BAIT1093 Introduction to Computer Security

Chapter 6: User Authentication and Access Control

Topics

- 6.1 Authentication Process
- 6.2 Means of Authentication
  - 6.2.1 Password Authentication
  - 6.2.2 Token-Based Authentication
  - 6.2.3 Biometric Authentication
  - 6.2.4 Remote User Authentication
- 6.3 User Authentication Security Issues
- 6.4 Access Control

6.1 Authentication Process [1]

- User authentication is the:
  - fundamental building block and the primary line of defense.
  - Basis for most types of access control and for user accountability.

6.1 Authentication Process [1]

- RFC 4949 defines user authentication as follows:
  - The process of verifying an identity claimed by or for a system entity.
  - An authentication process consists of two steps:
    - **Identification step**: Presenting an identifier to the security system. Example: User ID
    - **Verification step**: Presenting or generating authentication information that corroborates the binding between the entity and the identifier. Example: Password

6.2 Means of Authentication [1]

The four means of authenticating user identity are based on:

Something the individual knows	Something the individual possesses (token)	Something the individual is (static biometrics)	Something the individual does (dynamic biometrics)
• Password, PIN, answers to prearranged questions	• Smartcard, electronic keycard, physical key	• Fingerprint, retina, face	• Voice pattern, handwriting, typing rhythm

6.2.1 Password Authentication [2]

- The most common IT authentication credential is providing information that only the user would know.
- A password is a secret combination of letters, numbers, and/or characters.
- Despite their widespread use, passwords provide weak protection and are constantly under attack.

6.2.1 Password Authentication [2]

- Challenges of Password Authentication:
  - Difficult for users to memorize and recall long and complex passwords.
  - Difficult for users to remember different passwords for many accounts.
  - Difficult for users to remember unique passwords for different accounts.
  - Users have to repeatedly memorize new passwords if there are security policies that mandate that password expire after a set period of time and cannot reused old passwords.

6.2.1 Password Authentication [2]

- Due to challenges faced to remember passwords, users take shortcuts by:
  - using weak passwords. For eg, using common word (*morning*), short word (*girl*), predictable sequence of characters (*abc123*), or personal information (*Simon*).
  - reuse the same password (or a slight derivation of it) for multiple accounts.

6.2.1 Password Authentication [2]

- Although using stronger passwords, predictable patterns are generally used:
  - Appending: Users often add a number after letters (*simon1* or *food88*). If combining letters, numbers and punctuation, usually using this sequence: letters+punctuation+number (*simon.1* or *food$6*)
  - Replacing: Users also use replacements in predictable patterns. Generally, a zero is used instead of the letter o (*passw0rd*), the digit 1 for the letter i (*s1mon*), or a dollar sign for an s (*$imon*).

6.2.1 Password Authentication [2]

- The widespread use of weak passwords is alarming.
- An analysis of more than 562 million stolen passwords revealed that the most common length of a password was only nine characters, while fewer than 1 percent of the passwords were more than 14 characters.
- In addition, the percentage of passwords that used characters other than lowercase letters was remarkably low: uppercase characters were found in only 6% of passwords while special symbols were in just 4%.

6.2.1 Password Authentication [2]

Table 12-2 Ten most common passwords

Rank	Password
1	123456
2	123456789
3	abc123
4	password
5	password1
6	12345678
7	111111
8	1234567
9	12345
10	1234567890

6.2.1 Password Authentication [2]

Attacks of Passwords

- Pass the Hash Attack/Password Cracker
- Password Spraying
- Brute Force Attack
- Rule Attack
- Dictionary Attack
- Rainbow Tables
- Password Collections

6.2.1 Password Authentication [2]

Attacks of Passwords → 1) Pass the Hash Attack / Password Cracker

- When a user creates a password, it is not stored in an unencrypted plaintext format.
- Instead, a one-way hash algorithm creates a message digest (or hash) of the password.
- This digest is then stored instead of the original plaintext password.
- When a user later enters a password to log in, a digest is created. This digest is compared against the stored digest, and if they match, the user is authenticated.

6.2.1 Password Authentication [2]

Attacks of Passwords → 1) Pass the Hash Attack / Password Cracker

- Attackers steal the file of password digests.
- Once that file is in the hands of threat actors, it can be used in one of two ways.
  - **Pass the Hash attack**. use a stolen hash to impersonate the user. → vulnerability in the Microsoft Windows NTLM (New Technology LAN Manager) hash for storing passwords on a Windows endpoint computer. An attacker who can steal the digest of an NTLM password could pretend to be the user by sending that hash to the remote system to then be authenticated.

6.2.1 Password Authentication [2]

Attacks of Passwords → 1) Pass the Hash Attack / Password Cracker

- Once that file is in the hands of threat actors, it can be used in one of two ways (cont.).
  - **Password Cracker**. Password crackers create known digests (called candidates) and then compare them against the stolen digests. When a match occurs, the attacker knows the underlying password.

6.2.1 Password Authentication [2]

Attacks of Passwords → 2) Password Spraying

- a type of "targeted guessing."
- selects one or a few common passwords (*Password1* or *123456*) and then enters the same password when trying to login to several user accounts.
- As this targeted guess is spread across many accounts, instead of attempting multiple password variations on a single account, it is much less likely to raise any alarms or lock out the user account from too many failed password attempts.
- Although password spraying may result in occasional success, it is not considered the optimal means for breaking into accounts.

6.2.1 Password Authentication [2]

Attacks of Passwords → 3) Brute Force Attack

- In an automated brute force attack, every possible combination of letters, numbers, and characters is attempted to determine the user's password.
- The attack is not done in a random fashion but instead uses a meticulous approach to create the passwords.
- Unlike a password spraying attack, in which one password is used on multiple accounts, in an online brute force attack, the same account is continuously attacked (called pounded) by entering different passwords.

6.2.1 Password Authentication [2]

Attacks of Passwords → 3) Brute Force Attack

- An offline brute force attack begins with a stolen digest file.
- An attacker loads this file onto a computer and then uses password cracking software to create candidate digests of every possible combination of letters, numbers, and characters.
- The candidates are matched against those in a stolen digest file to find a match.
- Slowest yet most thorough method.

6.2.1 Password Authentication [2]

Attacks of Passwords → 4) Rule Attack

- A rule attack conducts a statistical analysis on the stolen passwords.
- The results of this analysis is then used to create a mask of the format of the candidate password. A mask of *?u ?l ?l ?l ?l ?d ?d ?d ?d* (u = uppercase, l = lowercase, and d = digit) would tell the password cracking program, *Use an uppercase letter for the first position, a lowercase letter for the next four positions, and digits for the remaining four positions*.
- Using a mask will significantly reduce the time needed to crack a password.

6.2.1 Password Authentication [2]

Attacks of Passwords → 4) Rule Attack

- There are three basic steps in a rule attack:

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.

6.2.1 Password Authentication [2]

Attacks of Passwords → 4) Rule Attack

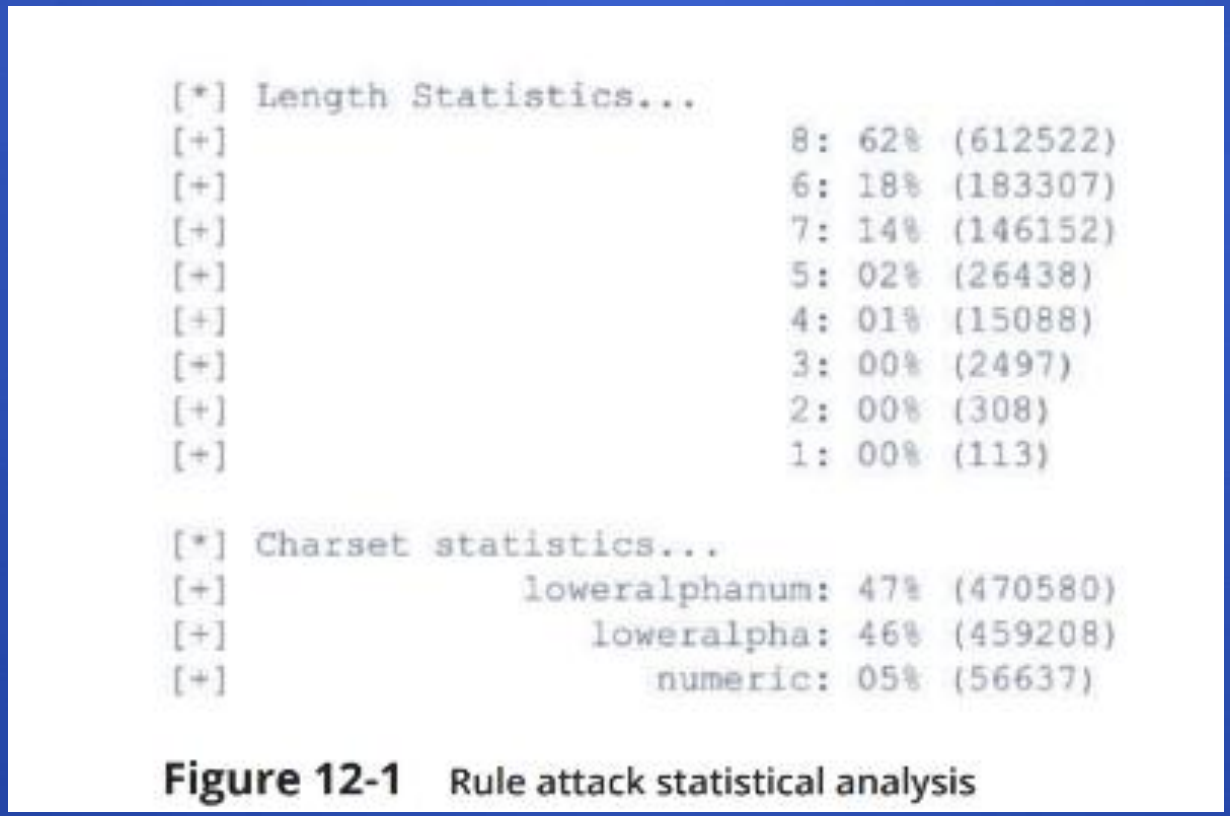


Figure 12-1 Rule attack statistical analysis

6.2.1 Password Authentication [2]

Attacks of Passwords → 4) Rule Attack

```
[*] 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?l: 03% (516862)
[+]            ?d?d?d?d?d?d?d?d: 03% (487437)
[+]      ?d?d?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?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?d?d?d: 02% (292318)
[+]        ?l?l?l?l?l?l?l?d?d?d: 01% (273640)
```

