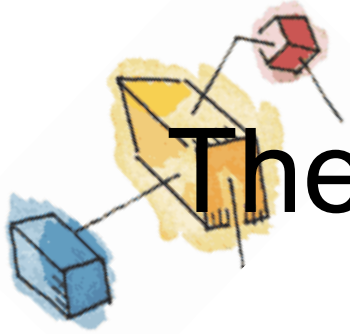




Computer Security

- Confidentiality
 - Data confidentiality
 - Privacy
- Integrity
 - Data integrity
 - System integrity
- Availability





The Security Requirements Triad

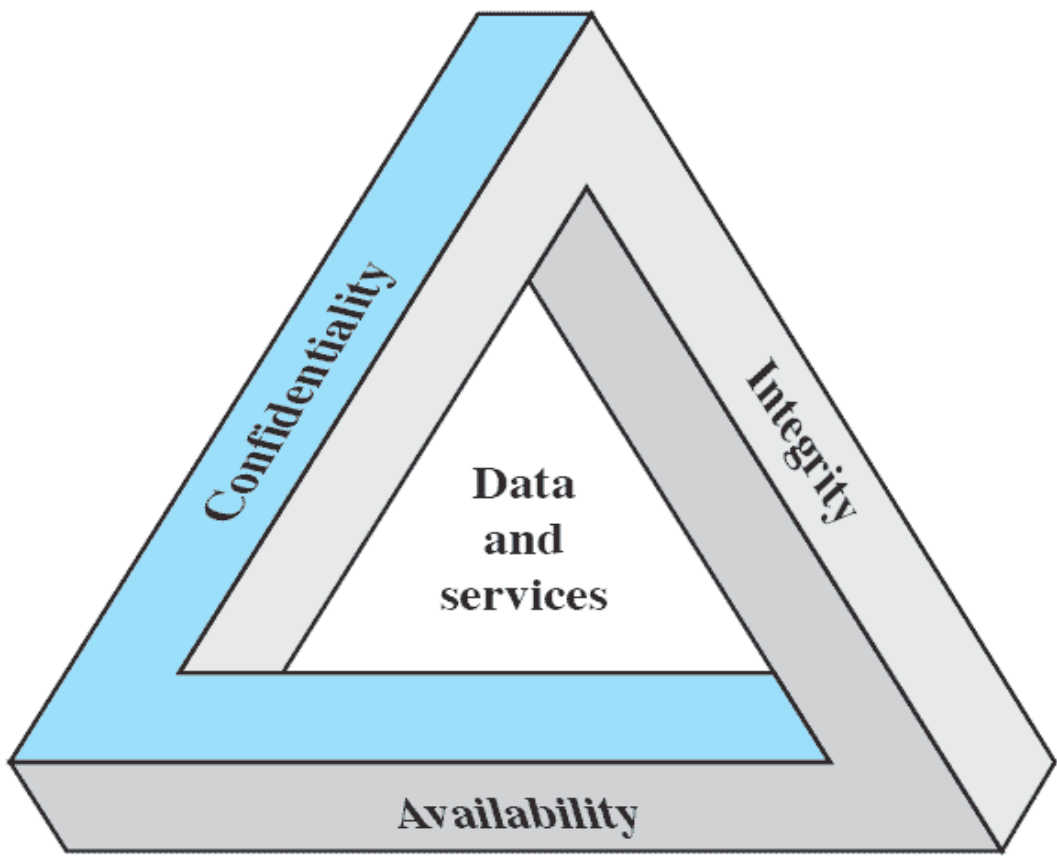
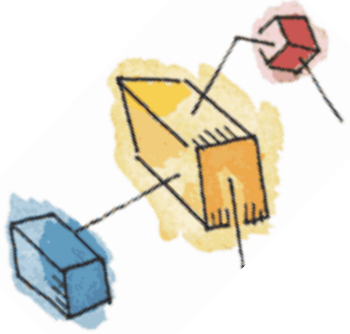


