COURSE TECHNOLOGY
CENGAGE Learning™

Security+ Guide to Network Security Fundamentals

Chapter 1

Introduction to Security

Objectives

- Describe the challenges of securing information
- Define information security and explain why it is important
- Identify the types of attackers that are common today
- List the basic steps of an attack
- Describe the five steps in a defense

Challenges of Securing Information

- There is no simple solution to securing information
- This can be seen through the different types of attacks that users face today

Difficulties in Defending against Attacks

- Difficulties include the following:
  - Speed of attacks
  - Greater sophistication of attacks
  - Simplicity of attack tools
  - Delays in patching hardware and software products
  - Most attacks are now distributed attacks, instead of coming from only one source
  - User confusion

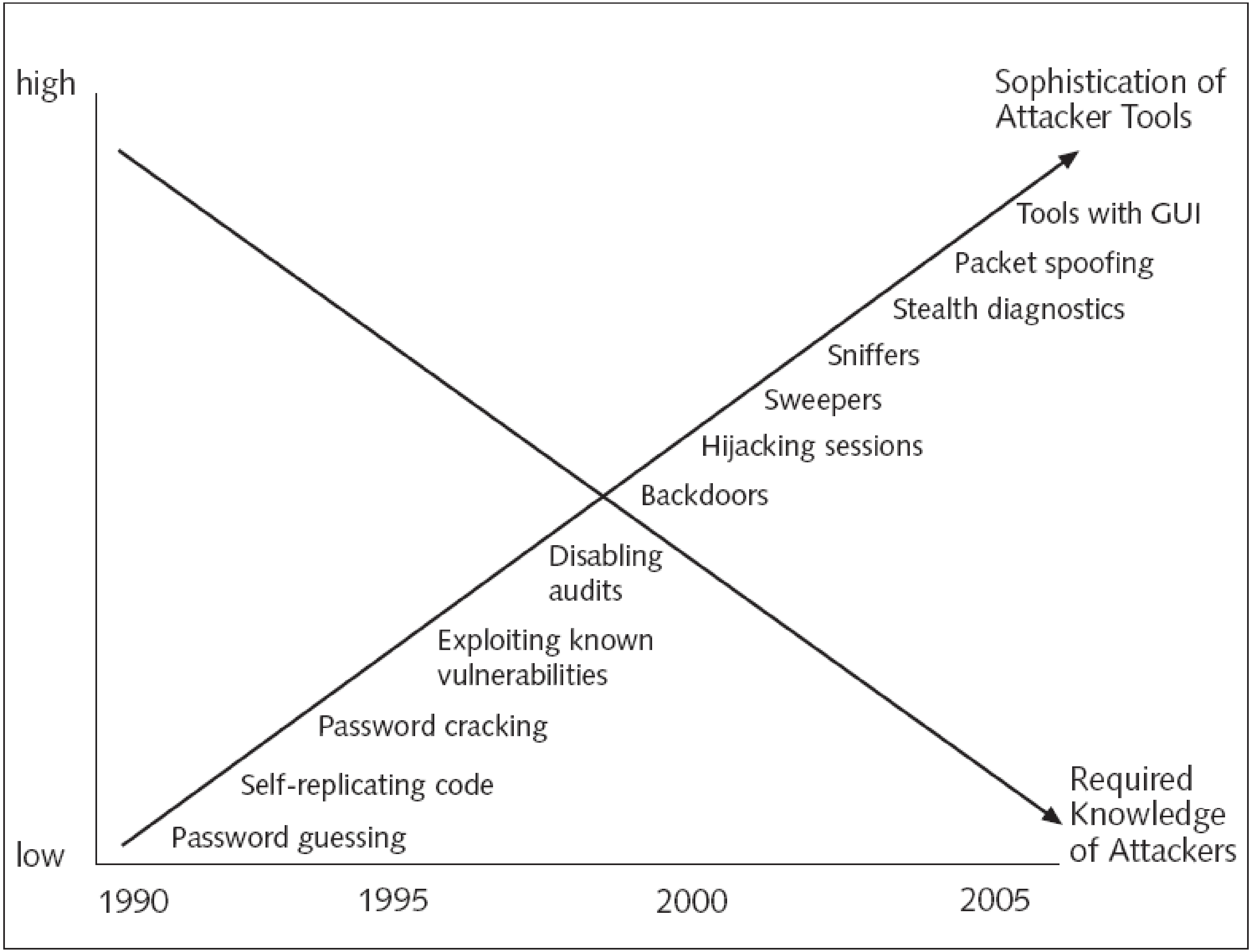


