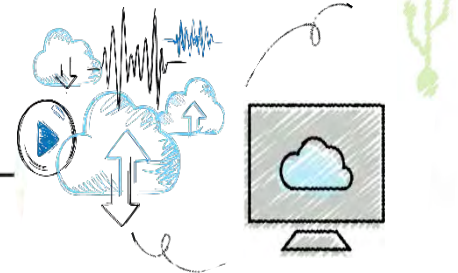
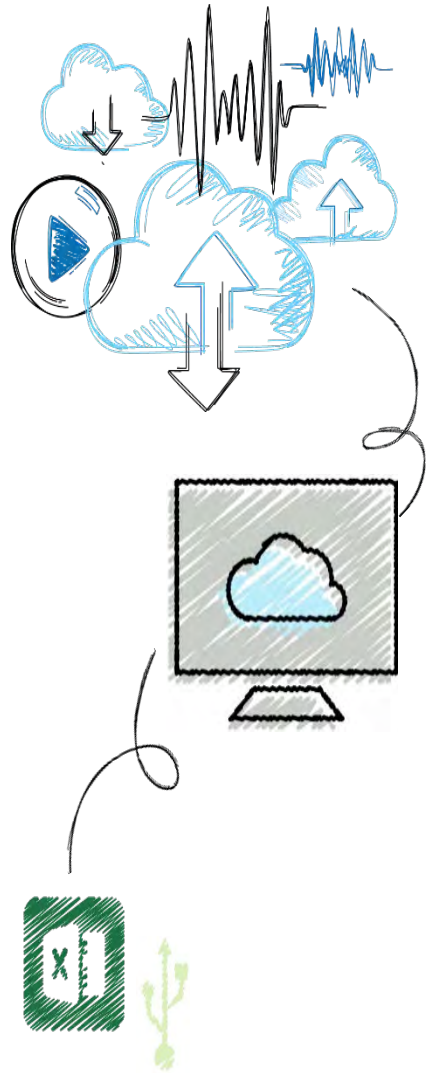


# CompTIA Security+

## Chapter 11

### Authentication and Account Management





## Objectives

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



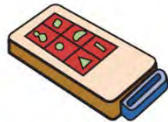
# Authentication Credentials (1 of 2)

- Types of authentication credentials
  - Where you are
    - Example: a military base
  - What you have
    - Example: key fob to lock your car
  - What you are
    - Example: facial characteristics recognized
  - What you know
    - Example: combination to health club locker
  - What you do
    - Example: do something to prove authenticity



# Authentication Credentials (2 of 2)

Key fob (what he has)



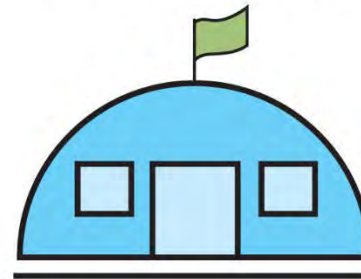
Facial characteristics (what he is)



Combination lock (what he knows)



Military base (where he is)



Pushups (what he does)



**Figure 11-1** Ermanno's authenticity



# 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 the most common type of authentication today
- Passwords provide only weak protection
  - Actions can be taken to strengthen passwords



# Password Weaknesses (1 of 3)

- Weakness of passwords is linked to human memory
  - Humans can memorize only a limited number of items
- Long, complex passwords are most effective
  - Most difficult to memorize
- Users must remember passwords for many different accounts
- Each account password should be unique
- Security policies mandate passwords must expire
  - Users must repeatedly memorize passwords



## Password Weaknesses (2 of 3)

- Users often take shortcuts
  - Using a weak password
    - Examples: common words, short password, or personal information
  - When attempting to create stronger passwords, they generally follow predictable patterns:
    - Appending: using letters, numbers, and punctuation in a pattern
    - Replacing: users use replacements in predictable patterns



# Password Weaknesses (3 of 3)

Top 10 Most Commonly Cracked Passwords [\(According to CNN\)](#)

Rank	Password
1	123456
2	123456789
3	qwerty
4	password
5	111111
6	12345678
7	abc123
8	1234567
9	password1
10	12345





# Attacks on Passwords (1 of 9)

- Attacks that can be used to discover 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



