



The image shows the cover of the book "CompTIA Security+ Guide to Network Security Fundamentals, Seventh Edition" by Mark Ciampa. The cover is white with a blue header and a yellow and orange abstract pattern at the bottom. The Cengage logo is in the top left corner.




A cluster of icons representing network security, including a cloud with a lock, a server, and a network diagram.

Module 12: Authentication



A decorative graphic consisting of overlapping colored squares (yellow, red, blue) and a black crosshair.

Module Objectives



A cluster of icons representing network security, including a cloud with a lock, a server, and a network diagram.

- By the end of this module, you should be able to:
 - Describe the different types of authentication credentials
 - Explain the different attacks on authentication
 - Describe how to implement authentication security solutions

2



Defining Access Control

■ Access Control

- The process of protecting a resource so that it is used only by those allowed to prevents unauthorized use
- Mitigations put into place to protect a resource from a threat

3 3



Identification

■ Identification

- The process of ascribing a computer ID to a specific user, computer, or network device.
- Usually takes the form of a unique logon ID or userid.
 - Links the logon ID or user ID to previously assigned credentials.
- User identification enables **authentication and authorization** – the basis for **accountability**.
 - Accountability traces activities to individual users or computer processes.
 - **establishes responsibility for actions.**

4 4



Establishing Proper Privileges

- **To establish proper privileges, three steps are used (AAA):**

- **Authentication**

- Matches user-supplied credentials to stored credentials – usually done with an account name and a password.

- **Authorization**

- Grants specific permissions based on the privileges held by the account.

- **Accounting**

- Keep detailed security logs to maintain an audit trail of tasks being performed.

Authentication and Authorization are often confused with each other, **but they are different**

5



Four Parts of Access Control

Access Control Component	Description
Identification	Who is asking to access the asset?
Authentication	Can their identities be verified?
Authorization	What, exactly, can the requestor access? And what can they do?
Accountability	How are actions traced to an individual to ensure the person who makes data or system changes can be identified?

6



Something You Know: Passwords



■ Passwords

- The most common type of IT authentication today
- 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

7



Something You Know: Passwords



■ 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

8

Password Defenses

▶ Good password management practices

- Change passwords frequently
- Do not reuse old passwords
- Never write password down
- Use unique passwords for each account
- Do not allow computer to automatically sign in to an account
- Avoid entering passwords on public access computers
- Do not enter a password while connected to an unencrypted wireless network



9

Something You Know: Passwords



■ 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

10



Something You Know: Passwords



■ 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

11



Something You Know: Passwords



■ Rule Attack

- One of the most complicated of all the attack modes.
- Conducts a statistical analysis on the stolen passwords that is used to create a mask to break the largest number of passwords
- It has functions to modify, cut or extend words and has conditional operators to skip some, etc. That makes it the most flexible, accurate and efficient attack.
- 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

12

Something You Know: Passwords



■ 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

13

Something You Know: Passwords



■ 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

14

Something You Have: Smartphone and Security Keys

■ Multifactor authentication (MFA)

- 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

- When a user is using just one type of authentication

■ Two-factor authentication (2FA)

- Using two types is called
- Most common items used for authentication are
 - Specialized devices
 - smartphones

15

Something You Have: Smartphone and Security Keys

■ 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
- 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**

16

Something You Have: Smartphone and Security Keys

■ 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
- 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
 - Hash-based message authentication codes (HMAC)-based one-time password (HOTP)
 - “Event-driven” and changes when a specific event occurs
 - Each time the HOTP is requested and validated, the moving factor is incremented based on a counter.
 - The code that’s generated is valid until you actively request another one and it’s validated by the authentication server.

17

Something You Have: Smartphone and Security Key

■ 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

18



Something You Have: Smartphone and Security Keys



■ 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

19



Something You Are: Biometrics



■ Physiological Biometrics

- *Physiological biometrics* uses a person's unique physical characteristics for authentication
- Several unique characteristics of a person's body can be 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

20



Something You Are: Biometrics



- 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

:21



Something You Are: Biometrics



- **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

:22



Something You Are: Biometrics



■ 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

:23



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

:24



Authentication Solutions



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

:25



Password Security



- **Protecting Password Digests**
 - Use **salts**, which consists of a random string that is used in hash algorithms
 - Passwords can be protected by adding a random string 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

:26



Password Security



■ 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

:27



Password Security



■ 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*

:28



Secure Authentication Technologies



■ Single Sign-On

- *Identity management* is using a single authentication credential shared across multiple networks
- Single sign-on (SSO) uses one authentication credential to access multiple accounts or applications

:29



Secure Authentication Technologies



■ 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

:30



Authentication- Kerberos

- A network authentication protocol designed for a client/server environment.
- Uses strong encryption so that clients can prove their identity to a server and the server can in turn authenticate itself to the clients.
- Communicates via “tickets” that serve to prove the identity of users
- Built around the idea of a trusted third party, termed a key distribution center (KDC),
- Key distribution center (KDC) consists of two logically separate parts
 1. An authentication server (AS)
 - It is an entity trusted by both the client and the server the client wishes to access.
 2. A ticket-granting server (TGS).

31



Kerbosis- Tickets

- **Ticket**
 - The basis for authentication in a Kerberos environment is a
 - Eliminates the inherently insecure transmission of items such as a password that can be intercepted on the network.
- **The Kerberos server**
 - Contains user IDs and hashed passwords for all users that will have authorizations to realm services.
 - Also has shared secret keys with every server to which it will grant access tickets.
- **Tickets are used in a two-step process with the client.**
 - The first ticket is a *ticket-granting ticket (TGT)* issued by the *authentication server (AS)* to a requesting client.
 - The client can then present this ticket to the Kerberos server with a request for a ticket to access a specific server.
 - This *client-to-server ticket* (also called a *service ticket*) is used to gain access to a server's service in the realm.
 - **Tickets are time-stamped, and cannot be reused.**

32

Secure Authentication Technologies



■ Directory Service

- A database stored on the network that contains information about users and network devices
- Make it easier to grant privileges or permissions to network users and provide authentication

■ 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

33

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

34



Summary (2 of 2)



- A network hardware security module is a special trusted network computer that performs cryptographic operations such as key management, key exchange, onboard random number generation, key storage facility, and symmetric and asymmetric encryption
- An access control list (ACL) contains rules that administer the availability of digital assets by granting or denying access to the assets
- Network access control (NAC) examines the current state of an endpoint before it can connect to the network
- Data loss prevention (DLP) is a system of security tools used to recognize and identify data critical to the organization and ensure that it is protected
- Broadcast storm prevention can be accomplished by loop prevention, which uses the IEEE 802.1d standard spanning-tree protocol (STP)