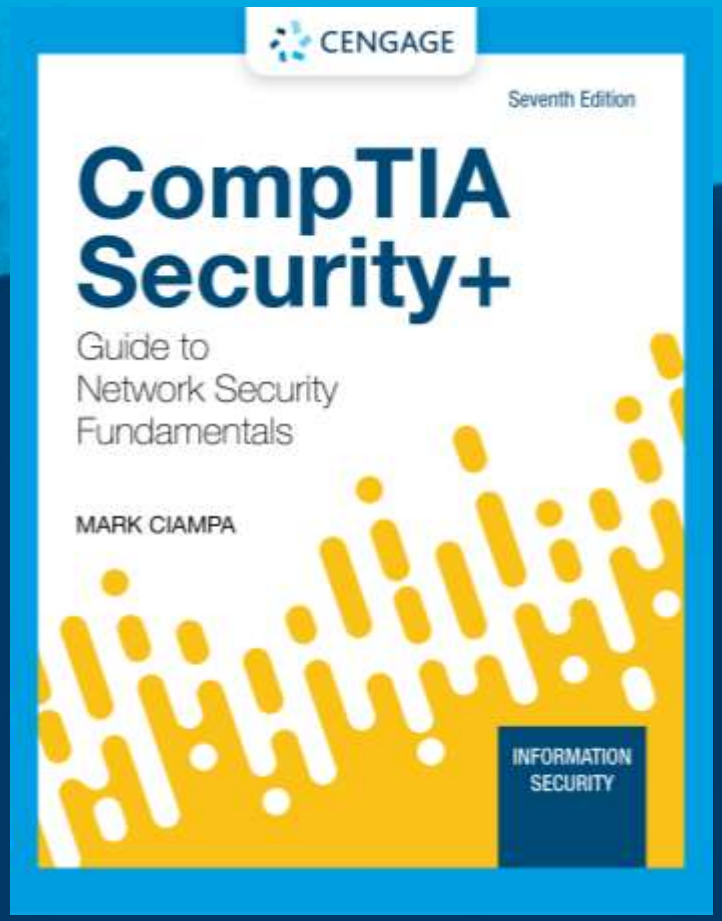

CompTIA Security+ Guide to Network Security Fundamentals, 7th Edition

Module 12: Authentication

CENGAGE

Module Objectives

By the end of this module, you should be able to:

1. Describe the different types of authentication credentials

2. Explain the different attacks on authentication

3. Describe how to implement authentication security solutions

Types of Authentication Credentials

Element	Description	Scenario example
Somewhere you are	Restricted location	Restricted military base
Something you are	Unique biological characteristic that cannot be changed	Fingerprint reader to enter building
Something you have	Possession of an item that nobody else has	Riker's RFID card
Someone you know	Validated by another person	Li knows Peyton
Something you exhibit	Genetically determined characteristic	Peyton's flaming red hair
Something you can do	Perform an activity that cannot be exactly copied	Paolo's signature
Something you know	Knowledge that nobody else possesses	Combination to unlock locker

Something You Know: Passwords (1 of 9)

- **Passwords** are the most common type of IT authentication today
- Passwords provide only weak protection and are constantly under attack
- Password Weaknesses
  - Weakness of passwords is linked to human memory
    - Humans can memorize only a limited number of items
  - Long, complex passwords are most effective
    - But they are the most difficult to memorize
  - Users must remember passwords for many different accounts
  - Each account password should be unique
  - Many security policies mandate that passwords must expire
    - Users must repeatedly memorize passwords

Something You Know: Passwords (2 of 9)

- Password Weaknesses (continued)
  - Users often take shortcuts and use a *weak password*
    - Examples: common words, short password, a predictable sequence of characters 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

Something You Know: Passwords (3 of 9)