Figure 14.1 The Security Requirements Triad

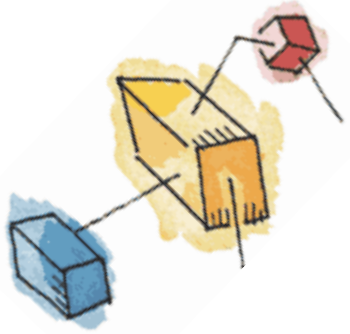


Additional Concepts

- Authenticity
- Accountability



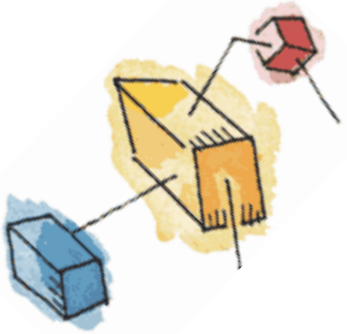
Threats



Threat Consequence	Threat Action (attack)
Unauthorized Disclosure A circumstance or event whereby an entity gains access to data for which the entity is not authorized.	Exposure: Sensitive data are directly released to an unauthorized entity. Interception: An unauthorized entity directly accesses sensitive data traveling between authorized sources and destinations. Inference: A threat action whereby an unauthorized entity indirectly accesses sensitive data (but not necessarily the data contained in the communication) by reasoning from characteristics or byproducts of communications. Intrusion: An unauthorized entity gains access to sensitive data by circumventing a system's security protections.



Threats



Deception

A circumstance or event that may result in an authorized entity receiving false data and believing it to be true.

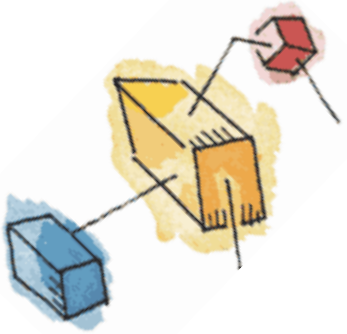
Masquerade: An unauthorized entity gains access to a system or performs a malicious act by posing as an authorized entity.

Falsification: False data deceive an authorized entity.

Repudiation: An entity deceives another by falsely denying responsibility for an act.



Threats



Disruption

A circumstance or event that interrupts or prevents the correct operation of system services and functions.

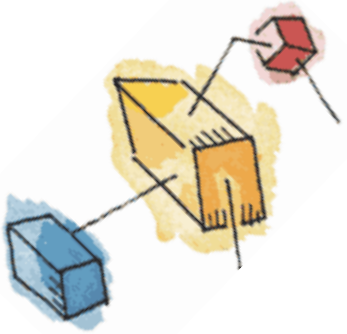
Incapacitation: Prevents or interrupts system operation by disabling a system component.

Corruption: Undesirably alters system operation by adversely modifying system functions or data.

Obstruction: A threat action that interrupts delivery of system services by hindering system operation.



Threats



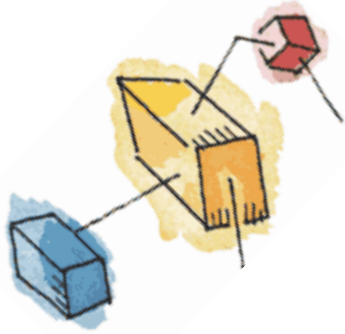
Usurpation

A circumstance or event that results in control of system services or functions by an unauthorized entity.

Misappropriation: An entity assumes unauthorized logical or physical control of a system resource.

Misuse: Causes a system component to perform a function or service that is detrimental to system security.





