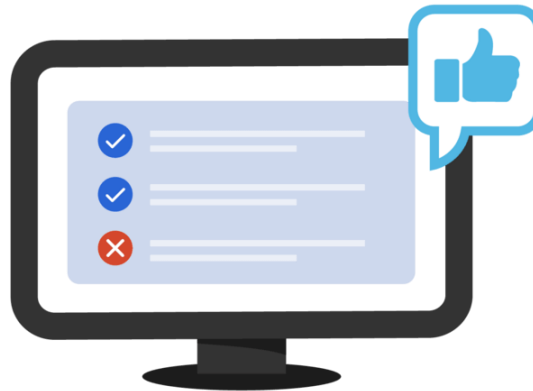


Authentication



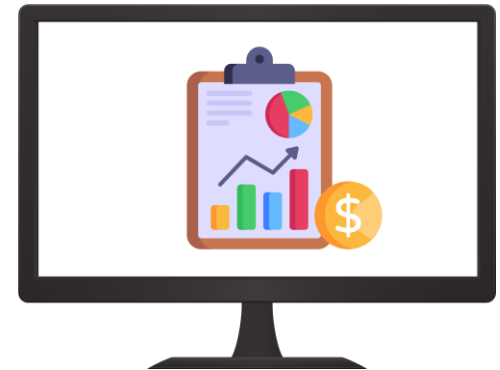
Confirms users are who they say they are.

Authorization



Gives users permission to access a resource.

Accounting



Measures the resources a user consumes during access

Authentication, Authorization, and Accounting (AAA)

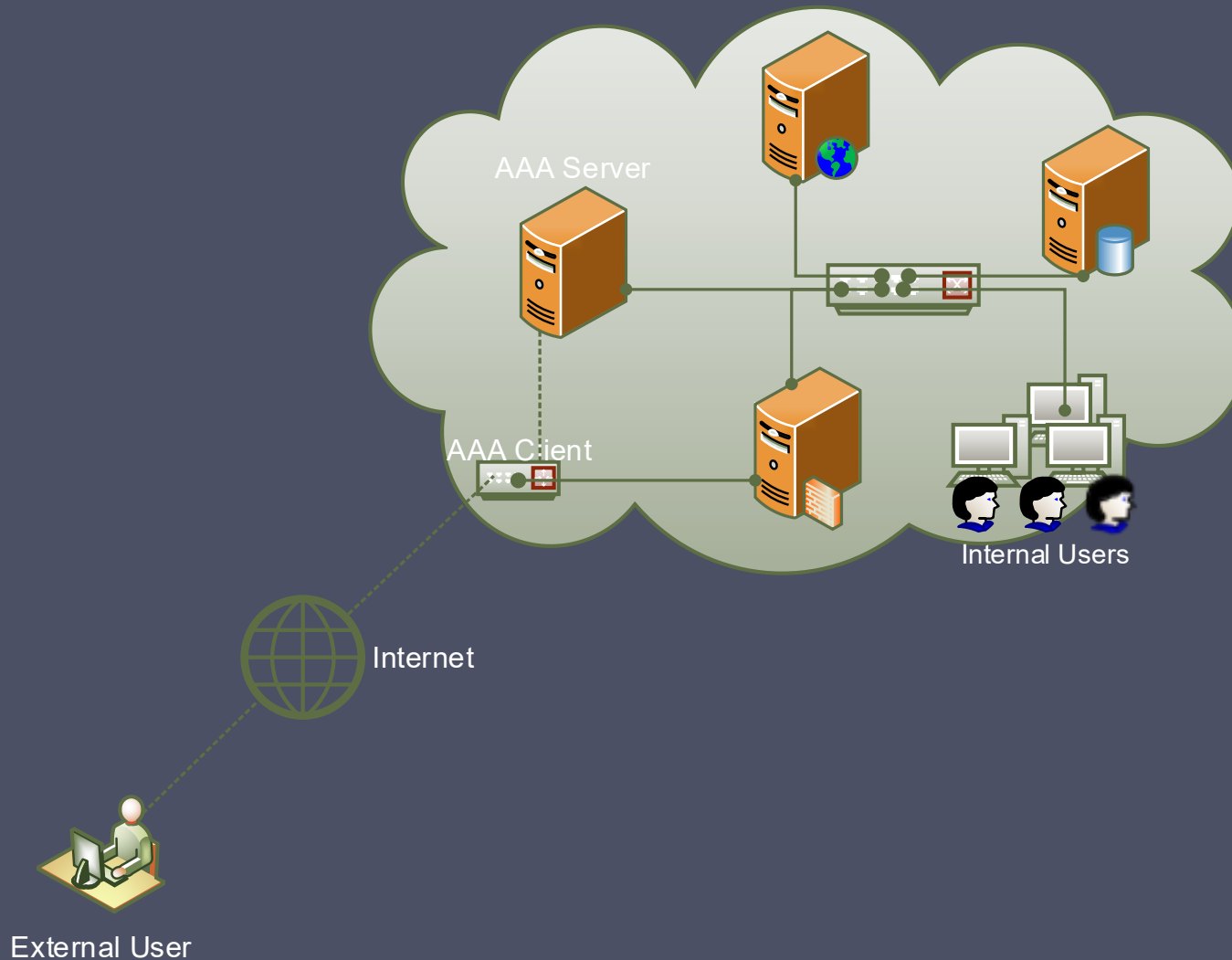
AAA is a term referred to the framework for