- Attacks on Passwords
  - When users create passwords, a one-way hash algorithm creates a message digest (or hash) of the password
  - Attackers work to steal the file of password digests
    - They can then use a stolen has to impersonate the user
    - They can also load that file onto their own computers and then use a sophisticated **password cracker**, which is software designed to break passwords
  - Password crackers create known digests called *candidates*
  - The different means of creating candidates include:
    - Brute force, rule, dictionary, rainbow tables, and password collections

Something You Know: Passwords (4 of 9)

- Password Spraying
  - A **password spraying** attack selects one or a few common passwords and then enters the same password when trying to login to several user accounts
- Brute Force Attack
  - In an **automated brute force attack**, every possible combination of letters, numbers, and characters used to create encrypted passwords are matched against the stolen hash file
  - In an **online brute force attack**, the same account is continuously attacked (called *pounded*) by entering different passwords
  - An **offline brute force attacks** uses the stolen hash file
    - This is the slowest yet most thorough method

Something You Know: Passwords (5 of 9)

- Rule Attack
  - A *rule attack* conducts a statistical analysis on the stolen passwords that is used to create a mask to break the largest number of passwords
  - There are three basic steps in a rule attacks:
    - 1. A small sample of the stolen password plaintext file is obtained
    - 2. Statistical analysis is performed on the sample to determine the length and character sets of the passwords
    - 3. A series of masks is generated that will be most successful in cracking the highest percentage of passwords

Something You Know: Passwords (6 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 12-1 Rule attack statistical analysis

Something You Know: Passwords (7 of 9)

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

Figure 12-2 Rule attack generated masks

Something You Know: Passwords (8 of 9)

- Dictionary Attack
  - In a **dictionary attack**, the attacker creates digests of common dictionary words and compares against a stolen digest file
  - *Pre-image attack* is a dictionary attack that uses a set of dictionary words and compares it with the stolen digests
  - *Birthday attack* is the search for any two digests that are the same
- Rainbow Tables
  - **Rainbow tables** create a large pregenerated data set of candidate digests
  - Rainbow table advantages over other attack methods
    - Can be used repeatedly
    - Faster than dictionary attacks
    - Less memory on the attacking machine is required

Something You Know: 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 gave attackers a large corpus of real-world passwords
  - Using stolen password collections as candidate passwords is the foundation of password cracking today
    - Almost all password cracking software tools accept these stolen “wordlists” as input

Something You Have: Smartphone and Security Keys (1 of 5)

- **Multifactor authentication** (**MFA**) is a type of authentication where 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* occurs when a user is using just one type of authentication
- Using two types is called *two-factor authentication* (*2FA*)
- Most common items used for authentication are specialized devices, smartphones, and security keys

Something You Have: Smartphone and Security Keys (2 of 5)

- Specialized Devices
  - A **smart card** holds information to be used as part of the authentication process
  - A *common access card* (*CAC*) that is issued by US Department of Defense
    - In addition to integrated chip, it has a bar code, magnetic strip, and the bearer's picture
  - There are several disadvantages to smart cards such as the following:
    - Each device that uses smart card authentication must have a specialized hardware reader and device driver software installed
    - Smart cards that have a magnetic strip are subject to unauthorized duplication called **card cloning**
      - Stealing the information is often done by a process called **skimming**

Something You Have: Smartphone and Security Keys (3 of 5)

- Specialized Devices (continued)
  - Windowed tokens create a one-time password (OTP) which is an authentication code that can be used only once or for a limited period of time
  - There are two types of OTPs
    - Time-based one-time password (TOTP)
      - Synched with an authentication server where the code is generated from an algorithm
      - The code changes every 30 to 60 seconds
    - HMAC-based one-time password (HOTP) is “event-driven” and changes when a specific event occurs

Something You Have: Smartphone and Security Keys (4 of 5)

- Smartphones
  - Once users enter their username and password, their smartphone is then used for the second authentication factor using one of the following methods:
    - A phone call
    - SMS text message
    - Authentication app
  - Using a smartphone for authentication is not considered secure
    - An OTP received through an SMS text message can be “phished”
    - A malware infection on the phone can target the authentication app

