COURSE TECHNOLOGY
CENGAGE Learning™

Security+ Guide to Network Security Fundamentals, Third Edition

Chapter 7

Access Control Fundamentals

Objectives

- Define access control and list the four access control models
- Describe logical access control methods
- Explain the different types of physical access control

What Is Access Control?

- **Access control**
  - The process by which resources or services are granted or denied on a computer system or network
- There are four standard access control models as well as specific practices used to enforce access control

Access Control Terminology

- **Identification**
  - A user accessing a computer system would present credentials or identification, such as a username
- **Authentication**
  - Checking the user's credentials to be sure that they are authentic and not fabricated
- **Authorization**
  - Granting permission to take the action
- A computer user is granted **access**
  - To only certain services or applications in order to perform their duties

Access Control Terminology (continued)

Action	Description	Scenario Example	Computer Process
Identification	Review of credentials	Delivery person shows employee badge	User enters username
Authentication	Validate credentials as genuine	Megan reads badge to determine it is real	User provides password
Authorization	Permission granted for admittance	Megan opens door to allow delivery person in	User authorized to log in
Access	Right given to access specific resources	Delivery person can only retrieve box by door	User allowed to access only specific data

Table 7-1 Basic steps in access control

Access Control Terminology (continued)

- Computer access control can be accomplished by one of three entities: hardware, software, or a policy
- Access control can take different forms depending on the resources that are being protected
- Other terminology is used to describe how computer systems impose access control:
  - **Object**
  - **Subject**
  - **Operation**

Access Control Terminology (continued)

Role	Description	Duties	Example
Owner	Person responsible for the information	Determines the level of security needed for the data and delegates security duties as required	Determines that file SALARY.XLSX can be read only by department managers
Custodian	Individual to whom day-to-day actions have been assigned by the owner	Periodically reviews security settings and maintains records of access by end users	Sets and reviews security settings on SALARY.XLSX
End User	User who accesses information in the course of routine job responsibilities	Follows organization's security guidelines and does not attempt to circumvent security	Opens SALARY.XLSX

