Chapter 3: Authentication

What is Authentication?

The process of authentication in the context of computer systems means assurance and confirmation of a user's identity. Before a user attempts to access information stored on a network, he or she must prove their identity and permission to access the data. When logging onto a network, a user must provide unique log-in information including a user name and password, a practice which was designed to protect a network from infiltration by hackers. Authentication has further expanded in recent years to require more personal information of the user, for example, biometrics, to ensure the security of the account and network from those with the technical skills to take advantage of vulnerabilities.

- The main objective of authentication is to allow authorized users to access the computer and to deny access to unauthorized users. Operating Systems generally identify/authenticates users using the following 3 ways: Passwords, Physical identification, and Biometrics. These are explained as following below.

  1. Passwords: Password verification is the most popular and commonly used authentication technique. A password is a secret text that is supposed to be known only to a user. In a password-based system, each user is assigned a valid username and password by the system administrator. The system stores all usernames and Passwords. When a user logs in, their user name and password are verified by comparing them with the stored login name and password. If the contents are the same then the user is allowed to access the system otherwise it is rejected.
  2. Physical Identification: This technique includes machine-readable badges(symbols), cards, or smart cards. In some companies, badges are required for employees to gain access to the organization's gate. In many systems, identification is combined with the use of a password i.e the user must insert the card and then supply his /her password. This kind of authentication is commonly used with ATMs. Smart cards can enhance this scheme by keeping the user password within the card itself. This allows authentication without the storage of passwords in the computer system. The loss of such a card can be dangerous.
  3. Biometrics: This method of authentication is based on the unique biological characteristics of each user such as fingerprints, voice or face recognition, signatures, and eyes.
  4. A scanner or other devices to gather the necessary data about the user.
  5. Software to convert the data into a form that can be compared and stored.
  6. A database that stores information for all authorized users.
  7. Facial Characteristics – Humans are differentiated on the basis of facial characteristics such as eyes, nose, lips, eyebrows, and chin shape.
  8. Fingerprints – Fingerprints are believed to be unique across the entire human population.
  9. Hand Geometry – Hand geometry systems identify features of the hand that includes the shape, length, and width of fingers.
  10. Retinal pattern – It is concerned with the detailed structure of the eye.

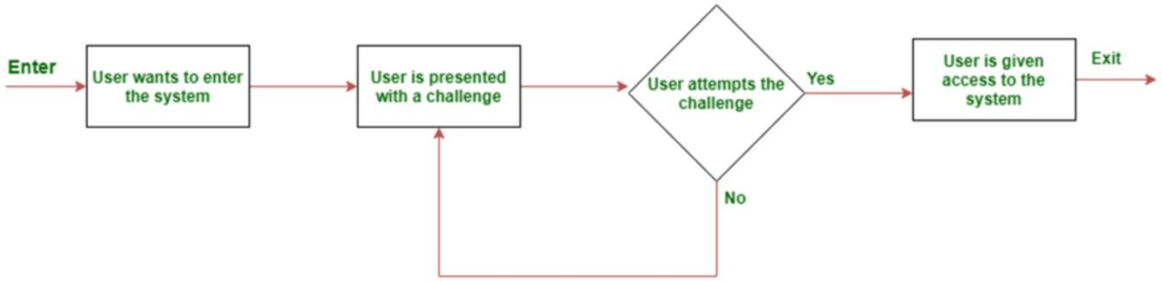
Note: This document is for reference purpose.

11. Signature – Every individual has a unique style of handwriting, and this feature is reflected in the signatures of a person.
12. Voice – This method records the frequency pattern of the voice of an individual speaker.

Challenge Response Authentication

Challenge Response Authentication Mechanism is also called CRAM. It refers to a set of protocols that helps validate actions to protect digital assets and services from unauthorized access. This protocol usually has two components – a question and a response – where a verifier presents a challenge to a user, who must provide a correct answer for authentication. Challenge-response protocols can be as simple as a password or a dynamically generated request.

A challenge response authentication mechanism provides businesses with an easy-to-use tool that they can use to control access to sensitive information and identify bad actors.


Enter
User wants to enter the system
User is presented with a challenge
User attempts the challenge
Yes
No
User is given access to the system
Exit

Types of challenge-response mechanisms

Challenge-response authentication is not a new approach. It has been in use since the early 20th century, when the US military used a paper cryptographic system called DRYAD to authenticate radio users. In this system, users at both ends would read out numbers corresponding to a combination of letters to verify their identities.

In the digital realm, there are two main types of challenges as described below:

Static: True to their name, static challenges are protocols where responses do not change over time. These challenges allow users to select a challenge for authentication purposes. The case of 'forgot password' is an example of a static challenge. Here, when a user forgets the password, he can reset the password by answering a security question that he saved while setting up the account. The answers to these questions remain static, that is, they do not change over a period of time.