Something You Have: Smartphone and Security Keys (5 of 5)

- Security Keys
  - A security key is a dongle that is inserted into the USB port or Lightning port or held near the endpoint
  - A feature of security keys is **attestation**
    - Attestation is a key pair that is “burned” into the security key during manufacturing and is specific to a device model
  - Attestation keys have associated attestation certificates and those certificates chain to a root certificate that the service trusts
  - Some security key systems require that users must initially enroll two security keys in the event that one is lost or destroyed

Something You Are: Biometrics (1 of 6)

- Physiological Biometrics
  - *Physiological biometrics* uses a person's unique physical characteristics for authentication
  - Several unique characteristics of a person's body can used to authenticate
- Specialized Biometric Scanners
  - Retinal scanner uses the human retina as a biometric identifier
    - It maps the unique patterns of a retina by directing a beam of low-energy infrared light (IR) into a person's eye
  - There are two basic types of fingerprint scanners:
    - *Static fingerprint scanner* takes a picture and compares with image on file
    - *Dynamic fingerprint scanner* uses a small slit or opening

Something You Are: Biometrics (2 of 6)

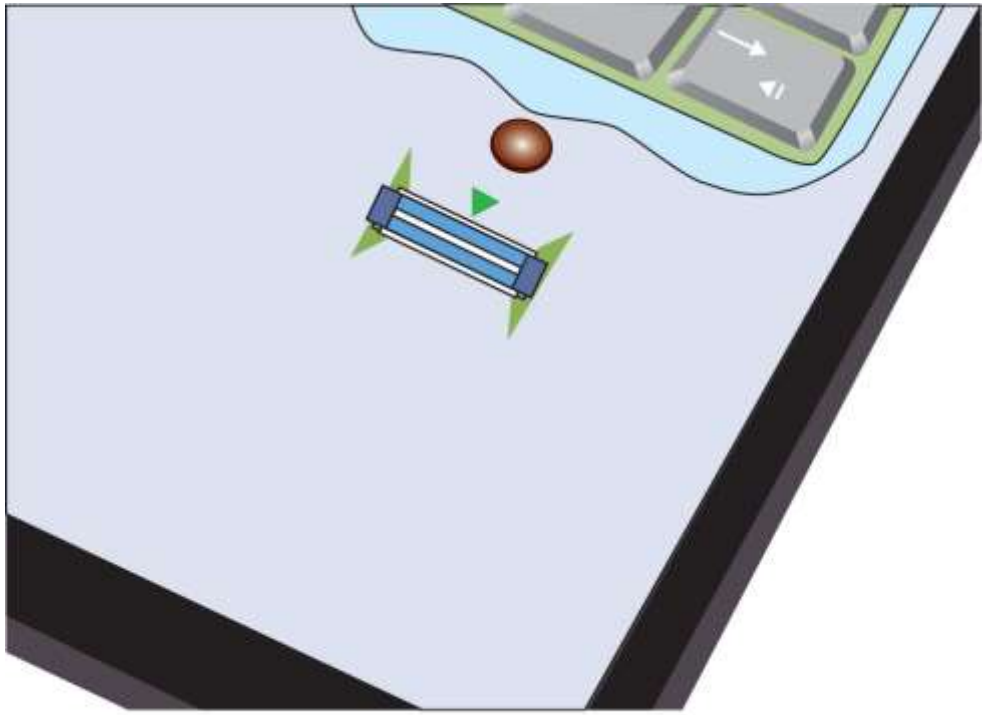

Figure 12-8 Dynamic fingerprint scanner

Figure 12-8 Dynamic fingerprint scanner

Something You Are: Biometrics (3 of 6)

- Other human characteristics that can be used for authentication include:
  - A person's vein can be identified through a vein-scanning tablet
  - A person's gait or manner of walking
- Standard Input Devices
  - **Voice recognition** uses a standard computer microphone to identify users based on the unique characteristics of a person's voice
  - An **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