Figure 12-2 Rule attack generated masks

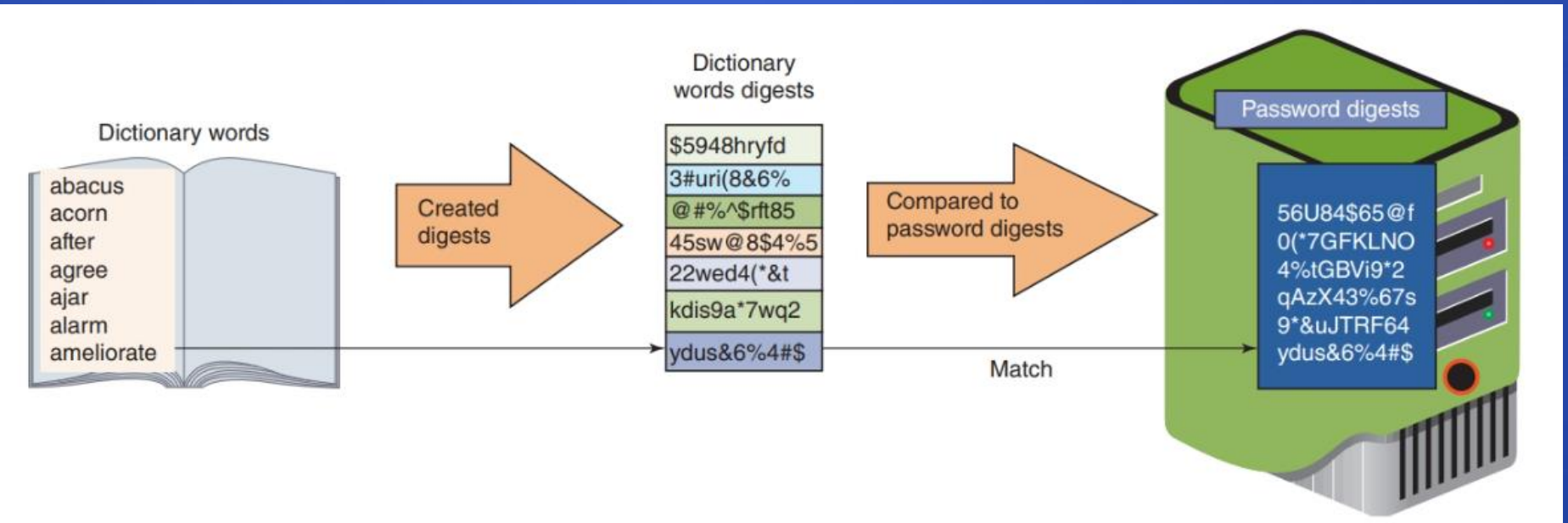
6.2.1 Password Authentication [2]

Attacks of Passwords → 5) Dictionary Attack

- A dictionary attack begins with the attacker creating digests of common dictionary words as candidates and then comparing them against those in a stolen digest file.
- Dictionary attacks are successful because users often create passwords from simple dictionary words.

6.2.1 Password Authentication [2]

Attacks of Passwords → 5) Dictionary Attack



6.2.1 Password Authentication [2]

Attacks of Passwords → 6) Rainbow Tables

- Rainbow tables make password attacks easier by creating a large pregenerated data set of candidate digests.
- A rainbow table is a compressed representation of passwords that are related and organized in a sequence (called a chain).
- Although generating a rainbow table requires a significant amount of time, once it is created, it has three significant advantages over other password attack methods. A rainbow table can be used repeatedly for attacks on other pass-words; rainbow tables are much faster than dictionary attacks; and the amount of memory needed on the attacking machine is greatly reduced.

6.2.1 Password Authentication [2]

Attacks of Passwords → 6) Rainbow Tables

- Although generating a rainbow table requires a significant amount of time, once it is created, it has three significant advantages over other password attack methods:
  - A rainbow table can be used repeatedly for attacks on other passwords
  - Rainbow tables are much faster than dictionary attacks;
  - The amount of memory needed on the attacking machine is greatly reduced.

6.2.1 Password Authentication [2]

Attacks of Passwords → 7) Password Collections

- Example of password collection: An attacker using an SQL injection attack broke into a server that contained more than 32 million user passwords, all in cleartext. These passwords were later posted on the Internet.
- Users usually repeat their passwords on multiple accounts, attackers could now use these passwords as candidate passwords in their attacks with a high probability of success.

6.2.1 Password Authentication [2]

Attacks of Passwords → 7) Password Collections

- Using stolen password collections as candidate passwords is the foundation of password cracking today, and almost all password cracking software tools accept these stolen “wordlists” as input.
- Websites host lists of these leaked passwords that attackers can download along with important statistics and masks for a rule attack.
- These sites also attempt to crack submitted password collections.

6.2.1 Password Authentication [2]

Attacks of Passwords

- Attackers usually used a combination of password attack tools and not only using one method.

Table 12-3 Common sequence of password attack tools

Order	Password attack	Explanation
1	Custom wordlist	Download a stolen password collection
2	Custom wordlist using rule attack	Generate password statistics using a rule attack to create specialized masks
3	Dictionary attack	Perform a dictionary attack on passwords
4	Dictionary attack using rules	Conduct a refined dictionary attack using results from a rule attack
5	Updated custom wordlist using rules	Input any cracked passwords from previous steps to create more refined rules
6	Hybrid attack	Perform a focused dictionary attack with a mask attack
7	Mask attack	Conduct a mask attack on harder passwords that have not already been cracked
8	Brute force attack	Last-resort effort on any remaining passwords

6.2.2 Token-Based Authentication [2]

- Another type of authentication credential is based on the approved user having a specific item in his possession (something you have). Ie Token-based Authentication.
- Such items are often used along with passwords.
- Because this involves more than one type of authentication credential—both what a user knows (the password) and what the user has—this type of authentication credential is called multifactor authentication (MFA).

6.2.2 Token-Based Authentication [2]

- Using just one type of authentication is called single-factor authentication, and using two types is called two-factor authentication (2FA).
- The most common items that are used for this type of authentication are
  - specialized devices
  - smartphones
  - security keys

6.2.2 Token-Based Authentication [2]

Specialized Devices → 1) Smart Cards

- A smart card is a credit-card-sized plastic card that can hold information to be used as part of the authentication process.
- Used for authentication generally require that the card be inserted into a card reader that is connected to the computer, or contactless smart cards that only require it to be in close proximity to the reader

6.2.2 Token-Based Authentication [2]

Specialized Devices → 1) Smart Cards

- Disadvantages:
  - 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 (called magnetic stripe cards) are subject to unauthorized duplication called card cloning. Stealing this information is often done by a process called skimming, in which a threat actor attaches a small device that fits just inside the card readers so that when the card is inserted and removed, both the actual reader and the skimming device capture the information from the magnetic strip.

6.2.2 Token-Based Authentication [2]

Specialized Devices → 2) Windowed Token

- A hardware windowed token is typically a small device with a window display.
- A windowed token display a dynamic value, which is a one-time password (OTP), - an authentication code that can be used only once or for a limited period of time.

Figure 12-4 Windowed token

6.2.2 Token-Based Authentication [2]

Specialized Devices → 2) Windowed Token

- There are two types of OTPs.
  - A time-based one-time password (TOTP)
  - An HMAC-based one-time password (HOTP)

6.2.2 Token-Based Authentication [2]

Specialized Devices → 2) Windowed Token → TOTP

- A time-based one-time password (ToTP) changes after a set period of time.
- The windowed token and a corresponding authentication server share an algorithm (each user's token has a different algorithm), and the token generates a code from the algorithm once every 30 to 60 seconds.
- The ToTP is not transmitted to the token; instead, both the token and authentication server have the same algorithm and time setting.
-

6.2.2 Token-Based Authentication [2]

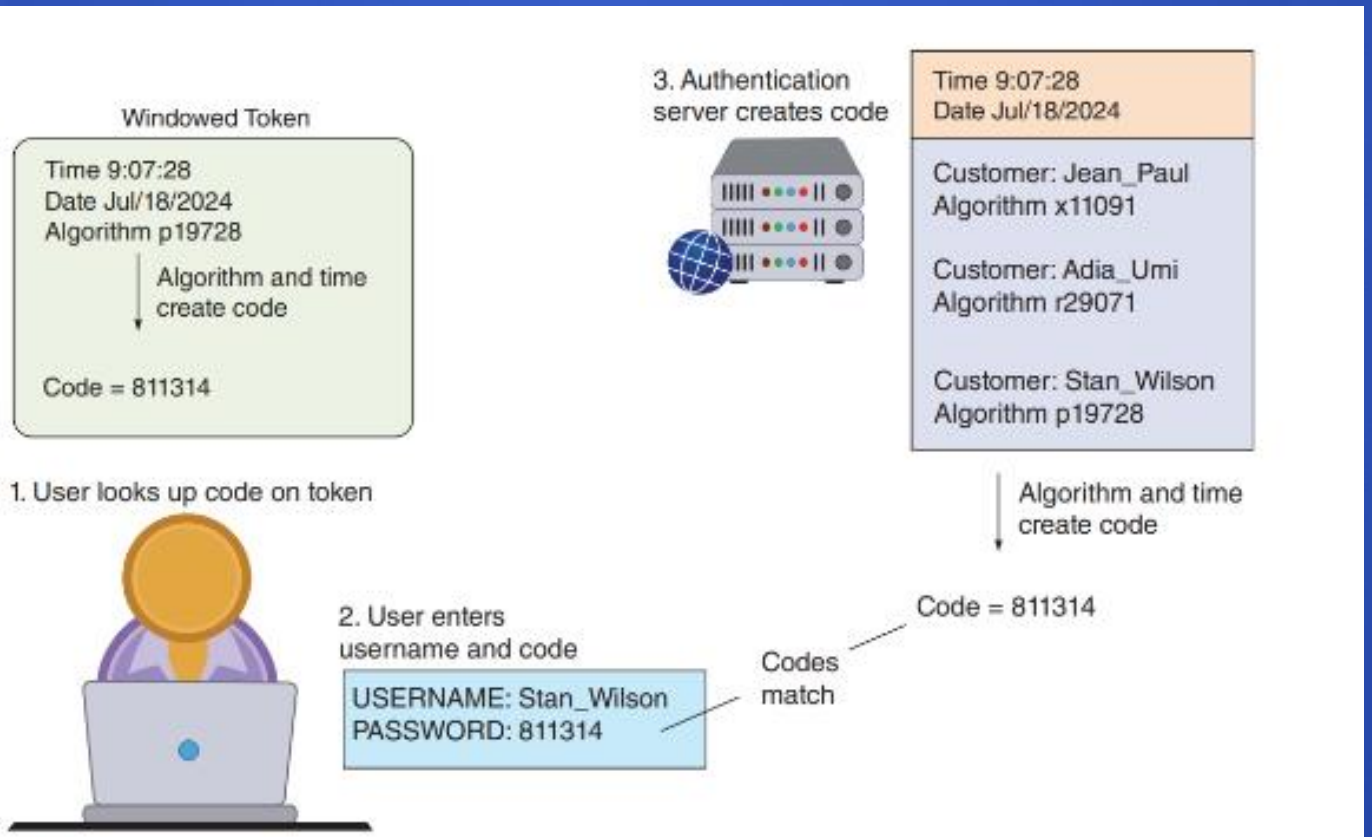


Figure 12-5 Time-based one-time password (TOTP)

6.2.2 Token-Based Authentication [2]

Specialized Devices → 2) Windowed Token → HOTP

- an HMAC-based one-time password (HOTP) password is "event driven" and changes when a specific event occurs, such as when a user enters a personal identification number (PIN) on the token's keypad, which triggers the token to create a random code. For example, after entering the PIN 1729, the code 833854 is displayed.