## Attacks on Passwords (2 of 9)

- Offline attack
  - Method used by most password attacks today
  - Attackers steal file of password digests
    - Compare with their own digests they have created
- Offline password attacks include:
  - Brute force
  - Mask
  - Rule
  - Dictionary
  - Rainbow tables
  - Password collections



# Attacks on Passwords (3 of 9)

- Brute force
  - Every possible combination of letters, numbers, and characters used to create encrypted passwords and matched against stolen file
  - Slowest, most thorough method
  - NTLM (New Technology LAN Manager) hash
    - An attacker who can steal the digest of an NTLM password would not need to try to break it
    - He would simply pretend to be the user and send that hash to the remote system to then be authenticated
    - Known as a pass the hash attack



# Attacks on Passwords (4 of 9)

- Mask Attack
  - A more targeted brute force attack that uses placeholders for characters in certain positions of the password
  - Parameters that can be entered in a mask attack include:
    - Password length
    - Character set
    - Language
    - Pattern
    - Skips
- Rule Attack
  - Conducts a statistical analysis on the stolen passwords then is used to create a mask to break the largest number of passwords



# Attacks on Passwords (5 of 9)

```
[*] Length Statistics...
[+]      8: 62% (612522)
[+]      6: 18% (183307)
[+]      7: 14% (146152)
[+]      5: 02% (26438)
[+]      4: 01% (15088)
[+]      3: 00% (2497)
[+]      2: 00% (308)
[+]      1: 00% (113)

[*] Charset statistics...
[+]      loweralphanum: 47% (470580)
[+]      loweralpha: 46% (459208)
[+]      numeric: 05% (56637)
```

**Figure 11-2** Rule attack statistical analysis

```
[*] Advanced Mask statistics...
[+]      ?l?l?l?l?l?l?l?l?l: 04% (688053)
[+]      ?l?l?l?l?l?l?l: 04% (601257)
[+]      ?l?l?l?l?l?l?l?l: 04% (585093)
[+]      ?l?l?l?l?l?l?l?l?l?l: 03% (516862)
[+]      ?d?d?d?d?d?d?d?d: 03% (487437)
[+]      ?d?d?d?d?d?d?d?d?d?d: 03% (478224)
[+]      ?d?d?d?d?d?d?d?d?d: 02% (428306)
[+]      ?l?l?l?l?l?l?l?d?d: 02% (420326)
[+]      ?l?l?l?l?l?l?l?l?l?l: 02% (416961)
[+]      ?d?d?d?d?d?d?d?d: 02% (390546)
[+]      ?d?d?d?d?d?d?d?d?d?d: 02% (307540)
[+]      ?l?l?l?l?l?l?d?d: 02% (292318)
[+]      ?l?l?l?l?l?l?l?l?d?d: 01% (273640)
```

**Figure 11-3** Rule attack generated masks



# Attacks on Passwords (6 of 9)

- Dictionary Attack
  - Attacker creates digests of common dictionary words
  - Compares against stolen digest file
  - Pre-image attack - a dictionary attack that uses a set of dictionary words and compares it with the stolen digests
  - Birthday attack - the search for any two digests that are the same

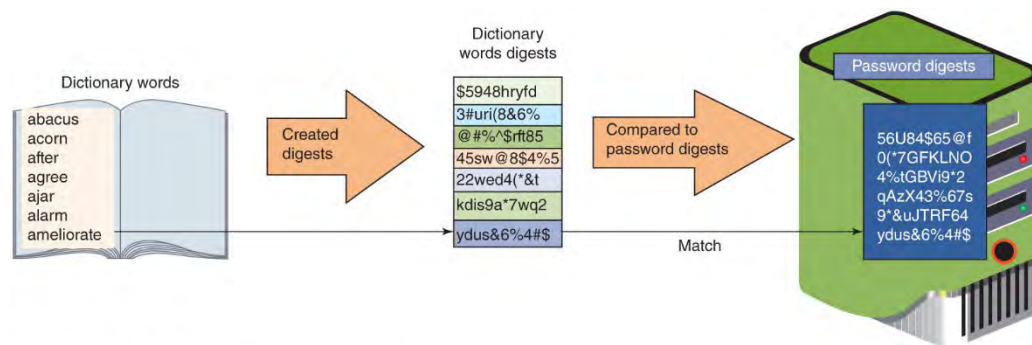


Figure 11-4 Dictionary attack



# Attacks on Passwords (7 of 9)

- Rainbow Tables
  - Creates a large pregenerated data set of candidate digests
- 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 through same procedure used to create initial table
    - Results in initial chain password