Figure 1-1 Increased sophistication of attack tools

Defining Information Security

- Security can be considered as a state of freedom from a danger or risk
  - This state or condition of freedom exists because protective steps are established and maintained
- **Information security**
  - The tasks of guarding information that is in a digital format
  - Ensures that protective measures are properly implemented
  - Cannot completely prevent attacks or guarantee that a system is totally secure

Defining Information Security (continued)

- Information security is intended to protect information that has value to people and organizations
  - This value comes from the characteristics of the information:
    - **Confidentiality**
    - **Integrity**
    - **Availability**
- Information security is achieved through a combination of three entities

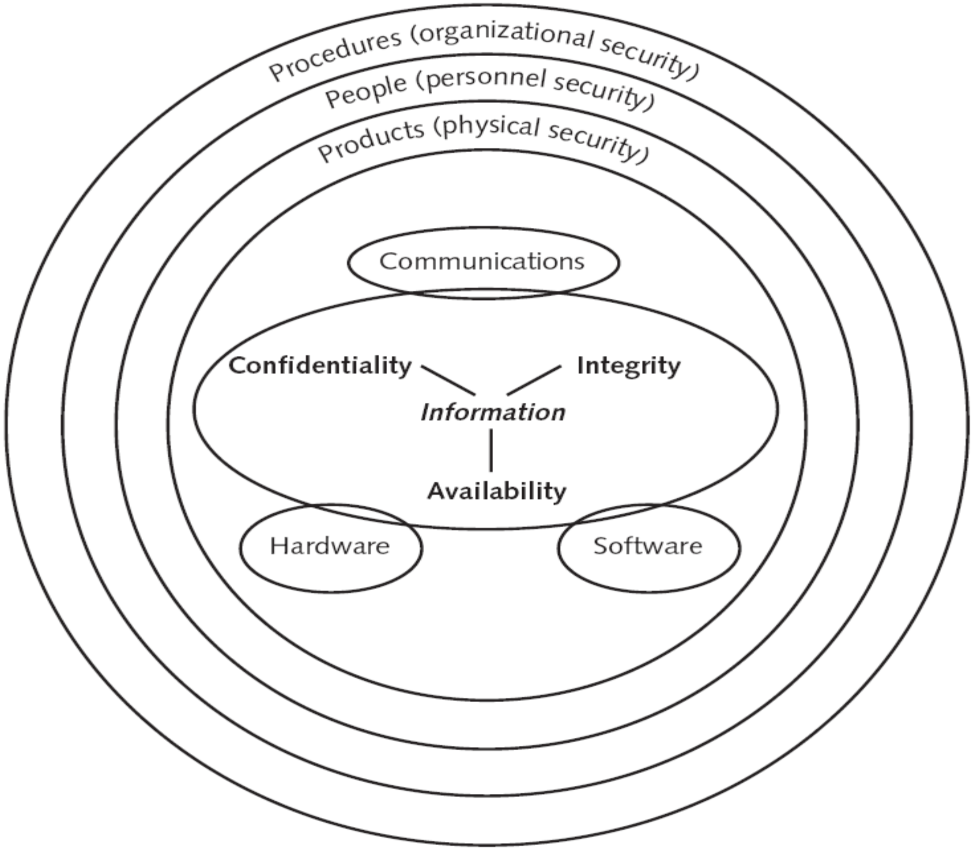
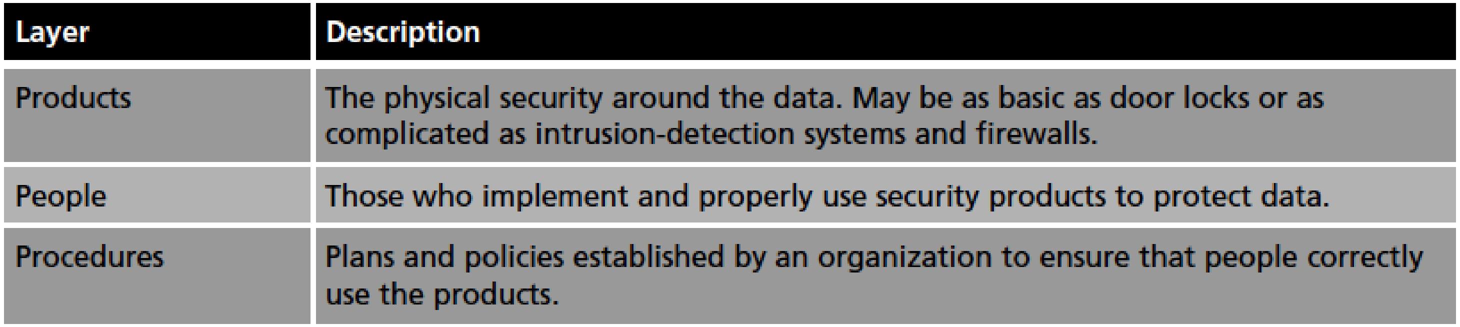