Table 7-2 Roles in access control

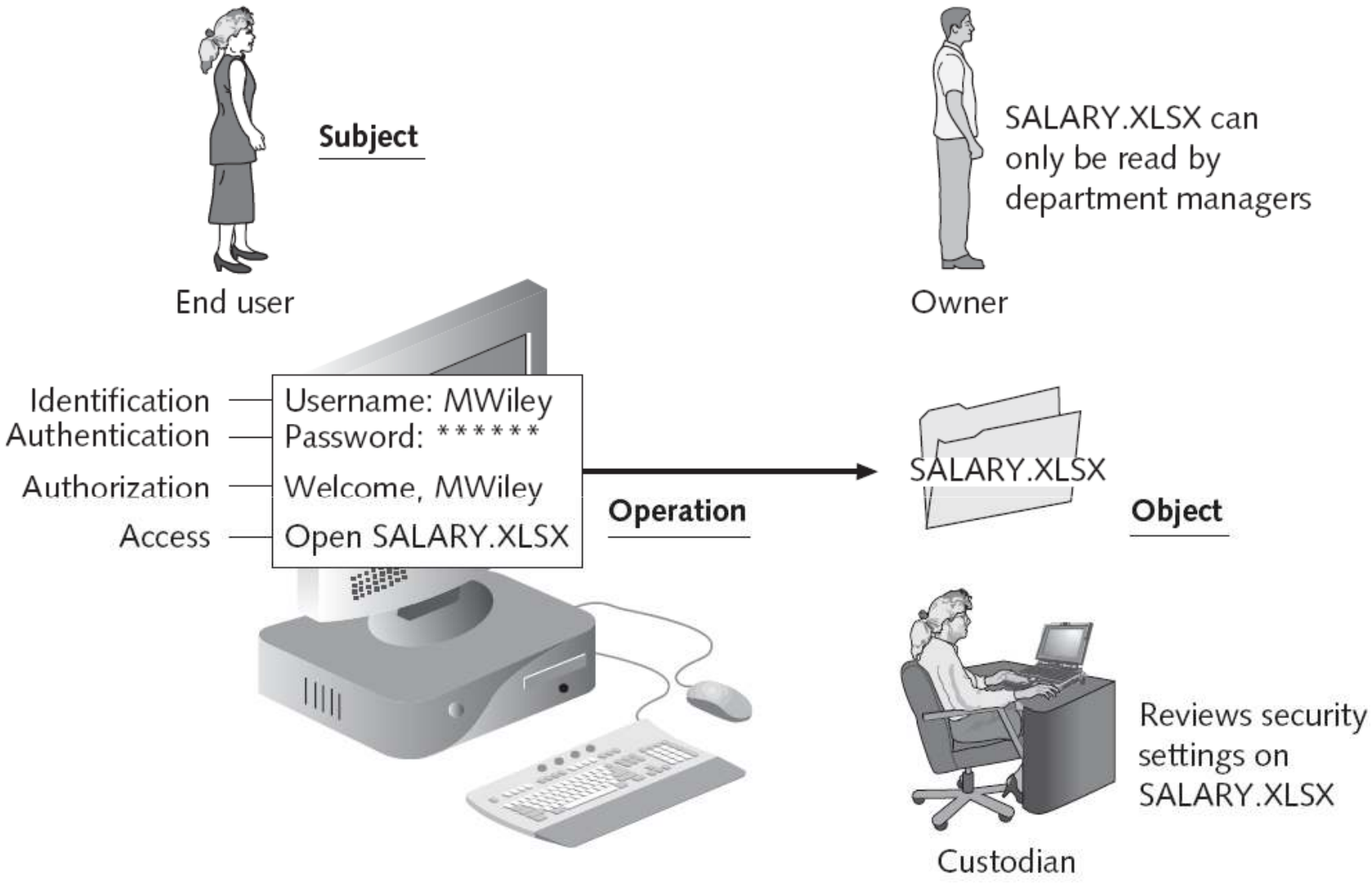

Figure 7-1 Access control process and terminology

Access Control Models

- **Access control model**
  - Provides a predefined framework for hardware and software developers who need to implement access control in their devices or applications
- Once an access control model is applied
  - Custodians can configure security based on the requirements set by the owner
    - So that end users can perform their job functions

Access Control Models (continued)

There are four AC models:

- Mandatory Access Control (MAC) model
- Discretionary Access Control (DAC) model
- Role Based Access Control (RBAC) model
- Rule Based Access Control (RBAC) model

Access Control Models (continued)

- **Mandatory Access Control (MAC)** model
  - The end user cannot implement, modify, or transfer any controls
  - The owner and custodian are responsible for managing access controls
- This is the most restrictive model because all controls are fixed
- In the original MAC model, all objects and subjects were assigned a numeric access level
  - The access level of the subject had to be higher than that of the object in order for access to be granted

Access Control Models (continued)

- **Discretionary Access Control (DAC)** model
  - The least restrictive
  - A subject has total control over any objects that he or she owns
    - Along with the programs that are associated with those objects
- In the DAC model, a subject can also change the permissions for other subjects over objects

Access Control Models (continued)

- **Role Based Access Control (RBAC)** model
  - Sometimes called **Non-Discretionary Access Control**
  - Considered a more “real world” approach than the other models
  - Assigns permissions to particular roles in the organization, and then assigns users to that role
  - Objects are set to be a certain type, to which subjects with that particular role have access

Access Control Models (continued)

- **Rule Based Access Control (RBAC)** model
  - Also called the **Rule-Based Role-Based Access Control (RB-RBAC)** model or **automated provisioning**
  - Can dynamically assign roles to subjects based on a set of rules defined by a custodian
  - Each resource object contains a set of access properties based on the rules
- Rule Based Access Control is often used for managing user access to one or more systems

Access Control Models (continued)

Name	Restrictions	Description
Mandatory Access Control (MAC)	End user cannot set controls	Most restrictive model
Discretionary Access Control (DAC)	Subject has total control over objects	Least restrictive model
Role Based Access Control (RBAC)	Assigns permissions to particular roles in the organization and then users are assigned to roles	Considered a more "real world" approach
Rule Based Access Control (RBAC)	Dynamically assigns roles to subjects based on a set of rules defined by a custodian	Used for managing user access to one or more systems

Table 7-3 Access control models

Practices for Access Control

- **Separation of duties**
  - Requires that if the fraudulent application of a process could potentially result in a breach of security
    - Then the process should be divided between two or more individuals
- **Job rotation**
  - Instead of one person having only responsibility for a function, individuals are periodically moved from one job responsibility to another

Practices for Access Control (continued)

- **Least privilege**
  - Each user should be given only the minimal amount of privileges necessary to perform his or her job function
- **Implicit deny**
  - If a condition is not explicitly met, then it is to be rejected

Logical Access Control Methods

- The methods to implement access control are divided into two broad categories
  - Physical access control and logical access control
- Logical access control includes access control lists (ACLs), group policies, account restrictions, and passwords

Access Control Lists (ACLs)

- **Access control list (ACL)**
  - A set of permissions that is attached to an object
  - Specifies which subjects are allowed to access the object
    - And what operations they can perform on it
- These lists are most often viewed in relation to files maintained by the operating system
- The structure behind ACL tables is a bit complex
- **Access control entry (ACE)**
  - Each entry in the ACL table in the Microsoft Windows, Linux, and Mac OS X operating systems

Access Control Lists (ACLs) (continued)

	File-A	File-B	File-C
User1	Read, write	Read, write	Read
User2	Read		
Administrator	Read, write, execute	Read, write, execute	Read, write, execute

