Information Security (CP3404)

Chapter 12 – Authentication and Account Management

Based on the Fifth Edition of:

M. Ciampa:. *CompTIA® Security + Guide to Network Security Fundamentals*

Department of Information Technology, College of Business, Law & Governance

Learning Objectives

- Describe the different types of authentication credentials
- Explain what single sign-on can do
- List the account management procedures for securing passwords

Outline

Preface

- Authentication – Process of ensuring person desiring to access resources is authentic (genuine) and not an imposter
- Chapter topics:
  - Authentication Credentials
  - Single sign-on
  - Account Management

Authentication Credentials

Key fob (what he has)

Facial characteristics (what he is)

Combination lock (what he knows)

Military base (where he is)

© Sasha Fenix/Shutterstock.com

Pushups (what he does)

Figure 12-1 Ermanno's authenticity

Authentication Credentials

Authentication Credentials

- Authentication credentials/factors) can be classified into one of the following five (5) categories:
  1. What you have (Example: key fob to lock your car)
  2. What you are (Example: facial characteristics)
  3. What you know (Example: combination to health club locker)
  4. Where you are (Example: on a restricted military base)
  5. What you do (Example: record number of pushups)

Authentication Credentials

What You Know: Passwords

- User logging in to system:
  - Asked to identify himself with username as identifier
  - Asked to authenticate himself with password as secret combination of letters, numbers, and/or characters that only user should have knowledge of
- Passwords most common type of authentication today
- Yet passwords provide only weak protection

Authentication Credentials

What You Know: Passwords — Weaknesses

- Human beings can memorize only limited number of items
- Most effective passwords are long and complex but difficult for users to memorize and then accurately recall when needed
- Users must remember passwords for many different accounts
- Each account password should be unique
- Many security policies mandate that passwords expire after set period of time, forcing users to repeatedly memorize new passwords

Authentication Credentials

What You Know: Passwords — Weaknesses

- Weak password – Passwords that use:
  - Common word as password (e.g., princess)
  - Short password (e.g., desk)
  - Predictable sequence of characters (e.g., abc123)
  - Personal information (e.g., Hannah)

Authentication Credentials

What You Know: Passwords — Weaknesses

- When attempt to create stronger passwords users often follow predictable patterns:
  - Appending – Combine letters, numbers, and punctuation (character sets) by appending one character set with another so add number after letters (e.g., caitlin1 or cheer99) or add character sets in sequence letters+punctuation+number (e.g., amanda.7)
  - Replacing – Zero used instead of letter o (e.g., passw0rd), digit 1 for letter i (e.g., denn1s), or dollar sign for s (e.g., be$tfriend)
- Attackers are aware of these patterns in passwords and can search for them

Authentication Credentials

What You Know: Passwords — Weaknesses

- Common shortcut the same password for multiple accounts
- Makes easier for an attacker who compromises one account to access other accounts
- Analysis of one theft of 32 million user passwords:
  - 30% of users had created passwords of only five (5) or six (6) characters
  - 12% of the user passwords were nine (9) characters in length
  - One (1) in every five (5) users created password that was one of the 5000 most common passwords (see Table 12-1)

Authentication Credentials

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 12-1 Ten most common passwords

Authentication Credentials

What You Know: Passwords — Attacks on Passwords

- Attacks that can be used to discover a password include:
  - 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

These attacks, however, have their limiytations. Most password attacks today instead use off-line cracking

Authentication Credentials

What You Know: Passwords — Attacks on Passwords

- Offline cracking – Method used by most password attacks today
- One-way hash algorithm creates a unique digital fingerprint digest when password first created
- When user logs in digest is created from entered password and compared to stored digest
- With offline cracking attackers steal password digests, load file onto own computers, and attempt to discover passwords by comparing stolen digests with their own created digests (candidates)

Authentication Credentials

What You Know: Passwords — Attacks on Passwords

- Brute force attack – Every possible combination of letters, numbers, and characters is used to create candidate digests then matched against those in stolen digest file
- Automated brute force attack program parameters:
  - Password length
  - Character set
  - Language
  - Pattern
  - Skips

Authentication Credentials

What You Know: Passwords — Attacks on Passwords

- Dictionary attack – Attacker creating digests of common dictionary words as candidates (see Figure 12-2)
- Pre-image attack – Dictionary attack that uses set of dictionary words and compares it with stolen digests when one known digest (dictionary word) compared to an unknown digest (stolen digest)
- Birthday attack – Search is for any two digests that are identical