Something You Are: Biometrics (4 of 6)

Figure 12-9 Iris

Figure 12-9 Iris

Something You Are: Biometrics (5 of 6)

- Biometric Disadvantages
  - Cost of specialized hardware scanning devices
  - Readers have some amount of error
    - The false acceptance rate (FAR) is the frequency at which imposters are accepted as genuine
    - The false rejection rate (FRR) is the frequency that legitimate users are rejected
  - Biometric systems can be “tricked”
  - A concern with biometrics is the efficacy rate
    - Efficacy may be defined as the benefit achieved
    - Critics question the sacrifice of user privacy

Something You Are: Biometrics (6 of 6)

- Cognitive Biometrics
  - *Cognitive biometrics* relates to perception, thought process, and understanding of the user
  - It is considered easier for the user to remember because it is based on user's life experiences
  - Cognitive biometrics is also called **knowledge-based authentication**
  - Picture Password was introduced by Microsoft for Windows 10 touch-enabled devices
    - 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

Something You Do: Behavioral Biometrics

- Behavioral biometrics
  - *Behavioral biometrics* authenticates by normal actions the user performs
  - A type of behavioral biometrics is *keystroke dynamics*
    - Attempts to recognize user's typing rhythm
  - Keystroke dynamics uses two unique typing variables
    - *Dwell time*, which is the time it takes to press and release a key
    - *Flight time* is the time between keystrokes
  - Keystroke dynamics holds a great amount of potential because it requires no specialized hardware

Knowledge Check Activity 1

What process can be done on smart cards that steals the information contained on them?

a. Skimming
b. Injection
c. Spraying
d. Cracking

Knowledge Check Activity 1: Answer

What process can be done on smart cards that steals the information contained in them?

Answer: a. Skimming

Skimming is a process in which a threat actor attaches a small device that fits inside a card reader that reads the card when it is inserted and removed from the reader.

Authentication Solutions

- Several solutions for securing authentication include the following:
  - Security surrounding passwords
  - Secure authentication technologies

Password Security (1 of 4)

- Protecting Password Digests
  - One method is to use **salts**, which 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
    - Salts make dictionary attacks and brute force attacks much slower and limit the impact of rainbow tables
  - Another method is to use **key stretching**
    - Key stretching is a specialized password hash algorithm that is intentionally designed to be slower
    - Two key stretching algorithms: **brypt** and **PBKDF2**

Password Security (2 of 4)

- Managing Passwords
  - The most critical factor in a strong password is length
  - The longer a password is, the more attempts an attacker must make to break it
  - Due to the limitations of human memory, security experts universally recommend using technology to store and manage passwords
  - Technology used for securing passwords includes using the following:
    - Password vaults
    - Password keys
    - Hardware modules

Password Security (3 of 4)

- Managing Passwords (continued)
  - A **password vault** is a secure repository where users can store passwords (also known as a *password manager*)
  - Three basic types of password vaults:
    - *Password generators*
    - *Online vaults*
    - *Password management applications*
  - **Password keys** are a secure hardware-based solution to store passwords
  - A **hardware security module** (**HSM**) is a removable external cryptographic device that includes an onboard random number generator and key storage facility
    - An HSM can also perform encryption and can back up sensitive material in an encrypted form

Password Security (4 of 4)

Source: OnlyKey

Figure 12-12 Password key

Figure 12-12 Password key

Secure Authentication Technologies (1 of 8)

- Single Sign-On
  - *Identity management* is using a single authentication credential shared across multiple networks
  - It is called **federation** (sometimes called *federated identity management* or *FIM*) when networks are owned by different organizations
  - Single sign-on (SSO) uses one authentication credential to access multiple accounts or applications

Secure Authentication Technologies (2 of 8)