Account Restrictions

- **Time of day restrictions**
  - Limit when a user can log on to a system
  - These restrictions can be set through a Group Policy
  - Can also be set on individual systems
- **Account expiration**
  - The process of setting a user's account to expire
  - Orphaned accounts are user accounts that remain active after an employee has left an organization
    - Can be controlled using account expiration

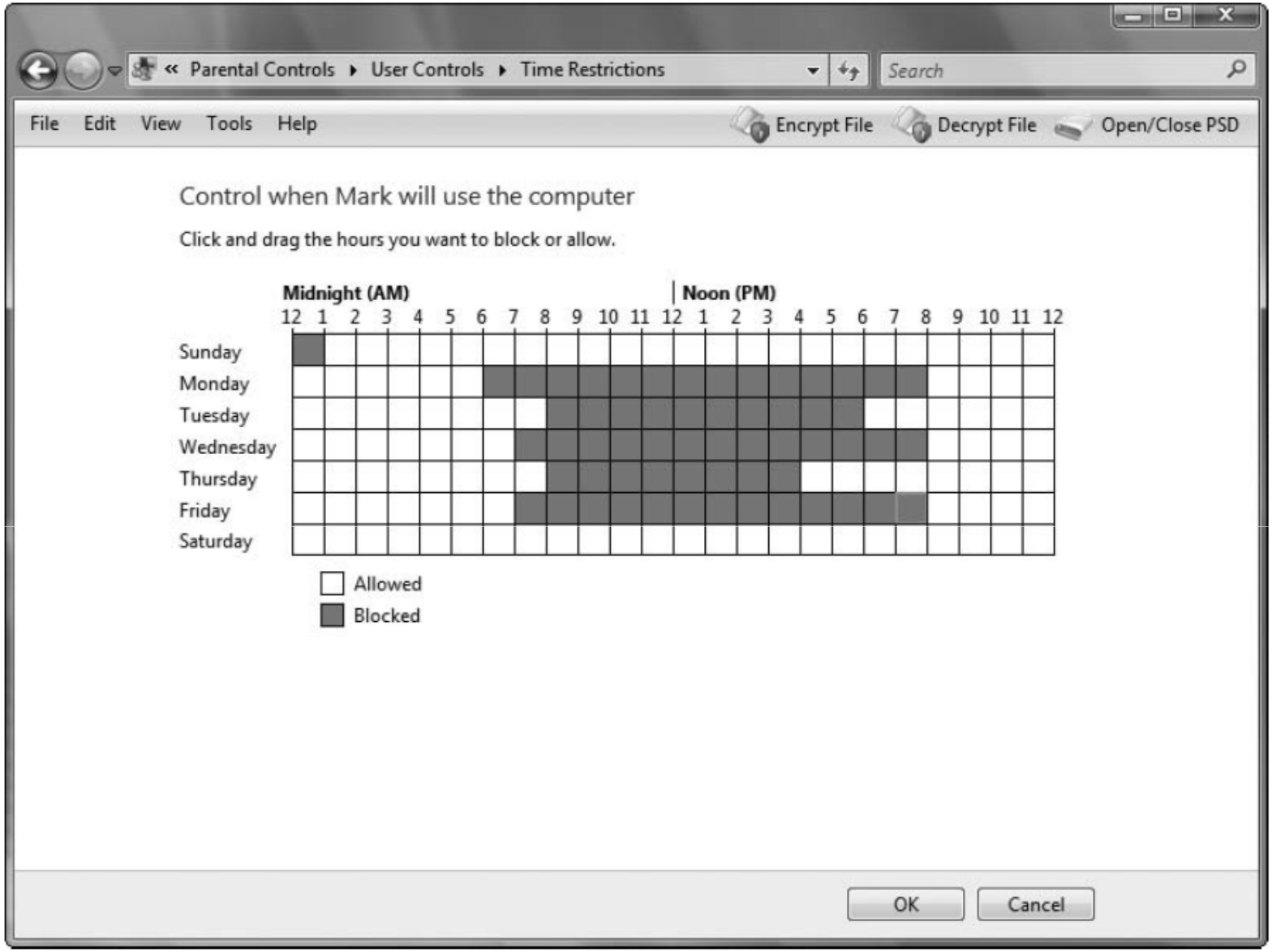

Figure 7-5 Windows Vista Parental Controls

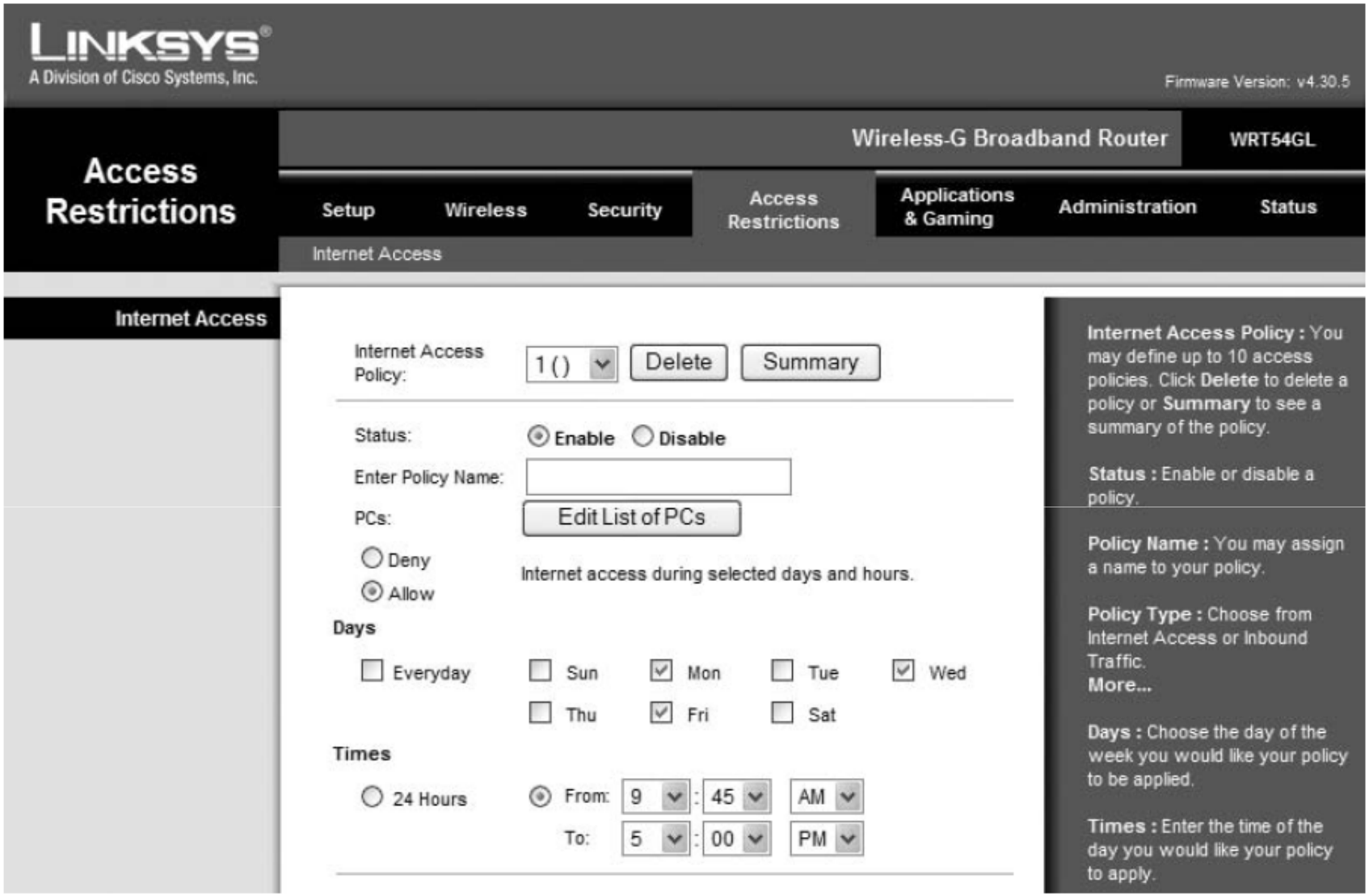

Figure 7-6 Wireless access point restrictions

Passwords

- Password
  - The most common logical access control
  - Sometimes referred to as a logical token
  - A secret combination of letters and numbers that only the user knows

Passwords (continued)

- Passwords are considered weak because:
  - A password should never be written down. Must also be of a sufficient length and complexity so that an attacker cannot easily guess it (password paradox)
  - Users have 20 or more accounts that needs passwords. Because of humans limited memorizing force users to use weak passwords.
  - There are several password myths.

Passwords (continued)

Myth	Explanation
P4T9#6@ is better than *this_is_a_very_long_password.*	Even though the first password is a combination of letters, numbers, and symbols, it is too short and can easily be broken.
The best length for a password is 8 characters.	Because of how systems store passwords, the minimum recommended length is 15 characters.
Replacing letters with numbers, such as *J0hn_ Sm1th,* is good.	Password-cracking programs can look for common words (John) as well as variations using numbers (J0hn).
Passwords cannot include spaces.	Many password programs can accept spaces as well as special characters.