Authentication Credentials

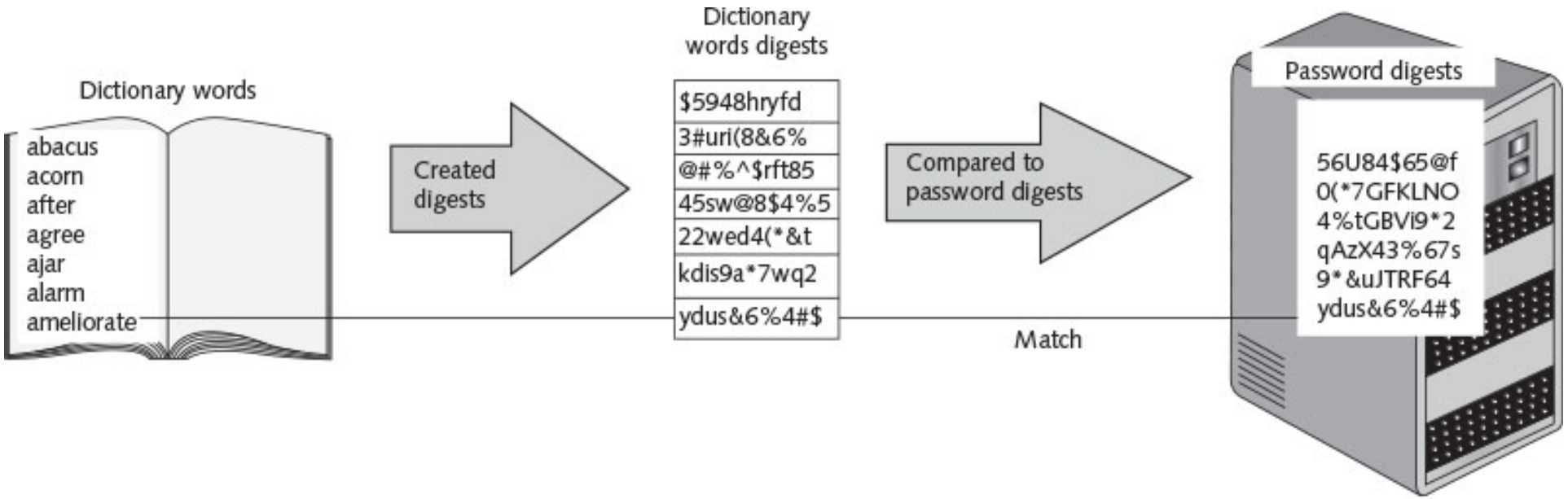

Figure 12-2 Dictionary attack

Authentication Credentials

What You Know: Passwords — Attacks on Passwords

- Hybrid attack – Variation of dictionary attack
- Combines dictionary attack with brute force attack
- Slightly alter dictionary words by:
  - Adding numbers to the end of the password
  - Spelling words backward
  - Slightly misspelling words
  - Including special characters (@,$,!, or %)

Authentication Credentials

What You Know: Passwords — Attacks on Passwords

- Rainbow tables – Creating a large pregenerated data set of candidate digests
- Generating a rainbow table requires a significant amount of time
- Once created has significant advantages:
  - Can be used repeatedly for attacks on other passwords
  - Rainbow tables are much faster than dictionary attacks
  - Amount of memory needed on attacking machine is greatly reduced

Authentication Credentials

What You Know: Passwords — Attacks on Passwords

- Password collections – Stolen passwords now posted on Internet provide key elements for password attacks:
  - Large corpus of real-world passwords available; because users repeat passwords on multiple accounts, attackers now use these passwords as candidate passwords in their attacks
  - Password collections provided attackers insight into strategic thinking of how users create passwords

Authentication Credentials

What You Know: Passwords — Password Defenses

- There are four (4) primary defenses against password attacks:
  1. Password Complexity
  2. Credential Management
  3. Password Hashing Algorithms
  4. Salts

Authentication Credentials

What You Know: Passwords — Password Defenses (Complexity)

- General observations regarding creating passwords:
  - Do not use passwords that consist of dictionary words or phonetic words
  - Do not repeat characters (xxx) or use sequences (abc, 123, qwerty)
  - Do not use birthdays, family member names, pet names, addresses, or any personal information
  - Do not use short passwords; strong password should be minimum of 15 characters in length

Authentication Credentials

What You Know: Passwords — Password Defenses (Complexity)

- Longer passwords require more attempts an attacker must make in order to break it

$$\text{Total-Number-of-Possible-Passwords} = K^{\ell}$$

where, K is the Number-of-Keyboard-Keys and ℓ is the Password-Length (see Table 12-2)

One way to make passwords stronger is to use nonkeyboard characters (see Figure 12-3)

Authentication Credentials

Keyboard keys	Password length	Number of possible passwords
95	2	9025
95	3	857,375
95	4	81,450,625
95	5	7,737,809,375
95	6	735,091,890,625