- Authentication Services
  - Different services can be used to provide authentication
- RADIUS or Remote Authentication Dial In User Service was developed in 1992 and became an industry standard
  - RADIUS was originally designed for remote dial-in access to a corporate network
  - RADIUS client is typically a device such as a wireless AP that is responsible for sending user credentials and connection parameters to the RADIUS server
  - RADIUS user profiles are stored in a central database that all remote servers can share
  - Advantages of a central service include the following:
    - Increases security due to a single administered network point
    - Easier to track usage for billing and keeping network statistics

Secure Authentication Technologies (3 of 8)

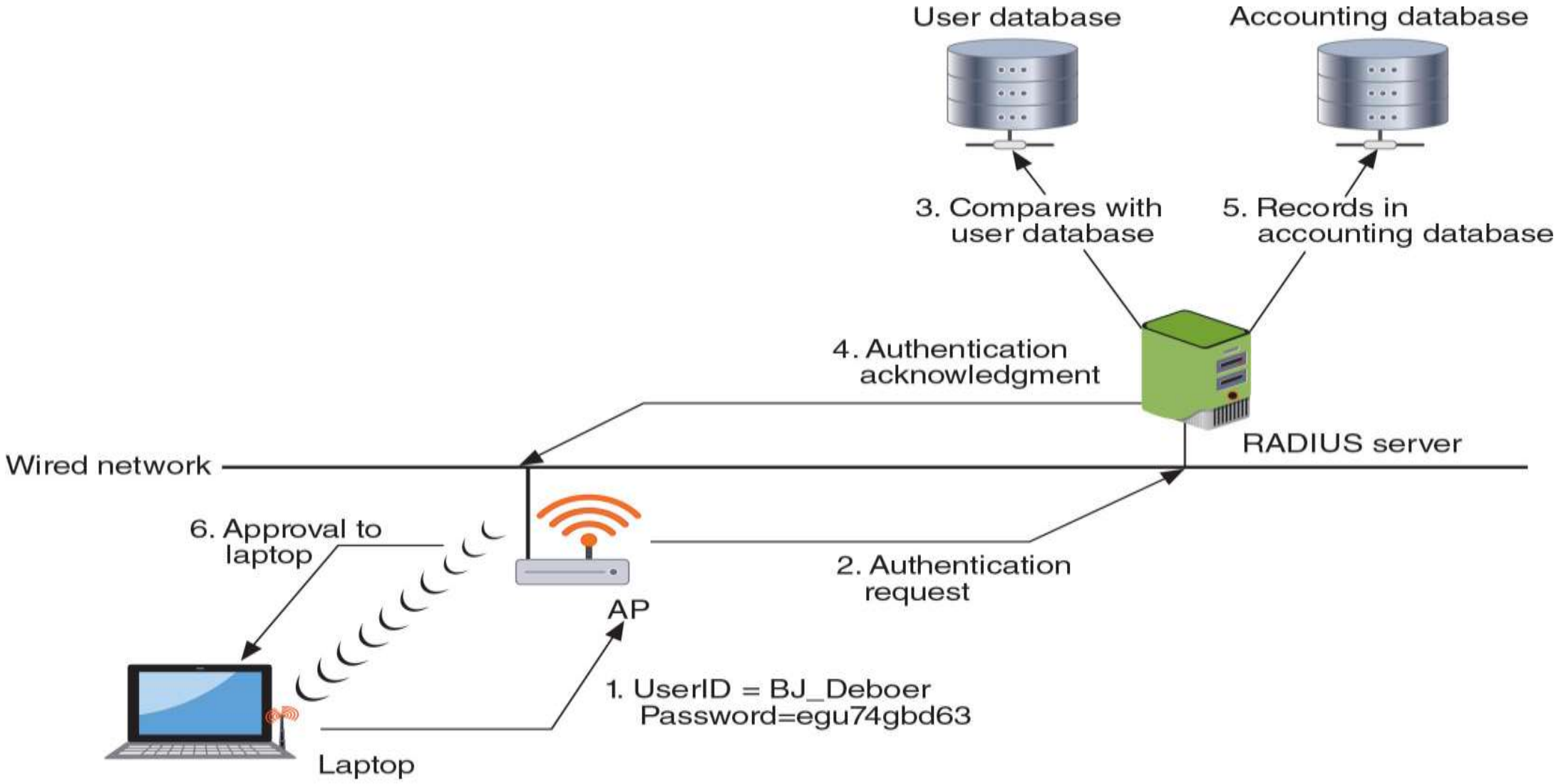

Figure 12-13 RADIUS authentication

Secure Authentication Technologies (4 of 8)

- **Kerberos** is an authentication system developed at MIT
  - It uses encryption and authentication for security
  - Works like using a driver's license to cash a check
  - Kerberos ticket characteristics:
    - Difficult to copy
    - Contains information linking it to the user
    - It lists restrictions
    - Expires at some future date
  - Kerberos is typically used when a user attempts to access a network service and that service requires authentication

Secure Authentication Technologies (5 of 8)

- Terminal Access Control Access Control System + (TACACS+)
  - *TACACS* is an authentication service similar to RADIUS
  - It is commonly used on UNIX devices that communicates by forwarding user authentication information to a centralized server
  - The current version is TACACS+

Secure Authentication Technologies (6 of 8)

- Directory Service
  - A **directory service** is a database stored on the network that contains information about users and network devices
  - Directory services make it easier to grant privileges or permissions to network users and provide authentication
- SAML
  - **Security Assertion Markup Language** (**SAML**) is an XML standard that allows secure web domains to exchange user authentication and authorization data
  - SAML allows a user's login credentials to be stored with a single identity provider instead of being stored on each web service provider's server
  - SAML is used extensively for online e-commerce business-to-business (B2B) and business-to-customer (B2C) transactions

Secure Authentication Technologies (7 of 8)

