COURSE TECHNOLOGY
CENGAGE Learning™

Security Awareness

Chapter 2
Personal Security

Objectives

After completing this chapter, you should be able to do the following:

- Define what makes a weak password
- Describe the attacks against passwords
- Identify the different types of social engineering attacks
- Describe identity theft and the risks of using social networking
- Describe personal security defenses

Introduction

- Goal of early attacks on computers
  - Deface or destroy
- Today's attacks
  - Designed to steal information
    - Use information for financial gain
  - Directed at a wide group of users
  - Affect wide variety of devices and operating systems

Passwords

- Types of authentication
  - What you have
  - What you are
  - What you know
- Example: man locks his car and enters health club
  - Key fob (what he has) used to lock car
  - Desk attendant recognizes him and lets him in (what he is)
  - Uses memorized combination to open locker (what he knows)

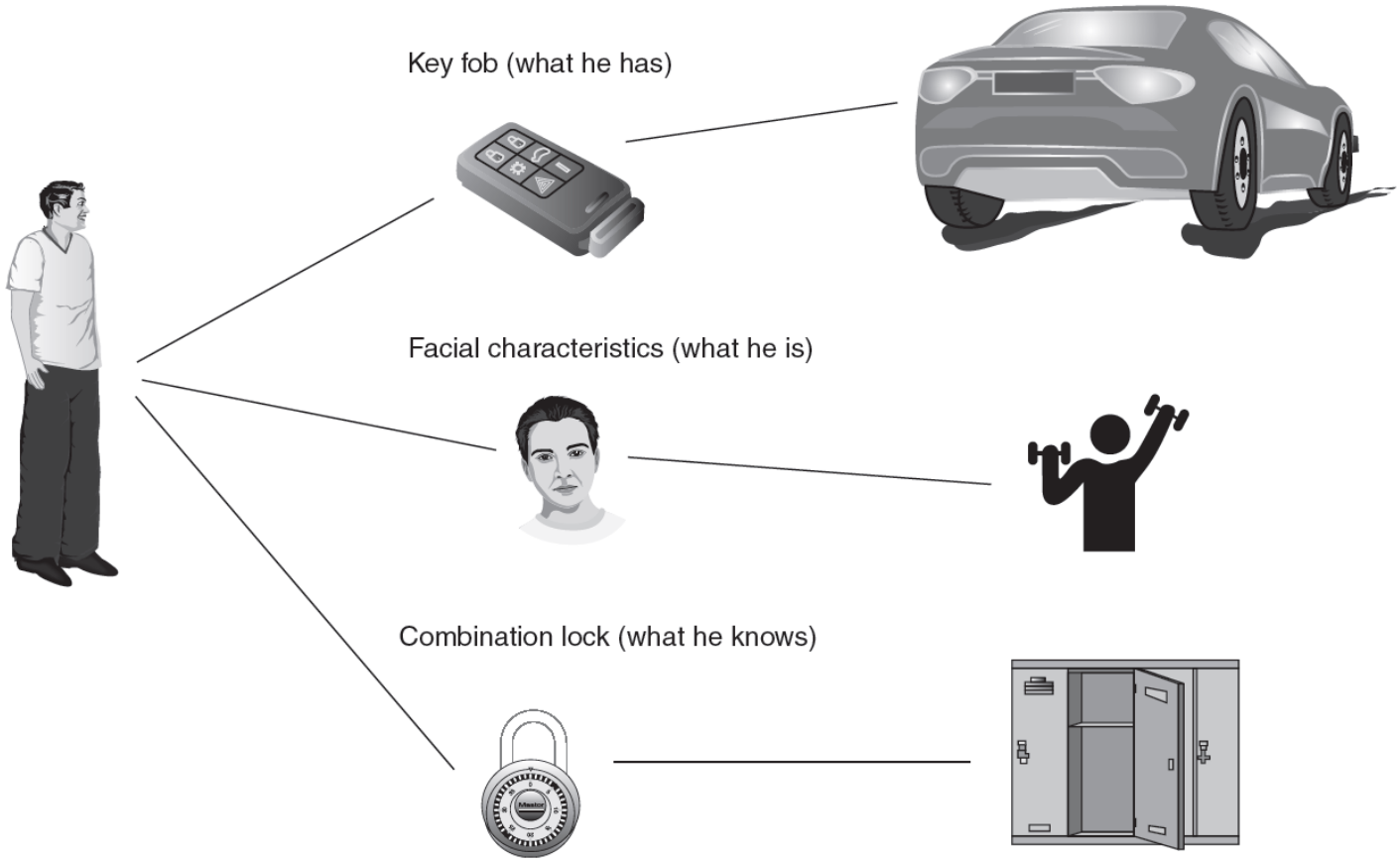

Figure 2-1 Three types of authentication

Passwords (cont'd.)

- Username and password
  - Primary means of authentication on a computer system
- Password
  - Secret combination of letters and numbers
  - Only known to the user
- Password not considered strong defense against attackers
  - Passwords can be weak
  - Passwords subject to different types of attacks

Password Weaknesses