Table 12-2 Number of possible passwords

Authentication Credentials

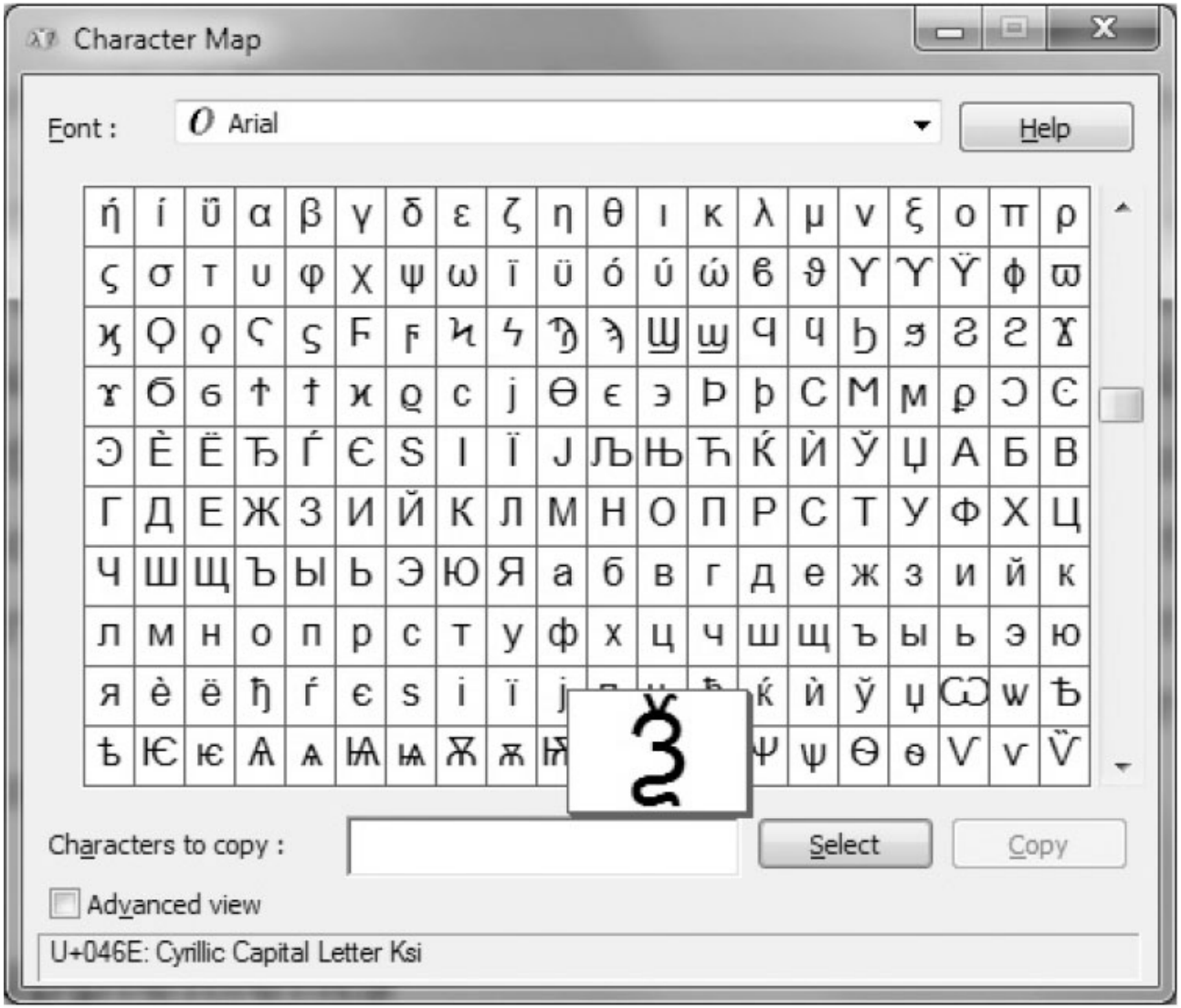

Figure 12-3 Windows character map
Source: Microsoft Windows

Authentication Credentials

What You Know: Passwords — Password Defenses (Management)

- Must properly manage password credentials
- Defenses against the theft of password digests:
  - Do not leave computer running unattended, even if in locked office; all screensavers should be set to resume only when password is entered
  - Do not set a computer to boot from optical drive or USB flash drive
  - Physically lock computer case so that cannot be opened

Authentication Credentials

What You Know: Passwords — Password Defenses (Management)

- Good credential management also includes:
  - Change passwords frequently
  - Do not reuse old passwords
  - Never write password down
  - Have unique password for each account
  - Do not allow computer to automatically sign into account or record a password so login not necessary
  - Do not enter passwords on public access computers or while using an unencrypted wireless network

Authentication Credentials

What You Know: Passwords — Password Defenses (Management)

- Secure solution to credential management is rely on technology rather than human memory to store and manage passwords
- Password management applications – Programs user can create and store multiple strong passwords in single user *vault* file protected by one strong master password
- Users can retrieve individual passwords as needed by opening user file, thus freeing user from need to memorize multiple passwords

Authentication Credentials

What You Know: Passwords — Password Defenses (Hashing)

- Microsoft Windows operating systems hash passwords in two (2) ways:
  1. LAN Manager (LM) hash – Instead of encrypting password with another key, password itself is key; LM hash considered very weak function
  2. New Technology LAN Manager (NTLM) hash – More secure password hash algorithm

Authentication Credentials

What You Know: Passwords — Password Defenses (Hashing)

- Key stretching – Specialized password hash algorithms intentionally designed be slower to limit ability of attacker to crack passwords because requires significantly more time to create each candidate digest
- Two (2) popular key stretching password hash algorithms are bcrypt and PBKDF2
- Network administrator can specify number of iterations (rounds), which sets how *expensive* (in terms of computer time and/or resources) password hash function is

Authentication Credentials

What You Know: Passwords — Password Defenses (Salts)

- Passwords can be protected by adding random string (a.k.a. salt) to user's cleartext password before hashed
- Salt advantages:
  - Make dictionary attacks and brute force attacks for cracking large number of passwords much slower
  - Limit impact of rainbow tables (see Table 12-3)

Authentication Credentials

Username	Password	Unsalted password hash	Random salt	Salted password	Salted password hash
Alice	apple	4r9g8	&hgu$	&hgu$apple	r$wdc
Bob	banana	3ca53	#x!@3	#x!@3banana	ei832
Carol	carrot	8dusi	5!%vX	5!%vXcarrot	5t9ri
Devin	banana	3ca53	9*^cs	9*^csbanana	xde4z
Elisa	eggplant	4v37d	={4*f	={4*feggplant	i8s74

Table 12-3 Unsalted and salted passwords

Authentication Credentials

What You Have

- Another type of authentication credential based on approved user having specific item in possession
- Multifactor authentication – Using more than one type of authentication credential
- Single-factor authentication – Using one type of authentication credential
- Common items used for authentication:
  - Tokens
  - Cards
  - Cell Phones

Authentication Credentials

What You Have — Tokens

- Token – Typically small device (usually one that can be affixed to keychain) with window display –See Figure 12-4
- Instead of user presenting password (what she knows), token introduces different form of authentication based on what person has (a token)
- One-time password (OTP) – Authentication code that can be used only once or for limited period of time

Authentication Credentials

Figure 12-4 Token

Authentication Credentials

What You Have — Tokens (cont.)

- Time-based one-time password (TOTP) – Changes after set time period
- Token and corresponding authentication server share an algorithm (each user's token has a different algorithm)
- The token generates code from algorithm once every 30 to 60 seconds and valid for only brief period of time
- User enters her username along with code currently being displayed on token (see Figure 12-5)