- Intelligently controlling access to the systems and resources
- Enforcing policies
- Auditing usage...

Illustration – Physical World



Illustration – Cyber World



IDENTITY & ACCESS MANAGEMENT



AAA vs. IAM

AAA

- AAA (Authentication, Authorization, and Accounting) is a general term that refers to a set of security processes that control access to computer resources.
- AAA servers are primarily used for network infrastructure.

IAM

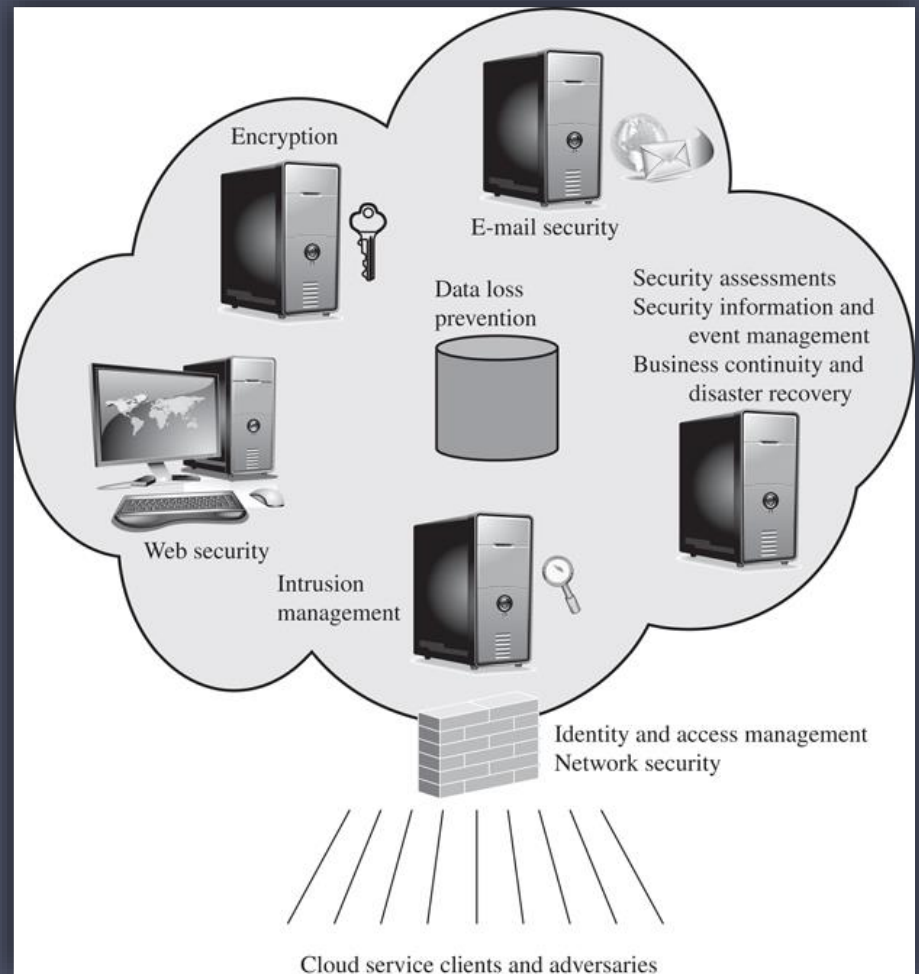
- IAM (Identity and Access Management) is a specific set of technologies and policies used to manage access to an organization's IT resources.
- IAM systems are used for managing access to enterprise applications and data.