6.2.2 Token-Based Authentication [2]

Specialized Devices → 2) Windowed Token

- While windowed tokens have some advantages, such as creating dynamic OTPs, they are considered cumbersome to use.
- Once an OTP is received, it must then be manually entered on the endpoint device. Because the OTP is valid for only a short time, the user must enter it quickly.
-

6.2.2 Token-Based Authentication [2]

Smartphones

- More practical approach as smartphones are used virtually everywhere and do not need additional device for authentication.
- Once enter username and password, authentication through a smartphone can be accomplished by the following:
  - Phone call
  - SMS text message
  - Authentication app

-

6.2.2 Token-Based Authentication [2]

Smartphones → 1) Phone call

- An automated phone call to the user's smartphone asks if the user has requested to log in and, if so, to press a digit on the keypad for approval or to decline if the user has not just tried to log in.
-

Smartphones → 2) SMS Text Message

- Receive OTP in an SMS Text Message and manually enter the OTP in the system
-

6.2.2 Token-Based Authentication [2]

Smartphones → 3) Authentication App

- An authentication app can be installed on the smartphone to authenticate the user.
- When the app is first installed, the user goes through a verification process.
- Whenever a user attempts to log in to an account by entering a username and password, a message is displayed on a specified phone (called a push notification) through the authentication app that asks the user to approve or deny the request.

6.2.2 Token-Based Authentication [2]

Smartphones → 3) Authentication App

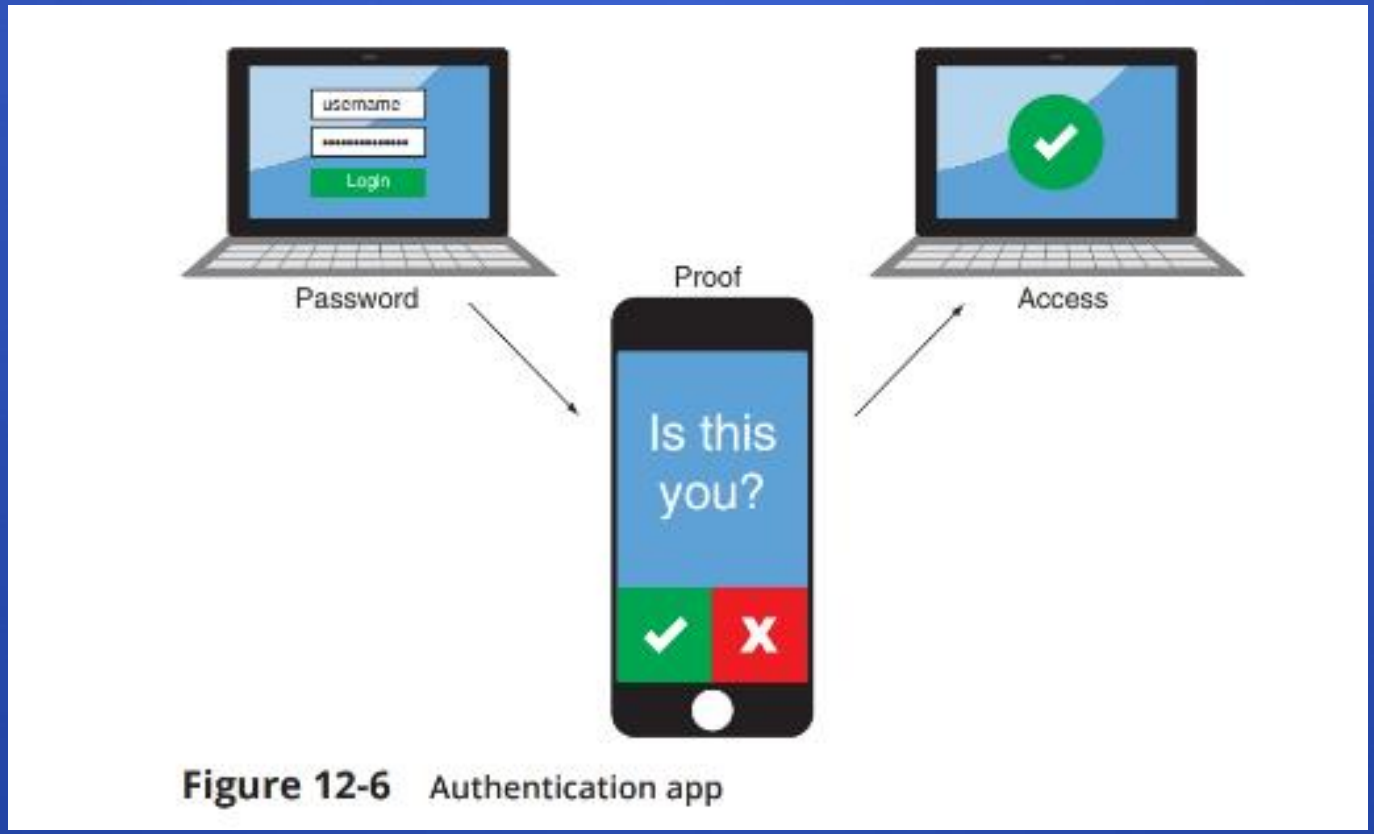


Figure 12-6 Authentication app

6.2.2 Token-Based Authentication [2]

Smartphones

- Despite its convenience and ability to reach a wide range of users, using a smartphone for authentication is not considered to be a secure option.
- An OTP received through an SMS text message can be “phished” (when a user is tricked into providing it to an attacker through a phishing attack), SMS text messages can be intercepted, and a malware infection on the phone can target the authentication app.

6.2.2 Token-Based Authentication [2]

Security Keys

- A secure option that is gaining acceptance is using a dedicated token key, more commonly called a security key.
- A security key is a dongle that is inserted into the USB port (Windows and Apple) or Lightning port (Apple) or held near the endpoint (such as a smartphone using near field communication, or NFC).
- It contains all the necessary cryptographic information to authenticate the user.

6.2.2 Token-Based Authentication [2]

Security Keys

Source: Google LLC

Figure 12-7 Security keys

6.2.2 Token-Based Authentication [2]

Security Keys

- One feature of security keys is attestation. Attestation is a key pair that is “burned” into the security key during manufacturing time and is specific to a device model.
- It can be used to cryptographically prove that a user has a specific model of device when it is registered.
- When a user creates a new credential key pair (that links to a specific service like Facebook or PayPal), the public key that is sent to the service is signed with the attestation private key.
- The service that is creating the new account for the user can verify that the attestation signature on the newly created public key came from the device.

6.2.2 Token-Based Authentication [2]

Security Keys

- Attestation keys have associated attestation certificates, and those certificates chain to a root certificate that the service trusts. This is how the service establishes its trust in the authenticator's attestation key.
- Security keys can be used when logging in to an endpoint device and when accessing online accounts.
- Security keys do not transmit OTPs that can be intercepted or phished and are considered easier to use. Many security professionals recommend that users consider security keys as alternatives to other types of MFA

6.2.3 Biometric Authentication [2]

- In addition to authentication based on what a person knows or has, another category rests on the features and characteristics of the individual. This type of authentication, something you are:
  - physiological biometrics
  - cognitive biometrics.

6.2.3 Biometric Authentication [2]

Physiological biometrics

- Physiological means relating to the way in which a body part functions.
- For authentication, physiological biometrics uses the way in which a body part uniquely functions in an individual. Several unique characteristics of a person's body can be used to authenticate a user.

6.2.3 Biometric Authentication [2]

Physiological biometrics

- Specialized Biometrics Scanners
  - Retinal scanner (static biometrics)
  - Fingerprint scanner (static biometrics)
  - Vein scanner (static biometrics)
  - Gait recognition (dynamic biometrics)
- Standard Input Devices (eg microphone, camera)
  - Voice Recognition (dynamic biometrics)
  - Iris scanner (static biometrics)
  - Facial Recognition (static biometrics)

6.2.3 Biometric Authentication [2]

Physiological biometrics → Specialized Biometrics Scanners → 1) Retinal scanner

- A retinal scanner uses the human retina as a biometric identifier.
- The retina is a layer at the back (posterior) portion of the eyeball that contains cells sensitive to light, which trigger nerve impulses that pass these through the optic nerve to the brain, where a visual image is formed.
- Due to the complex structure of the capillaries that supply the retina with blood, each person's retina is unique

6.2.3 Biometric Authentication [2]

Physiological biometrics → Specialized Biometrics Scanners → 1) Retinal scanner

- A retinal scanner maps the unique patterns of a retina by directing a beam of low-energy infrared light (IR) into people's eyes as they look in the scanner's eyepiece.
- Because retinal blood vessels are more absorbent of IR than the rest of the eye, the amount of reflection varies during the scan. This pattern of variations is recorded and used for comparison when the user attempts to authenticate

6.2.3 Biometric Authentication [2]

Physiological biometrics → Specialized Biometrics Scanners → 1) Retinal scanner

- The network of blood vessels in the retina is so complex that even identical twins do not share a similar pattern. even though retinal patterns may be altered in cases of diabetes, glaucoma, or retinal degenerative disorders, the retina generally remains unchanged through a person's lifetime.

6.2.3 Biometric Authentication [2]

Physiological biometrics → Specialized Biometrics Scanners → 2) Fingerprint scanner

- most common type of biometric authentication.
- Every user's fingerprint consists of several ridges and valleys, with ridges being the upper skin layer segments of the finger and valleys the lower segments.
- In one method of fingerprint scanning, the scanner locates the point where these ridges end and split, converts them into a unique series of numbers, and then stores the information as a template.
- A second method creates a template from selected locations on the finger.

6.2.3 Biometric Authentication [2]

Physiological biometrics → Specialized Biometrics Scanners → 2) Fingerprint scanner

- There are two basic types of fingerprint scanners.
  - **A static fingerprint scanner**
    - user to place the entire thumb or finger on a small oval window on the scanner. The scanner takes an optical "picture" of the fingerprint and compares it with the fingerprint image on file.
  - **A dynamic fingerprint scanner**
    - has a small slit or opening

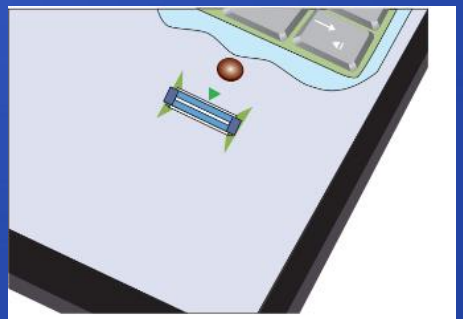


Figure 12-8 Dynamic fingerprint scanner

6.2.3 Biometric Authentication [2]

Physiological biometrics → Specialized Biometrics Scanners → 3) Vein scanner

- Vein - one of the “tubes” that form part of the blood circulation system in the human body that carries oxygen-depleted blood back toward the heart
- Vein images in a user’s palm or finger for authentication can be identified through a vein-scanning tablet.