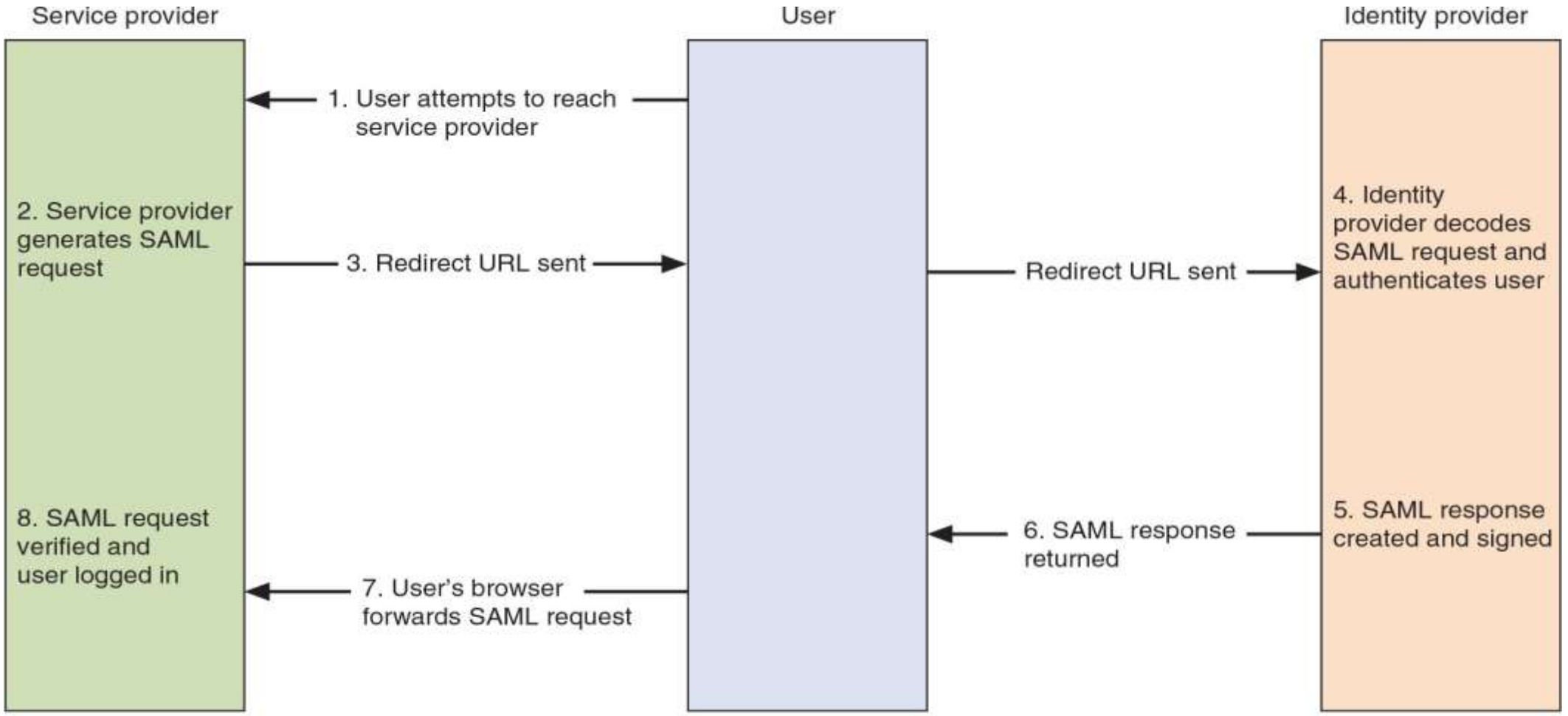

Figure 12-14 SAML transaction

Secure Authentication Technologies (8 of 8)

- Authentication Framework Protocols
  - A framework for transporting authentication protocols is known as the Extensible Authentication Protocol (EAP)
  - EAP was created as a more secure alternative to **Challenge-Handshake Authentication Protocol (CHAP),** the Microsoft version of CHAP **(MS-CHAP),** and **Password Authentication Protocol (PAP)**
  - EAP is a framework for transporting authentication protocols instead of the authentication protocol itself
  - EAP defines the format of the messages and uses four types of packets:
    - *Request, response, success, and failure*

Knowledge Check Activity 2

Which standard allows secure web domains to exchange user authentication and authorization data?

a. LDAP
b. SAML
c. MS-CHAP
d. TACACS

Knowledge Check Activity 2: Answer

Which standard allows secure web domains to exchange user authentication and authorization data?

Answer: b. SAML

Security Assertion Markup Language (SAML) is an XML standard that allows secure web domains to exchange user authentication and authorization data.

Self-Assessment

One of the ways to help remember technical information is to relate where and how a technology is implemented. If possible, ask an IT professional at your school or your place of work which of the authentication technologies are being used in the school's or workplace's network. As the person why that particular technology was chosen and relate the information you learned back to the contents of this module.

Summary (1 of 2)

- Authentication credentials can be classified into five categories: what you know, what you have, what you are, what you do, and where you are
- Passwords provide a weak degree of protection because they rely on human memory
- Most password attacks today use offline attacks where attackers steal encrypted password file
- A dictionary attack begins with the attacker creating digests of common dictionary words, which are compared with those in a stolen password file
- Another type of authentication credential is based on the approved user having a specific item in her possession
  - A hardware token is a small device that generates a code from an algorithm once every 30 to 60 seconds

Summary (2 of 2)

- Biometrics bases authentication on characteristics of an individual
  - Standard and cognitive biometrics are examples
- Behavioral biometrics authenticates by normal actions the user performs
- One way for an enterprise to protect stored digests is to add a salt, which consists of a random string that is used in hash algorithms
- Single sign-on (SSO) allows a single username and password to gain access to all accounts
- Different services can be used to provide authentication