Objectives

• Describe the three types of authentication credentials
• Explain what single sign-on can do
• List the account management procedures for securing passwords
• Define trusted operating systems
Introduction

• Authentication
  – Process of ensuring a person desiring to access resources is authentic

• Chapter topics
  – Authentication and secure management of user accounts
  – Different types of authentication credentials
  – Single sign-on
  – Techniques and technology to manage user accounts securely
  – Trusted operating systems
Authentication Credentials

• Types of authentication credentials
  – What you have
    • Example: key fob to lock your car
  – What you are
    • Example: facial characteristics recognized by health club attendant
  – What you know
    • Example: combination to health club locker
Figure 10-1 Authentication credentials
© Cengage Learning 2012
What You Know: Passwords

• User logging in to a system
  – Asked to identify himself
    • User enters username
  – User asked to authenticate
    • User enters password
• Passwords are most common type of authentication today
• Passwords provide only weak protection
Password Weaknesses

• Weakness of passwords is linked to human memory
  – Humans can only memorize a limited number of items
  – Long, complex passwords are most effective
    • Most difficult to memorize
• Users must remember passwords for many different accounts
• Security policies mandate passwords must expire
  – Users must repeatedly memorize passwords
Password Weaknesses (cont’d.)

• Users often take shortcuts
  – Using a weak password
    • Examples: common words, short password, or personal information
  – Reuse the same password for multiple accounts
    • Easier for attacker who compromises one account to access others
Attacks on Passwords

• Social engineering
  – Phishing, shoulder surfing, dumpster diving
• Capturing
  – Keylogger, protocol analyzer
  – Man-in-the-middle and replay attacks
• Resetting
  – Attacker gains physical access to computer and resets password
• Online guessing
  – Not really practical
Attacks on Passwords (cont’d.)

• Offline cracking
  – Method used by most password attacks today
  – Attackers steal file with encrypted password
    • Compare with encrypted passwords they have created

• Offline cracking types
  – Brute force
    • Every possible combination of letters, numbers, and characters used to create encrypted passwords and matched against stolen file
    • Slowest, most thorough method
Attacks on Passwords (cont’d.)

• Automated brute force attack program parameters
  – Password length
  – Character set
  – Language
  – Pattern
  – Skips

• Dictionary attack
  – Attacker creates encrypted versions of common dictionary words
  – Compares against stolen password file
Figure 10-2 Dictionary attack

© Cengage Learning 2012
Attacks on Passwords (cont’d.)

• Hybrid attack
  – Slightly alter dictionary words
    • Adding numbers to the end of the password
    • Spelling words backward
    • Slightly misspelling words
    • Including special characters

• Rainbow tables
  – Large pregenerated data set of encrypted passwords
Attacks on Passwords (cont’d.)

• Steps for using a rainbow table
  – Creating the table
    • Chain of plaintext passwords
    • Encrypt initial password
    • Feed into a function that produces different plaintext passwords
    • Repeat for a set number of rounds
  – Using the table to crack a password
    • Run encrypted password though same procedure used to create initial table
    • Results in initial chain password
Attacks on Passwords (cont’d.)

• Using the table to crack a password (cont’d.)
  – Repeat, starting with this initial password until original encryption is found
  – Password used at last iteration is the cracked password

• Rainbow table advantages over other attack methods
  – Can be used repeatedly
  – Faster than dictionary attacks
  – Less machine memory needed
Password Defenses

• Creating strong passwords
  – Insight into how to create strong passwords gained by examining attack methods

• Most passwords consist of:
  – Root
  – Attachment
    • Prefix or suffix

• Attack program method
  – Tests password against 1000 common passwords
Password Defenses (cont’d.)

• Attack program method (cont’d.)
  – Combines common passwords with common suffixes
  – Uses 5000 common dictionary words, 10,000 names, 100,000 comprehensive dictionary words
  – Uses lowercase, initial uppercase, all uppercase, and final character uppercase
  – Makes common substitutions for letters in the dictionary words
    • Examples: $ for s, @ for a
Password Defenses (cont’d.)