Scope of System Security

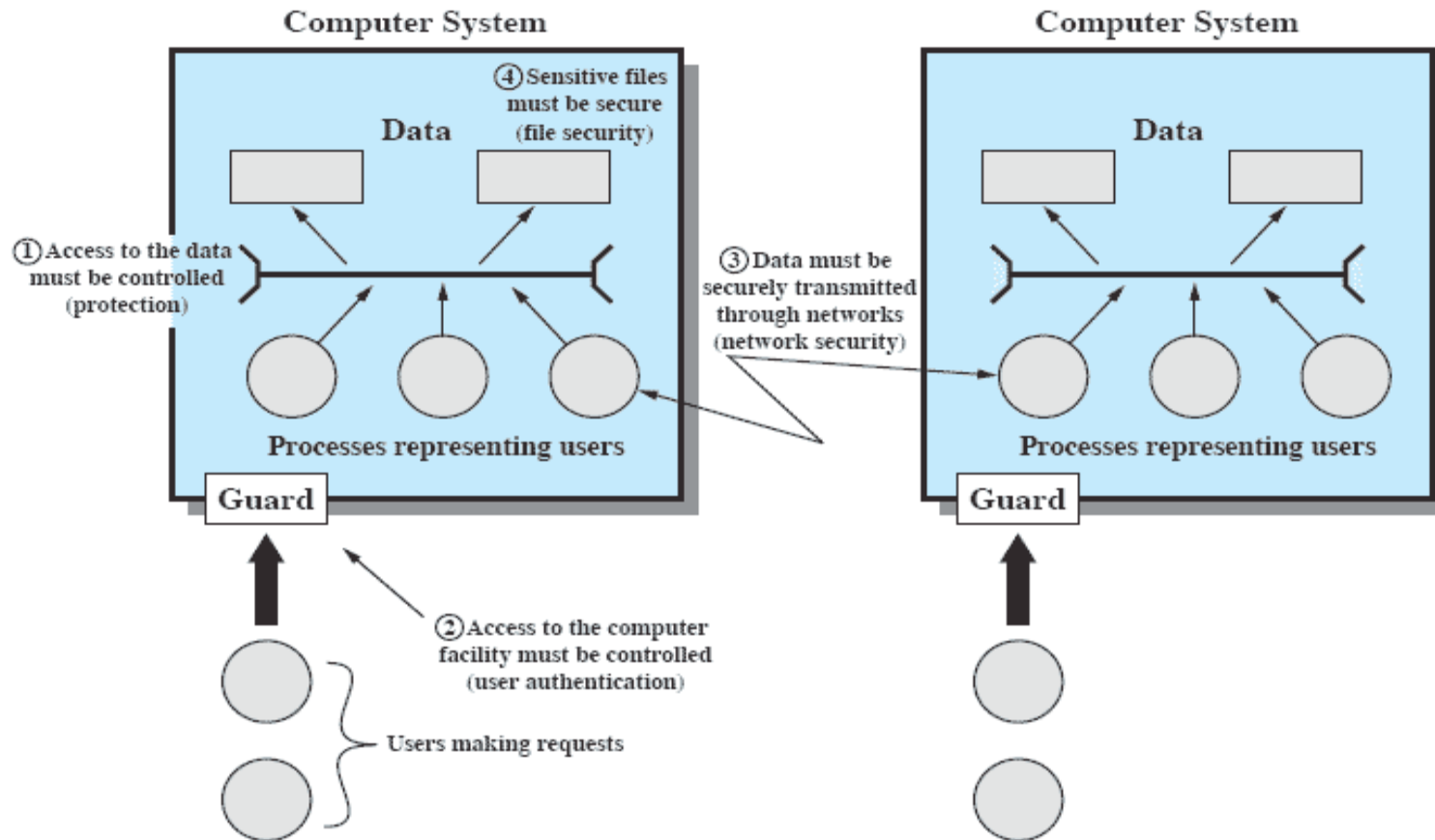
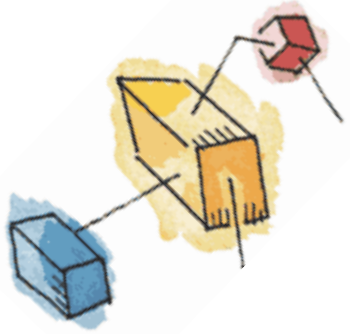


Figure 14.2 Scope of System Security



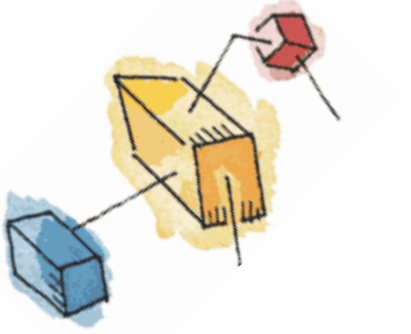
Assets



	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.		
Software	Programs are deleted, denying access to users.	An unauthorized copy of software is made.	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task.
Data	Files are deleted, denying access to users.	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.	Existing files are modified or new files are fabricated.
Communication Lines	Messages are destroyed or deleted. Communication lines or networks are rendered unavailable.	Messages are read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.



