Chapter 7: Identity and Access Management

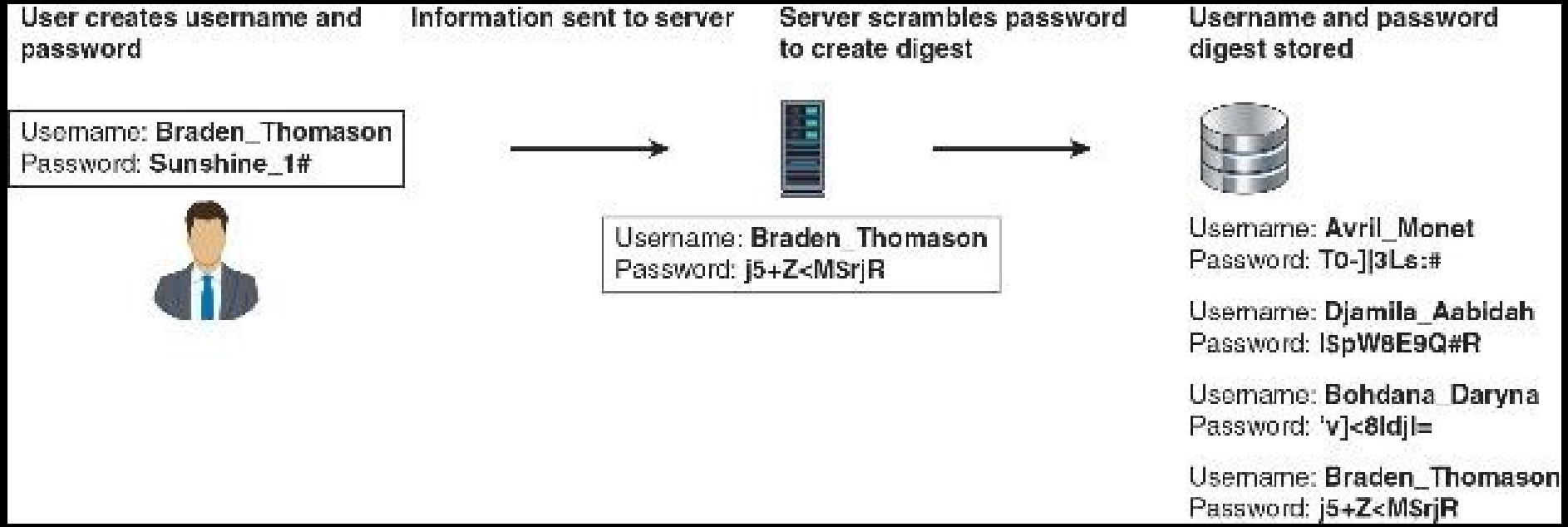
Types of Authentication Credentials

Element	Description	Scenario
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