## Attacks on Passwords (8 of 9)

- 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 memory on the attacking machine is required





# Attacks on Passwords (9 of 9)

- Password Collections
  - In 2009, an attacker used an SQL injection attack, and more than 32 million user passwords (in cleartext) were stolen
  - These passwords provided two key elements for password attacks:
    - Gave attackers a large collection of real-world passwords
    - Have provided attackers advanced insight into the strategic thinking of how users create passwords



# Password Security (1 of 5)

- Securing passwords from attacks depends upon the user as well as the enterprise
- For the user
  - It involves properly managing passwords
- For the enterprise
  - It involves protecting password digests



## Password Security (2 of 5)

- Managing Passwords
  - Most critical factor in a strong password is length
  - In addition to having long passwords, other recommendations are:
    - Do not use passwords that consist of dictionary words or phonetic words
    - Do not repeat characters or use sequences
    - Do not use birthdays, family member names, pet names, addresses, or any personal information
  - Also, use non-keyboard characters
    - Created by holding down the ALT key while typing a number on the numeric keypad



# Password Security (3 of 5)



Figure 11-5 Windows character map



# Password Security (4 of 5)

- Password managers
    - Technology used for securing passwords
    - Three basic types of password manager:
      - Password generators
      - Online vaults
      - Password management applications
  - Protecting Password Digests
    - One method is to use salts
      - Consists of a random string that is used in hash algorithms
      - Passwords can be protected by adding a random strong to the user's cleartext password before it is hashed
      - Make dictionary attacks and brute force attacks much slower and limit the impact of rainbow tables
-



# Password Security (5 of 5)

- Protecting Password Digests (continued)
  - Another method is to use key stretching
    - A specialized password hash algorithm that is intentionally designed to be slower
    - Two key stretching algorithms: bcrypt and PBKDF2
- Recommendation for enterprises using salts and key stretching:
  - Use a strong random number generator to create a salt of at least 128 bits
  - Input the salt and the user's plaintext password into the PBKDF2 algorithm that is using HMAC-SHA-256 as the core hash
  - Perform at least 30,000 iterations on PBKDF2
  - Capture the first 256 bits of output from PBKDF2 as the password digest
  - Store the iteration count, the salt, and the password digest in a secure password database



# What You Have: Tokens, Cards, and Cell Phones

- Multifactor authentication
  - When a user is using more than one type of authentication credential
  - Example: what a user knows and what a user has could be used together for authentication
- Single-factor authentication
  - Using just one type of authentication
- Most common items used for authentication:
  - Tokens, cards, and cell phones



# Tokens (1 of 3)

- Tokens
  - Used to create a one-time password (OTP)
    - Authentication code that can be used only once or for a limited period of time
  - Hardware security token
    - Typically a small device with a window display
  - Software security token
    - Stored on a general-purpose device like a laptop computer or smartphone
- Two types of OTPs
  - Time-based one-time password (TOTP)
    - Synched with an authentication server
    - Code is generated from an algorithm
    - Code changes every 30 to 60 seconds





## Tokens (2 of 3)

- Two types of OTPs (continued)
  - HMAC-based one-time password (HOTP)
    - “Event-driven” and changes when a specific event occurs
- Advantages over passwords
  - Token code changes frequently
    - Attacker would have to crack code within time limit
  - User may not know if password has been stolen
    - If token is stolen, it becomes obvious and steps could be taken to disable account