Procedures (organizational security)
People (personnel security)
Products (physical security)
Communications
Confidentiality
Integrity
Information
Availability
Hardware
Software

Figure 1-3 Information security components

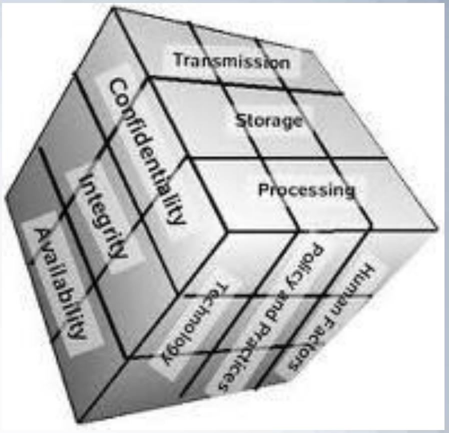


Layer	Description
Products	The physical security around the data. May be as basic as door locks or as complicated as intrusion-detection systems and firewalls.
People	Those who implement and properly use security products to protect data.
Procedures	Plans and policies established by an organization to ensure that people correctly use the products.

Table 1-3 Information security layers

Defining Information Security (continued)

- A more comprehensive definition of information security is:
  - *That which protects the integrity, confidentiality, and availability (CIA) of information on the devices that store, manipulate (process), and transmit the information through products, people, and procedures*



Information Security Terminology

- **Asset**
  - Something that has a value (examples?)
- **Threat**
  - An event or object that may occure negative impact and result in a loss (examples?)
- **Threat agent**
  - A person or thing that has the power to carry out a threat (examples?)

Information Security Terminology (continued)

- **Vulnerability**
  - Weakness that allows a threat agent to bypass security (i.e. configuration errors or software “bugs”)
- **Risk**
  - The probability, that a threat agent will exploit a vulnerability
  - Risk is usually expressed as a percentage (90% chance of a web server being hacked in a year)
  - Realistically, risk cannot ever be entirely eliminated

Information Security Terminology (continued)