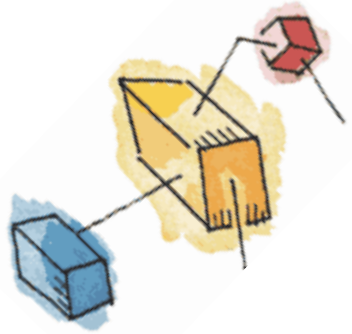
Intruders



- Masquerader
- Misfeasor
- Clandestine user



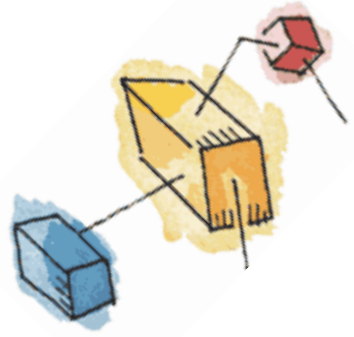
Intruders



(a) Hacker

1. Select the target using IP lookup tools such as NSLookup, Dig, and others.
2. Map network for accessible services using tools such as NMAP.
3. Identify potentially vulnerable services (in this case, pcAnywhere).
4. Brute force (guess) pcAnywhere password.
5. Install remote administration tool called DameWare.
6. Wait for administrator to log on and capture his password.
7. Use that password to access remainder of network.



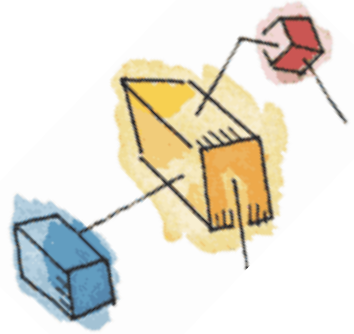


Intruders

(b) Criminal Enterprise

1. Act quickly and precisely to make their activities harder to detect.
2. Exploit perimeter through vulnerable ports.
3. Use Trojan horses (hidden software) to leave back doors for reentry.
4. Use sniffers to capture passwords.
5. Do not stick around until noticed.
6. Make few or no mistakes.





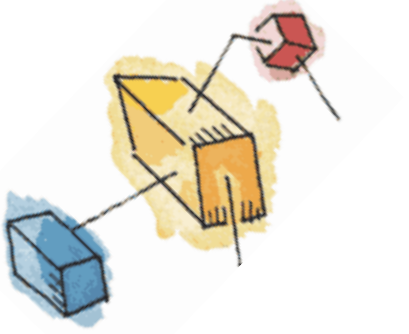
Intruders

(c) Internal Threat

1. Create network accounts for themselves and their friends.
2. Access accounts and applications they wouldn't normally use for their daily jobs.
3. E-mail former and prospective employers.
4. Conduct furtive instant-messaging chats.
5. Visit Web sites that cater to disgruntled employees, such as fdcompany.com.
6. Perform large downloads and file copying.
7. Access the network during off hours.

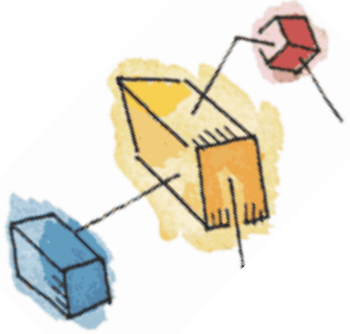


Backdoor



- Trapdoor
- Secret entry point
- Useful for programmers debuggin

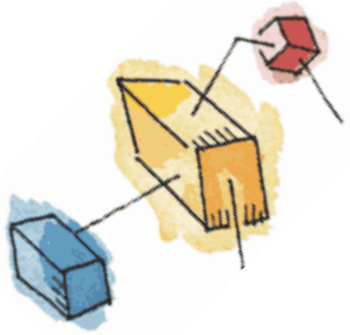




Logic Bomb

- Explodes when certain conditions are met
 - Presence or absence of certain files
 - Particular day of the week
 - Particular user running application

