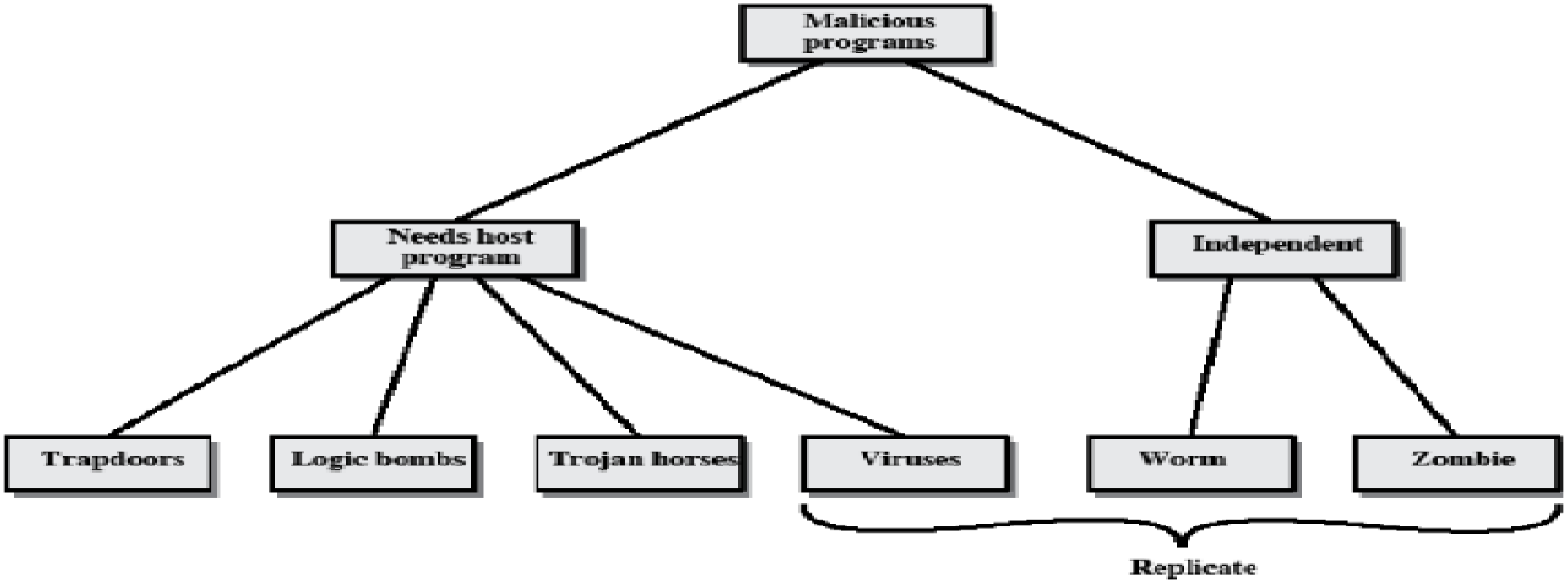
CHAPTER 7: MALICIOUS LOGIC

- Malicious Logic, Types of Malicious Logic: Virus, Worm, Trojan Horse, Zombies, Denial of Service Attacks,
- Intrusion, Intruders and their types (Masquerader, Misfeasor, Clandestine),Intrusion Detection System: Statistical anomaly detection, Rule-based detection

MALICIOUS LOGIC

- *Malicious logic* is a set of instructions that cause a site’s security policy to be violated.


Malicious programs
Needs host program
Independent
Trapdoors
Logic bombs
Trojan horses
Viruses
Worm
Zombie
Replicate

VIRUS

- *A computer virus is a program that inserts itself into one or more files and then performs some (possibly null) action.*
- *The first phase, in which the virus inserts itself into a file, is called the insertion phase. The second phase, in which it performs some action, is called the execution phase.*

VIRUS

Several types of computer viruses have been identified.

- ***Boot Sector Infectors***
- ***Executable Infectors***
- ***Multipartite Viruses***
- ***TSR Viruses***
- ***Stealth Viruses***
- ***Encrypted Viruses***
- ***Polymorphic Viruses***
- ***Macro Viruses***

BOOT SECTOR VIRUS

- The *boot sector* is the part of a disk used to bootstrap the system or mount a disk. Code in that sector is executed when the system “sees” the disk for the first time.
- When the system boots, or the disk is mounted, any virus in that sector is executed.
- A boot sector infector is a virus that inserts itself into the boot sector of a disk.