Identity and Access Management (IAM)

To ensure that the right people and things have

- ☞ the right access to
- ☞ the right resources
- ☞ at the right time.

IAM include establishing trusted user profile and policy information, using it to control access within the cloud service, and doing this in an auditable way.



Elements of Cloud Security as a Service

Identity Theft

- Consumers lost \$56 billion to identity fraud in America during 2021 [CNBC]
- The COVID-19 pandemic has created more points of vulnerability
- Identity theft scams - criminals interact directly with consumers to steal their information through methods such as robocalls and phishing emails.
- Three common red flags to watch
 - **Unsolicited calls or emails**
 - **High-pressure tactics**
 - **Outdated passwords**



MEANS OF USER AUTHENTICATION

Recap

Authentication



Confirms users
are who they say they are.

Authorization



Gives users permission
to access a resource.

Accounting

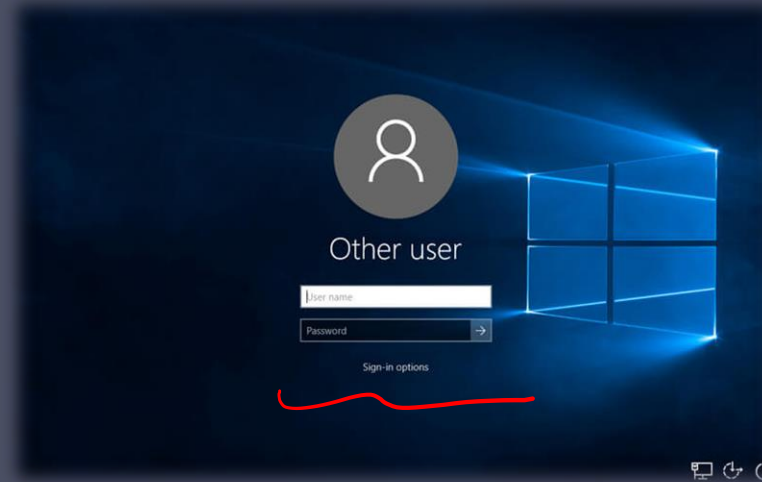


Measures the resources a user
consumes during access

The four means of authenticating user identity are based on:

1/4
Something
the
individual
knows

- Password, PIN, answers to prearranged questions



The four means of authenticating user identity are based on:

2/4

Something the individual possesses (token)

- Smartcard, electronic keycard, physical key



The four means of authenticating user identity are based on:

3/4

Something
the individual
is (static
biometrics)

- Fingerprint, retina, face



The four means of authenticating user identity are based on:

4/4

Something the individual does
(dynamic biometrics)

- Voice pattern, handwriting, typing rhythm



Summary

The four means of authenticating user identity are based on:

Something
the
individual
knows

- Password, PIN, answers to prearranged questions

Something
the
individual
possesses
(token)