6.2.3 Biometric Authentication [2]

Physiological biometrics → Specialized Biometrics Scanners → 4) Gait Recognition

- A person's gait, or manner of walking, can also uniquely authenticate an individual.
- Research has shown that gait recognition can achieve greater than 99 percent accuracy.
- Typically, small sensors less than an inch in height can be placed on a floor at intervals of about 65 feet (20 meters) to measure gait.

6.2.3 Biometric Authentication [2]

Physiological biometrics → Standard Input Devices → 1) Voice Recognition

- Because all users' voices are different, voice recognition, using a standard computer microphone, can be used to authenticate users based on the unique characteristics of a person's voice.
- Several characteristics make each person's voice unique, from the size of the head to age.
- These differences can be quantified to create a user voice template.

6.2.3 Biometric Authentication [2]

Physiological biometrics → Standard Input Devices → 1) Voice Recognition

- One of the concerns regarding voice recognition is that an attacker could record the user's voice and then create a recording to use for authentication. However, this would be difficult to do. Humans speak in phrases and sentences instead of isolated words.

6.2.3 Biometric Authentication [2]

Physiological biometrics → Standard Input Devices → 2) Iris Scanner

- An iris scanner, which can use a standard computer webcam, uses the unique characteristic of the iris, which is a thin, circular structure in the eye.
- The iris is responsible for controlling the diameter and size of the pupils to regulate the amount of light reaching the retina.
- Iris recognition identifies the unique random patterns in an iris for authentication.

6.2.3 Biometric Authentication [2]

Physiological biometrics → Standard Input Devices → 3) Facial Recognition

- A biometric authentication that is becoming increasingly popular is facial recognition.
- Every person's face has several distinguishable "landmarks" that make up their facial features.
- These landmarks are called nodal points. Each human face has approximately 80 nodal points, such as the width of the nose, the depth of the eye sockets, the shape of the cheekbones, and the length of the jaw line.
- Using a standard computer webcam, facial recognition software can measure the nodal points and create a numerical code (faceprint) that represents the face.

6.2.3 Biometric Authentication [2]

Physiological biometrics

- Disadvantages:
  - Cost of specialized biometric scanners
  - Not foolproof
    - genuine users may be rejected while imposters are accepted
  - Can be “tricked”
    - Example: fingerprints can be collected from water glasses and trick fingerprint readers on smartphones
  - Concern with the efficacy rate
    - Benefits vs trade-offs (user privacy)

6.2.3 Biometric Authentication [2]

Cognitive biometrics

- Whereas most biometrics considers a person's physical characteristics, the field of cognitive biometrics is related to the perception, thought process, and understanding of the user.
- Much easier for the user to remember because it is based on the user's life experiences.
- More difficult for an attacker to imitate.
- Also called knowledge-based authentication.

6.2.3 Biometric Authentication [2]

Cognitive biometrics

- One type of cognitive biometrics introduced by Microsoft is called Windows Picture Password for Windows 10 touch-enabled devices.
- Users select a picture that has at least 10 “points of interest” that can serve as “landmarks” or places to touch, connect with a line, or draw a circle around. Specific gestures—tap, line, or circle—are then used to highlight any parts of the picture while these gestures are recorded.

6.2.3 Biometric Authentication [2]

Cognitive biometrics

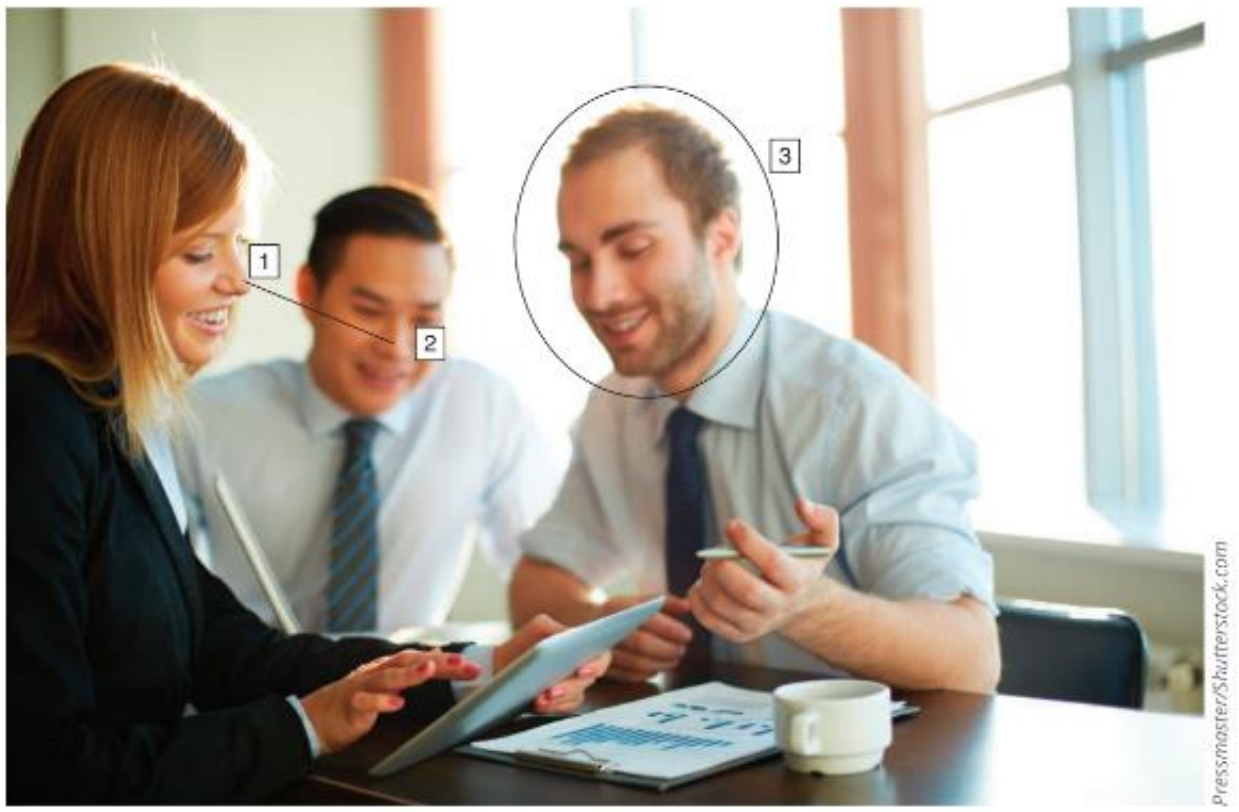


Figure 12-10 Picture password authentication

6.2.3 Biometric Authentication [2]

Cognitive biometrics

- For attackers to replicate these actions, they would need to know the parts of the image that were highlighted, the order of the gestures, the direction, and the starting and ending points of the circles and lines.
- However, security researchers have found that one of the most common methods used in Picture Password was using a photo of a person and triple tapping on the face, with the most common face tap is the eyes, followed by nose and jaw.

6.2.3 Biometric Authentication [2]

Cognitive biometrics

- Other examples of cognitive biometrics include requiring someone to identify specific faces or recall "memorable events," such as taking a special vacation, celebrating a personal achievement, or attending a specific family dinner. The user is asked specific questions about that memorable event, such as what type of food was served, how old the person was when the event occurred, where the event was located, who was in attendance, and the reason for the event. The user authenticates by answering the same series of questions when logging in.

6.2.4 Remote User Authentication [1]

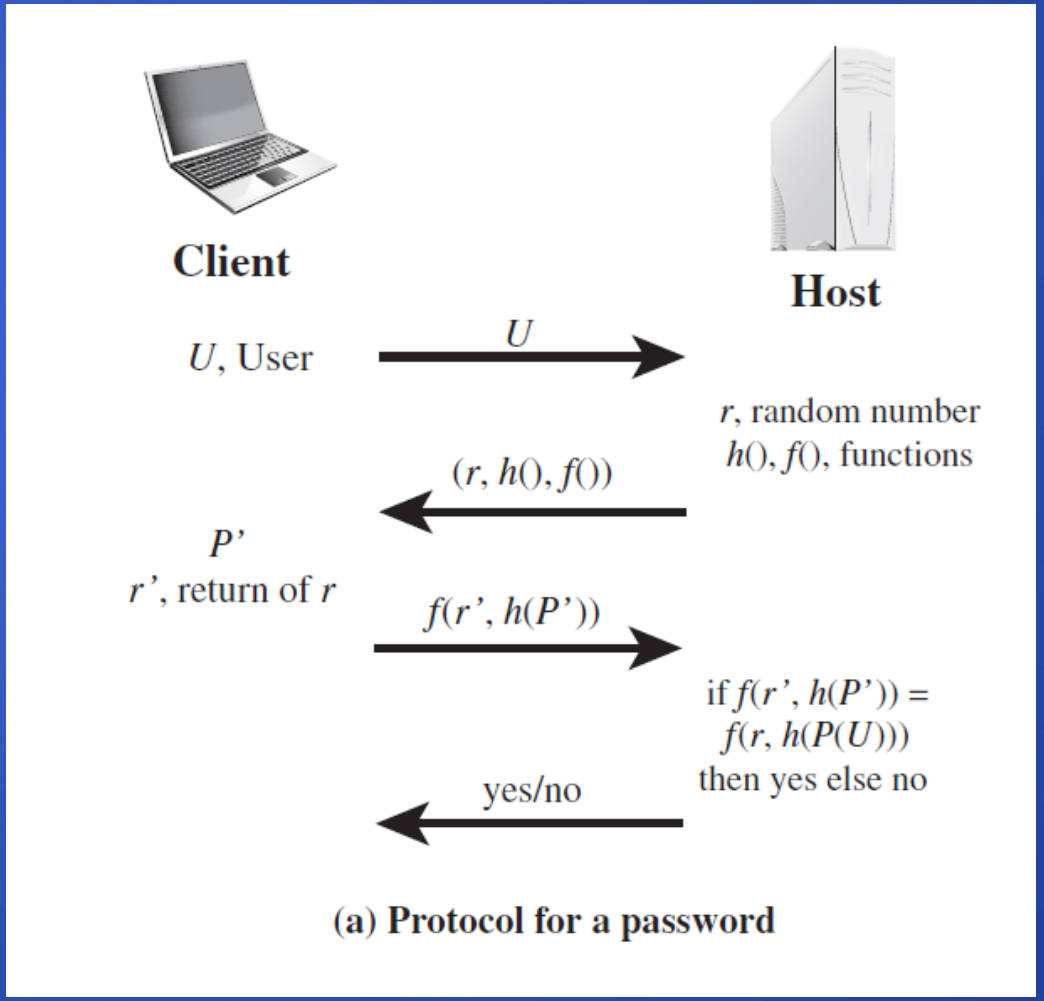
- The simplest form of user authentication is local authentication, in which a user attempts to access a system that is locally present, such as a stand-alone office PC or an ATM machine.
- The more complex case is that of remote user authentication, which takes place over the Internet, a network, or a communications link.