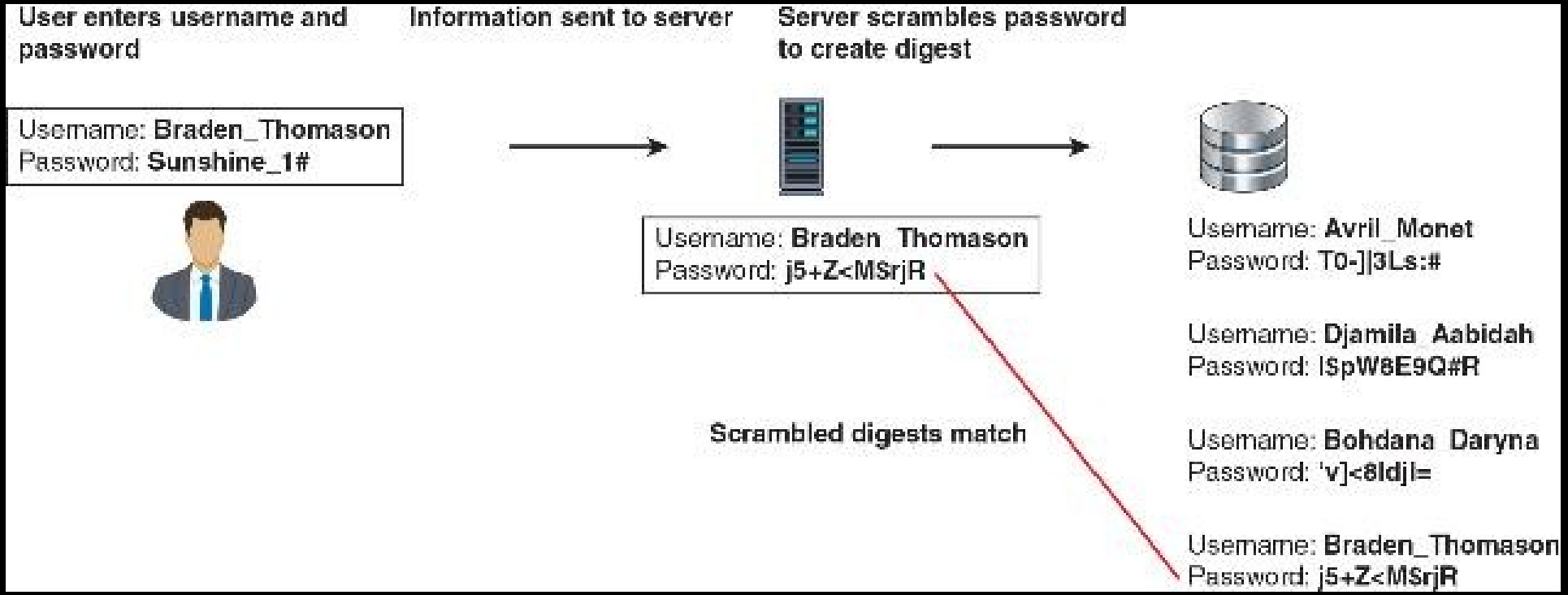
Something You Know: Passwords

- **Passwords** are the most common type of IAM authentication today
- Passwords provide weak protection and are constantly under attack
- Password Weaknesses
  - Weakness of passwords is linked to human memory
  - Long, complex passwords are most effective
  - Users must remember passwords for many different accounts
  - Each account password should be unique
  - Many security policies mandate that passwords must expire

Creating a Password



Retrieving a Password



Something You Know: Passwords

- In a **brute force attack**, every possible combination of letters, numbers, and characters is combined to attempt to determine the user's password
- 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
- Attackers work to steal the file of password digests
  - They can also load that file onto their own computers and then use a sophisticated **password cracker**, which is software designed to break passwords

Something You Know: Passwords

- An **offline brute force attacks** uses a stolen digest file
  - The attacker then uses password cracking software to create candidate digests of every possible combination of letters, numbers, and characters that are then matched against those in a stolen digest file
- In a **dictionary attack**, the attacker creates digests of common dictionary words and compares against a stolen digest file
- **Credential stuffing** occurs when an attacker injects stolen username and password credentials across multiple websites

Something You Know: Passwords

- 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

Rule Attack Statistical Analysis

```
[*] 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)
```