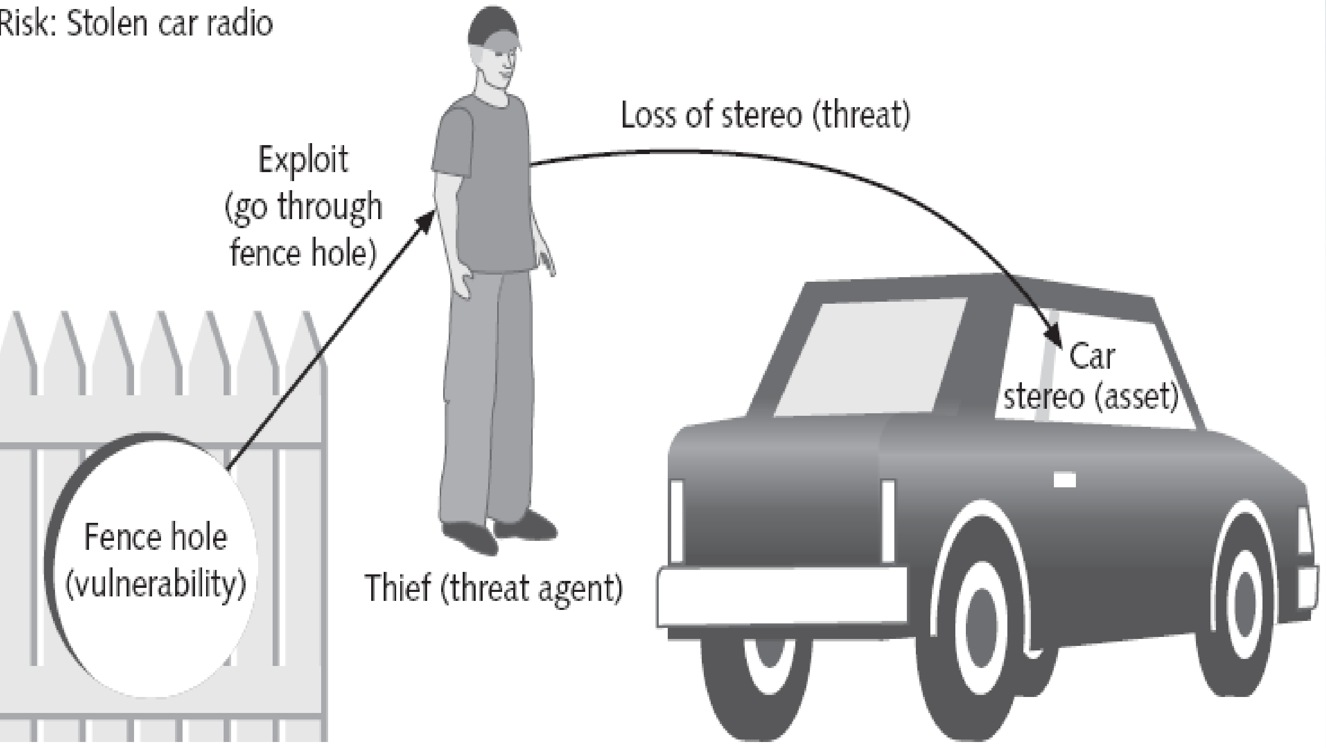
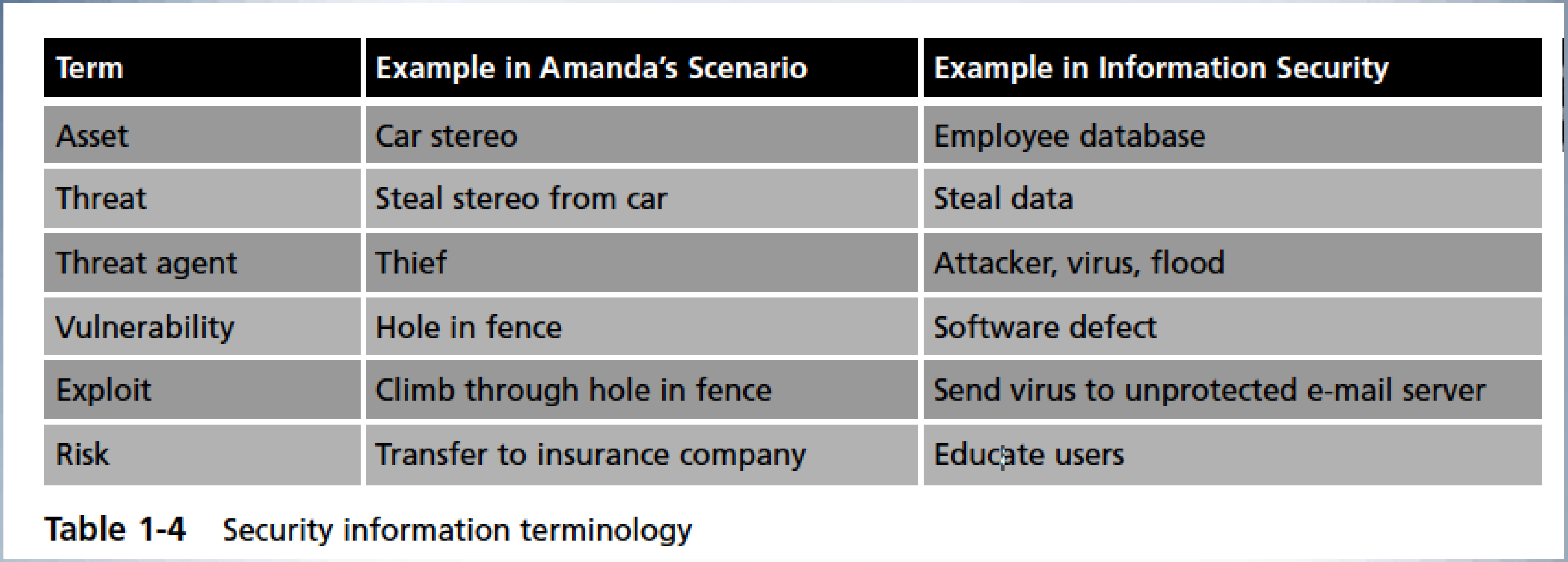