6.2.4 Remote User Authentication [1]

- Remote user authentication raises additional security threats, such as an eavesdropper being able to capture a password, or an adversary replaying an authentication sequence that has been observed.
- To counter threats to remote user authentication, systems generally rely on some form of challenge-response protocol.

6.2.4 Remote User Authentication [1]

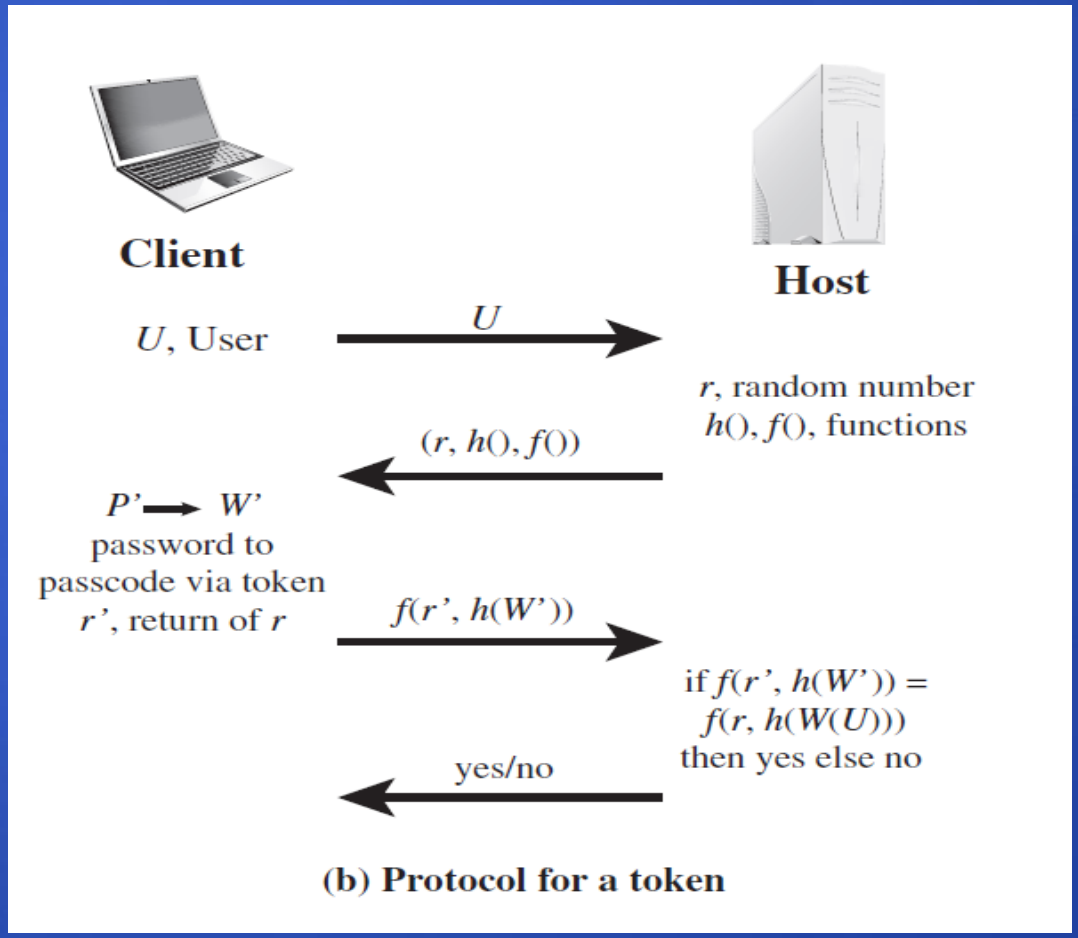
- Challenge-Response Protocol → Password Protocol



(a) Protocol for a password

6.2.4 Remote User Authentication [1]

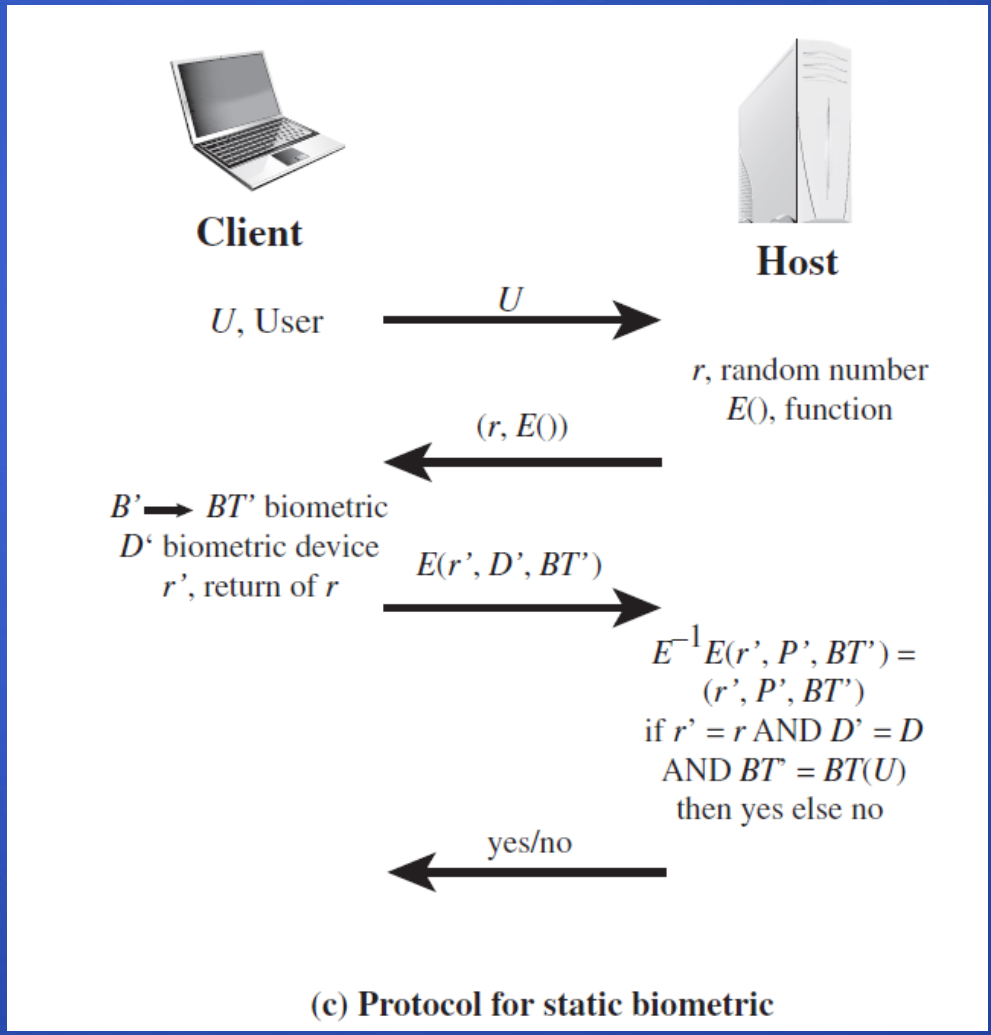
- Challenge-Response Protocol → Token Protocol



(b) Protocol for a token

6.2.4 Remote User Authentication [1]

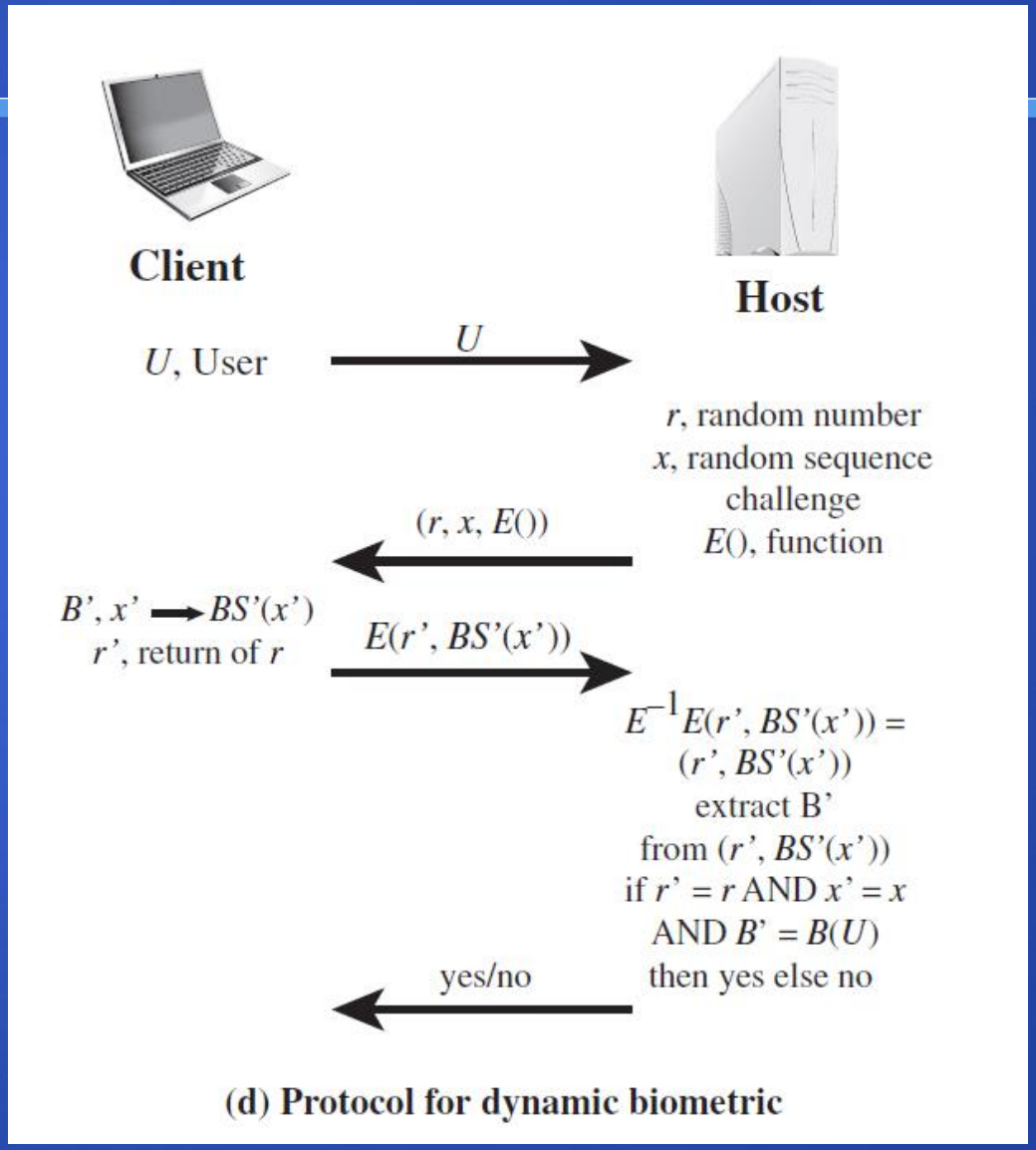
- Challenge-Response Protocol → Static Biometric Protocol