Authentication Credentials

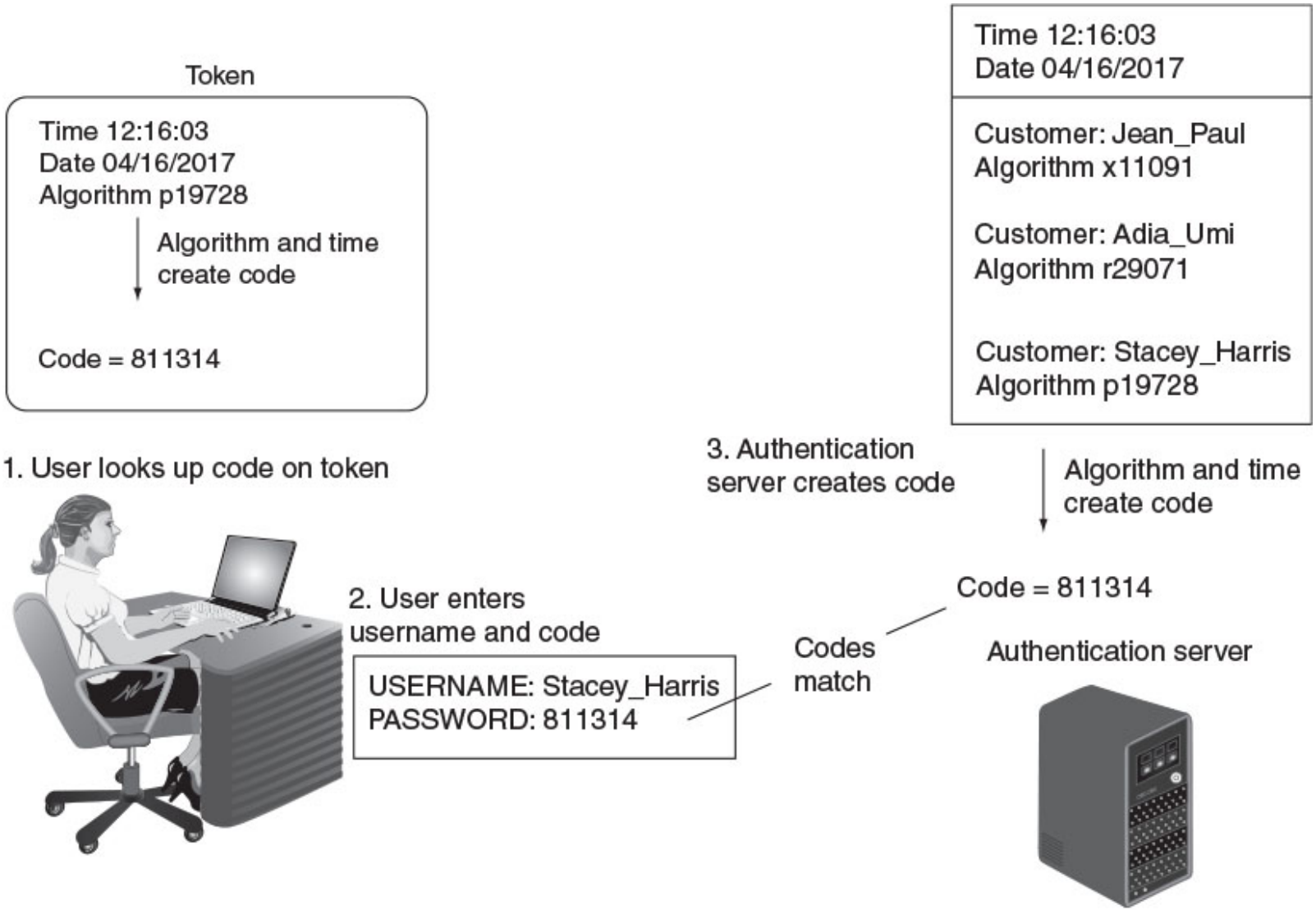

Figure 12-5 Time-based one-time password (TOTP)

Authentication Credentials

What You Have — Tokens (cont.)

- TOTP – Changes after set number of seconds
- Instead of changing after a set number of seconds, an HMAC-based one-time password (HOTP) is *event-driven* and changes when specific event occurs
- Example: when user enters personal identification number (PIN) on tokens keypad triggers token to create random code

Authentication Credentials

What You Have — Token Advantages

- Standard passwords are static and do not change unless user forced to create new password
- Tokens produce dynamic passwords that change frequently
- User might not know if an attacker has stolen her password
- If token is stolen, become obvious and steps could be taken immediately to disable account

Authentication Credentials

What You Have — Cards

- Smart card – Contains integrated circuit chip that can hold information to be used as part of authentication process (see Figure 12-6)
- Common access card (CAC) – U.S. Department of Defense (DoD) smart card used for identification of active-duty and reserve military personnel along with civilian employees and special contractors
- Personal Identity Verification (PIV) – Standard smart card standard covering all U.S. government employees