Figure 1-4 Amanda's car stereo

There are three options when dealing/facing with risks:

1. Accept the risk
2. Diminish the risk
3. Transfer the risk

Information Security Terminology (continued)



Term	Example in Amanda's Scenario	Example in Information Security
Asset	Car stereo	Employee database
Threat	Steal stereo from car	Steal data
Threat agent	Thief	Attacker, virus, flood
Vulnerability	Hole in fence	Software defect
Exploit	Climb through hole in fence	Send virus to unprotected e-mail server
Risk	Transfer to insurance company	Educate users

Table 1-4 Security information terminology

Information Security Terminology

Loss of USB Thumb Drive

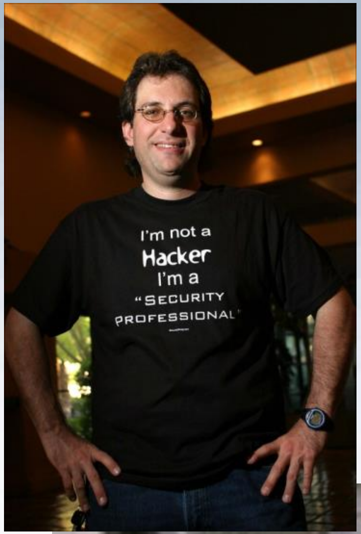
Asset	Threat	Threat Agent	Vulnerability	Impact	Mitigation
Customer Data	Loss or theft of data	Employee or thief	Data is in plain text on the drives.	loss of customer confidence (loss of sales)	Enable encryption on all drives (including USB drives)

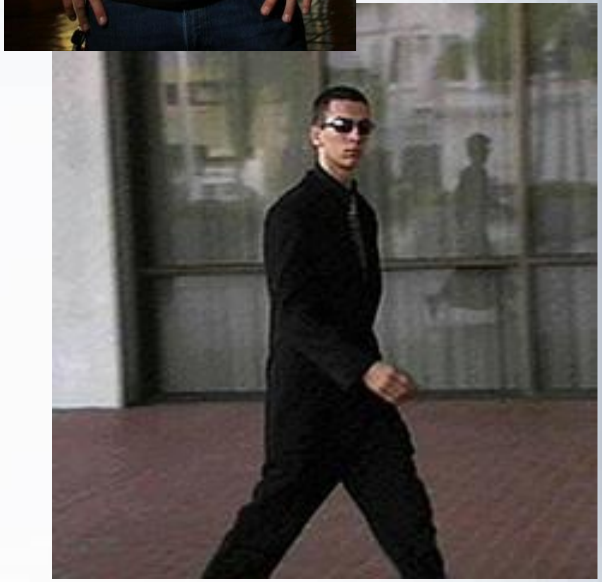
Who Are the Attackers?