Rule Attack Generated Masks

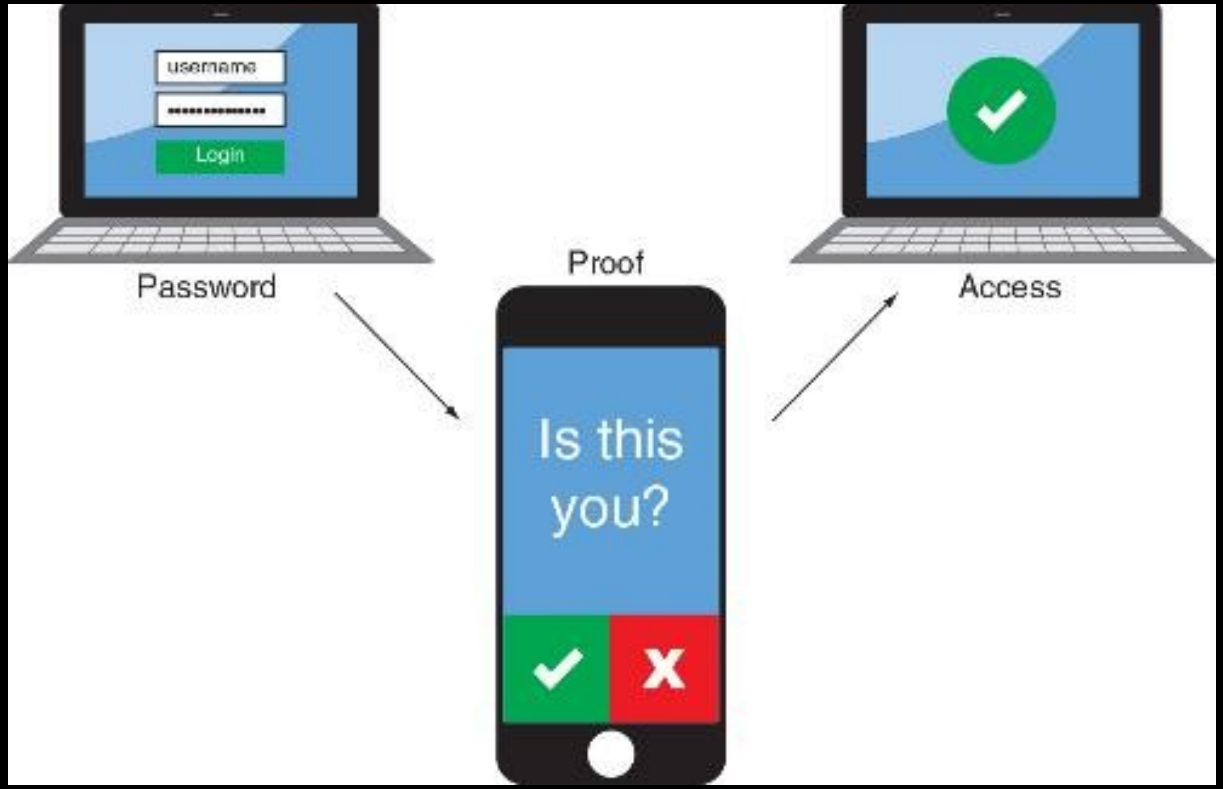
```
[*] Length Statistics...
[+]                              8: 62% (612522)
[+]                              6: 18% (183307)
[+]                              7: 14% (146152)
[+]                              5: 02% (26438)
[+]                              4: 01% (15088)
[+]                         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

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

Something You Have: Tokens & Keys

- The most common items used for “something you have” authentication are tokens, security keys, and smart cards
- A token is a type of object that can be hardware or software
  - One type of hardware token is a windowed token that displays a dynamic value called a **one-time password** (**OTP**)
  - A software OTP is generated through an app on a user’s smartphone
- **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

Authentication App



Something You Have: Tokens & Keys

- A more secure option is using a dedicated token key, known as a security key
- One feature of security keys is **attestation**, which is a key pair that is “burned” into the security key during manufacturing time and is specific to a device model
- A smart card is a credit-card-sized plastic card that can hold information to be used as part of the authentication process
  - A smart card standard covering all U.S. government employees is called the Personal Identity Verification (PIV) standard

Security Keys

Something You Are: 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
  - A 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

Something You Are: Biometrics

- The following are two basic types of fingerprint scanners:
  - A static fingerprint scanner takes a picture and compares with image on file
  - A dynamic fingerprint scanner uses a small slit or opening
- 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

Something You Are: Biometrics

- 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

- Biometric Disadvantages
  - The cost of specialized hardware scanning devices
  - Readers have some amount of error
  - Biometric systems can be “tricked”
  - A final concern with biometrics is the efficacy rate (which is the benefit achieved)

Something You Are: 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 Are: Behavioral Bio

- **Behavioral biometrics** authenticates by normal actions the user performs
- A type of behavioral biometrics is keystroke dynamics, which recognizes a user's typing rhythm
  - Keystroke dynamics uses the following 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

Securing Passwords

- One method of protecting password digests is called **salting**, 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
- Another strategy is called **peppering** where a message digest is created as normal but then encrypted with a symmetrical encryption key before being stored

Securing Passwords

- A more secure approach for creating password digests is to use **key stretching**