Authentication Credentials

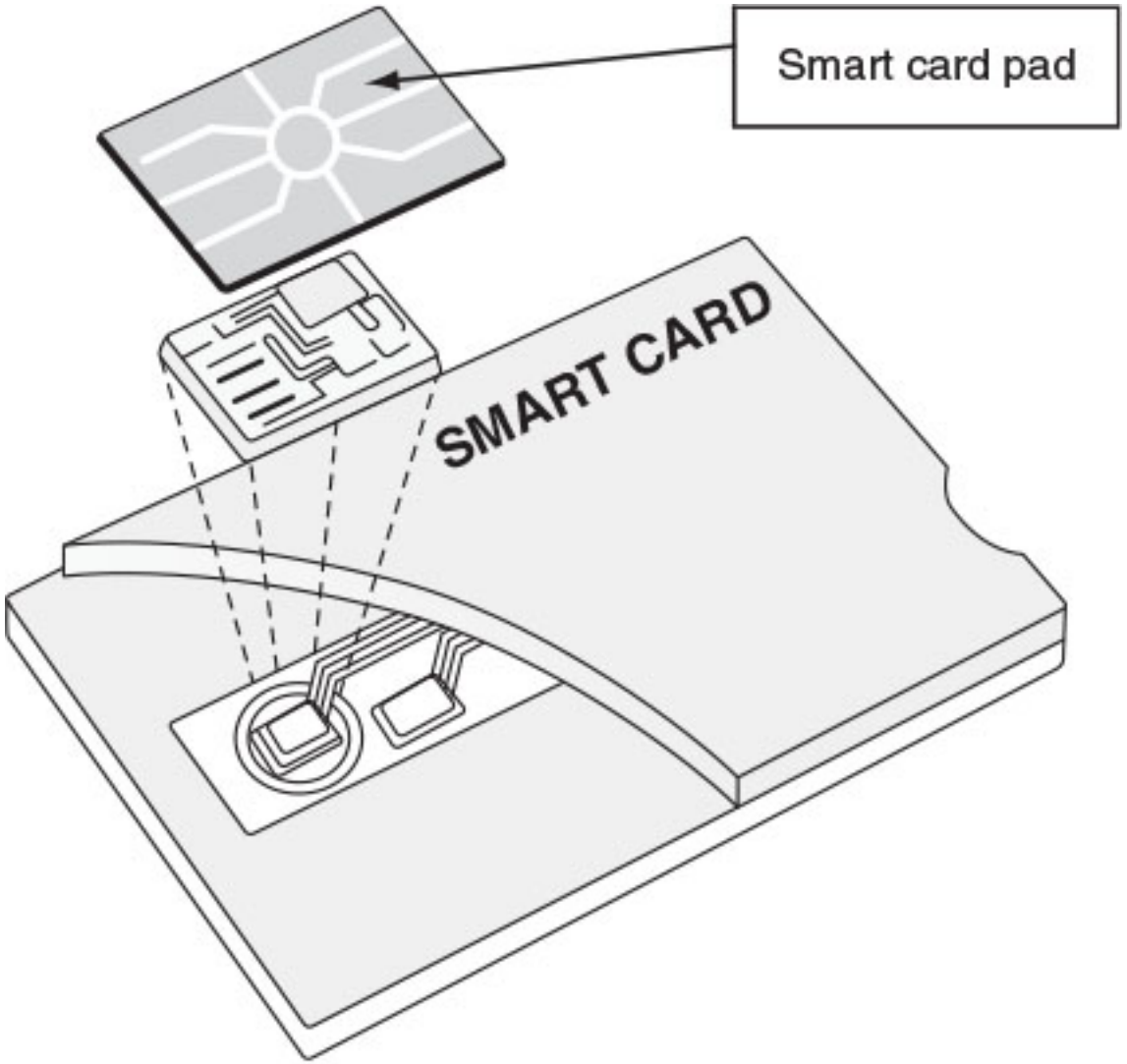

Figure 12-6 Smart card

Authentication Credentials

What You Have — Cell Phones

- Tokens and cards increasingly being replaced today with cell phones
- Code can be sent to user's cell phone through an app on the device or as a text message when using TOTP
- Cell phones also allow user to send request via phone to receive HOTP authorization code

Authentication Credentials

What You Are: Biometrics

- In addition to authentication based on what person knows or has, another category rests on features and characteristics of individual
- *What you are* authentication incolves:
  - Standard Biometrics
  - Cognitive Biometrics

Authentication Credentials

What You Are: Standard Biometrics

- Standard biometrics – Uses person's unique physical characteristics for authentication
- Fingerprint scanners most common type
- Face, hand, or eye characteristics also used
- Biometrics commonly used in physical security: access to secure area restricted to only those who fingerprint or retina is scanned

Authentication Credentials

What You Are: Standard Biometrics (cont.)

- Fingerprint consists of number of ridges and valleys, with ridges being the upper skin layer segments of the finger and valleys the lower segments
- Fingerprint scanner types:
  - Static fingerprint scanner – Takes picture and compares with image on file

    Dynamic fingerprint scanner – Uses small slit or opening (see Figure 12-7)