- The types of people behind computer attacks are generally divided into several categories
  - These include hackers, script kiddies, spies, employees, and cyberterrorists

Hackers

- **Hacker**
  - Generic sense: anyone who illegally breaks into or attempts to break into a computer system
  - Narrow sense: a person who uses advanced computer skills to attack computers only to expose security flaws
- Although breaking into another person's computer system is illegal
  - Some hackers believe it is ethical as long as they do not commit theft, vandalism.
  - Q: What is the difference between a "Cracker" and a "Hacker"





Script Kiddies

- **Script kiddies**
  - Want to break into computers to create damage
  - Unskilled users
  - Download automated hacking software (scripts) from Web sites and use it to break into computers
- They are sometimes considered more dangerous than hackers
  - Script kiddies have almost unlimited amounts of leisure time, which they can use to attack systems

Spies

- Computer **spy**
  - A person who has been hired to break into a computer and steal information
- Spies are hired to attack a specific computer or system that contains sensitive information
  - Their goal is to break into that computer or system and take the information without drawing any attention to their actions
- Spies, like hackers, possess excellent computer skills

Employees

- One of the largest information security threats to a business actually comes from its employees
- Reasons
  - An employee might want to show the company a weakness in their security
  - Disgruntled employees may be intent on retaliating against the company
  - Blackmailing

Cyberterrorists

- **Cyberterrorists**
  - Their motivation may be defined as ideology, or attacking for the sake of their principles or beliefs
- Goals of a cyberattack:
  - To spread misinformation
  - To deny service to legitimate computer users

Attacks and Defenses

- Although there are a wide variety of attacks that can be launched against a computer or network
  - The same basic steps are used in most attacks
- these steps in an attack calls for five fundamental security principles

Steps of an Attack

- The five steps that make up an attack
  - Probe/identify for information
  - Penetrate any defenses
  - Modify security settings
  - Circulate to other systems
  - Paralyze networks and devices