• General observations to create strong passwords
  – Do not use dictionary words or phonetic words
  – Do not use birthdays, family member or pet names, addresses or any personal information
  – Do not repeat characters or use sequences
  – Do not use short passwords

• Managing passwords
  – One important defense: prevent attacker from obtaining encrypted password file
Password Defenses (cont’d.)

• Managing passwords (cont’d.)
  – Defenses against password file theft
    • Do not leave computer unattended
    • Screensavers should be set to resume with a password
    • Password protect the ROM BIOS
    • Physically lock the computer case so it cannot be opened
  – Good password management practices
    • Change passwords frequently
    • Do not reuse old passwords
Password Defenses (cont’d.)

• Good password management practices (cont’d.)
  – Never write password down
  – Use unique passwords for each account
  – Set up temporary password for another user’s access
  – Do not allow computer to automatically sign in to an account
  – Do not enter passwords on public access computers
  – Never enter a password while connected to an unencrypted wireless network
Password Defenses (cont’d.)

• Other guidelines
  – Use non-keyboard characters
    • Created by holding down ALT key while typing a number on the numeric keypad

• Password supplements
  – Problem: managing numerous strong passwords is burdensome for users
  – One solution: rely on technology to store and manage passwords
Figure 10-3 Windows character map
© Cengage Learning 2012
Password Defenses (cont’d.)

• Password supplements (cont’d.)
  – Internet Explorer (IE) and Firefox Web browsers contain function that allows user to save passwords

• AutoComplete Password in IE
  – Encrypted and stored in Windows registry

• Disadvantages of password supplements
  – Password information specific to one computer
  – Passwords vulnerable if another user allowed access to the computer
Password Defenses (cont’d.)

• Password management applications
  – User creates and stores passwords in single user “vault” file protected by one strong master password

• Password management application features
  – Drag and drop capability
  – Enhanced encryption
  – In-memory protection prevents OS cache from being exposed
  – Timed clipboard clearing
<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installed application</td>
<td>Installed as a program on the local computer</td>
<td>Allows the user to access passwords without having to memorize them</td>
<td>It must be installed on each computer used and the vault file must also be updated on every computer used</td>
</tr>
<tr>
<td>Portable application</td>
<td>Stand-alone application carried on a USB flash drive</td>
<td>The user is not limited to computers that have the application preinstalled with the vault file</td>
<td>User must always have flash drive present to use the application</td>
</tr>
<tr>
<td>Internet storage</td>
<td>Application and/or vault is stored online</td>
<td>Can access program and/or vault from any computer</td>
<td>Storing passwords online may expose them to attacks</td>
</tr>
</tbody>
</table>

Table 10-1 Password management applications
What You Have: Tokens and Cards

- Tokens
  - Small devices with a window display
  - Synched with an authentication server
  - Code is generated from an algorithm
  - Code changes every 30 to 60 seconds
What You Have: Tokens and Cards (cont’d.)

• User login steps with a token
  – User enters username and code from token
  – Authentication server looks up algorithm associated with that user, generates its own code, and compares it to user’s code
  – If a match, user is authenticated

• Advantages over passwords
  – Token code changes frequently
    • Attacker would have to crack code within time limit
Figure 10-5 Code generation and comparison

© Cengage Learning 2012
What You Have: Tokens and Cards (cont’d.)

• Advantages over passwords (cont’d.)
  – User may not know if password has been stolen
  – If token is stolen, it becomes obvious
    • Steps could be taken to disable account

• Token system variations
  – Some systems use token code only
  – Others use code in conjunction with password
  – Some combine PIN with token code
What You Have: Tokens and Cards (cont’d.)

• Cards
  – Smart card contains integrated circuit chip that holds information
  – Contact pad allows electronic access to chip contents
  – Contactless cards
    • Require no physical access to the card
  – Common access card (CAC)
    • Issued by US Department of Defense
    • Bar code, magnetic strip, and bearer’s picture
Figure 10-6 Smart card
© Cengage Learning 2012
What You Are: Biometrics

- Standard biometrics
  - Uses person’s unique physical characteristics for authentication
  - Fingerprint scanners most common type
  - Face, hand, or eye characteristics also used
- Fingerprint scanner types
  - Static fingerprint scanner
    - Takes picture and compares with image on file
  - Dynamic fingerprint scanner
    - Uses small slit or opening
Figure 10-7 Dynamic fingerprint scanner
© Cengage Learning 2012
What You Are: Biometrics (cont’d.)

