1. Overview of Computer Security

Roadmap

Computer Security Concepts

- Threats, Attacks, and Assets
- Malicious Software Overview
- Viruses, Worms, and Bots
- Rootkits

Security definition

- The NIST Computer Security Handbook defines ***computer security*** as:

  – The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources

Computer Security Triad

- THREE key objectives are at the heart of computer security
  - Confidentiality
  - Integrity
  - Availability

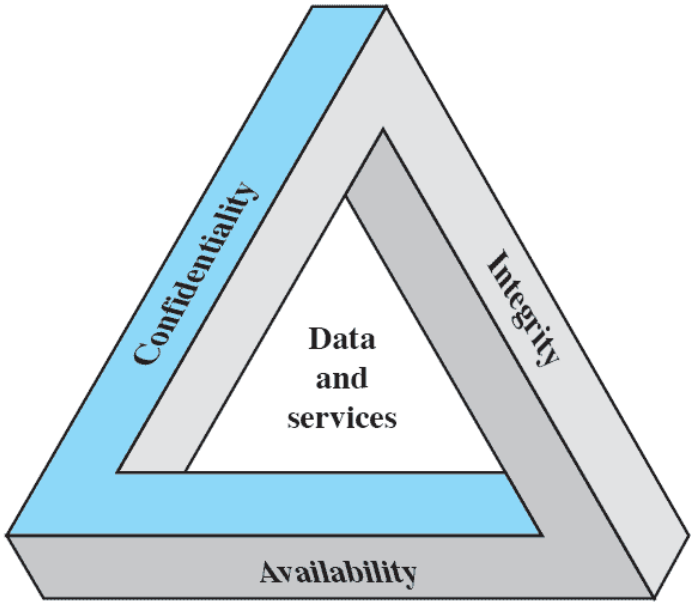


Figure 14.1 The Security Requirements Triad

Additional Concepts

- Two further concepts are often added to the core of computer security
  - Authenticity (genuine; able to be verified and trusted; confidence in the validity of a transmission, message or message originator)
  - Accountability / Non-repudiation (actions of an entity can be traced uniquely to that entity)

Roadmap

- Computer Security Concepts
- Threats, Attacks, and Assets
- Intruders
- Malicious Software Overview
- Viruses, Worms, and Bots
- Rootkits

Threats

- ISO 27005 defines threat as:
  - *A potential cause of an incident, that may result in harm of systems and organization*

Threats

- RFC 2828, describes FOUR kinds of **threat consequences**
  - ***Unauthorised Disclosure***
    - Entity gains access to data for which the entity is not authorised
  - ***Deception***
    - An event that may result in an authorised entity receiving false data and believing it to be true.
  - ***Disruption***
    - An event that interrupts or prevents the correct operation of system of system services and functions.
  - ***Usurpation***
    - An event that results in control of system services or functions by an unauthorised entity

Attacks resulting in Unauthorised Disclosure

- Unauthorised Disclosure is a threat to **confidentiality**.
- Attacks include:
  - ***Exposure*** (deliberate or through error)
    - Release of sensitive information such as credit card number, to an outsider.
  - ***Interception***
    - On the Internet, a hacker can gain access to email traffic or other data transfers.
  - ***Inference***
    - An adversary is able to gain information from observing the pattern of traffic on a network, such as the amount of traffic between particular pairs of hosts on the network.
  - ***Intrusion***
    - An adversary gaining unauthorized access to sensitive data by overcoming the system's access control protections.

Attacks resulting in Deception

- Deception is a threat to either system **integrity** or data integrity.
- Attacks include:
  - ***Masquerade***
    - An attempt by an unauthorized user to gain access to a system by posing as an authorized user; this could happen if the unauthorized user has learned another user's logon ID and password.
  - ***Falsification***
    - This refers to the altering or replacing of valid data or the introduction of false data into a file or database. For example, a student my alter his or her grades on a school database.
  - ***Repudiation***
    - A user either denies sending data or a user denies receiving or possessing the data.