# Tokens (3 of 3)

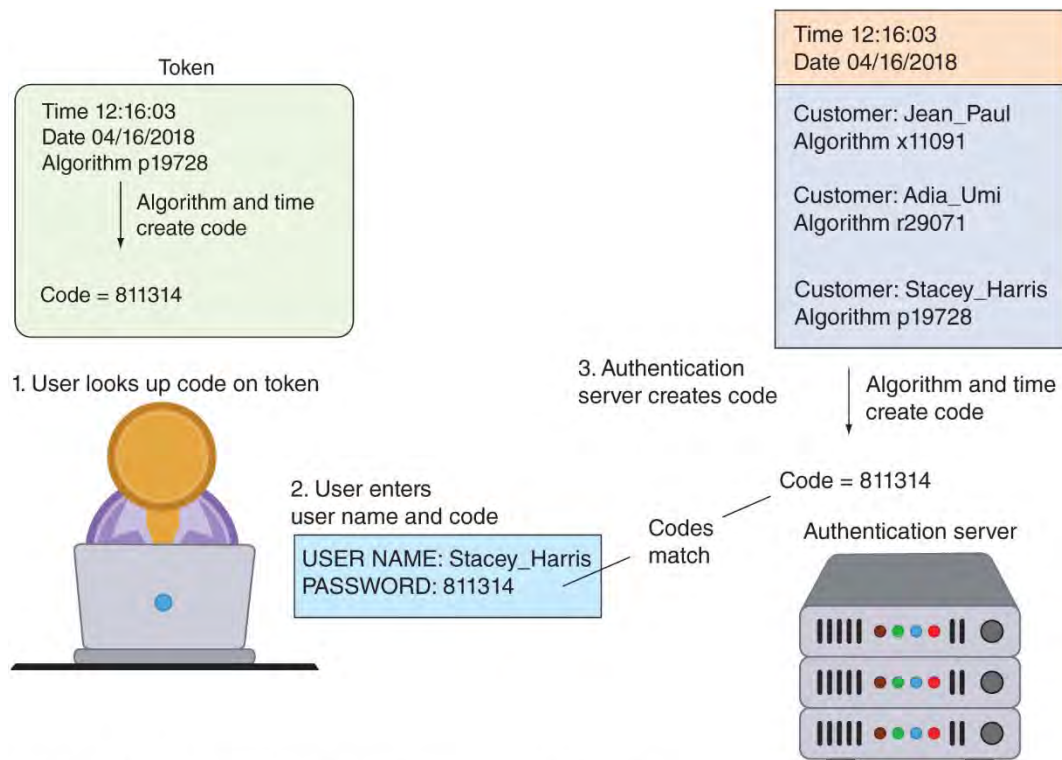


Figure 11-7 Time-based one-time password (TOTP)



## Cards (1 of 2)

- Smart card contains integrated circuit chip that holds information and can be either:
  - Contact card – a “pad” that allows electronic access to chip contents
  - Contactless cards (proximity 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
- The smart card standard covering all U.S. government employees is the Personal Identity Verification (PIV) standard



## Cards (2 of 2)

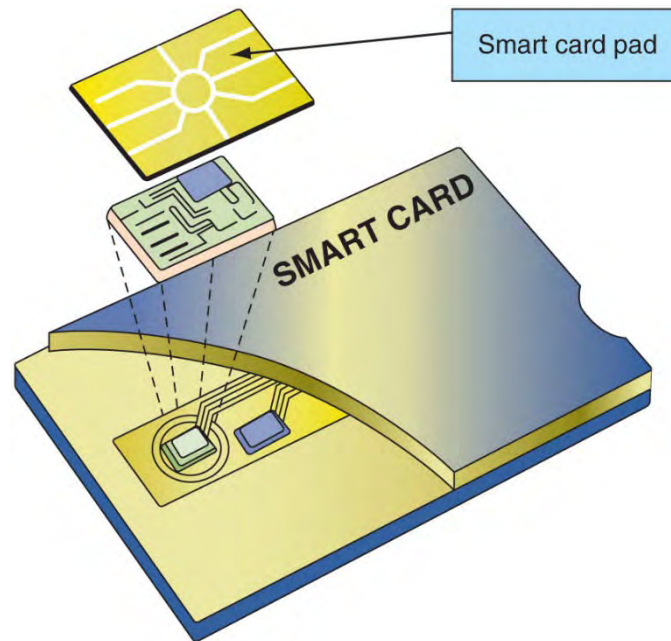


Figure 11-8 Smart card



# Cell Phones

- Cell Phones are increasingly replacing tokens and cards
  - A code can be sent to a user's cell phone through an app on the device
  - Allow a user to send a request via the phone to receive an HOTP authorization code