- Human beings can only memorize a limited number of items
- Long, complex passwords are difficult to memorize
- Users must remember multiple passwords for multiple accounts
- Users may take shortcuts that compromise security

Password Weaknesses (cont'd.)

- Characteristics of weak passwords
  - Use a common word
  - Short passwords
  - Using personal information in a password
  - A static password

Rank	Password	Number of Users with Password
1	123456	290,731
2	12345	79,078
3	123456789	76,790
4	Password	61,958
5	iloveyou	51,622
6	princess	35,231
7	rockyou	22,588
8	1234567	21,726
9	12345678	20,553
10	abc123	17,542

Table 2-1 Ten most common passwords

Attacks on Passwords

- Variety of attacks used on passwords
- Technique not used: online guessing
  - Offline cracking more prevalent
- Digest
  - Digital representation of password
  - Stored on computer or Web site
  - Created by a hash algorithm
- Attackers try to steal file of password digest
  - Compare with hashes of known passwords

Attacks on Passwords (cont'd.)

- Primary offline cracking techniques
  - Dictionary attack
  - Brute force attack
- Dictionary attack
  - Attacker creates digests of common dictionary words
  - Compares digests to stolen password file
- Variations of dictionary attack
  - Attacker slightly alters dictionary words
    - Adds numbers as prefix or suffix
    - Substitutes symbols for letters