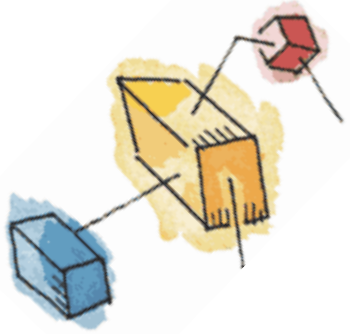




Trojan Horse

- Useful program that contains hidden code that when invoked performs some unwanted or harmful function
- Can be used to accomplish functions indirectly that an unauthorized user could not accomplish directly
 - User may set file permission so everyone has access

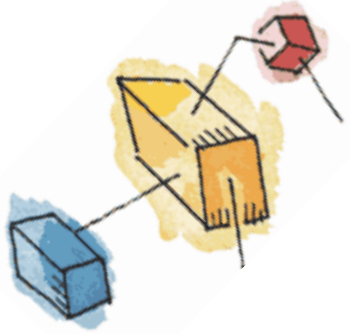




Mobile Code

- Transmitted from remote system to local system
- Executed on local system without the user's explicit instruction



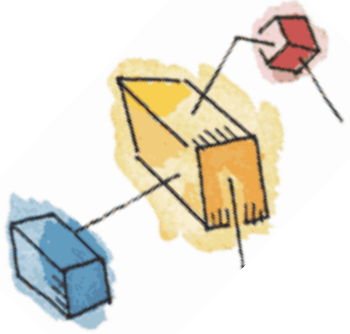


Multiple-Threat Malware

- Multipartite virus infects in multiple ways
- Blended attack uses multiple methods
- Ex: Nimda has worm, virus, and mobile code characteristics

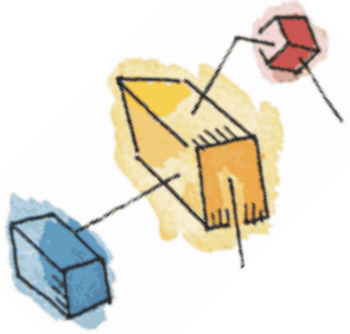


Parts of Virus



- Infection mechanism
- Trigger
- Payload

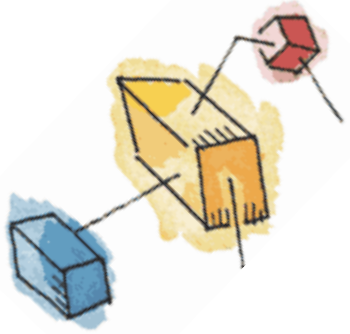




Virus Stages

- Dormant phase
 - Virus is idle
- Propagation phase
 - Virus places an identical copy of itself into other programs or into certain system areas on the disk





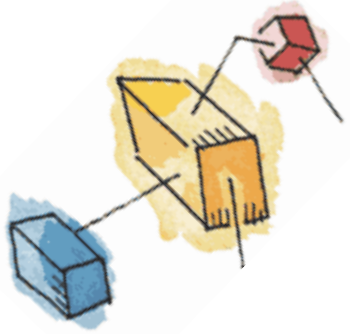
Virus Stages

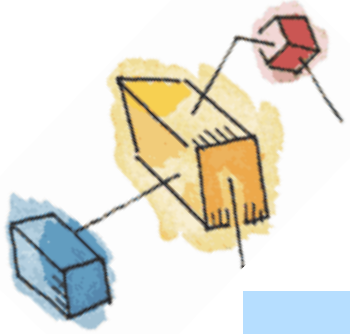
- Triggering phase
 - Virus is activated to perform the function for which it was intended
 - Caused by a variety of system events
- Execution phase
 - Function is performed



Simple Virus

```
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:  
}
```





Compression Virus

```
program CV :=  
  
{goto main;  
 01234567;  
  
subroutine infect-executable :=  
  {loop:  
   file := get-random-executable-file;  
   if (first-line-of-file = 01234567) then goto loop;  
  (1) compress file;  
  (2) prepend CV to file;  
  }  
  
main: main-program :=  
  {if ask-permission then infect-executable;  
  (3) uncompress rest-of-file;  
  (4) run uncompressed file;}  
}
```