# What You Are: Biometrics

- “Something you are” biometrics involves:
  - Standard biometrics
  - Cognitive biometrics

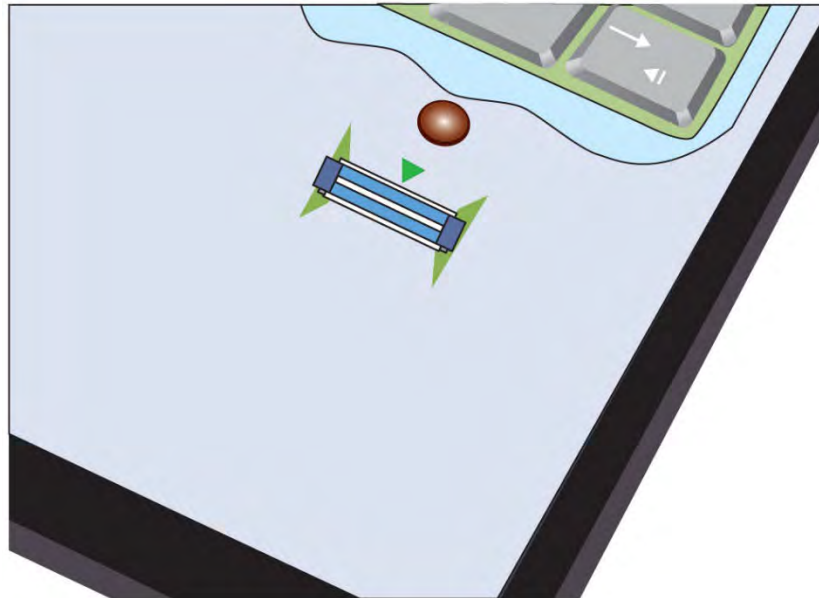


# Standard Biometrics (1 of 4)

- Standard biometrics
  - Uses a person's unique physical characteristics for authentication
  - Face, hand, or eye characteristics are used to authenticate
- Specialized Biometric Scanners
  - Retinal scanner uses the human retina as a biometric identifier
    - Maps the unique patterns of a retina by directing a beam of low-energy infrared light (IR) into a person's eye
  - Fingerprint scanner types
    - Static fingerprint scanner - takes a picture and compares with image on file
    - Dynamic fingerprint scanner - uses small slit or opening



## Standard Biometrics (2 of 4)



**Figure 11-9** Dynamic fingerprint scanner





# Standard Biometrics (3 of 4)

- Standard Input Devices
  - Voice recognition uses a standard computer microphone to identify users based on the unique characteristics of a person's voice
  - Iris scanner uses a standard webcam to identify the unique characteristics of the iris
  - Facial recognition uses landmarks called nodal points on human faces for authentication



**Figure 11-10** Iris  
*creativemarc/Shutterstock.com*



# Standard Biometrics (4 of 4)

- Biometric Disadvantages
  - Cost of hardware scanning devices
  - Readers have some amount of error
    - Reject authorized users
    - Accept unauthorized users
  - Biometric systems can be “tricked”