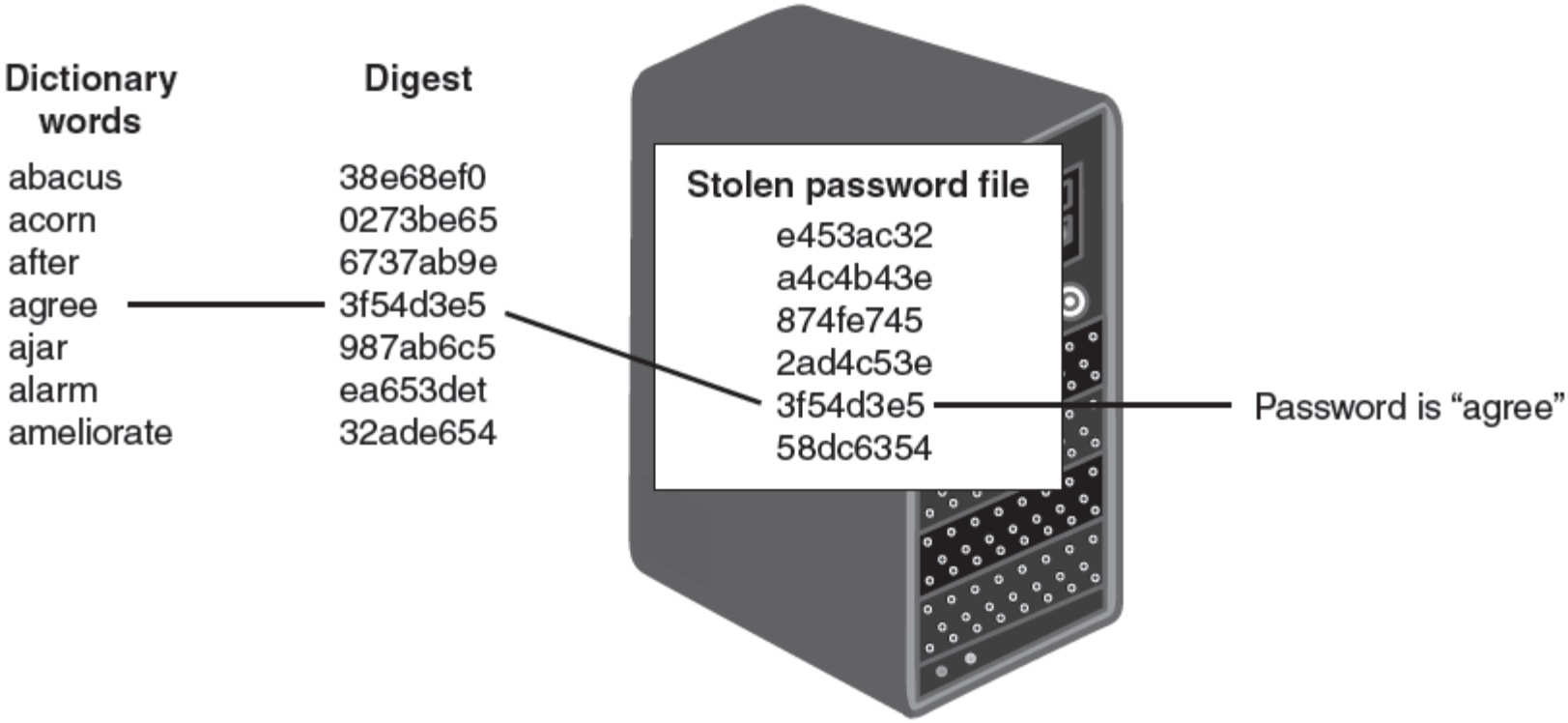

Figure 2-2 Dictionary attack

Attacks on Passwords (cont'd.)

- Brute force attack
  - Every possible combination of letters, numbers, and characters is attempted
  - Slower than dictionary attack
    - More thorough

Social Engineering Attacks

- Example of actual social engineering attack
  - Group of people walk into corporate offices and walk out with sensitive information
  - No technical skills or tools used
  - Group member called company's HR and obtained names of key employees
  - Attacker pretended to have lost key card
    - Employee let group enter building
  - Attacker walked into CFO's office
    - Knew he was absent from voicemail greeting

Social Engineering Attacks (cont'd.)

- Example of social engineering attack (cont'd.)
  - Called company help desk from CFO's office
    - Pretended to be CFO and said he urgently needed his password
    - Help desk agent gave out the password
  - Group left the building with complete access to the network
- Social engineering
  - Gathering information needed for an attack by relying on human weaknesses

Psychological Approaches

- Social engineering attacks rely on psychology
  - Manipulation of human nature
- Methods of persuasion
  - Ingratiation (flattery or insincerity)
  - Conformity (idea that everyone else is doing it)
  - Friendliness
  - Attacker attempts to gain victim's trust
- Approaches use person-to-person contact
  - Not asking for too much information at once

Psychological Approaches (cont'd.)

- Request needs to be believable
- Flattery used to gain victim's cooperation
- Attacker pushes just far enough to gain needed information without arousing suspicion
- Pretending to be confused and asking for help can be a means of gathering information

Psychological Approaches (cont'd.)

- Impersonation
  - Attacker creates a fictitious character
  - Play the role of the character to the victim
  - Example: repair person, help desk technician
- Individuals in positions of authority often impersonated
  - Victims resist saying "no" to person in authority

Psychological Approaches (cont'd.)

- Phishing
  - Most common social engineering attack
  - Sending bogus e-mail claiming to be from a legitimate business
  - Attempts to trick user into providing personal information
  - Users directed to imposter Web site controlled by attacker
- Estimate: 15,000-20,000 new phishing attacks launched each month

Psychological Approaches (cont'd.)