Dynamic: In this approach, users must respond to a challenge presented dynamically. These dynamic challenges are based on the premise that if the user is real, he will have a valid answer to the challenge. Therefore, the answers may be different for every challenge. For instance, a one-time password (OTP) or randomly generated token that the user must input to complete the authentication process.

Examples of challenge-response authentication systems

Challenge-response authentication is a method that businesses use to stop bad actors – as well as bots and scripts – from accessing crown-jewel business assets. Commonly used challenge response authentication mechanisms are:

- CAPTCHA: An automated method to distinguish between humans and bots, CAPTCHA is designed to prevent bots from disseminating spam, registering fake new accounts and hacking into genuine user accounts.
- Password: A server validates the password provided by the user with the correct password.
- Biometrics: To authenticate themselves users must provide their biometric details (such as iris or fingerprint scans) that are matched with those saved in the authentication system.
- Salted Challenge Response Authentication Mechanism (SCRAM): A hashed challenge is used such that the password can be used only once. The server validates the user-provided hash by matching with the saved hash, protecting the password from exposure through replay or man-in-the-middle attacks.
- SSH (Secure SHell): This is a cryptographic network protocol that facilitates secure operation of network services securely over an unsecured network. It authenticates communication sessions between servers using a public key infrastructure (PKI).
- Password proof system: This is a cryptographic method that helps verify passwords between two users without sharing their passwords mutually.
- Challenge-Handshake Authentication Protocol: CHAP is a three-way handshake where hash values are generated and verified between the authenticating system, challenge message, and the local system. If these hash values match, further action is allowed else the session is terminated.
- OATH Challenge-Response Algorithm: Developed by the Initiative for Open Authentication, OCRA is a cryptographically strong challenge-response authentication protocol.
- MD5: In this mechanism, the RADIUS server directs a challenge to the client, which creates an MD5 hash of the challenge and the password that the user enters. These are then sent back to the server which uses the correct plaintext password from the database to validate the MD5 hash.

Uses of challenge-response authentication

Challenge-response authentication is mainly used in the following three areas.

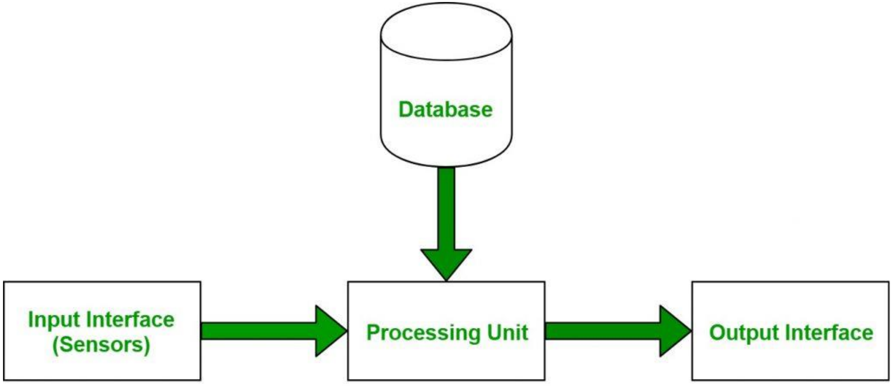
To verify passwords: When a user enters a password to log into a digital account, the password is matched with that saved on the server. In case the two passwords match, the user is successfully authenticated and allowed to continue with the onward digital journey. In case of a mismatch, appropriate countermeasures are used.

To distinguish between bots and humans: Bot attacks can disrupt business operations and degrade user experience. For instance, scalper bots can shop items in bulk during an online sale event, denying genuine consumers a fair chance to score a deal. Bad actors deploy bots and use stolen consumer details to complete unauthorized transactions at scale. Many businesses use challenge-response authentication for human verification to stop bots by affording consumers an opportunity to prove they are not bots. One of the common examples of human verification challenge-response authentication is CAPTCHA.

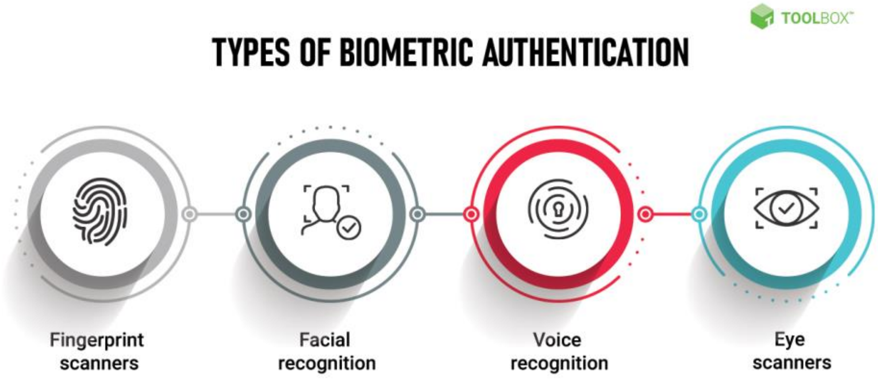
To train machine learning programs: Challenge-response authentication trains machine learning and artificial intelligence programs to solve complex programs. For instance, they are made to solve human verification puzzles and the outcome is matched with that of a human user. The programs learn from the feedback which improves their decision-making over time.