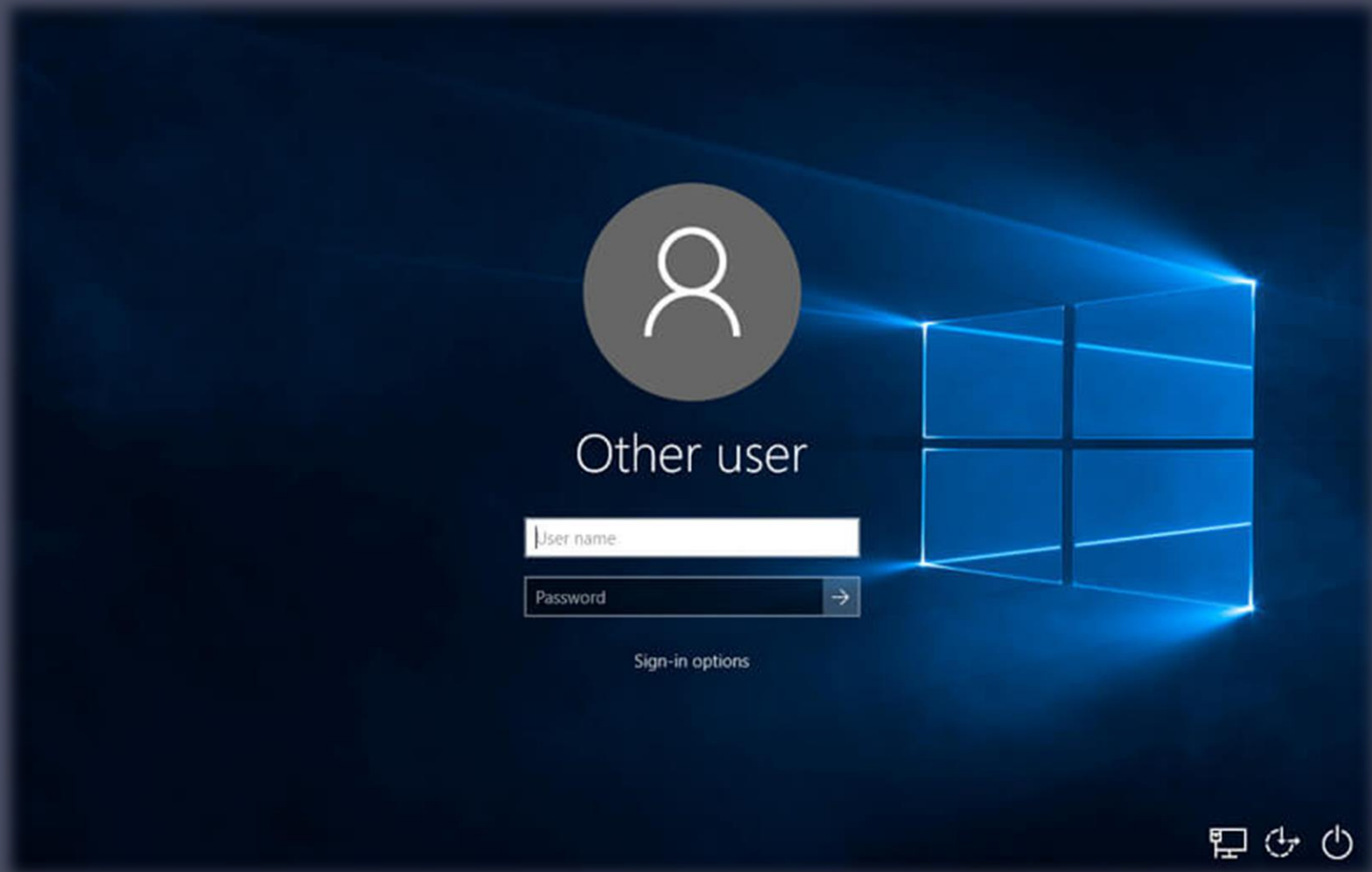
- Smartcard, electronic keycard, physical key

Something
the
individual is
(static
biometrics)

- Fingerprint, retina, face

Something
the
individual
does
(dynamic
biometrics)