Authentication Credentials

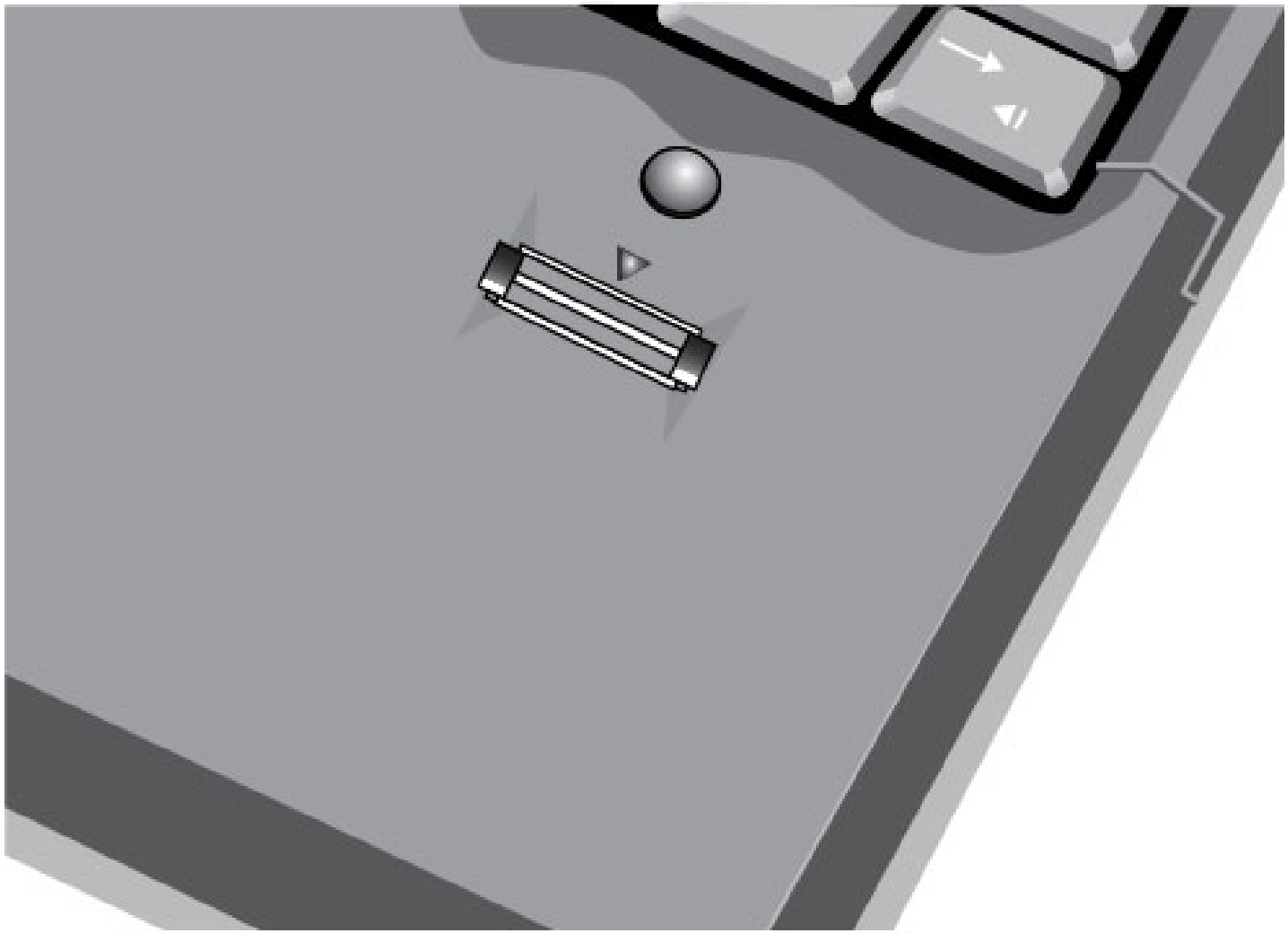

Figure 12-7 Dynamic fingerprint scanner

Authentication Credentials

What You Are: Disadvantages of Standard Biometrics

- Cost of hardware scanning devices
- Readers not foolproof
  - Reject authorized users
  - Accept unauthorized users
- Errors are mainly due to many facial or hand characteristics that must be scanned and then compared

Authentication Credentials

What You Are: Cognitive Biometrics

- Cognitive biometrics – Related to perception, thought process, and understanding of user
- Considered to be much easier for user to remember and more difficult for attacker to imitate
- Examples:
  - Picture gesture authentication (PGA) for touch-enabled devices (see Figure 12-8)
  - Identify specific faces
  - Recall memorable event

Authentication Credentials

Figure 12-8 Picture gesture authentication

Photo © Pressmaster/Shutterstock.com (numbers and lines added)

Authentication Credentials

What You Do: Behavioral Biometrics

- Behavioral biometrics – Authentication based on actions that user is uniquely qualified to perform
- Two (2) examples of Behevioral biometrics includes:
  1. Keystroke Dynamics
  2. Voice Recognition

Authentication Credentials

What You Do: Behavioral Biometrics — Keystroke Dynamics

- Keystroke Dynamics – Attempts to recognize user's typing rhythm
- All users type at different pace
- Provides up to 98 percent accuracy
- Uses two (2) unique typing variables
  1. Dwell time – Time it takes to press and release a key
  2. Flight time – Time between keystrokes
- Multiple samples collected to form user typing template that are used in authentication (see Figures 12-9 and 12-10)