- Variations on phishing
  - Pharming
    - Automatically redirects user to fake Web site
    - Attackers penetrate Internet servers that direct traffic
  - Spear phishing
    - Targets specific users
  - Whaling
    - Attacks on wealthy individuals
  - Vishing
    - Uses telephone (voice phishing)

Psychological Approaches (cont'd.)

- Hoaxes
  - False warnings
  - Can be used as first step in attack
  - May warn of virus and ask user to take action
  - May even ask user to call attacker for help

Physical procedures

- Dumpster diving
  - Digging through trash receptacles for useful information
  - Many different types of items can be useful in an attack
  - Target may be an organization or an individual
- Shoulder surfing
  - Information entered is observed by another person
  - Examples: ATM PIN, computer password

Item Retrieved	Why Useful
Calendars	A calendar can reveal which employees are out of town at a particular time.
Inexpensive computer hardware, such as USB flash drives or portal hard drives	These devices are often improperly disposed of and may contain valuable information.
Memos	Seemingly unimportant memos can often provide small bits of useful information for an attacker who is building an impersonation.
Organizational charts	These identify individuals within the organization who are in positions of authority.
Phone directories	A phone directory can provide the names and telephone numbers of individuals in the organization to target or impersonate.
Policy manuals	These may reveal the true level of security within the organization.
System manuals	A system manual can tell an attacker the type of computer system that is being used so that other research can be conducted to pinpoint vulnerabilities.

Table 2-2 Dumpster diving items and their usefulness

Physical procedures (cont'd.)

- Tailgating
  - Occurs at restricted access points
  - Holding the door open to allow multiple people to enter

Identity Theft

- Using another's personal information to commit financial fraud
- Actions of identity thieves
  - Produce counterfeit checks or debit cards to remove money from account
  - Establish phone service in victim's name
  - File for bankruptcy under victim's name to avoid eviction
  - Purchase big-ticket items with stolen credit card numbers
  - Open bank or credit accounts in victim's name

Technique	Explanation
Dumpster diving	Discarded credit card statements, charge receipts, and bank statements can be retrieved for personal information.
Phishing	Attackers convince victims to enter their personal information at an imposter Web site after receiving a fictitious e-mail from a bank.
Change of address form	Using a standard change-of-address form the attackers divert all mail to their post office box so that the victim never sees any charges made.
Pretexting	An attacker who pretends to be from a legitimate research firm asks for personal information.
Stealing	Stolen wallets and purses contain personal information that can be used in identity theft.

Table 2-3 How attackers steal personal information

Identity Theft (cont'd.)

- Growing area of identity theft
  - Filing fictitious tax returns with the IRS
  - Claiming refund
- 1.5 million undetected false returns processed by the IRS in 2011
  - Thieves assumed identity of deceased person, child, or other person who would not normally file return

Social Networking Risks

- Social networking
  - Grouping individuals and organizations based on likes and dislikes
  - Links individuals with common interests
  - Functions as online user community
- Additional risks of social networking sites
  - Malicious use of personal data
  - Users can be too trusting
  - Social networking security is lax or confusing
  - Unforeseen consequences of accepting friends

Personal Security Defenses

- Defenses against attacks on personal security
  - Strong passwords
  - Recognizing phishing attacks
  - Taking steps to avoid identity theft
  - Securing social networking sites
- Surprising characteristics of weak passwords
  - Password that can be memorized
  - Repeated use of the same password

Personal Security Defenses (cont'd.)

- Password management tool
  - Stores and manages passwords securely
  - Password-protected list of passwords
- Other capabilities of password management tools
  - In-memory protection
  - Key files
  - Lock to user account
  - Import and export
  - Password groupings
  - Random password generator

Type	Description	Advantages	Disadvantages
Installed application	Installed as a program on the local computer	Allows the user to access passwords without having to memorize them	It must be installed on each computer used and the database file must also be updated on every computer used.
Portable application	Stand-alone application carried on a USB flash drive	The user is not limited to computers that have the application preinstalled with the vault file.	User must always have flash drive present to use the application
Internet storage	Application and/or vault is stored online	Can access program and/or database from any computer	Storing passwords online may expose them to attacks.