(c) Protocol for static biometric

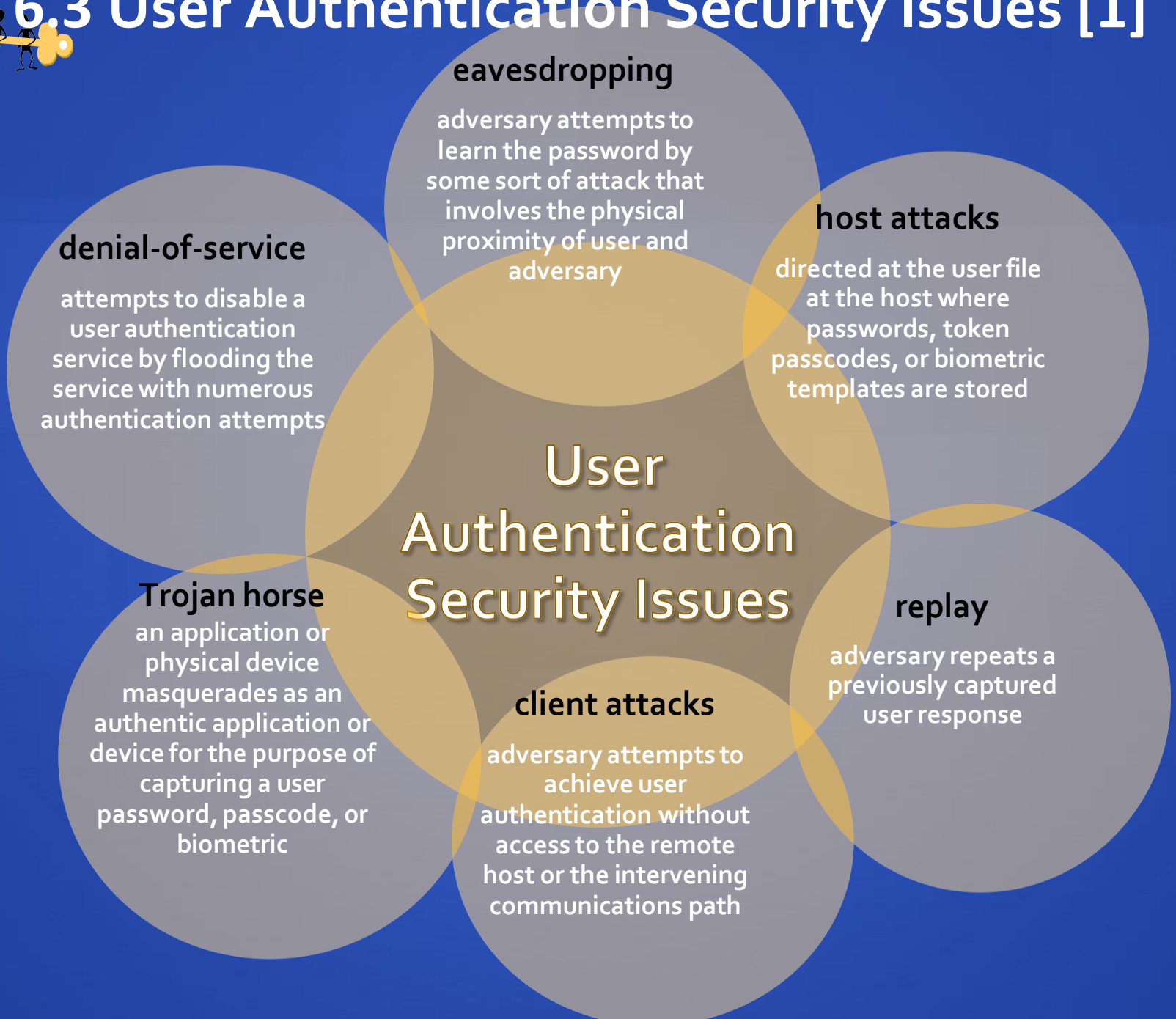
6.2.4 Remote User Authentication [1]

- Challenge-Response Protocol → Dynamic Biometric Protocol



(d) Protocol for dynamic biometric

6.3 User Authentication Security Issues [1]



6.3 User Authentication Security Issues [1]

Table 3.4 **Some Potential Attacks, Susceptible Authenticators, and Typical Defenses**

Attacks	Authenticators	Examples	Typical Defenses
Client attack	Password	Guessing, exhaustive search	Large entropy; limited attempts
	Token	Exhaustive search	Large entropy; limited attempts; theft of object requires presence
	Biometric	False match	Large entropy; limited attempts
Host attack	Password	Plaintext theft, dictionary/exhaustive search	Hashing; large entropy; protection of password database
	Token	Passcode theft	Same as password; 1-time passcode
	Biometric	Template theft	Capture device authentication; challenge response
Eavesdropping, theft, and copying	Password	"Shoulder surfing"	User diligence to keep secret; administrator diligence to quickly revoke compromised passwords; multifactor authentication
	Token	Theft, counterfeiting hardware	Multifactor authentication; tamper resistant/evident token
	Biometric	Copying (spoofing) biometric	Copy detection at capture device and capture device authentication

6.3 User Authentication Security Issues [1]

Table 3.4 **Some Potential Attacks, Susceptible Authenticators, and Typical Defenses**

Attacks	Authenticators	Examples	Typical Defenses
Replay	Password	Replay stolen password response	Challenge-response protocol
	Token	Replay stolen passcode response	Challenge-response protocol; 1-time passcode
	Biometric	Replay stolen biometric template response	Copy detection at capture device and capture device authentication via challenge-response protocol
Trojan horse	Password, token, biometric	Installation of rogue client or capture device	Authentication of client or capture device within trusted security perimeter
Denial of service	Password, token, biometric	Lockout by multiple failed authentications	Multifactor with token

6.4 Access Control [1]

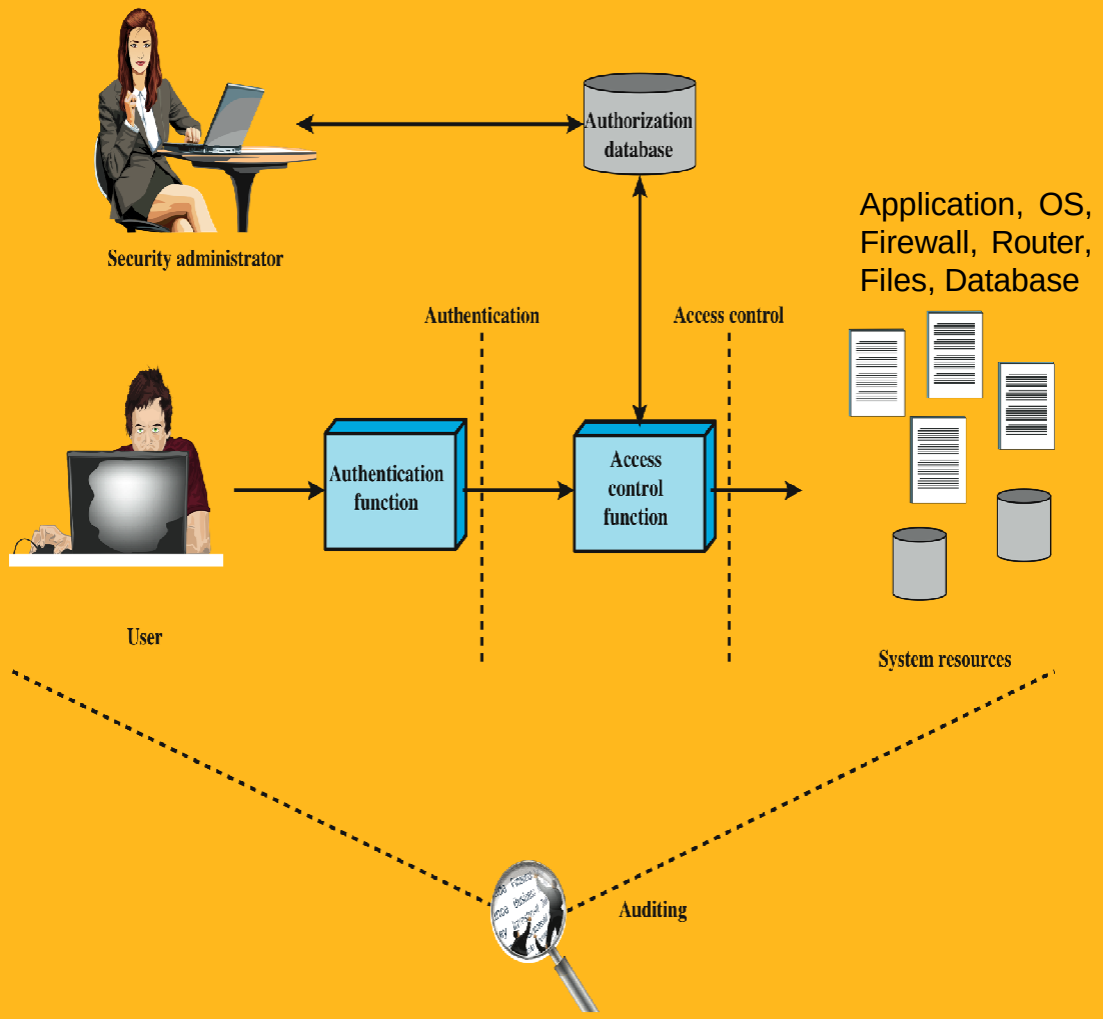
Two definitions of access control are useful in understanding its scope.

1. NIST IR 7298 defines access control as the process of granting or denying specific requests to:
   (1) obtain and use information and related information processing services; and
   (2) enter specific physical facilities.
2. RFC 4949 defines access control as a process by which use of system resources is regulated according to a security policy and is permitted only by authorized entities (users, programs, processes, or other systems) according to that policy.

6.4 Access Control [1]

- Access control implements a security policy that specifies who or what (e.g., in the case of a process executing on behalf of a user) may have access to each specific system resource (such as applications, operating systems, firewalls, routers, files and databases) and the type of access that is permitted in each instance.

6.4 Access Control [1]



Authentication: Verification that the credentials of a user or other system entity are valid.

Authorization: The granting of a right or permission to a system entity to access a system resource. This function determines who is trusted for a given purpose.

Audit: An independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, to detect breaches in security, and to recommend any indicated changes in control, policy and procedures.

6.4 Access Control [1]

- The system must first authenticate an entity seeking access. The authentication function determines whether the user is permitted to access the system at all.
- Then the access control function determines if the specific requested access by this user is permitted.
- A security administrator maintains an authorization database that specifies what type of access to which resources is allowed for this user.
- The access control function consults this database to determine whether to grant access.
- An auditing function monitors and keeps a record of user accesses to system resources.