• Disadvantages of standard biometrics
  – Cost of hardware scanning devices
  – Readers have some amount of error
    • Reject authorized users
    • Accept unauthorized users

• Behavioral biometrics
  – Authenticares by normal actions the user performs
  – Keystroke dynamics
  – Voice recognition
  – Computer footprinting
What You Are: Biometrics (cont’d.)

• Keystroke dynamics
  – Attempts to recognize user’s typing rhythm
    • All users type at a different pace
    • Provides up to 98 percent accuracy
  – Uses two unique typing variables
    • Dwell time (time it takes to press and release a key)
    • Flight time (time between keystrokes)
Figure 10-8 Typing template
© Cengage Learning 2012

Figure 10-9 Authentication by keystroke dynamics
© Cengage Learning 2012
What You Are: Biometrics (cont’d.)

• Voice recognition
  – Several characteristics make each person’s voice unique
  – Voice template can be created
  – Difficult for an attacker to authenticate using a recording of user’s voice
    • Phonetic cadence of putting words together is part of real speech pattern
What You Are: Biometrics (cont’d.)

• Computer footprinting
  – Relies on typical access patterns
  – Geographic location
  – Time of day
  – Internet service provider
  – Basic PC configuration

• Cognitive biometrics
  – Relates to perception, thought process, and understanding of the user
What You Are: Biometrics (cont’d.)

• Cognitive biometrics (cont’d.)
  – Easier for user to remember because it is based on user’s life experiences
  – Difficult for an attacker to imitate
  – Example: identifying specific faces
  – Example: user selects memorable lifetime events and is asked for details about them
  – Predicted to become a key element of authentication in the future
Single Sign-On

• Identity management
  – Using a single authentication credential shared across multiple networks
  – Called federated identity management (FIM) when networks are owned by different organizations
  – Single sign-on (SSO) holds promise to reduce burden of usernames and passwords to just one
Windows Live ID

- Introduced in 1999 as .NET passport
- Name changed to Microsoft Passport Network, then Windows Live ID
- Designed as an SSO for Web commerce
- Authentication process
  - User enters username and password
  - User given time limited “global” cookie stored on computer with encrypted ID tag
  - ID tag sent to Web site
Windows Live ID (cont’d.)

• Authentication process (cont’d.)
  – Web site uses ID tag for authentication
  – Web site stores encrypted, time-limited “local” cookie on user’s computer

• Windows Live ID was not widely supported

• Currently used for authentication on:
  – Windows Live, Office Live, Xbox Live, MSN, and other Microsoft online services
OpenID

• Decentralized open source FIM
• Does not require specific software to be installed on the desktop
• URL-based identity system
• OpenID provides a means to prove a user owns the URL
• Authentication process
  – User goes to free site and given OpenID account of Me.myopenid.com
OpenID (cont’d.)

• Authentication process (cont’d.)
  – User visits Web commerce or other site and signs in using his Open ID
  – Site redirects user to MyOpenID.com where he enters password to authenticate
  – MyOpenID.com sends him back to Web site, now authenticated

• Security weaknesses
  – Relies on DNS which may have own weaknesses
  – Not considered strong enough for most banking and e-commerce Web sites
Open Authorization (OAuth)

- Permits users to share resources stored on one site with a second site
  - Without forwarding authentication credentials
- Allows seamless data sharing among sites
- Relies on token credentials
  - Replaces need to transfer user’s username and password
  - Tokens are for specific resources on a site
    - For a limited time period
Account Management

• Managing user account passwords
  – Can be done by setting password rules
  – Too cumbersome to manage on a user-by-user basis
    • Security risk if one user setting is overlooked