Table 7-4 Common password myths

Passwords (continued)

- **Attacks on passwords:**
  - Brute force attack
  - Dictionary attack
  - Rainbow tables

Passwords (continued)

- Attacks on passwords
  - **Brute force attack**
    - Simply trying to guess a password through combining a random combination of characters.
    - By changing one character at a time, using each newly generated password to access the system
  - Passwords typically are stored in an encrypted form called a “hash”
    - Attackers try to steal the file of hashed passwords and then break the hashed passwords offline

Passwords (continued)

- **Time calculations:**
  - Four digit = 10x10x10x10 = 10,000 (0.01 Second)
  - Four capital letters = 26x26x26x26 = 456,976 (.45 Second)
  - Four capital and small letters = 52x52x52x52 = 7,311,616 (7.3 Seconds)
  - Four digit, capital and small letters= 62x62x62x62 = 14,776,336 (14.7 Seconds)
  - Four digit, special character (10), capital and small letters = 72x72x72x72 = 1,934,917,632 (32 Minutes)
  - Eight digit, special character (10), capital and small letters = 72x72x72x72x72x72x72x72= 722,204,136,308,736 **(23 Years)**

Passwords (continued)

- Attacks on passwords (continued)
  - **Dictionary attack**
    - Begins with the attacker creating hashes of common dictionary words
      - And compares those hashed dictionary words against those in a stolen password file

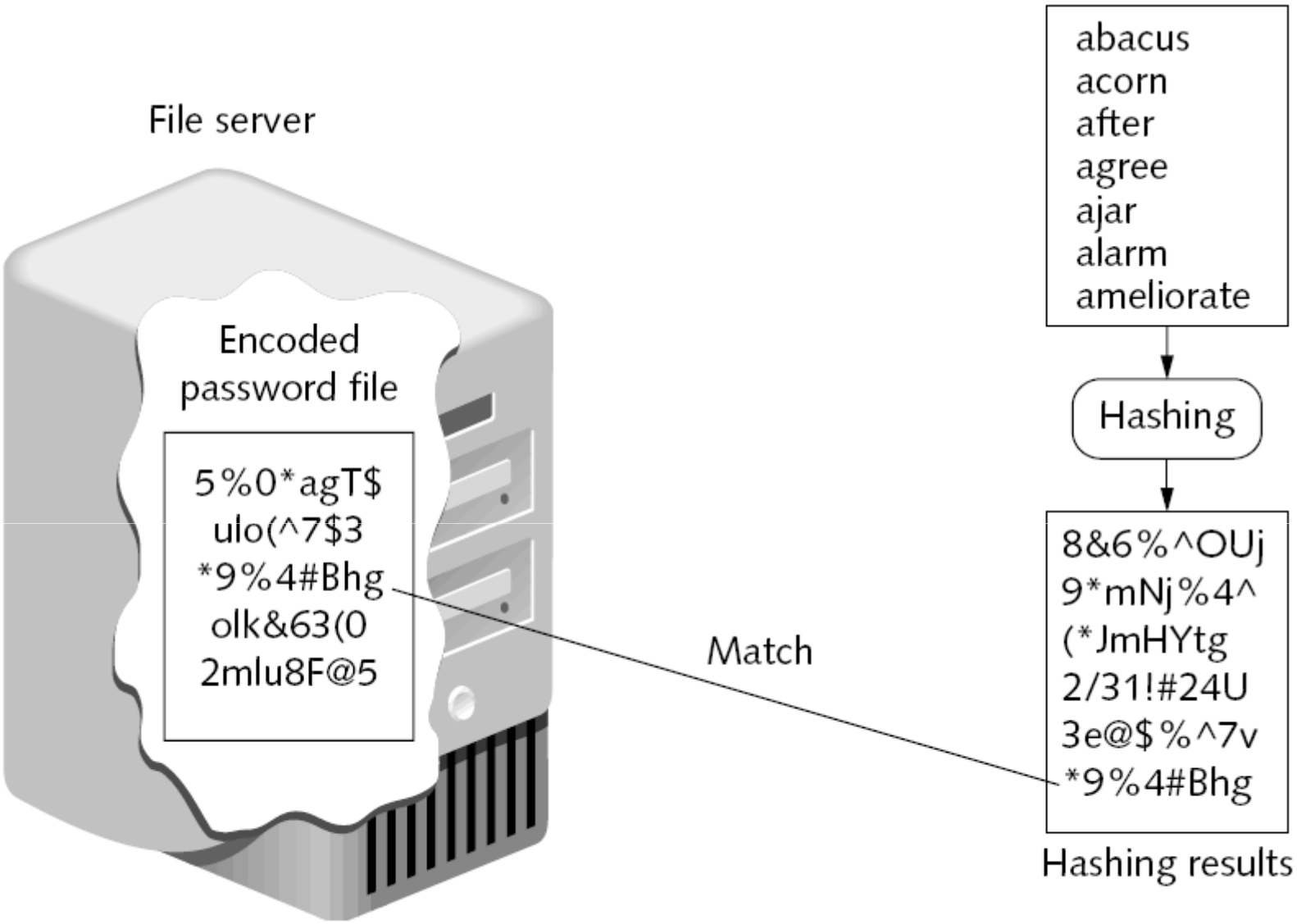

Figure 7-7 Dictionary attack

Passwords (continued)

- Attacks on passwords (continued)
  - **Rainbow tables**
    - Make password attacks easier by creating a large pregenerated data set of hashes from nearly every possible password combination

- Steps for using Rainbow tables:
  - Creating tables.
  - Use the table to crack the password.