  - Key stretching is a specialized password hash algorithm that is intentionally designed to be slower
  - Three key stretching algorithms are bcrypt, PBKDF2, and Argon2

Securing Passwords

- Solutions for managing passwords include the following:
  - Password vaulting, user password managers, hardware password keys, and using password best practices
- **Password vaulting** stores user password credentials in a highly protected database (vault) that is stored on the organization's network
- A user **password manager** is a software application or online website that stores user passwords along with login information
- A hardware **password key** often serves as a hardware-based password manager

Password Key

Securing Passwords

- Password best practices include the following:
  - **Default passwords** should be changed
  - **Password reuse** should be prohibited
  - **Password expiration** should not be utilized
  - **Password age** should be set to at least 1
  - **Provisioning** (initially setting up user accounts) should include policies that address password best practices
  - **De-provisioning** should have policies such as suspending accounts when an employee leaves an organization

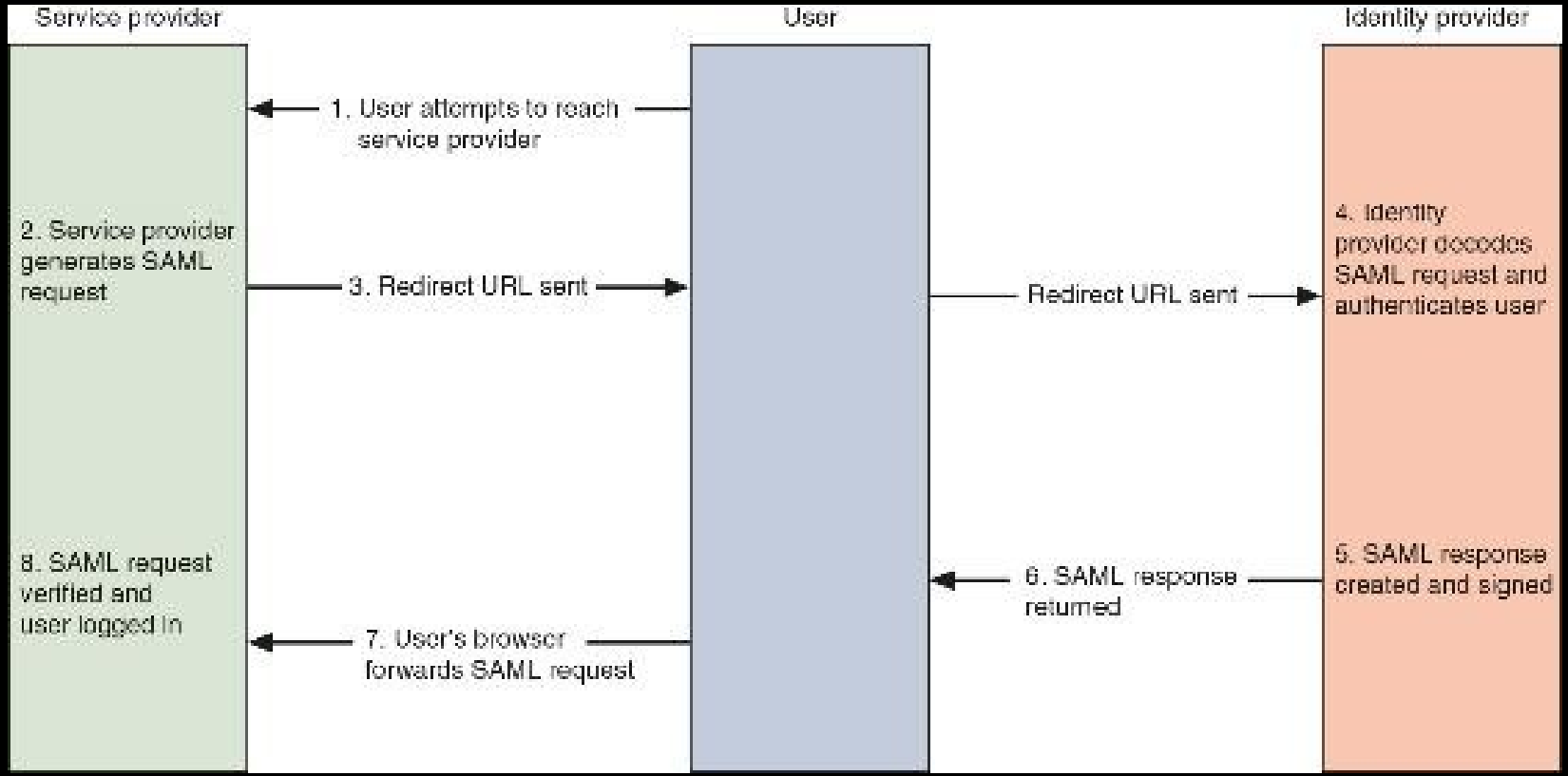
Secure Authentication Technologies

- Single-Sign On
  - Identity management is using a single authentication credential shared across multiple networks
  - **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
- Technologies for SSO include Security Assertion Markup Language (SAML) and Lightweight Directory Access Protocol (LADP)

Secure Authentication Technologies

- **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
- **Lightweight Directory Access Protocol** (**LDAP**) makes it possible for almost any application to obtain directory information
  - Developers use LDAP to allow SSO if a single login were to grant access to all databases, apps, and devices on that server

SAML Transaction



Secure Authentication Technologies

Name	Description	Explanation
OAuth (Open Authorization)	Open-source federation framework	OAuth 2.0 is a framework to support the development of authorization protocols
OpenID	Open standard decentralized authentication protocol	Authentication protocol that can be used in OAuth 2.0 as a standard means to obtain a user identity
Shibboleth	Open-source software package for designing SSO	Uses federation standards to provide SSO and exchanging attributes

Secure Authentication Technologies

- **Passkeys** refer to various methods for storing authenticating information in hardware
- Passkeys do not rely on passwords
  - They combine multiple authentication factors into a single package that is managed by the device's OS
- Passkeys are also "discoverable," which means an enrolled device can automatically push a passkey through an encrypted tunnel to another device that is attempting to sign in

Access Control Schemes