- Voice pattern, handwriting, typing rhythm



PASSWORD-BASED AUTHENTICATION

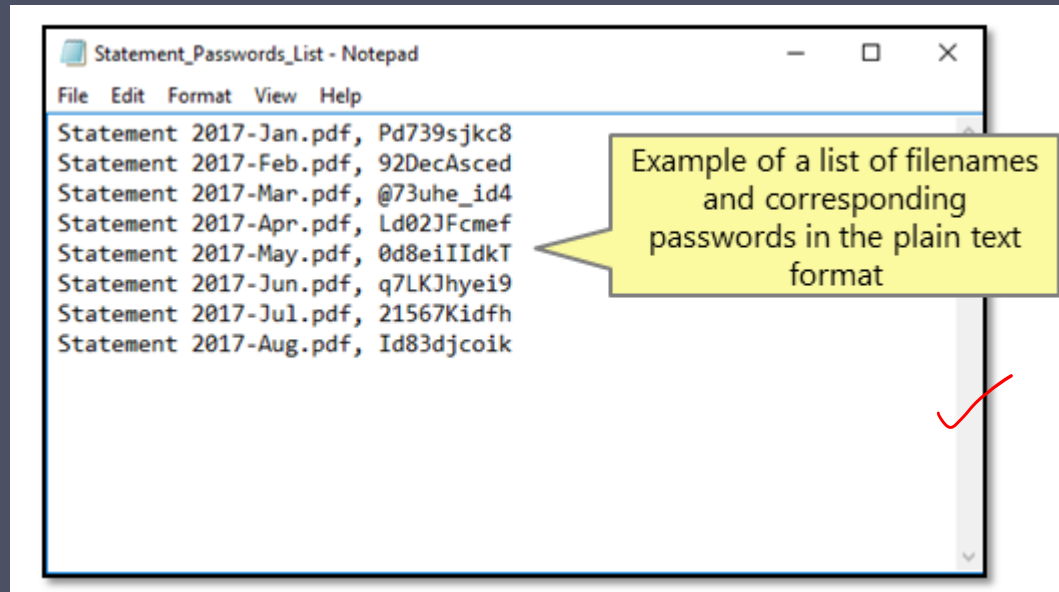
Password-Based Authentication



- Widely used line of defense against intruders
 - User provides name/login and password
 - System compares password with the one stored for that specified login
- The user ID:
 - Determines that the user is authorized to access the system
 - Determines the user's privileges
 - Is used in discretionary access control

PASSWORD STORAGE

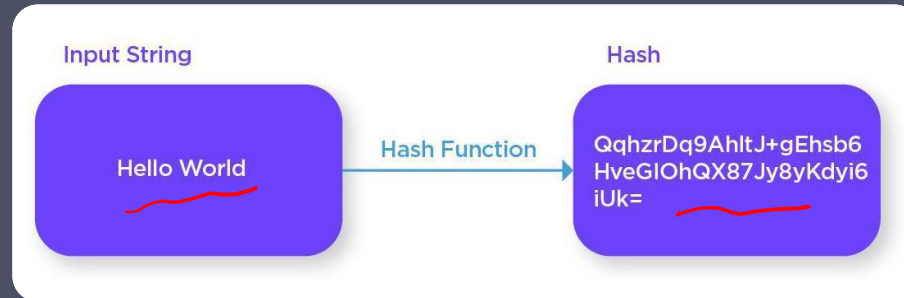
Plain Text



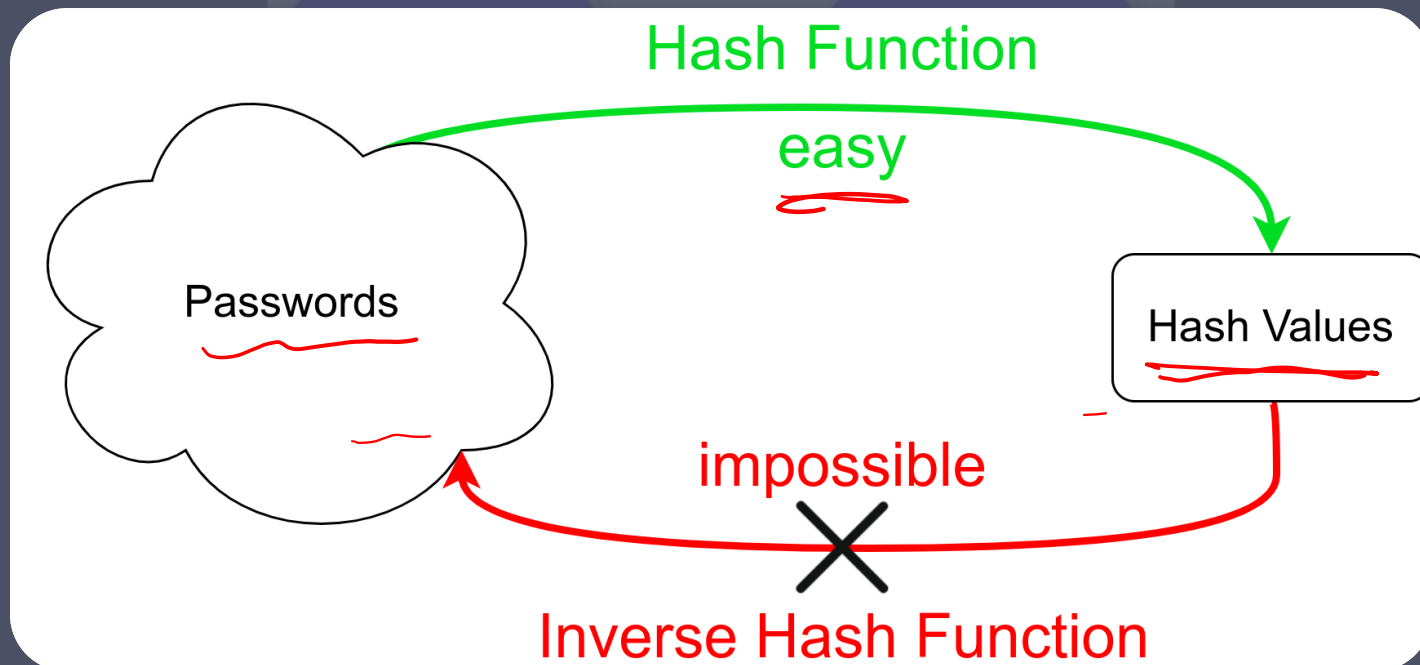
- Storing passwords in plaintext dangerous
 - because it puts both the system and users at risk.