Passwords (continued)

- Generating a rainbow table requires a significant amount of time
- Rainbow table advantages
  - Can be used repeatedly for attacks on other passwords
  - Rainbow tables are much faster than dictionary attacks
  - The amount of memory needed on the attacking machine is greatly reduced

Passwords (continued)

- Password policy
  - A strong password policy can provide several defenses against password attacks
  - The first password policy is to create and use strong passwords
- One of the best defenses against rainbow tables is to prevent the attacker from capturing the password hashes
- A final defense is to use another program to help keep track of passwords

Physical Access Control

- Physical access control primarily protects computer equipment
  - Designed to prevent unauthorized users from gaining physical access to equipment in order to use, steal, or vandalize it
- Physical access control includes computer security, door security, mantraps, video surveillance, and physical access logs
- We will only cover door security,

Door Security

- Hardware locks
  - **Preset lock**
    - Also known as the **key-in-knob lock**
    - The easiest to use because it requires only a key for unlocking the door from the outside
    - Automatically locks behind the person, unless it has been set to remain unlocked
    - Security provided by a preset lock is minimal

Door Security (continued)

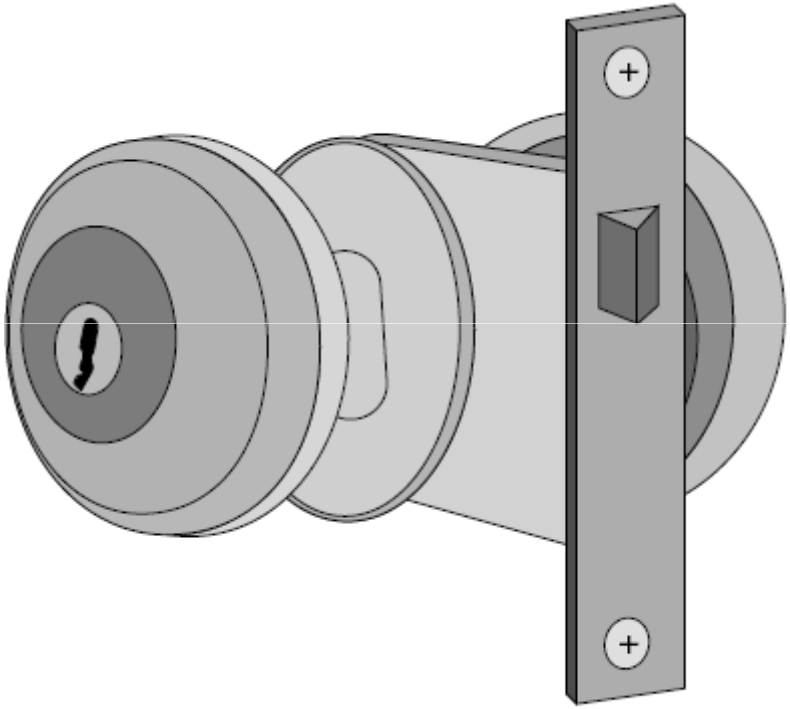

Figure 7-10 Preset lock

Door Security (continued)

- Hardware locks (continued)
  - **Deadbolt lock**
    - Extends a solid metal bar into the door frame for extra security
    - Is much more difficult to defeat than preset locks
    - Requires that the key be used to both open and lock the door

Door Security (continued)