6.4 Access Control [1]

- Access control policies are generally grouped into the following categories:
  - Discretionary access control (DAC)
  - Mandatory access control (MAC)
  - Role-based access control (RBAC)
  - Attribute-based access control (ABAC):

6.4 Access Control [1]

- Discretionary access control (DAC)
  - Controls access based on the identity of the requestor and on access rules (authorizations) stating what requestors are (or are not) allowed to do
- Mandatory access control (MAC)
  - Controls access based on comparing security labels with security clearances
- Role-based access control (RBAC)
  - Controls access based on the roles that users have within the system and on rules stating what accesses are allowed to users in given roles
- Attribute-based access control (ABAC)
  - Controls access based on attributes of the user, the resource to be accessed, and current environmental conditions

6.4 Access Control [1]

Subject

An entity capable of accessing objects

Three classes
- Owner
- Group
- World

Object

A resource to which access is controlled

Entity used to contain and/or receive information

Access right

Describes the way in which a subject may access an object

Could include:
- Read
- Write
- Execute
- Delete
- Create
- Search

6.4 Access Control [1]

Discretionary Access Control (DAC)

- Controls access based on the identity of the requestor and on access rules (authorizations) stating what requestors are (or are not) allowed to do.
- This policy is termed discretionary because an entity might have access rights that permit the entity, by its own volition, to enable another entity to access some resource.
- DAC means that the owner of the file (i.e. the user) determines what information is accessible to whom.
- DAC is widely implemented in most operating systems, e.g. UNIX. In UNIX file system– RWX assigned by file owners.

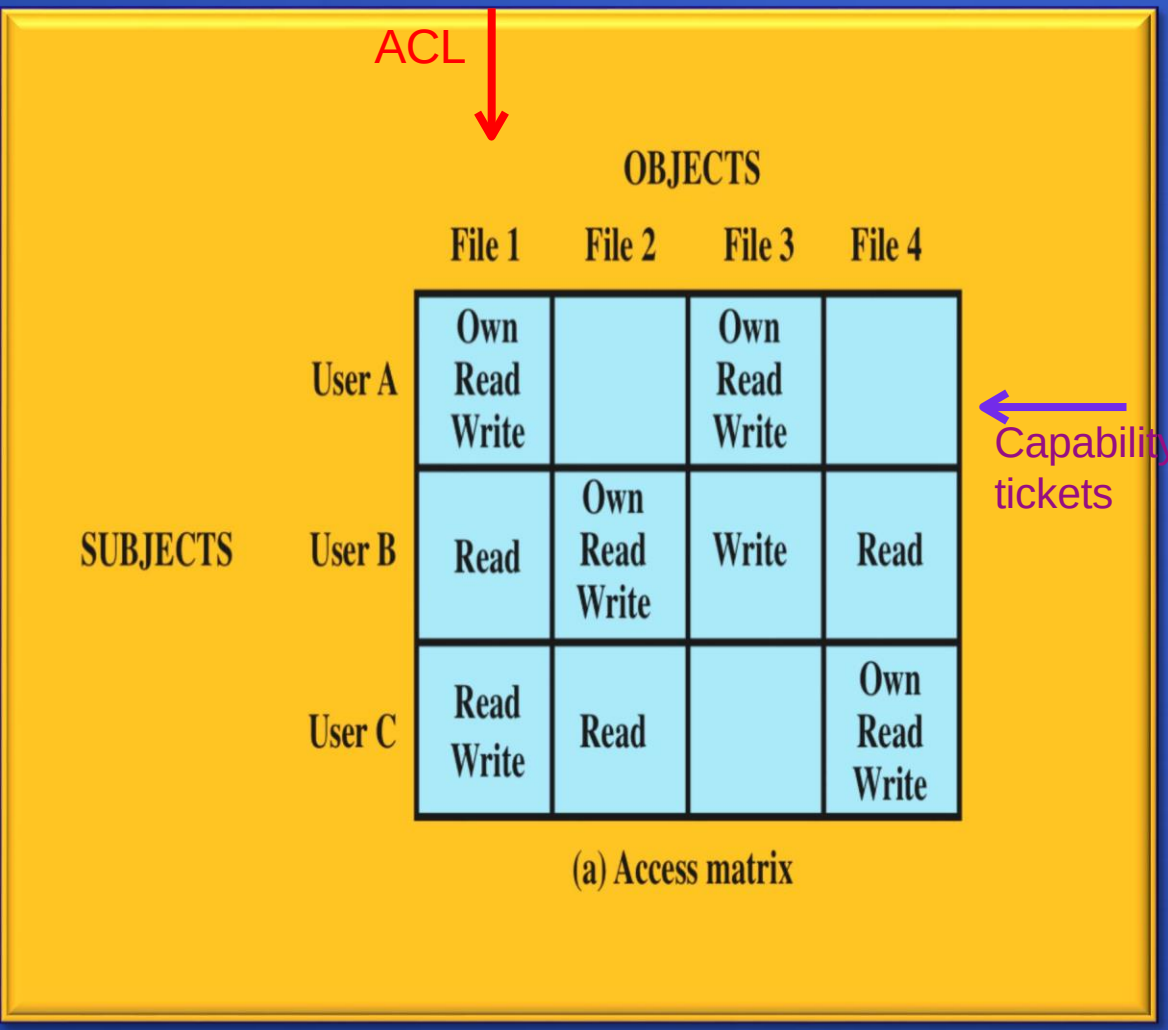
6.4 Access Control [1]

Discretionary Access Control (DAC)

- A general approach to DAC, as exercised by an operating system or a database management system, is that of an access matrix.
- often provided using an access control matrix
  - one dimension consists of identified subjects that may attempt data access to the resources
  - the other dimension lists the objects that may be accessed
- each entry in the matrix indicates the access rights of a particular subject for a particular object

6.4 Access Control [1]

Discretionary Access Control (DAC) → Access Control Matrix

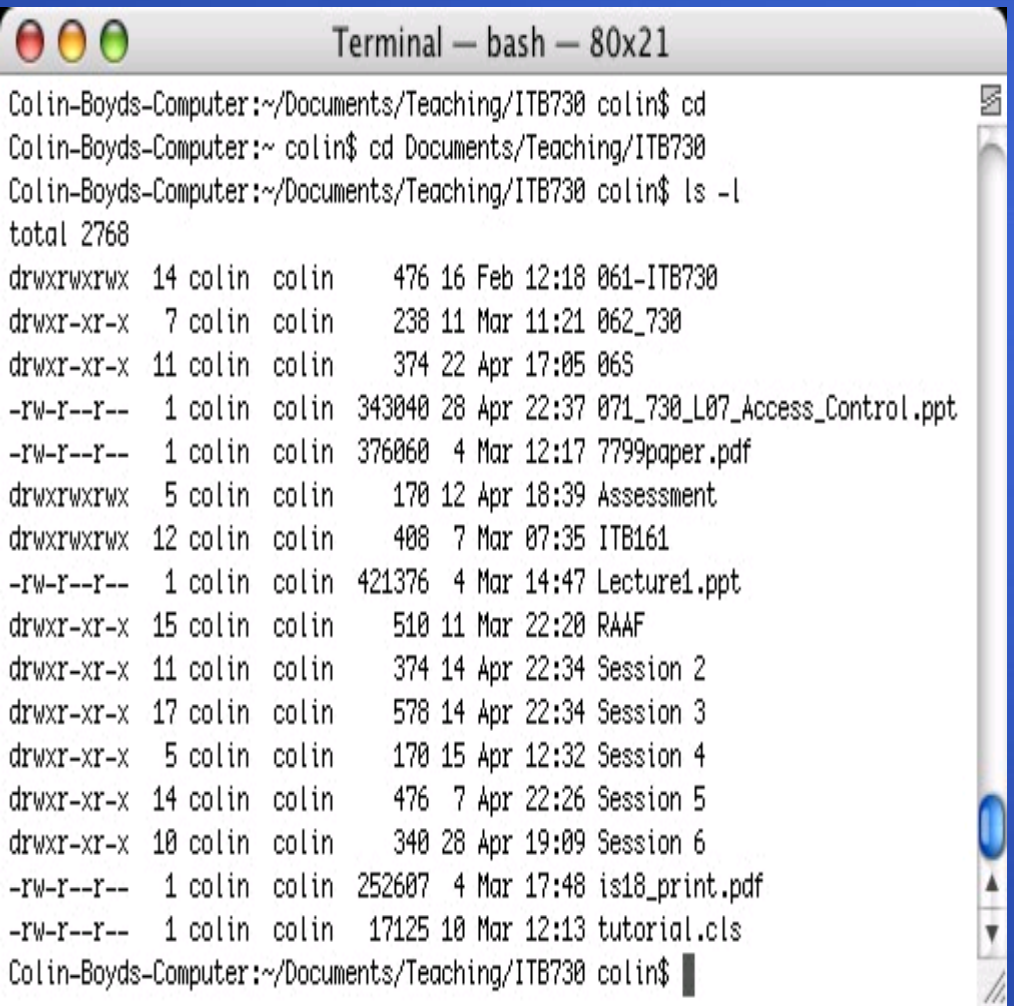


- often provided using an access control matrix
  - lists subjects in one dimension (rows)
  - lists objects in the other dimension (columns)
  - each entry specifies access rights of the specified subject to that object
- Access control matrix is often sparse
  - can decompose by either row (Capability Tickets) or column (ACLs)

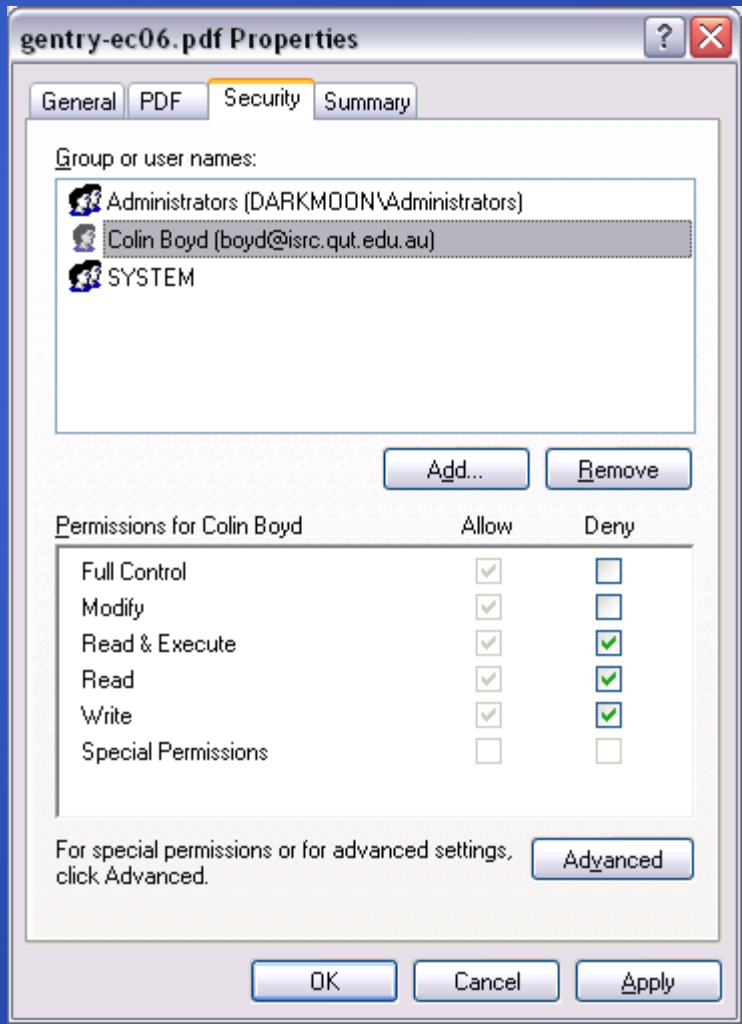
6.4 Access Control [1]

Discretionary Access Control (DAC)

Apple OS X



Windows



6.4 Access Control [1]

Mandatory Access Control (MAC)

- Controls access based on comparing security labels (which indicate how sensitive or critical system resources are) with security clearances (which indicate system entities are eligible to access certain resources). This policy is termed mandatory because an entity that has clearance to access a resource may not, just by its own volition, enable another entity to access that resource.
- Therefore, MAC means that some central authority (e.g. the security officer) determines what information is accessible to whom. This class of policies includes examples from both industry and government. The philosophy underlying these policies is that information belongs to an organization (rather than individual members of it), and it is that organization which should control the security policy.
- Individual user cannot alter that access.