PASSWORD STORAGE

Hash Function



Demo

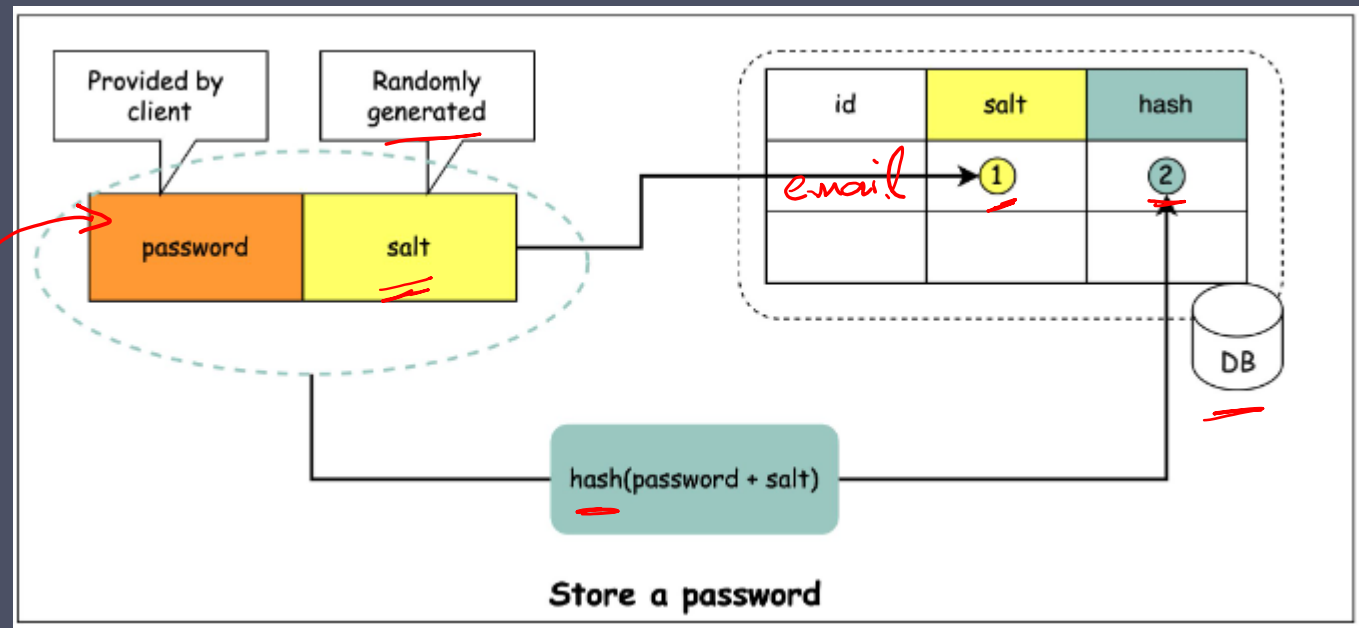


SIGN UP

Email

Password

SIGN UP

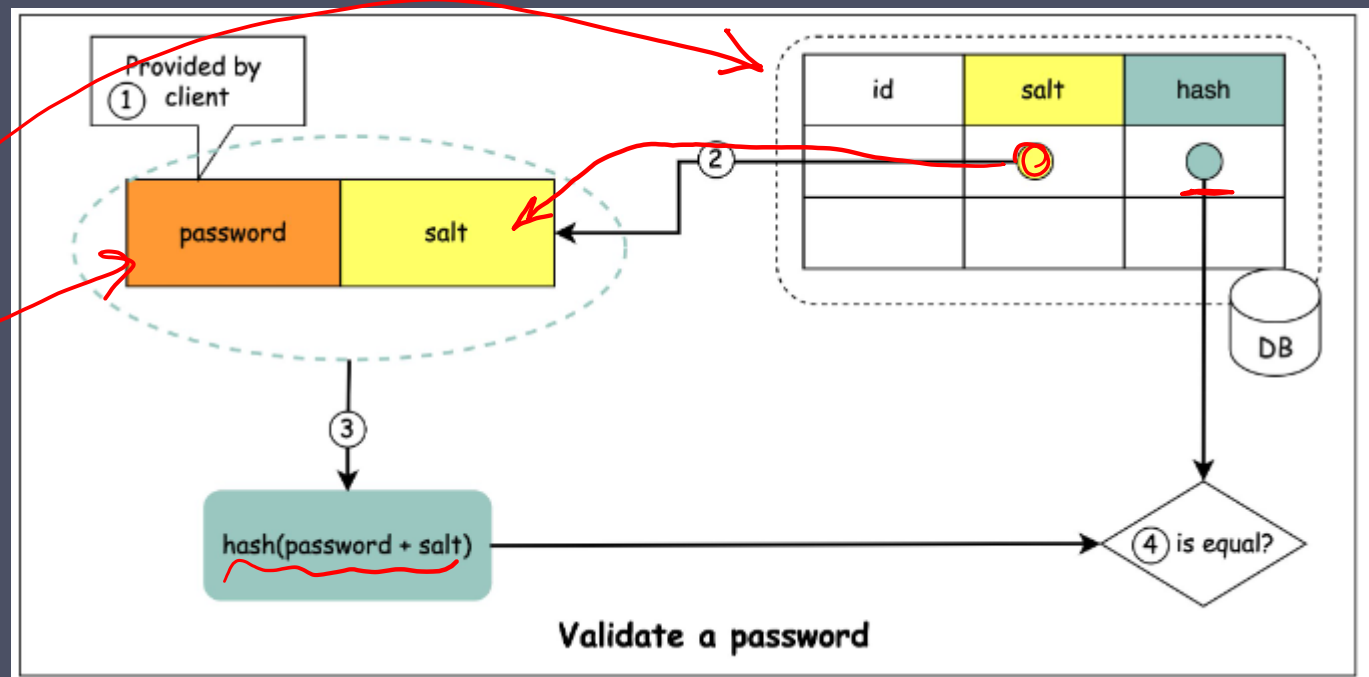


Login

Username*

Password*

Login





Password Vulnerabilities

Password Hacking and Cracking

- Password hacking and password cracking are terms that are often used interchangeably, but there is a subtle difference between the two.
- Password Hacking
 - refers to gaining unauthorized access to a system
 - Usually, original password is changed
- Password Cracking
 - to the process of attempting to recover a password
 - Usually, original password is NOT changed

Password Vulnerabilities

Exploiting user mistakes

- Users more likely use default passwords, write or share the passwords through social engineering tactics

Exploiting multiple password use

- Different network devices share the same or a similar password for a given user

Electronic monitoring

- Password communicated across a network in plaintext format

Brute force Attack

- Try all possible passwords

Offline dictionary attack

- Compares the password hashes against hashes of commonly used passwords

Rainbow table attacks

- Pre-compute tables of hash values of ALL passwords*

Offline Dictionary Attack

Dictionary of Commonly Used Passwords

Password	Password Hash
Jhon	Hkdjutye ✗
Secret	Lfjaskebad ✗
Bold	Fasf572dnas ✗
2023	Adnskjf30 ✗
World	42n34nasd
...	...
...	...
<u>Cooler</u>	Af45xbc2js ✓
...	...

Target User

UID	Password Hash
Admin	<u>af45xbc2js</u>

Rainbow Table Attack

Hash Values of ALL Passwords
(of Length 04 in this example)

Password	Password Hash
<u>Aaaa</u>	Kfj8673hdb
Aaab	Hfge7w95j
Aaac	Jfhty673
Aaad	Hdg486hd
Aaae	Hdri9274
...	...
...	...
<u>Cool</u> ✓	Rh75jd3h5 ✓
...	...

Target User

UID	Password Hash
Admin	<u>Rh75jd3h5</u>

2222