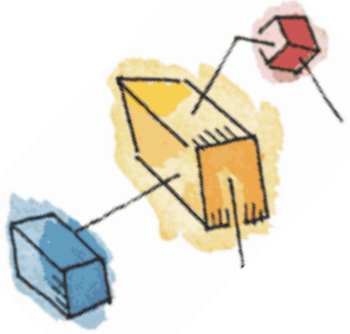




Virus Classification by Target

- Boot sector infector
- File infector
- Macro virus

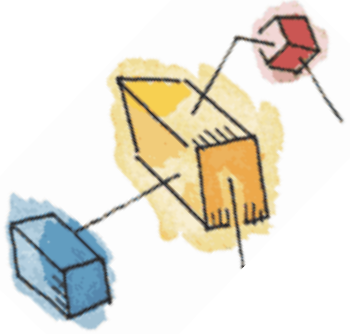




Virus Classification by Concealment Strategy

- Encrypted virus
 - Random encryption key encrypts remainder of virus
- Stealth virus
 - Hides itself from detection of antivirus software

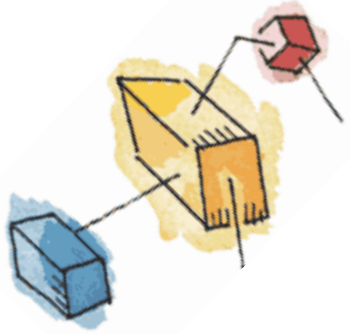




Virus Classification by Concealment Strategy

- Polymorphic virus
 - Mutates with every infection
- Metamorphic virus
 - Mutates with every infection
 - Rewrites itself completely after every iteration

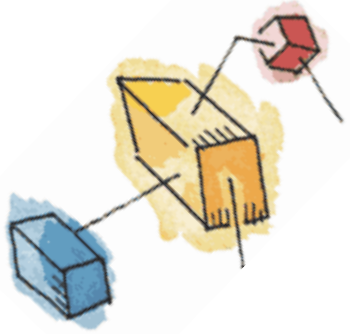




Macro Viruses

- Platform independent
 - Most infect Microsoft Word documents
- Infect documents, not executable portions of code
- Easily spread
- File system access controls are of limited use in preventing spread



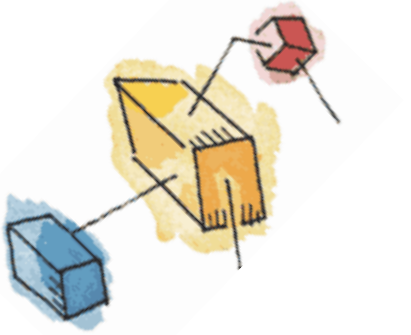


E-Mail Viruses

- Attachment
- Open e-mail
- Uses e-mail software to replicate



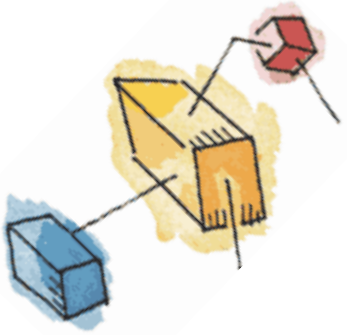
Worms



- Use network connections to spread from system to system
- Electronic mail facility
 - A worm mails a copy of itself to other systems