Attacks resulting in Disruption

- Disruption is a threat to availability or **system integrity.**
- Attacks include:
  - ***Incapacitation***
    - This could occur as a result of physical destruction of or damage to system hardware.
    - Often malicious software, such as Trojan horses, viruses, or worms, could operate in such a way as to disable a system or some of its services.
  - ***Corruption***
    - Malicious software in this context could operate in such a way that system resources or services function in an unintended manner
  - ***Obstruction***
    - to interfere with communications by disabling communication links or altering communication control information.
    - to overload the system by placing excess burden on communication traffic or processing resources.

Attacks resulting in usurpation

- Usurpation is a threat to **system integrity**.
- Attacks include:
  - ***Misappropriation***
    - This can include theft of service.
    - An example is an a distributed denial of service attack, when malicious software is installed on a number of hosts to be used as platforms to launch traffic at a target host.
    - In this case, the malicious software makes unauthorized use of processor and operating system resources.
  - ***Misuse***
    - Misuse can occur either by means of malicious logic or a hacker that has gained unauthorized access to a system.
    - In either case, security functions can be disabled or thwarted.

Assets

- The assets of a computer system can be categorized as
  - hardware,
  - software,
  - data,
  - communication lines and networks.

Assets in Relation to the CIA Triagle

	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.

Roadmap

- Computer Security Concepts
- Threats, Attacks, and Assets
- Intruders
- Malicious Software Overview
- Viruses, Worms, and Bots
- Rootkits

Malware

- General term for any Malicious softWare
  - Software designed to cause **damage**
  - Or **use up the resources** of a target computer.
- Some malware is ***parasitic***
  - Contained within other software
- Some malware is **self-replicating**, others require some other means to ***propogate***.

Backdoor

- **Trapdoor**
  - Secret entry point
    - allows someone who is aware of the backdoor to gain access without going through the usual security access procedures.
  - Useful for programmers debugging
    - But allows unscrupulous programmers to gain unauthorized access.

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
- Common example is cross-site scripting attacks

Multiple-Threat Malware

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

Roadmap

- Computer Security Concepts
- Threats, Attacks, and Assets
- Intruders
- Malicious Software Overview
- Viruses, Worms, and Bots
- Rootkits

Parts of Virus

- Software that “infects” other software by modifying them
- Modification includes
  - An infection mechanism
  - Trigger
  - Payload

Virus Stages

- During its lifetime, a typical virus goes through the following four phases:
  - Dormant phase
  - Propagation phase
  - Triggering phase
  - Execution phase

Virus Structure

- May be prepended, postpended, or embedded in an executable
- When the executable runs, it first executes the virus, then calls the original code of the program

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:

}
```

Figure 14.3 **A Simple Virus**

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

- There is no simple or universally agreed upon classification scheme for viruses,
- It is possible to classify a virus by a number of means including
  - By target
  - By Concealment strategy

by Target

- Boot sector infector
- File infector
- Macro virus

by Concealment Strategy

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

- May make use of MS Word macro's
- If someone opens the attachment it
  - Accesses the local address book and sends copies of itself to contacts
  - May perform local damage

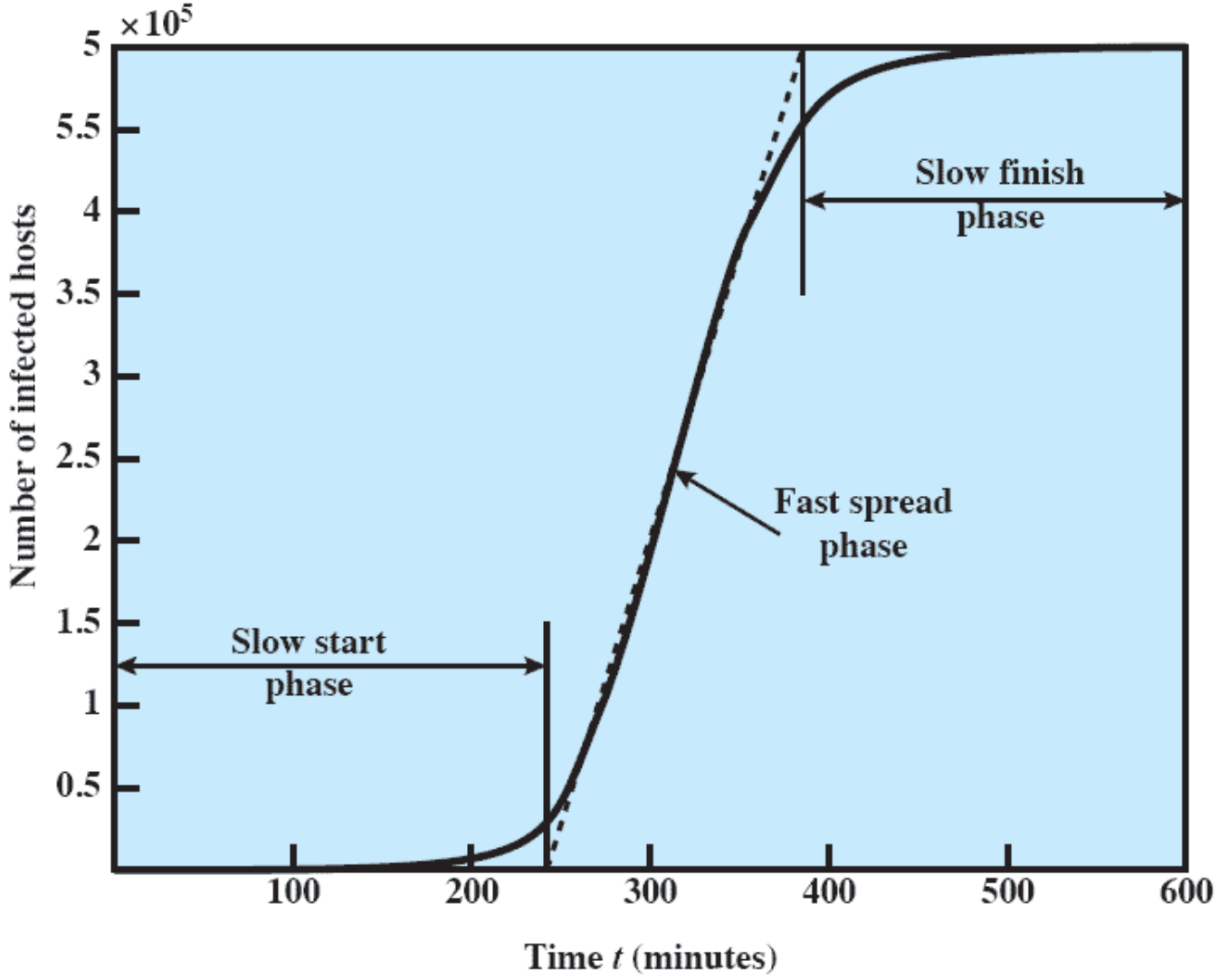
Worms

- Replicates itself
- Use network connections to spread form system to system
- Email virus has elements of being a worm (self replicating)
  - But normally requires some intervention to run, so classed as a virus rather than worm

Worm Propagation

- Electronic mail facility
  - A worm mails a copy of itself to other systems
- 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

- From Robot
  - Also called 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

Roadmap

- Computer Security Concepts
- Threats, Attacks, and Assets
- Intruders
- Malicious Software Overview
- Viruses, Worms, and Bots
- Rootkits

Rootkit

- Set of programs installed on a system to maintain administrator (or root) access to that system
- Hides its existence
- Attacker has complete control of the system.

Rootkit classification

- Rootkits can be classified based on whether they can survive a reboot and execution mode.
  - Persistent
  - Memory based
  - User mode
  - Kernel mode

Rootkit installation

- Often as a trojan
  - Commonly attached to pirated software
- Installed manually after a hacker has gained root access

Revision questions

1. Define computer security.
2. What are the fundamental requirements addressed by computer security?
3. What is the difference between passive and active security threats?
4. List and briefly define THREE classes of intruders.
5. List and briefly define THREE intruder behavior patterns.

Revision questions

6. What is the role of compression in the operation of a virus?
7. What is the role of encryption in the operation of a virus?
8. What are typical phases of operation of a virus or worm?
9. In general terms, how does a worm propagate?
10. What is the difference between a bot and a rootkit?