BOOT SECTOR VIRUS

EXAMPLE:

The Brain virus for the IBM PC is a boot sector infector. When the system boots from an infected disk, the virus is in the boot sector and is loaded. It moves the disk interrupt vector (location 13H or 19) to an alternative interrupt vector (location 6DH or 109) and sets the disk interrupt vector location to invoke the Brain virus now in memory. It then loads the original boot sector and continues the boot.

EXECUTABLE INFECTORS

An executable infector is a virus that infects executable programs. The PC variety of executable infectors are called COM or EXE viruses because they infect programs with those extensions.

Multipartite Viruses

A *multipartite virus* is one that can infect either boot sectors or applications.
Such a virus typically has two parts, one for each type. When it infects an executable, it acts as an executable infector; when it infects a boot sector, it works as a boot sector infector.

TSR VIRUSES

- A terminate and stay resident (TSR) virus is one that stays active (resident) in memory after the application (or bootstrapping, or disk mounting) has terminated.
- TSR viruses can be boot sector infectors or executable infectors

STEALTH VIRUSES

- Stealth viruses are viruses that conceal the infection of files.

ENCRYPTED VIRUSES

- An encrypted virus is one that enciphers all of the virus code except for a small decryption routine.
- Computer virus detectors often look for known sequences of code to identify computer viruses.
- To conceal these sequences, some viruses encipher most of the virus code, leaving only a small decryption routine and a random cryptographic key in the clear.

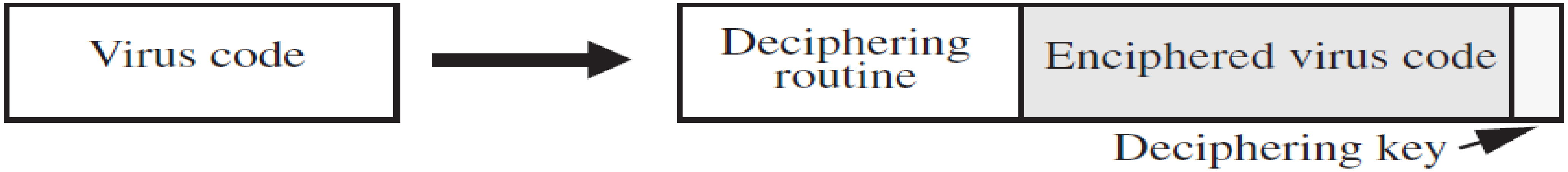


Figure 19–2 An encrypted virus. The ordinary virus code is at the left. The encrypted virus, plus encapsulating decryption information, is at the right.

POLYMORPHIC VIRUSES

- A polymorphic virus is a virus that changes its form each time it inserts itself into another program.
- **Macro Viruses**
- A *macro* virus is a virus composed of a sequence of instructions that is interpreted, rather than executed directly
- A macro virus can infect either executables or data files.

WORM

- A *computer worm* is a program that copies itself from one computer to another.

TROJAN HORSE

- *A Trojan horse is a program with an overt (documented or known) effect and a covert (undocumented or unexpected) effect.*
- *Trojan horses can make copies of themselves.*
- *A propagating Trojan horse (also called a replicating Trojan horse) is a Trojan horse that creates a copy of itself.*

RABBITS AND BACTERIA

- Some malicious logic multiplies so rapidly that resources become exhausted. This creates a denial of service attack.
- A bacterium or a rabbit is a program that absorbs all of some class of resource.