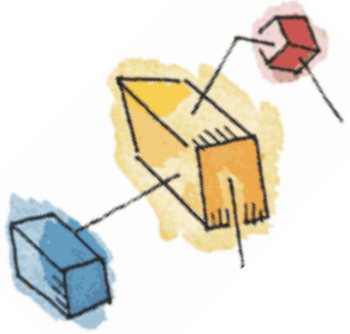


Worms

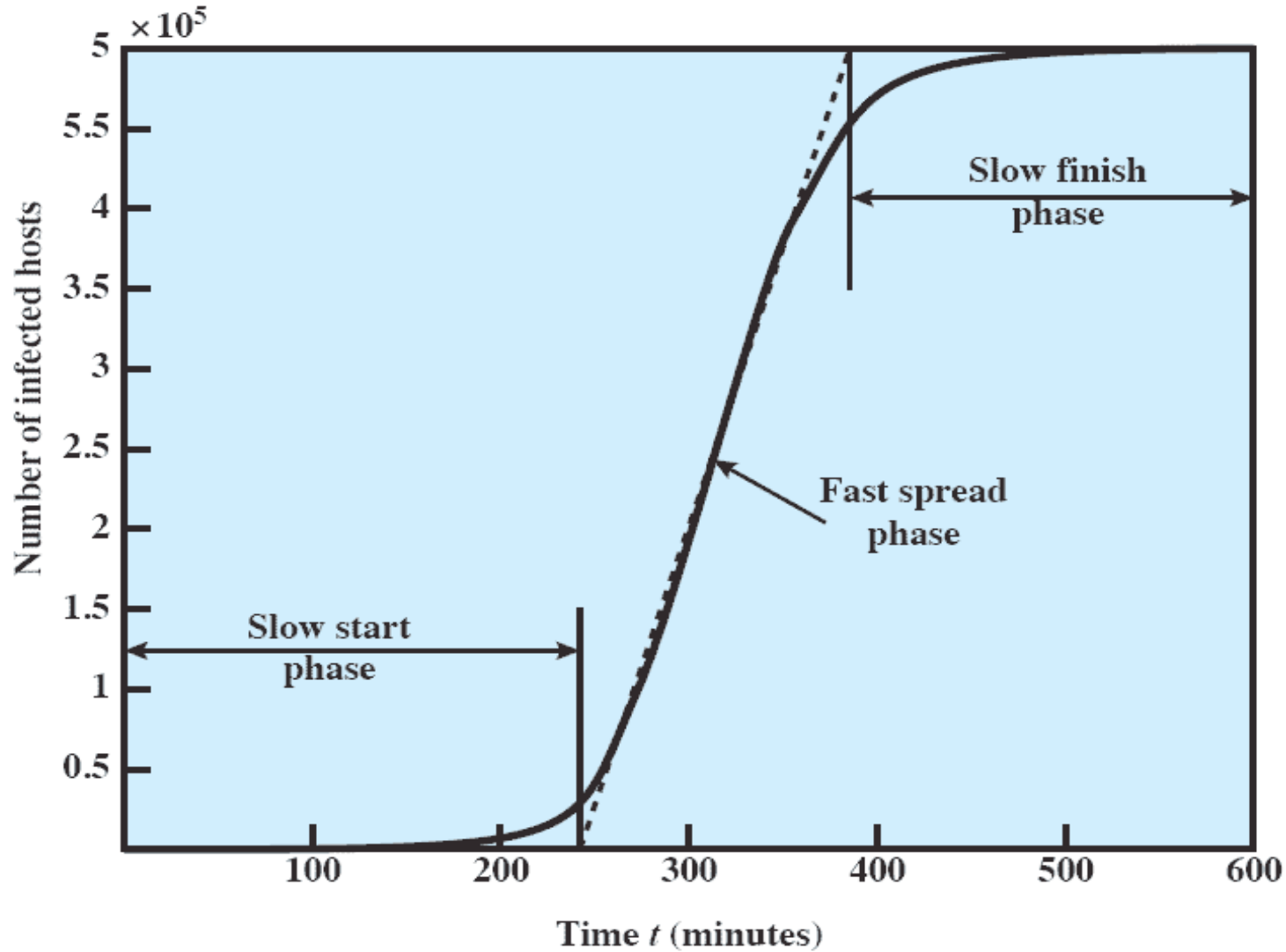


- Remote execution capability
 - A worm executes a copy of itself on another system
- Remote log-in capability
 - A worm logs on to a remote system as a user and then uses commands to copy itself from one system to the other