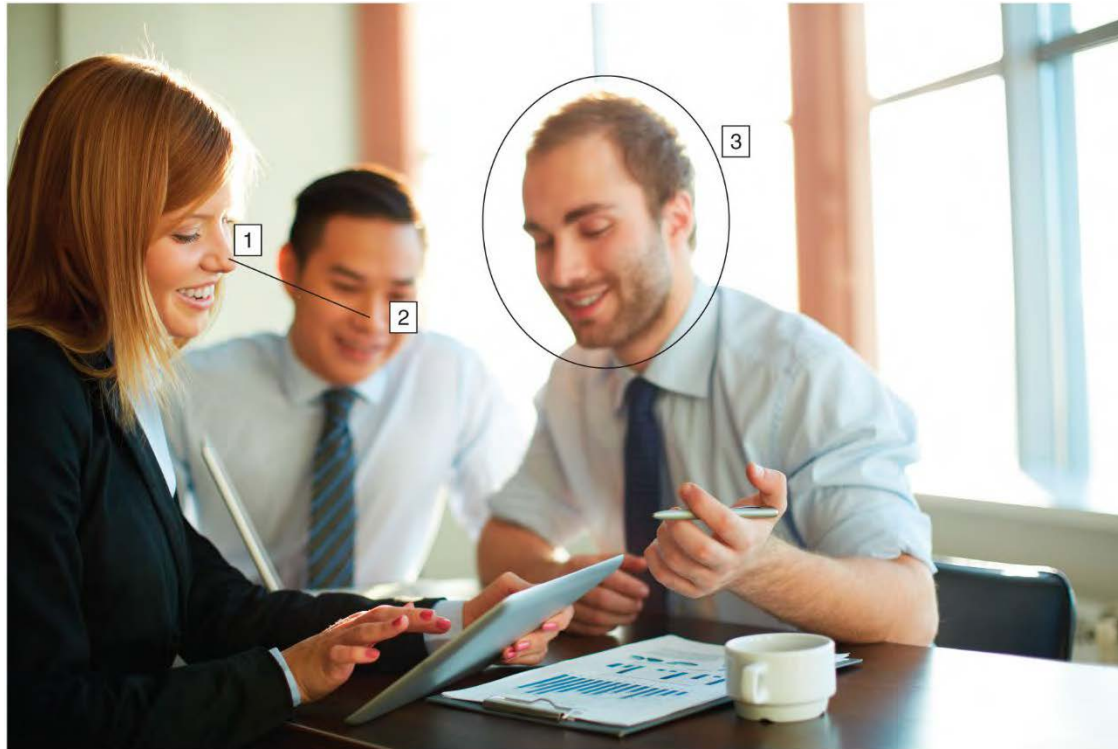


# Cognitive Biometrics (1 of 2)

- Cognitive biometrics
    - Relates to perception, thought process, and understanding of the user
    - Easier for user to remember because it is based on user's life experiences
    - Difficult for an attacker to imitate
  - Picture password
    - Introduced by Windows
    - Users select a picture to use for which there should be at least 10 "points of interest" that could serve as "landmarks" or places to touch
  - Other examples of cognitive biometrics:
    - Requires user to identify specific faces
    - User selects one of several "memorable events"
-



# Cognitive Biometrics (2 of 2)



**Figure 11-11** Picture password authentication

*Pressmaster/Shutterstock.com*

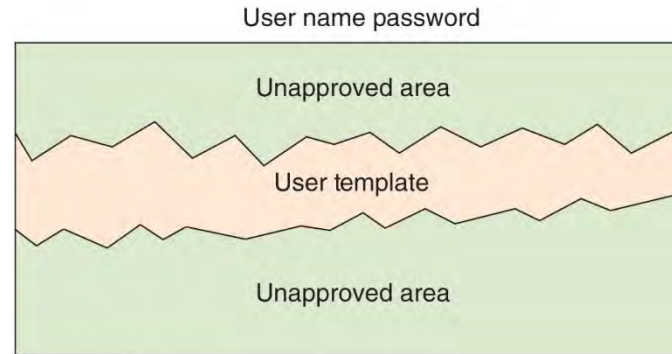


# What You Do: Behavioral Biometrics (1 of 2)

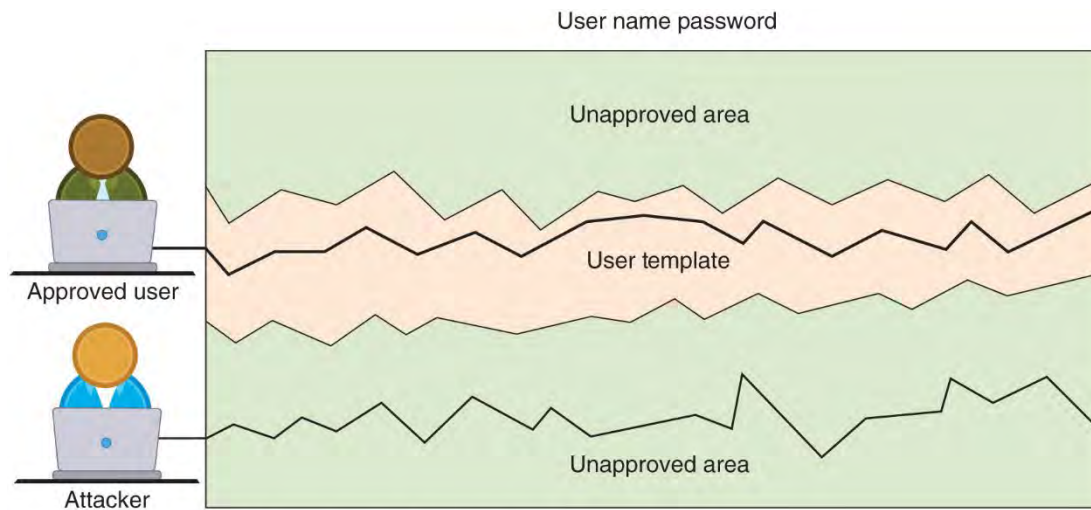
- Behavioral biometrics
  - Authenticates by normal actions the user performs
- Keystroke dynamics
  - Attempts to recognize user's typing rhythm
    - All users type at a different pace
    - Provides up to 98 percent accuracy
  - Uses two unique typing variables
    - Dwell time (time it takes to press and release a key)
    - Flight time (time between keystrokes)
  - Holds a great amount of potential
    - It requires no specialized hardware