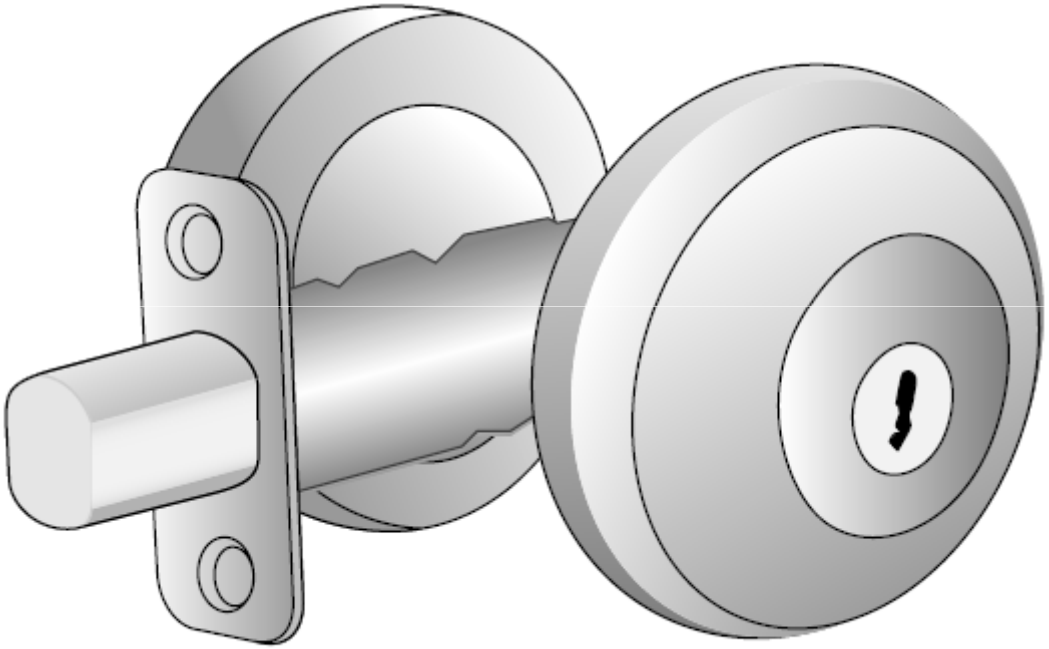

Figure 7-11 Deadbolt lock

Door Security (continued)

- Most organizations observe the following practices:
  - Change locks immediately upon loss or theft of keys
  - Inspect all locks on a regular basis
  - Issue keys only to authorized persons
  - Keep records of who uses and turns in keys
  - Keep track of keys issued, with their number and identification
  - Master keys should not have any marks identifying them as masters

Door Security (continued)

- Most organizations observe the following practices: (continued)
  - Secure unused keys in a locked safe
  - Set up a procedure to monitor the use of all locks and keys and update the procedure as necessary
  - When making duplicates of master keys, mark them “Do Not Duplicate,” and wipe out the manufacturer’s serial numbers to keep duplicates from being ordered

Door Security (continued)

- Door access systems
  - **Cipher lock**
    - Combination locks that use buttons that must be pushed in the proper sequence to open the door
    - Can be programmed to allow only the code of certain individuals to be valid on specific dates and times
  - Cipher locks also keep a record of when the door was opened and by which code
  - Cipher locks are typically connected to a networked computer system
    - Can be monitored and controlled from one central location

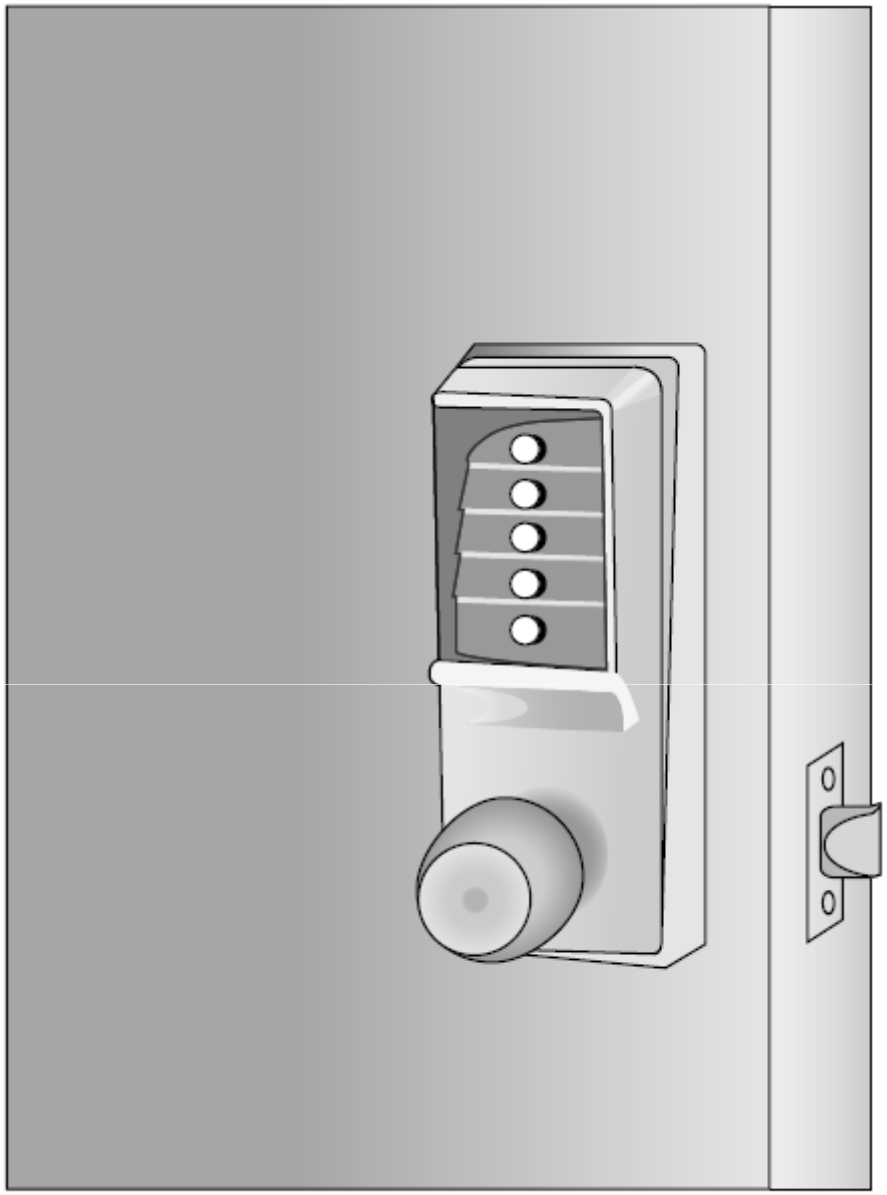

Figure 7-12 Cipher lock

Door Security (continued)