• Preferred approach: assign privileges by group
  – Microsoft Windows group password settings
    • Password Policy Settings
    • Account Lockout Policy
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Recommended setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enforce password history</td>
<td>Determines the number of unique new passwords a user must use before an old password can be reused (from 0 to 24)</td>
<td>24 new passwords</td>
</tr>
<tr>
<td>Maximum password age</td>
<td>Determines how many days a password can be used before the user is required to change it; the value of this setting can be between 0 and 999</td>
<td>60 days</td>
</tr>
<tr>
<td>Minimum password age</td>
<td>Determines how many days a new password must be kept before the user can change it (from 0 to 999); this setting is designed to work with the Enforce password history setting so that users cannot quickly reset their passwords the required number of times, and then change back to their old passwords</td>
<td>1 day</td>
</tr>
<tr>
<td>Minimum password length</td>
<td>Determines the minimum number of characters a password can have (0 to 28)</td>
<td>12 characters</td>
</tr>
<tr>
<td>Passwords must meet complexity requirements</td>
<td>Determines whether the following are used in creating a password: Passwords cannot contain the user's account name or parts of the user's full name that exceed two consecutive characters; must contain characters from three of the following four categories: English uppercase characters (A through Z), English lowercase characters (a through z), digits (0 through 9), and nonalphanumeric characters (!, $, #, %)</td>
<td>Enabled</td>
</tr>
<tr>
<td>Store passwords using reversible encryption</td>
<td>Provides support for applications that use protocols that require knowledge of the user's password for authentication purposes; storing passwords using reversible encryption is essentially the same as storing plaintext versions of the passwords</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

Table 10-2 Password policy settings (Windows group policy)
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Recommended setting</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account lockout duration</td>
<td>Determines the length of time a locked account remains unavailable before a</td>
<td>15 minutes</td>
<td>Setting this attribute too high may increase help desk calls from users who unintentionally locked themselves out</td>
</tr>
<tr>
<td></td>
<td>user can try to log on again (a value of 0 sets account to remain locked out</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>until an administrator manually unlocks it)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Account lockout threshold</td>
<td>Determines the number of failed login attempts before a lockout occurs</td>
<td>30 invalid attempts</td>
<td>Setting this attribute too low may result in attackers using the lockout state as a denial of service (DoS) attack by triggering a lockout on a large number of accounts</td>
</tr>
<tr>
<td>Reset account lockout</td>
<td>Determines the length of time before the account lockout threshold setting</td>
<td>15 minutes</td>
<td>This reset time must be less than or equal to the value for the account</td>
</tr>
<tr>
<td>counter after</td>
<td>resets to zero</td>
<td></td>
<td>lockout duration setting</td>
</tr>
</tbody>
</table>

Table 10-3 Account lockout policy settings (Windows Active Directory)
Trusted Operating Systems

• Operating system basic flaws
  – Size: millions of lines of code make vulnerabilities difficult to recognize
  – One compromised application can impact entire computer
  – Applications cannot authenticate themselves to each other
  – No trusted path between users and applications
  – Operating systems do not use principle of least privilege
Trusted Operating Systems (cont’d.)

• Trusted operating system (trusted OS)
  – OS designed to be secure from the ground up
  – Can keep attackers from accessing critical parts of the system
  – Can prevent administrators from inadvertently making harmful changes

• Vendors developing trusted OSs
  – Focusing on securing OS components and other platform elements

• One approach: compartmentalize services within trusted OS for individual customers
Summary

• Authentication credentials can be classified into three categories: what you know, what you have, and what you are
• Passwords provide a weak degree of protection
  – Must rely on human memory
• Most password attacks today use offline cracking
  – Attackers steal encrypted password file
• A token is a small device that generates a code from an algorithm once every 30 to 60 seconds
Summary (cont’d.)

• Biometrics bases authentication on characteristics of an individual
  – Standard, behavioral, and cognitive biometrics
• Single sign-on allows a single username and password to gain access to all accounts
• Group Policy settings allow an administrator to set password restrictions for an entire group at once
• Trusted operating systems are designed for security from the ground up