- An **access control scheme** is a predefined framework, embedded in the software and hardware, that administrators can use for controlling access
- The **Discretionary Access Control** (**DAC**) scheme is the least restrictive, where every object has an owner, who has total control over that object
- Two weaknesses of DAC include the following:
  - DAC relies on decisions by the user to set security
  - Permission will be inherited by any programs the subject executes

Windows DAC

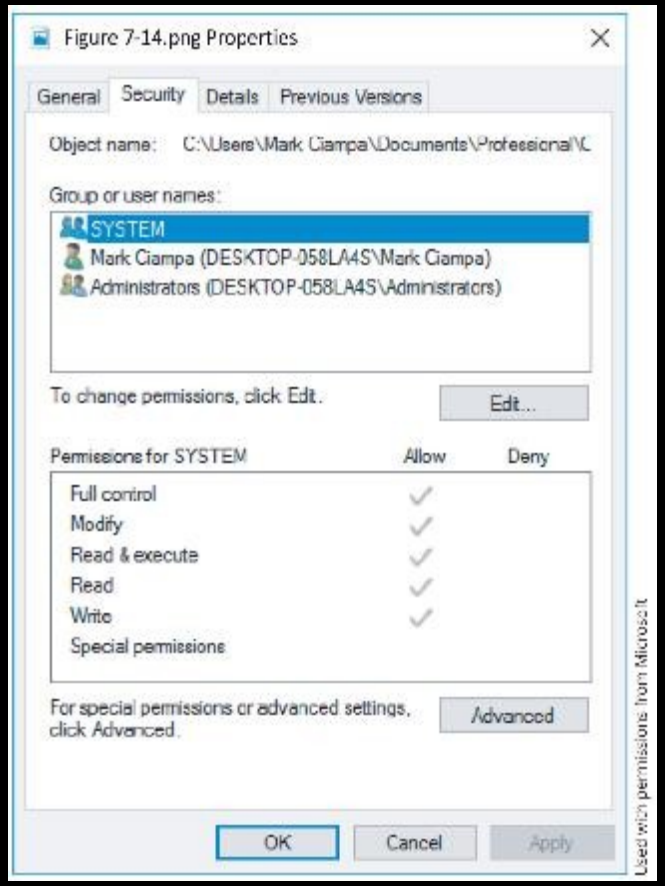


Figure 7-14.png Properties
General
Security
Details
Previous Versions
Object name: C:\Users\Mark Ciampa\Documents\Professional\C
Group or user names:
SYSTEM
Mark Ciampa (DESKTOP-058LA4S\Mark Ciampa)
Administrators (DESKTOP-058LA4S\Administrators)
To change permissions, click Edit.
Edit...
Permissions for SYSTEM
Allow
Deny
Full control
Modify
Read & execute
Read
Write
Special permissions
For special permissions or advanced settings, click Advanced.
Advanced
OK
Cancel
Apply
Used with permission from Microsoft

Access Control Schemes

- **Mandatory Access Control** (**MAC**) assigns users' access controls strictly according to the custodian's desires
- The following are two key elements to MAC:
  - Labels – every entity is assigned a classification label
  - Levels – a hierarchy based on the labels is used for objects and subjects
- Microsoft Windows uses **Mandatory Integrity Control** (**MIC**) that ensures data integrity by controlling access using a **security identifier** (**SID**)

Access Control Schemes

- **Role-Based Access Control (RBAC)** is based on a user's job function within an organization
  - The RBAC scheme assigns permissions to particular roles and then assigns users to those roles
- **Rule-Based Access Control** is used for managing user access to one or more systems, where business changes may change access rules
- **Attribute-Based Access Control** (**ABAC**) uses more flexible policies that can combine attributes

Access Control Schemes

Name	Explanation	Description
Mandatory Access Control (MAC)	End-user cannot set controls	Most restrictive scheme
Discretionary Access Control (DAC)	Subject has total control over objects	Least restrictive scheme
Role-Based Access Control (RBAC)	Assigns permissions to particular roles in the organization and then users are assigned to roles	Considered a more “real-world” approach
Rule-Based Access Control	Dynamically assigns roles to subjects based on a set of rules defined by a custodian	Used for managing user access to one or more systems
Attribute-Based Access Control (ABAC)	Uses policies that can combine attributes	Most flexible scheme

Access Control Lists (ACLs)

- An **access control list** (**ACL**) is a set of permissions (authorizations) that is attached to an object
  - The list specifies who are allowed to access an object and what operations they can perform on it
- ACLs provide filesystem permissions for protecting files managed by the OS
- Some disadvantages of ACLs includes inefficiency and difficulty to manage in an enterprise setting