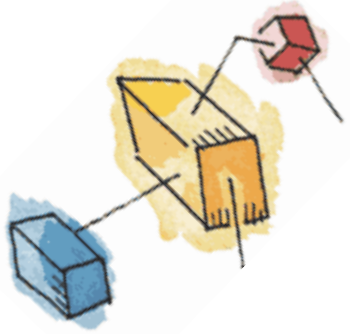




Worm Propagation Model



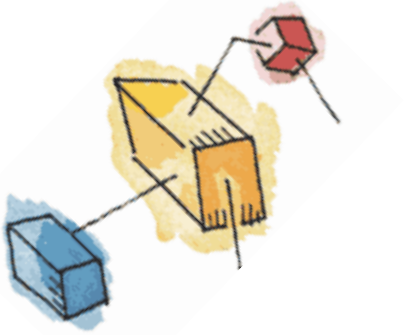
Bots



- Zombie or drone
- Program secretly takes of another Internet -attached computer
- Launch attacks that are difficult to trace to bot's creator
- Collection of bots is a botnet

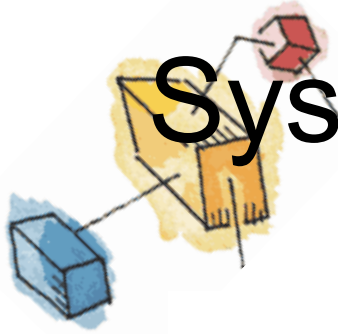


Rootkit

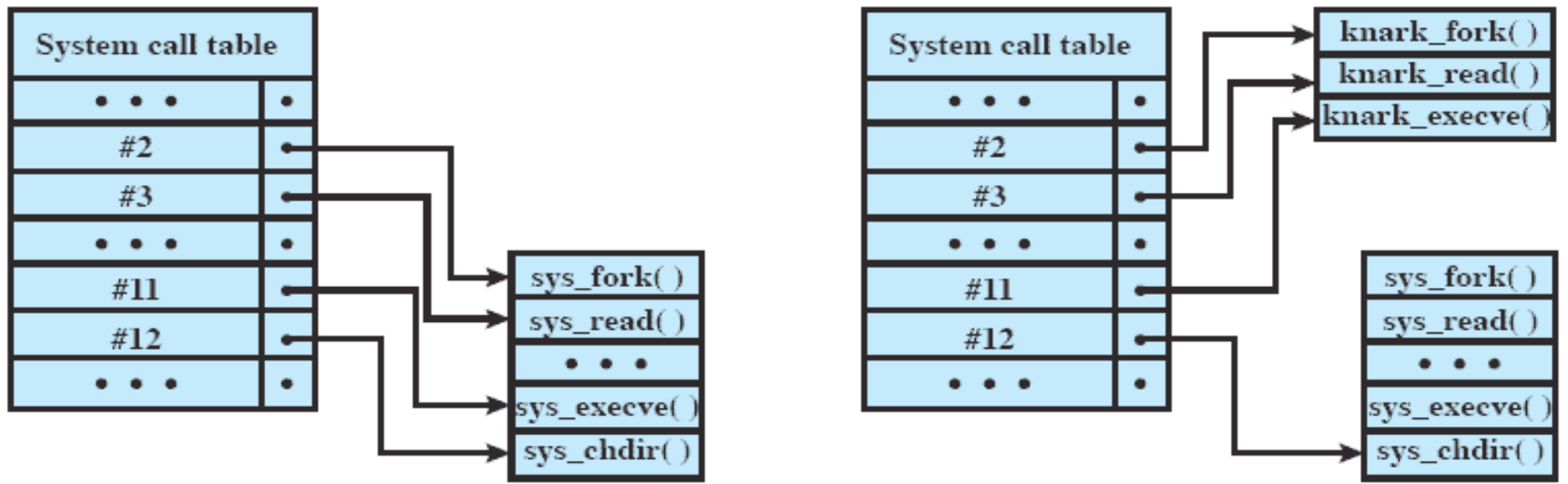


- Set of programs installed on a system to maintain administrator (or root) access to that system
- Hides its existence





System Call Table Modification by Rootkit



(a) Normal kernel memory layout

(b) After nkark install

Figure 14.6 System Call Table Modification by Rootkit