6.4 Access Control [1]

Mandatory Access Control (MAC)

- MAC policies strive to defend against Trojan horse attacks.
- MAC-enabled systems allow policy administrators to implement organization-wide security policies.
- Unlike with DAC, users cannot override or modify this policy, either accidentally or intentionally.
- This allows security administrators to define a central policy that is guaranteed (in principle) to be enforced for all.
- MAC is more secure than DAC.

6.4 Access Control [1]

Role-Based Access Control (RBAC)

- The relationship of users to roles is many to many, as is the relationship of roles to resources, or system objects
- The set of users changes, in some environments frequently, and the assignment of a user to one or more roles may also be dynamic.
- The set of roles in the system in most environments is relatively static, with only occasional additions or deletions.
- Each role will have specific access rights to one or more resources.
- The set of resources and the specific access rights associated with a particular role are also likely to change infrequently.

6.4 Access Control [1]

Role-Based Access Control (RBAC)

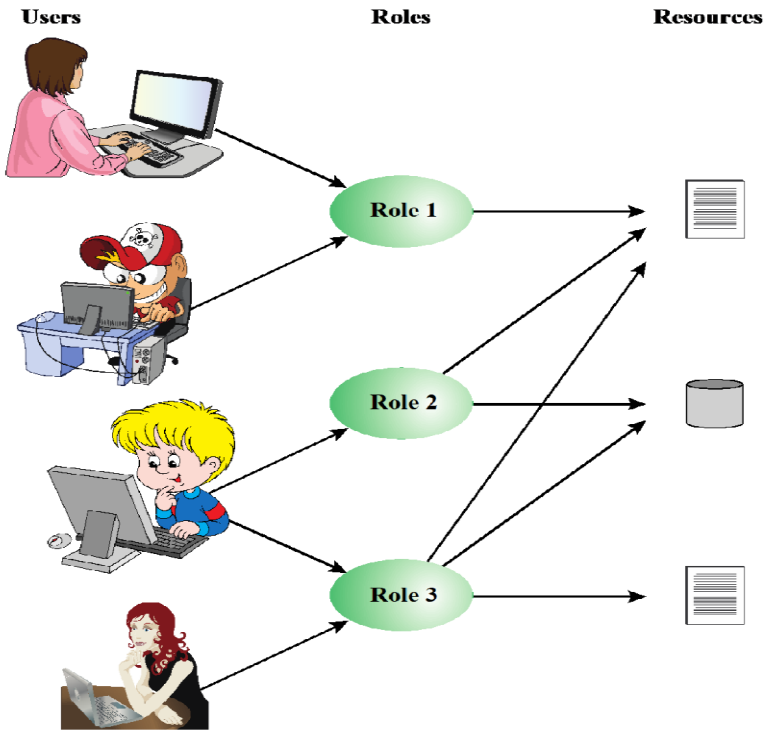


Figure 4.6 Users, Roles, and Resources

6.4 Access Control [1]

Role-Based Access Control (RBAC)

	R_1	R_2	. . .	R_n
U_1	X			
U_2	X			
U_3		X		X
U_4				X
U_5				X
U_6				X
. . .				
U_m	X			

		OBJECTS							
		R_1	R_2	R_n	F_1	F_1	P_1	P_2	D_1	D_2
ROLES	R_1	control	owner	owner control	read *	read owner	wakeup	wakeup	seek	owner
	R_2		control		write *	execute			owner	seek *
	. . .									
	R_n			control		write	stop			

Figure 4.7 Access Control Matrix Representation of RBAC

6.4 Access Control

Attribute-Based Access Control (ABAC)

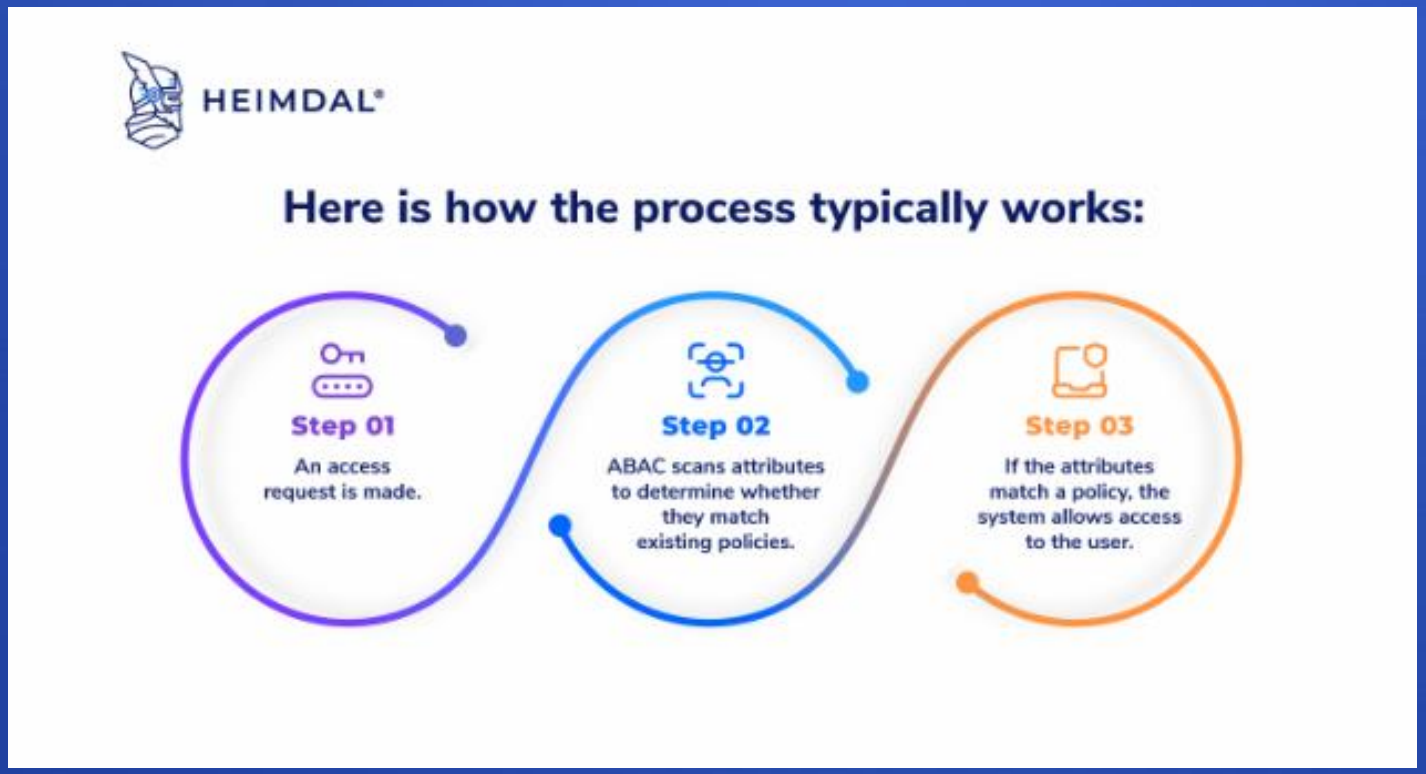
- An identity management-related authentication and authorization system that determines user access based on attributes (or characteristics) rather than roles.
- The attributes associated with subjects (requesters), objects to be accessed, and others have a set of related characteristics, such as location, time of creation, access privileges, and so on.

Source: https://heimdalsecurity.com/blog/what-is-abac-attribute-based-access-control-explained/

6.4 Access Control

Attribute-Based Access Control (ABAC)

- ABAC is to solve RBAC limitation in the complexities of today's digital environment – cloud services, data repositories, mobile, and IoT.



Source: https://heimdalsecurity.com/blog/what-is-abac-attribute-based-access-control-explained/

6.4 Access Control

Attribute-Based Access Control (ABAC)

- Attributes can be categorized as:
  - Subject attributes
  - Action attributes
  - Object attributes
  - Contextual (Environment) attributes

Source: https://heimdalsecurity.com/blog/what-is-abac-attribute-based-access-control-explained/

6.4 Access Control

Attribute-Based Access Control (ABAC) → 1) Subject Attributes

- Attributes of a user
- Example: username, age, job title, user ID, department/company affiliation, security clearance

Attribute-Based Access Control (ABAC) → 2) Action Attributes

- Actions a user wants to perform regarding a resource.
- Example: read, transfer, delete, view, approve

Source: https://heimdalsecurity.com/blog/what-is-abac-attribute-based-access-control-explained/

6.4 Access Control

Attribute-Based Access Control (ABAC) → 3) Object Attributes

- Resource/Object such as file, application, server
- Example: creation date, ownership, file name, data sensitivity

Source: https://heimdalsecurity.com/blog/what-is-abac-attribute-based-access-control-explained/

6.4 Access Control

Attribute-Based Access Control (ABAC) → 4) Environment Attributes

- Indicated the context in which access is requested, like time and place from where access is required, and the type of communication or device type (PC, smartphone, etc)
- Example: the number of transactions already made in the past 24 hours, normal user behavior patterns, relations with a third party, and so on.

Source: https://heimdalsecurity.com/blog/what-is-abac-attribute-based-access-control-explained/

Main References

[1] William Stallings and Lawrie Brown. 2018. Computer Security: Principles and Practice. Pearson.
[2] Mark Ciampa. 2022. CompTIA Security+ Guide To Network Security Fundamentals. Cengage Learning.