# What You Do: Behavioral Biometrics (2 of 2)



**Figure 11-12** Typing template



**Figure 11-13** Authentication by keystroke dynamics



# Where You Are: Geolocation

- Geolocation
  - The identification of the location of a person or object using technology
- Used most often to reject imposters instead of accepting authorized users
  - Can indicate if an attacker is trying to perform a malicious action from a location different from the normal location of the user
  - Many websites will not allow a user to access an account if the computer is located in a different state
  - Some websites may require a second type of authentication
    - A code sent as a text message to a cell phone number on file



# Single Sign-on

- Identity management
  - Using a single authentication credential shared across multiple networks
  - It is 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
- Examples of popular SSOs:
  - OAuth, Open ID Connect, and Shibboleth





# Account Management (1 of 2)

- 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 (group policy)
  - Microsoft Windows group password settings
    - Password Policy Settings
    - Account Lockout Policy



## Account Management (2 of 2)

- Other steps to take:
  - A shared account, a generic account, and a guest account should be prohibited
  - Closely monitor any privileged accounts
  - Disable account passwords instead of deleting accounts no longer being used
  - Create strict policies regarding password recovery
- Transitive trust
  - A two-way relationship that is automatically created between parent and child domains in a Microsoft Active Directory Forest
  - When a new domain is created, it shares resources with its parent domain by default
    - Can enable an authenticated user to access resources in both the child and the parent



# Review Questions

Which of these is NOT a characteristic of a weak password?

- A. A common dictionary word
- B. A length of 15 or more
- C. Using personal information
- D. Using a predictable sequence of characters



# Review Questions

Which of these is NOT a characteristic of a weak password?

- A. A common dictionary word
- B. **A length of 15 or more**
- C. Using personal information
- D. Using a predictable sequence of characters



## Review Questions

What is a token system that requires the user to enter the code along with a PIN called?

- A. Single-factor authentication system
- B. Token-passing authentication system
- C. Dual-prong verification system
- D. Multifactor authentication system



## Review Questions

What is a token system that requires the user to enter the code along with a PIN called?

- A. Single-factor authentication system
- B. Token-passing authentication system
- C. Dual-prong verification system
- D. **Multifactor authentication system**



# Review Questions

Which human characteristic is NOT used for biometric identification?

- A. Retina
- B. Iris
- C. Height
- D. Fingerprint



# Review Questions

Which human characteristic is NOT used for biometric identification?

- A. Retina
- B. Iris
- C. **Height**
- D. Fingerprint





## Review Questions

Why should the account lockout threshold not be set too low?

- A. It could decrease calls to the help desk.
- B. The network administrator would have to reset the account manually.
- C. The user would not have to wait too long to have her password reset.
- D. It could result in denial of service (DoS) attacks.



## Review Questions

Why should the account lockout threshold not be set too low?

- A. It could decrease calls to the help desk.
- B. The network administrator would have to reset the account manually.
- C. The user would not have to wait too long to have her password reset.
- D. **It could result in denial of service (DoS) attacks.**

# Coming Up Next...

## CompTIA Security+

### Chapter 12

#### Access Management