Example

```
while true
do
mkdir x
chdir x
done
```

LOGIC BOMBS

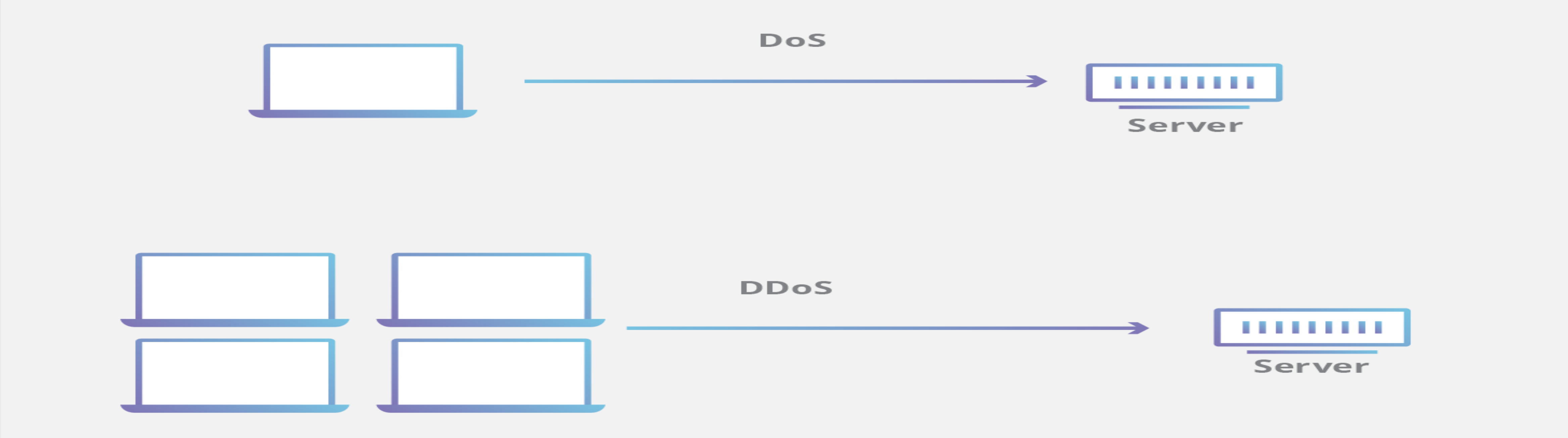
- Some malicious logic triggers on an external event, such as a user logging in or the arrival of midnight, Friday the 13th
- A logic bomb is a program that performs an action that violates the security policy when some external event occurs.
- Disaffected employees who plant Trojan horses in systems use logic bombs.
- The events that cause problems are related to the troubles the employees have, such as deleting the payroll roster when that user’s name is deleted.

DENIAL OF SERVICE ATTACK

- A denial-of-service (DoS) attack is a type of attack in which a malicious actor aims to render a computer or other device unavailable to its intended users by interrupting the device's normal functioning.
- DoS attacks typically function by overwhelming or flooding a targeted machine with requests until normal traffic is unable to be processed, resulting in denial-of-service to addition users.
- A DoS attack is characterized by using a single computer to launch the attack.

DISTRIBUTED DENIAL OF SERVICE ATTACK(DDOS)

- A distributed denial-of-service (DDoS) attack is a type of DoS attack that comes from many distributed sources, such as a botnet DDoS attack.



INTRUDER

- One of the two most publicized threats to security is the intruder (the other is viruses), often referred to as a hacker or cracker.
- In an important early study of intrusion, Anderson identified three classes of intruders:
  - Masquerader
  - Misfeasor:
  - Clandestine user:

INTRUDER TYPES

- **Masquerader**

An individual who is not authorized to use the computer and who penetrates a system's access controls to exploit a legitimate user's account

- **Misfeasor**

A legitimate user who accesses data, programs, or resources for which such access is not authorized, or who is authorized for such access but misuses his or her privileges .

- **Clandestine user**

An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection.

The masquerader is likely to be an outsider; the misfeasor generally is an insider; and the clandestine user can be either an outsider or an insider

EXAMPLES OF INTRUSION

- Performing a remote root compromise of an e-mail server
- Defacing a Web server
- Guessing and cracking passwords
- Copying a database containing credit card numbers
- Viewing sensitive data, including payroll records and medical information, without authorization
- Running a packet sniffer on a workstation to capture usernames and passwords
- resetting the executive’s e-mail password, and learning the new password
- Using an unattended, logged-in workstation without permission

INTRUSION DETECTION

- **Statistical anomaly detection**
- **Rule-based detection**

STATISTICAL ANOMALY DETECTION

- Involves the collection of data relating to the behavior of legitimate users over a period of time. Then statistical tests are applied to observed behavior to determine with a high level of confidence whether that behavior is not legitimate user behavior.

a. Threshold detection: This approach involves defining thresholds, independent of user, for the frequency of occurrence of various events.

b. Profile based: A profile of the activity of each user is developed and used to detect changes in the behavior of individual accounts.

RULE-BASED DETECTION

- Involves an attempt to define a set of rules that can be used to decide that a given behavior is that of an intruder.

a. Anomaly detection: Rules are developed to detect deviation from previous usage patterns.

b. Penetration identification: An expert system approach that searches for suspicious behavior.

- In a nutshell, statistical approaches attempt to define normal, or expected, behavior, whereas rule-based approaches attempt to define proper behavior.
- In terms of the types of attackers listed earlier, statistical anomaly detection is effective against masqueraders, who are unlikely to mimic the behavior patterns of the accounts they appropriate. On the other hand, such techniques may be unable to deal with misfeasors. For such attacks, rule-based approaches may be able to recognize events and sequences that, in context, reveal penetration. In practice, a system may exhibit a combination of both approaches to be effective against a broad range of attacks.