- Door access systems (continued)
  - Cipher lock disadvantages
    - Basic models can cost several hundred dollars while advanced models can be even more expensive
    - Users must be careful to conceal which buttons they push to avoid someone seeing or photographing the combination **(shoulder surfing)**

Door Security (continued)

- Door access systems (continued)
  - **Tailgate sensor**
    - Use multiple infrared beams that are aimed across a doorway and positioned so that as a person walks through the doorway
      - Some beams are activated and then other beams are activated a short time later
    - Can detect if a second person walks through the beam array immediately behind ("tailgates") the first person
      - Without presenting credentials

Door Security (continued)

Door Security (continued)

- Physical tokens
  - Objects to identify users
- **ID badge**
  - The most common types of physical tokens
  - ID badges originally contains a magnetic strip that is swiped or scand to identify users
  - Today, ID badges can be fitted with tiny **radio frequency identification (RFID) tags**
    - Can be read by an RFID transceiver as the user walks through the door with the badge in her pocket

Door Security (continued)

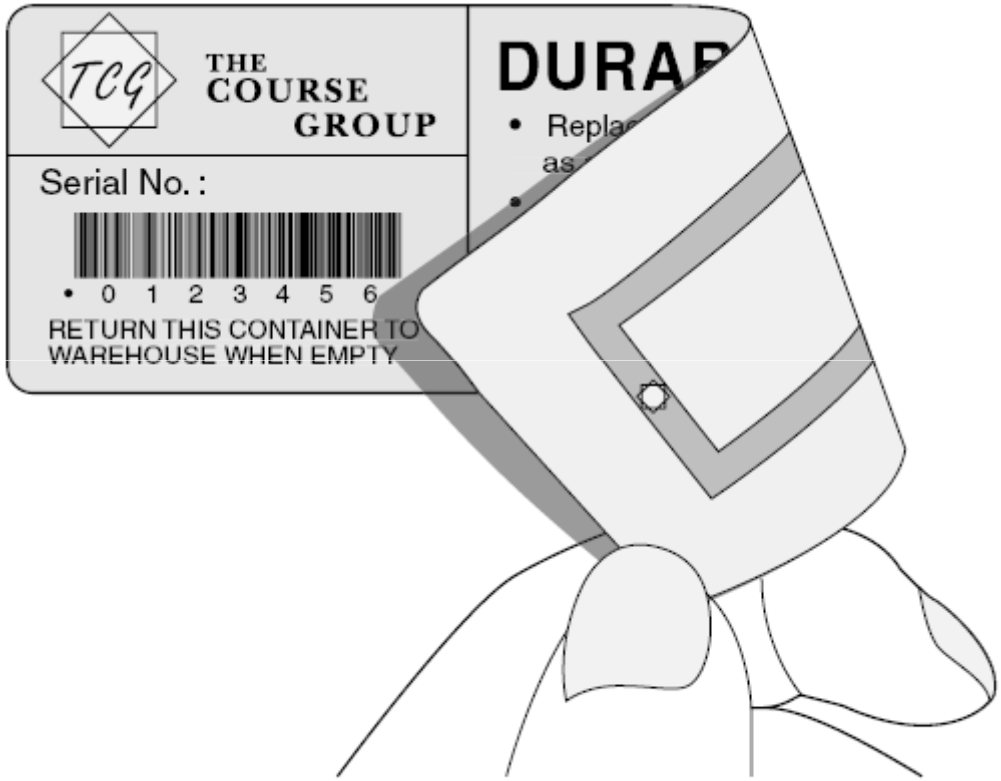

Figure 7-13 RFID tag

Door Security (continued)

- RFID can be:
  - Passive RFID:
    - No power supply.
    - Small in size and send very small data.
    - Small range (19 ft)
  - Active RFID:
    - Has power supply.
    - Larger in size and can store additional data.
    - Larger range (98 ft)

Summary

- Access control is the process by which resources or services are denied or granted
- Best practices for implementing access control include separation of duties, job rotation, using the principle of least privilege, and using implicit deny
- Logical access control methods include using access control lists (ACLs), which are provisions attached to an object
- Passwords, sometimes known as logical tokens, are a secret combination of letters and numbers that only the user should know

Summary (continued)

- Physical access control attempts to limit access to computer equipment by unauthorized users