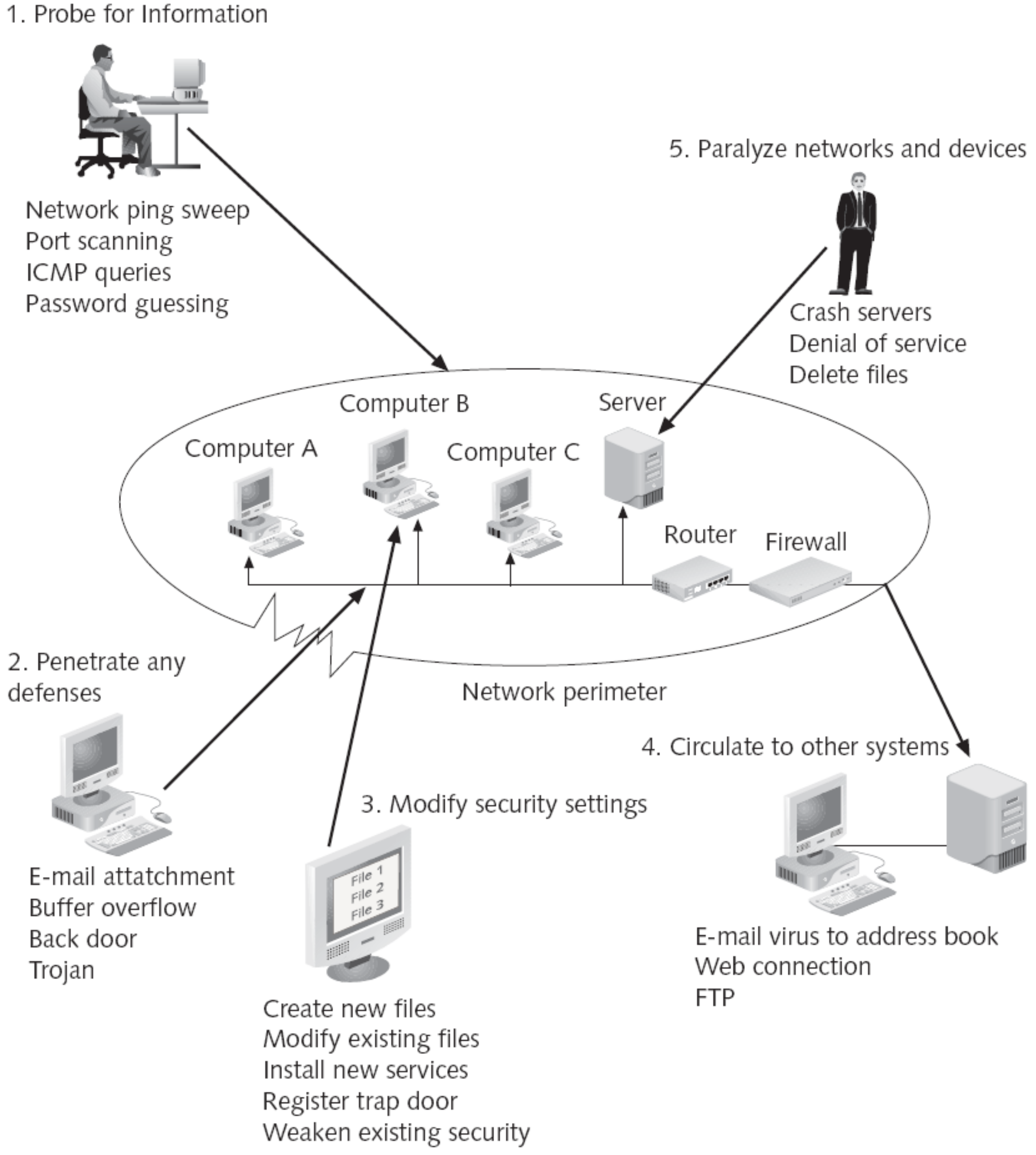


Figure 1-5 Steps of an attack

Defenses against Attacks

- Multiple defenses may be necessary to protect an attack
  - These defenses should be based on five fundamental security principles:
  - Protecting systems by
    - Layering
    - Limiting
    - Diversity
    - Obscurity
    - Simplicity

Layering

- Information security must be created in layers
- One defense mechanism may be relatively easy for an attacker to break system
  - a security system must have layers, impossible that an attacker has the tools and skills to break through *all* the layers of defenses
- A layered approach can also be useful in protect a variety of attacks

Limiting

- Limiting access to information reduces the threat against it
- Only those who must use data should have access to it
  - In addition, the amount of access granted to someone should be limited to what that person needs to know
- Some ways to limit access are technology-based, while others are procedural

Diversity

- Layers must be different (diverse)
  - If attackers penetrate one layer, they cannot use the same techniques to break through all other layers
- Using diverse layers of defense means that breaching one security layer does not compromise the whole system

Obscurity

- An example of obscurity would be not revealing the type of computer, operating system, software, and network connection a computer uses
  - An attacker who knows that information can more easily determine the weaknesses of the system to attack it
- Obscuring information can be an important way to protect information

Simplicity

- Complex security systems can be hard to understand, troubleshoot, and maintain
- As much as possible, a secure system should be simple, so easy to understand and use
- Keeping a system simple from the inside but complex on the outside can sometimes be difficult but gain a major benefit

Summary

- Attacks against information security have grown exponentially in recent years
- There are several reasons why it is difficult to defend against today's attacks
- The main goals of information security are to prevent data theft, thwart identity theft, maintain productivity, and foil cyberterrorism
- The types of people behind computer attacks are generally divided into several categories
- There are five general steps that make up an attack.