Authentication Credentials

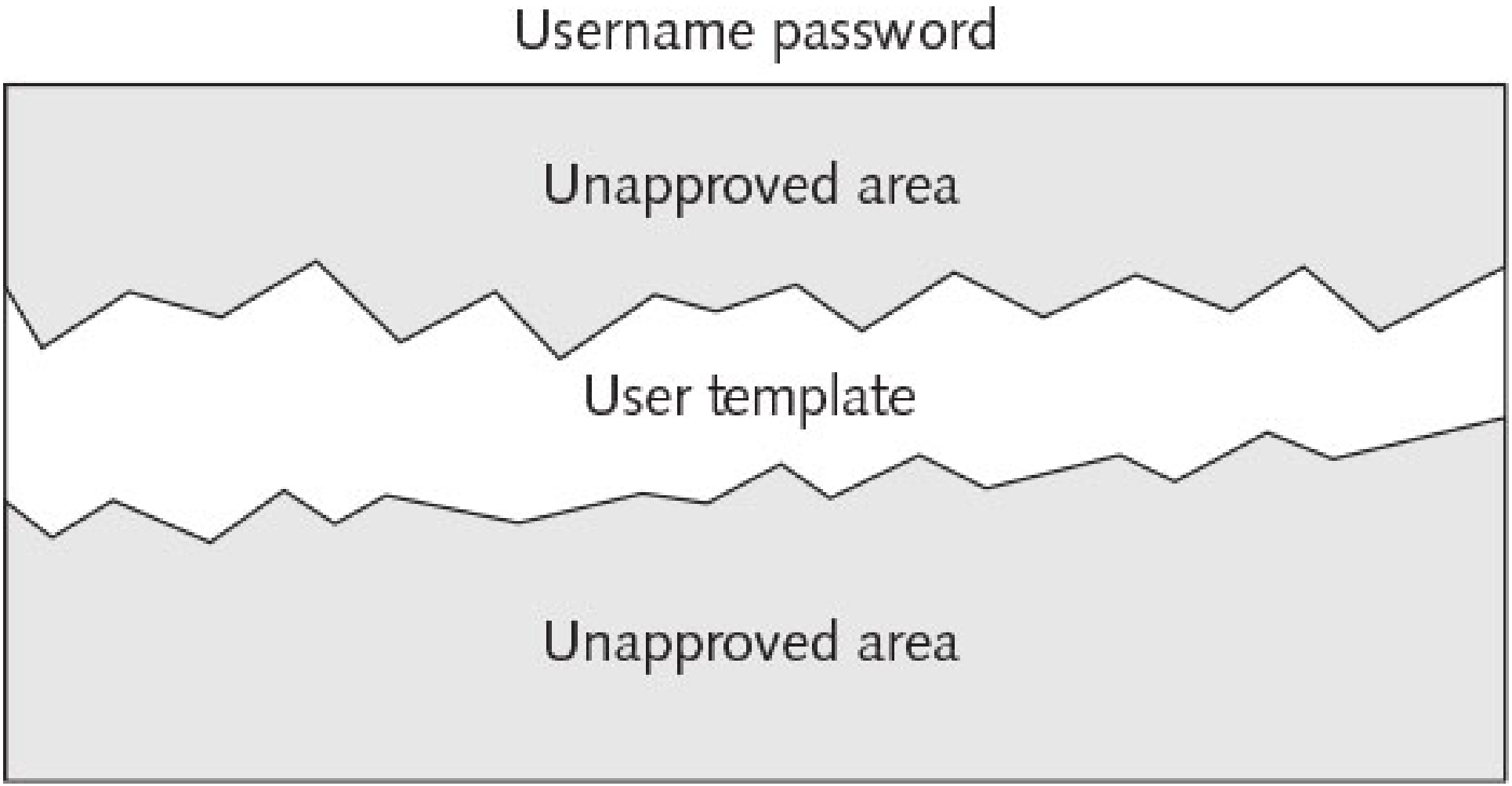

Figure 12-9 Typing template

Authentication Credentials

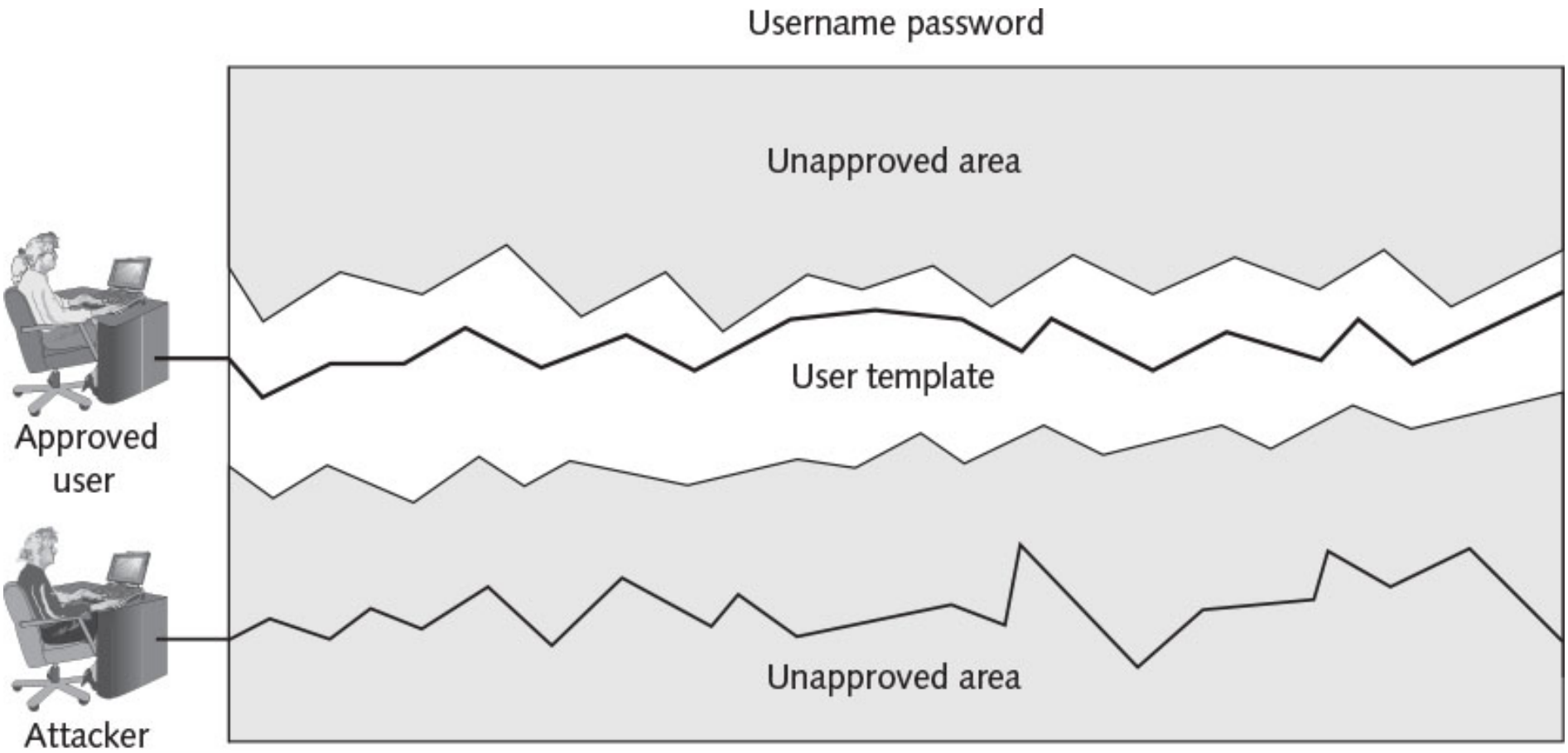

Figure 12-10 Authentication by keystroke dynamics

Authentication Credentials

What You Do: Behavioral Biometrics — Voice Recognition

- 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

Authentication Credentials

Where You Are: Geolocation

- Geolocation – Identification of the location of person or object using technology
- Geolocation may not uniquely identify user but can indicate if attacker trying to perform malicious action at location different from normal location
- If computer in China attempts to access user's bank's website this may be an indication that an attacker is at work
- Many websites not allow user to access an account if the computer is located, for example, in North Carolina when normally access from Tennessee

Quick Quiz

1. A(n) _____ is a secret combination of letters, numbers, and/or characters that only the user should know.
   Answer:

Quick Quiz

1. A(n) _____ is a secret combination of letters, numbers, and/or characters that only the user should know.
   Answer: password

Quick Quiz

1. A(n) _____ is a secret combination of letters, numbers, and/or characters that only the user should know.
   Answer: password

2. **True or False:** A token is typically a small device (usually one that can be affixed to a keychain) with a window display.
   Answer:

Quick Quiz

1. A(n) _____ is a secret combination of letters, numbers, and/or characters that only the user should know.
   Answer: password

2. **True or False:** A token is typically a small device (usually one that can be affixed to a keychain) with a window display.
   Answer: True

Quick Quiz

1. A(n) _____ is a secret combination of letters, numbers, and/or characters that only the user should know.
   Answer: password

2. **True or False:** A token is typically a small device (usually one that can be affixed to a keychain) with a window display.
   Answer: True

3. **True or False:** Cognitive biometrics is considered to be much more difficult for the user to remember.
   Answer:

Quick Quiz

1. A(n) _____ is a secret combination of letters, numbers, and/or characters that only the user should know.
   Answer: password

2. **True or False:** A token is typically a small device (usually one that can be affixed to a keychain) with a window display.
   Answer: True

3. **True or False:** Cognitive biometrics is considered to be much more difficult for the user to remember.
   Answer: False

Quick Quiz

1. A(n) _____ is a secret combination of letters, numbers, and/or characters that only the user should know.
   Answer: password

2. **True or False:** A token is typically a small device (usually one that can be affixed to a keychain) with a window display.
   Answer: True

3. **True or False:** Cognitive biometrics is considered to be much more difficult for the user to remember.
   Answer: False

4. Authentication that interprets a users physical whereabouts is known as _____.
   Answer:

Quick Quiz

1. A(n) _____ is a secret combination of letters, numbers, and/or characters that only the user should know.
   Answer: password

2. **True or False:** A token is typically a small device (usually one that can be affixed to a keychain) with a window display.
   Answer: True

3. **True or False:** Cognitive biometrics is considered to be much more difficult for the user to remember.
   Answer: False

4. Authentication that interprets a users physical whereabouts is known as _____.
   Answer: Geolocation

Single Sign-On

Single Sign-On

- Identity Management – Using single authentication credential shared across multiple networks
- Federated Identity Management (FIM) – When networks are owned by different organizations
- Single sign-on (SSO) – One application of FIM using one authentication credential to access multiple accounts or applications, e.g.:
  - Microsoft Account
  - OpenID
  - Open Authorization (OAuth)

Single Sign-On

Single Sign-On — Microsoft Account

- Introduced in 1999 as .NET Passport, then name changed to Microsoft Passport Network, then Windows Live ID, now Microsoft Account
- Designed as an SSO for Web commerce but today serves as authentication system for different Microsoft products
- 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

Single Sign-On

Single Sign-On — OpenID

- OpenID – Decentralized open source FIM
- Does not require specific software to be installed on the desktop
- URL-based identity system
- One weakness is it depends on URL identifier routing to correct server, which depends on domain name server (DNS) that may have its own security weaknesses

Single Sign-On

Single Sign-On — Open Authorization (OAuth)

- Open Authorization (Oauth) – Permits users to share resources stored on one site with 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 limited time period

Account Management

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 (see Table 12-4)
  - Account Lockout Policy (see Table 12-5)

Account Management

Attribute	Description	Recommended setting
Enforce password history	Determines the number of unique new passwords a user must use before an old password can be reused (from 0 to 24).	24 new passwords
Maximum password age	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.	90 days
Minimum password age	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.	1 day
Minimum password length	Determines the minimum number of characters a password can have (0–28).	12 characters
Passwords must meet complexity requirements	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 nonalphabetic characters (!, $, #, %).	Enabled
Store passwords using reversible encryption	Provides support for applications that use protocols which require knowledge of the user's password for authentication purposes. An attacker who can circumvent the encryption will be able to log on to the network with these passwords.	Disabled

Table 12-4 Password policy settings (Windows Group Policy)

Account Management

Attribute	Description	Recommended setting	Comments
Account lockout duration	Determines the length of time a locked account remains unavailable before a user can try to log in again (a value of *0* sets account to remain locked out until an administrator manually unlocks it).	15 minutes	Setting this attribute too high may increase help desk calls from users who unintentionally lock themselves out.
Account lockout threshold	Determines the number of failed login attempts before a lockout occurs.	30 invalid attempts	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.
Reset account lockout counter after	Determines the length of time before the account lockout threshold setting resets to zero.	15 minutes	This reset time must be less than or equal to the value for the account lockout duration setting.

Table 12-5 Account lockout policy settings (Windows Active Directory)

Quick Quiz

1. _____ is a decentralized open source Federated Identity Management (FIM) that does not require specific software to be installed on the desktop.
   Answer:

Quick Quiz

1. _____ is a decentralized open source Federated Identity Management (FIM) that does not require specific software to be installed on the desktop.
   Answer: OpenID

Quick Quiz

1. _____ is a decentralized open source Federated Identity Management (FIM) that does not require specific software to be installed on the desktop.
   Answer: OpenID

2. Open Authorization (OAuth) is an open-source service that authenticates a user on multiple sites using _____ credentials.
   Answer:

Quick Quiz

1. _____ is a decentralized open source Federated Identity Management (FIM) that does not require specific software to be installed on the desktop.
   Answer: OpenID

2. Open Authorization (OAuth) is an open-source service that authenticates a user on multiple sites using _____ credentials.
   Answer: token

Quick Quiz

1. _____ is a decentralized open source Federated Identity Management (FIM) that does not require specific software to be installed on the desktop.
   Answer: OpenID

2. Open Authorization (OAuth) is an open-source service that authenticates a user on multiple sites using _____ credentials.
   Answer: token

3. The Active Directory Domain Service policy that can block a login after a specified number of failed logins over a specified time period is named _____.
   Answer:

Quick Quiz

1. _____ is a decentralized open source Federated Identity Management (FIM) that does not require specific software to be installed on the desktop.
   Answer: OpenID

2. Open Authorization (OAuth) is an open-source service that authenticates a user on multiple sites using _____ credentials.
   Answer: token

3. The Active Directory Domain Service policy that can block a login after a specified number of failed logins over a specified time period is named _____.
   Answer: Account Lockout Policy