Biometric authentication:

is defined as a security measure that matches the biometric features of a user looking to access a device or a system. Access to the system is granted only when the parameters match those stored in the database for that particular user. Biometric characteristics are the physical and biological features unique to every individual. These are saved in a database and can be easily compared to the user attempting to access the data or device. Such biometric authentication can be placed in various physical environments such as doors, gates, server rooms, military bases, airports, and ports. Today, biometric authentication tools have become a part of most consumer devices, particularly computers and smartphones.



Biometric System



Authentication can be in one of the following forms

Note: This document is for reference purpose.

Identification: Matching an individuals features against all records to check whether his/her record is present in the database.

Verification: To check whether the person is who he/she is claiming to be. In this case the features of the person is matched only with the features of the person they claims to be.

Types of Biometrics:

There are two broad categories of biometrics:

Physiological Biometrics

Behavioral Biometrics

Physiological Biometrics:

Physical traits are measured for identification and verification in this type of biometrics. The trait should be chosen such that it is unique among the population, and resistant to changes due to illness, aging, injury, etc.

Physiological Biometric Techniques:

Fingerprint: Fingerprints are unique for every individual. They can be measured in several ways. Minutiae-based measurement uses graphs to match ridges whereas image-based measurement finds similarities between the individuals' fingertips image and fingerprint images present in the database. It has high level of security and used both for identification and verification. However, due to old age or diseases/injury, fingerprint may get altered. Common usage: in mobiles for verification, in offices for identification.

Facial Recognition: Features of the face like distance between nose, mouth, ears, length of face, skin color, are used for verification and identification. Accuracy can be affected by fog, sunglasses, aging, etc.

Iris and Retina:Patterns found in the eye are unique and can be used for both identification and recognition. Devices to analyze retina are expensive and hence it is less common. Diseases like cataract may alter iris patterns

Voice Recognition: The pitch, voice modulation, and tone, among other things are measured. Security is medium, due to the similarity in voice of people, hence used mostly for verification. The accuracy can be hindered due to the presence of noise, or due to aging or illness.

DNA: DNA is unique and persistent throughout lifetime. Thus security is high and can be used for both identification and verification

Behavioral Biometrics:

Traits of human behavior are measured in this case. Monitoring is required in this type of biometrics to prevent impersonation by the claimant

Signature: Signature is one of the most commonly used biometrics. They are used to verify checks by matching the signature of the check against the signature present in the database. Signature tablets and special pens are used to compare the signatures. Duration required to write the signature can also be used to increase accuracy. Signatures are mostly used for verification.

Keystroke Dynamics: This technique measures the behavior of a person when typing on a keyboard. Some of the characteristics take into account are:

Typing speed.

Frequency of errors

Duration of key depressions

Criteria for selection of Biometric:

- Universality: Each person should possess the biometric trait which is being used. For example, everyone has a face but it is not the case with GAIT biometric (for wheelchair users).
- Uniqueness: No two persons must be same in terms of the biometric trait being used i.e. everyone must be unique in terms of the biometric trait being used.
- Permanence: Biometric trait must be invariant over time i.e. it shouldn’t change over time.
- Collectability: Biometric trait must be easily measurable.
- Performance: Processing of the biometric trait must be accurate and fast.
- Secure: It must be secure and can’t be copied.
- Acceptability: People should be willing to accept the biometric system.

Benefits of using Biometric system over traditional authentication systems:

Invariant: Biometric traits are invariant over time as smart cards get damaged over time but biometric traits doesn’t.

Accountability: If there is a security breach, then biometric ensures who can be the responsible person for the breach but in traditional methods, smart cards can be stolen and used by someone else. Hence, accountable person is easily identifiable nowadays by using biometric.

Easy to use: Biometric systems are easy to use.

Convenient: User doesn’t have to remember passwords, pins and keep safe the smart cards like before.

More secure: Biometric trait can’t be stolen or copied.

Privacy Issues Surrounding Biometrics:

Biometrics requires data of individuals like physiological and behavioural traits be stored in order for identification and verification. This may hinder their privacy, which is considered as a basic fundamental right. Also, there is fear of the stored data being used against them. Since biometric data for an individual is mostly unique, there is fear of it being used to monitor measurement of individuals. Therefore, the data must be stored securely and access to the database must be hierarchical.

Note: This document is for reference purpose.