MIS

CHAPTER 5

PROTECTING INFORMATION RESOURCES

Hossein BIDGOLI

Biometrics

Identity theft

Mary Stewart

Computer and Network Security: Basic Safeguards

- Critical for most organizations
  - Especially in recent years, with “hackers” becoming more numerous and adept at stealing and altering private information
  - 1. Comprehensive security system
  - 2. Threats:

Computer and Network Security: Basic Safeguards

- Comprehensive security system
  - Includes hardware, software, procedures, and personnel that collectively protect information resources
- **A. Confidentiality**
  - System must not allow disclosing information to anyone who isn't authorized to access it
- **B. Integrity**
  - Ensures the accuracy of information resources in an organization
- **C. Availability**
  - Ensures that computers and networks are operating

Computer and Network Security: Basic Safeguards

- **Fault-tolerant systems**
  - Combination of hardware and software for improving reliability
  - Uninterruptible power supply (UPS)
  - Redundant array of independent disks (RAID)
  - Mirror disks

Security Threats: An Overview

- Some threats can be controlled completely or partially, but some can't be controlled
- Categories
  - Unintentional
  - Intentional

Intentional Threats

- Viruses
- Worms
- Trojan programs
- Logic bombs
- Backdoors
- Blended threats (e.g., worm launched by Trojan)
- Rootkits
- Denial-of-service attacks
- Social engineering

Viruses

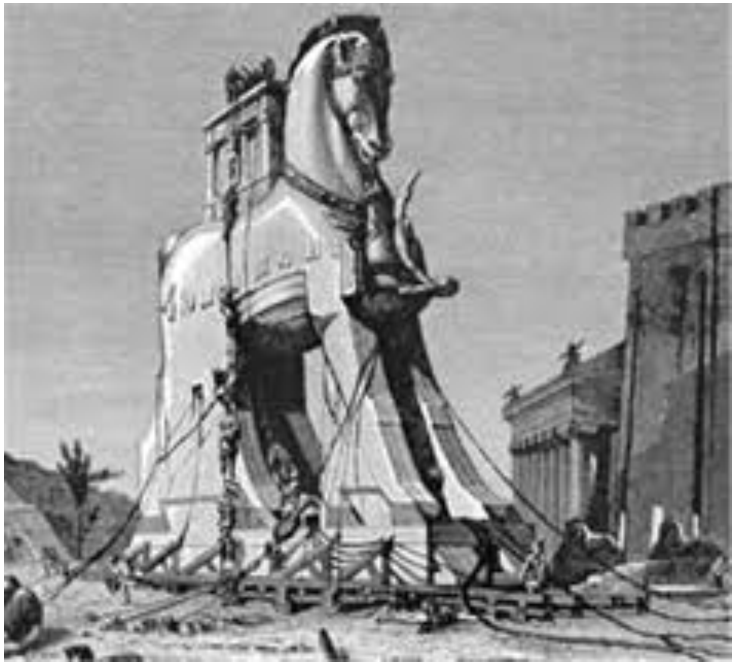
- Type of malware
- In 2008, the # of computer viruses in existence exceeded one million
- Consists of self-propagating program code that's triggered by a specified time or event
- Seriousness of viruses varies
- Transmitted through a network & e-mail attachments
- Indications of a computer infected by a virus
- Best measure against viruses
  - Installing and updating antivirus programs

Worms

- Travels from computer to computer in a network
    - Does not usually erase data
- Independent programs that can spread themselves without having to be attached to a host program
- Replicates into a full-blown version that eats up computing resources
- Well-known worms
    - Code Red, Melissa, and Sasser

Trojan Programs

- Named after the Trojan horse the Greeks used to enter Troy during the Trojan Wars
- Contains code intended to disrupt a computer, network, or Web site
- Usually hidden inside a popular program



Logic Bombs

- Type of Trojan program used to release a virus, worm, or other destructive code
- Triggered at a certain time or by an event

Backdoors

- Programming routine built into a system by its designer or programmer
- Enables the designer or programmer to bypass system security and sneak back into the system later to access programs or files
- System users aren’t aware a backdoor has been activated

Denial-of-Service Attacks

- Floods a network or server with service requests
  - Prevent legitimate users' access to the system
- Target Internet servers
- Distributed denial-of-service (DDoS) attack
  - Hundreds or thousands of computers work together to bombard a Web site with thousands of requests for information in a short period
  - Difficult to trace

Social Engineering

- Using “people skills” to trick others into revealing private information
  - Takes advantage of the human element of security systems
- Commonly used social-engineering techniques
  - “Dumpster diving” and “shoulder surfing”