Table 2-4 Password management applications

Personal Security Defenses (cont'd.)

- Creating strong passwords
  - Length more important than complexity
  - Longer passwords are stronger
- General recommendations for strong passwords
  - Avoid dictionary and phonetic words
  - Avoid birthdays, names, addresses or personal information
  - Avoid repeating characters
  - Use a minimum of 12 characters
  - Consider using a passphrase

Personal Security Defenses (cont'd.)

- Using non-keyboard characters
  - Method of making passwords stronger
  - Accessed by holding down Alt key while typing a number on numeric keypad
  - Disadvantage: not all applications can accept

Recognizing Phishing Attacks

- Common traits of phishing e-mails
  - Official logos
  - Web links
  - Urgent request

Avoiding Identity Theft

- Two basic steps for avoiding identity theft
  - Deter theft by safeguarding information
  - Monitor financial statements and accounts
- Best practices
  - Shred financial documents
  - Avoid carrying social security card in wallet
  - Secure personal information at home
  - Do not provide personal information over the phone or via e-mail
  - Be alert to signs of unusual activity in accounts

Avoiding Identity Theft (cont'd.)

- Legislation to help users monitor financial information
  - Fair and Accurate Credit Transactions Act (2003)
  - Allows consumers free access to credit report
  - Consumers can report inaccuracies
    - Agency must investigate and respond

Setting Social Networking Defenses

- Be cautious about what information you post
  - Posting travel plans can invite burglary
  - Consider your boss and mother reading the post
- Consider allowing acquaintances and business associates access to a limited version of profile
- Pay attention to information about new or updated security settings
- Disable options and enable only when necessary

Feature	Description	Risks
Games and applications	When your Facebook friends use games and applications, these can request information about friends like you, even if you do not use the application.	Information such as your biography, photos, and places where you check in can be exposed.
Social advertisements	A "social ad" pairs an advertisement with an action that a friend has taken, such as "liking" it.	Your Facebook actions could be associated with an ad.
Places	If you use Places, you could be included in a "People Here Now" list once you check in to a location.	Your name and Facebook profile picture appear in the list, which is visible to anyone who checks in to the same location, even if they are not a friend.
Web Search	Entering your name in a search engine like Google can display you Facebook profile, profile picture, and information you have designated as public.	Any Web user can freely access this information about you.
Photo Albums	Photos can be set to be private but that may not include photo albums.	The albums Profile Pictures, Mobile Uploads, and Wall Photos are usually visible to anyone.

Table 2-5 Facebook features and risks

Option	Recommended Setting	Explanation
Profile	Only my friends	Facebook networks can contain hundreds or thousands of users, and there is no control over who else joins the network to see the information.
Photos or photos tagged of you	Only my friends	Photos and videos have often proven to be embarrassing. Only post material that would be appropriate to appear with a resume or job application.
Status updates	Only my friends	Because changes to status such as "Going to Florida on January 28" can be useful information for thieves, only approved friends should have access to it.
Online status	No one	Any benefits derived by knowing who is online are outweighed by the risks.
Friends	Only my friends (minimum setting)	Giving unknown members of the community access to a list of friends may provide attackers with opportunities to uncover personal information through friends.

Table 2-6 Recommended Facebook profile settings

Summary

- Computers and Web sites generally use passwords for authentication
  - Passwords no longer considered strong defense against attacks
- Dictionary and brute force attacks are main types of password attacks
- Social engineering is means of gathering information for an attack
  - Relies on human weakness

Summary (cont'd.)

- Social engineering attacks can rely on psychological manipulation or physical acts
- Identity theft involves using another's personal information to commit financial fraud
- Personal data posted on social networking sites can be used maliciously
- Password management tool best approach for establishing strong security with passwords
- Phishing attacks start with an e-mail claiming to be from a reputable source