Security Measures and Enforcement: An Overview

- Biometric security measures
- Nonbiometric security measures
- Physical security measures
- Access controls
- Virtual private networks
- Data encryption
- E-commerce transaction security measures
- Computer Emergency Response Team

Biometric Security Measures

- Use a physiological element to enhance security measures
- Devices and measures
  - Facial recognition
  - Fingerprints
  - Hand geometry
  - Iris analysis
  - Palmprints
  - Retinal scanning
  - Signature analysis
  - Vein analysis
  - Voice recognition

Firewalls – Nonbiometric Security Measures

- Combination of hardware and software
- Acts as a filter or barrier between a private network and external computers or networks
- Network administrator defines rules for access
- Examine data passing into or out of a private network

Firewall Capability

Firewall can

- Focus for security decisions
- Enforce security policy
- Log internet activity
- Limit exposure
  - keeps one section of intranet separate from another

Firewall can not

- Protect against malicious insiders
- Protect against connections that do not go through it
- Protect against new threats
- Protect against viruses

Intrusion Detection Systems–

Nonbiometric Security Measures

- Protect against both external and internal access
- Placed in front of a firewall
- Prevent against DoS attacks
- Monitor network traffic
- “Prevent, detect, and react” approach
- Require a lot of processing power and can affect network performance

Physical Security Measures

- Primarily control access to computers and networks
- Include
  - Cable shielding
  - Corner bolts
  - Electronic trackers
  - Identification (ID) badges
  - Proximity-release door openers
  - Room shielding
  - Steel encasements

Lost and Stolen Laptops

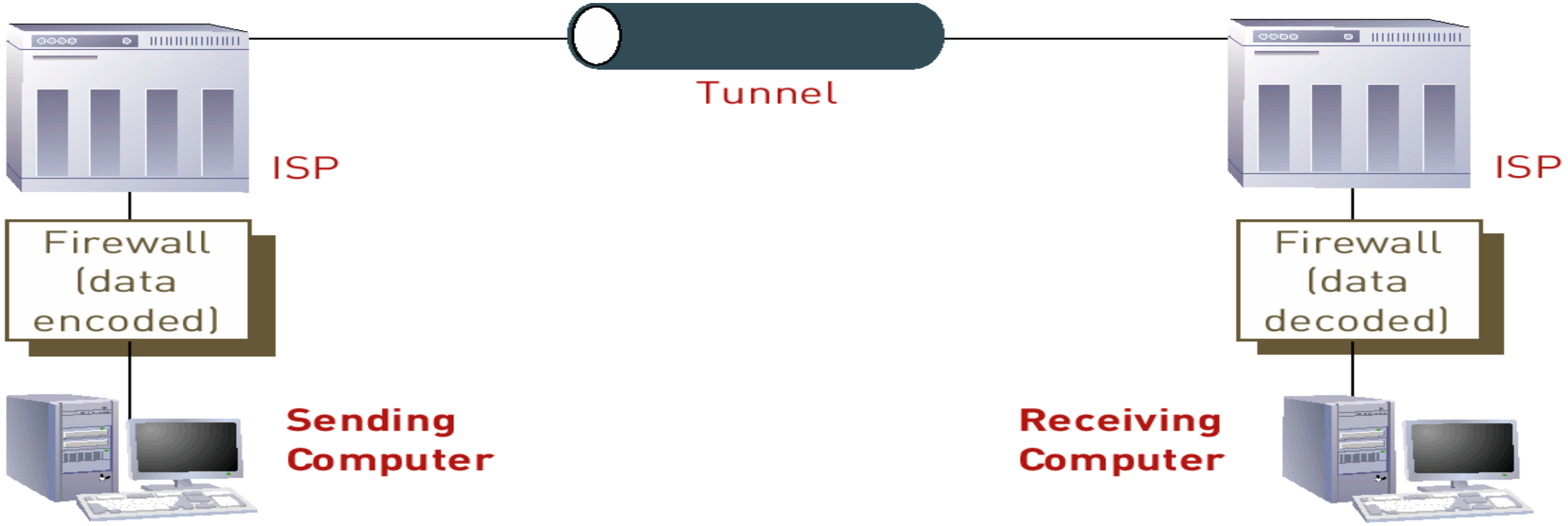
- Recommendations:
  - Install cable locks and use biometric measures
  - Only store confidential data when necessary
  - Use passwords
  - Encrypt data
  - Install security chips

Access Controls

- Terminal resource security
  - Software feature that erases the screen and signs the user off automatically after a specified length of inactivity
- Password
  - Combination of numbers, characters, and symbols that’s entered to allow access to a system
  - Length and complexity determines its vulnerability to discovery
  - Guidelines for strong passwords

Virtual private network

- **Virtual private network (VPN):** a secure connection between two points across the Internet



Tunneling: the process by which VPNs transfer information by encapsulating traffic in IP packets over the Internet

Mary Queen of Scots

All because of weak encryption.

On 8 February, 1587 Elizabeth I of England signed Mary's death warrant, and she was executed at Fotheringay Castle. The execution did not go well for Mary as the executioner was unable to sever her neck with one blow, and was forced to use a grinding motion on her to complete the task.

Mary Stewart

How Encryption Works

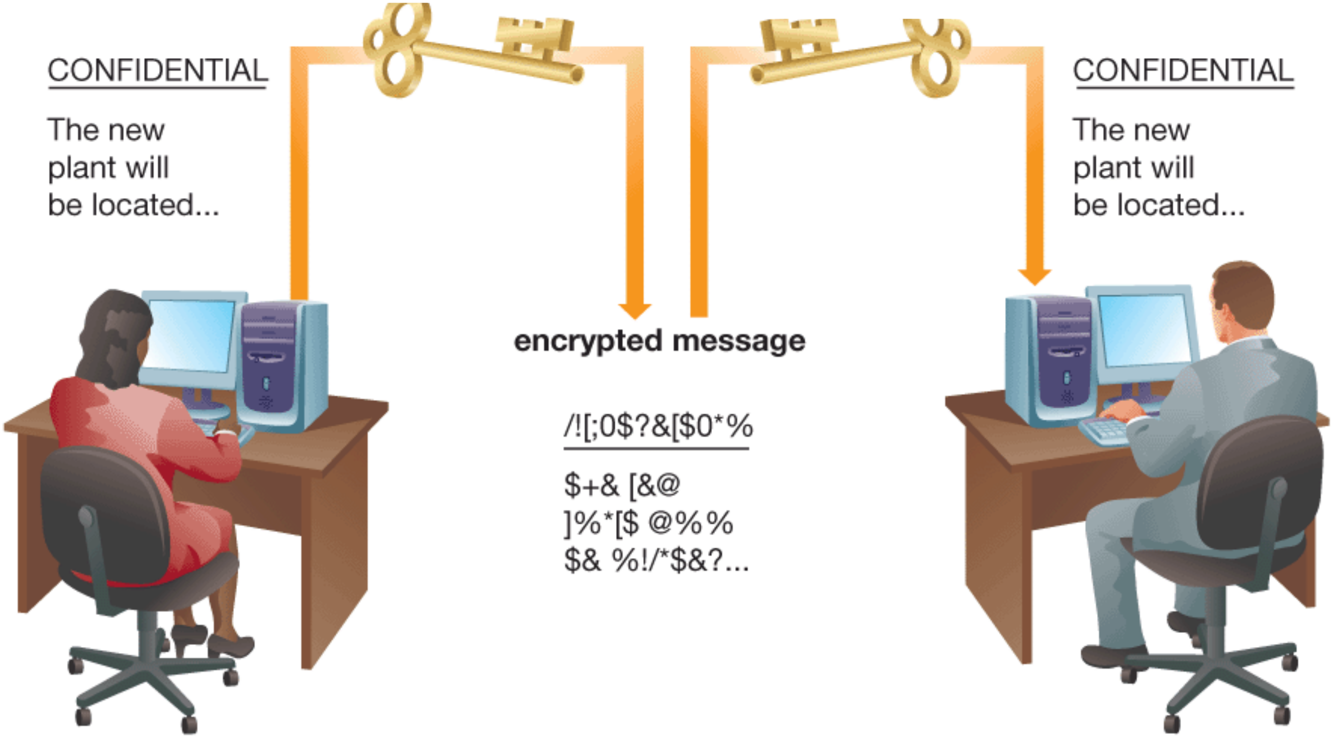


Figure 4.15 How keys are used to encrypt and decrypt information.

Guidelines for Comprehensive Security System

- Train employees
- Guidelines and steps involved:
  - People
  - Procedures
  - Equipment and technology

Business Continuity Planning

- Outlines procedures for keeping an organization operational
- Prepare for disaster
- Plan steps for resuming normal operations as soon as possible

Summary

- Types of threat
- Basic safeguards
  - Biometric
  - Nonbiometric
- Fault-tolerance
- Establish comprehensive security system and business continuity plan