

Information Security

Authentication

Lecturer: Nguyễn Thị Thanh Vân – FIT - HCMUTE

Objective

- ☞ Understand the importance of authentication
- ☞ Learn how authentication can be implemented
- ☞ Understand threats to authentication

Contents

- 🔗 Introduction
- 🔗 Electronic User Authentication Principles
- 🔗 Password-Based Authentication
- 🔗 Token-Based Authentication
- 🔗 Biometric Authentication
- 🔗 Remote User Authentication
- 🔗 Security Issues for User Authentication

04/03/2025

3

AAA architectures

- 🔗 AAA is an architectural framework for configuring:



Authentication - Who is allowed access?

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



Authorization - What are they allowed to do?

The granting of a right/permission to a system entity to access a system resource



Accounting - What did they do?

examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures



04/03/2025

4

AAA architectural

Authentication
Who are you?



Accounting
What did you spend it on?

Authorization
How much can you spend?

Statement of Personal Credit Card Account

Cardmember Name: JOE EMPLOYEE Account Number: 1234-456-890 Statement Closing Date: 01-31-01

Statement Cycle: 02-01-01 to 01-31-01 Payment Due Date: 03-01-01

Credit Limit: \$1,000.00 Credit Available: \$1221.50

New Balance: \$278.50 Minimum Payment Due: \$20.00

Account Summary

Previous Balance:	+74.24	Transaction Fees:	+3.50
Purchases:	+250.50	Annual Fees:	+25.50
Cash Advances:	+0	Current Amount Due:	+250.50
Payments:	-74.25	Amount Paid Due:	+0
Finance Charge:	+0	Amount Over Credit Limit:	+0
Late Charge:	+0	NEW BALANCE:	\$278.50

Reference Number	Date	Posted	Activity Since Last Statement	Amount
43234567	01-03	01-13	Payment, Thank You	-\$14.25
11234567	01-12	01-13	Wings 'N' Things	\$25.25
78901234	01-14	01-17	Record Release	\$40.00
45678901	01-14	01-17	Sports Stadium	\$75.25
3210987	01-22	01-23	Tie Tack	\$20.75
76543210	01-29	01-30	Electronic World	\$89.25
2345678	01-30	01-30	Transaction Fees	\$3.00
34567890	01-01	01-01	Annual Fee	\$25.00

PAGE 1 OF 1

04/03/2025

5

What is Authentication?



Authentication
Who are you?
Prove it.

You are who you say you are.

Authorization
Does this person have permission to access the requested resources?

You have permission to access these resources

Computer Resources

Authentication Goals

❖ Availability:

- ❖ when the correct credentials are presented, the resources should be made available to the processor (on behalf of the user).

❖ No false negatives:

- ❖ if a process presents incorrect credentials but is given access
- ❖ These should not happen.

❖ No false positives:

- ❖ if a process presents the correct credentials but is denied access
- ❖ These should not happen either



Login Attacks Quiz

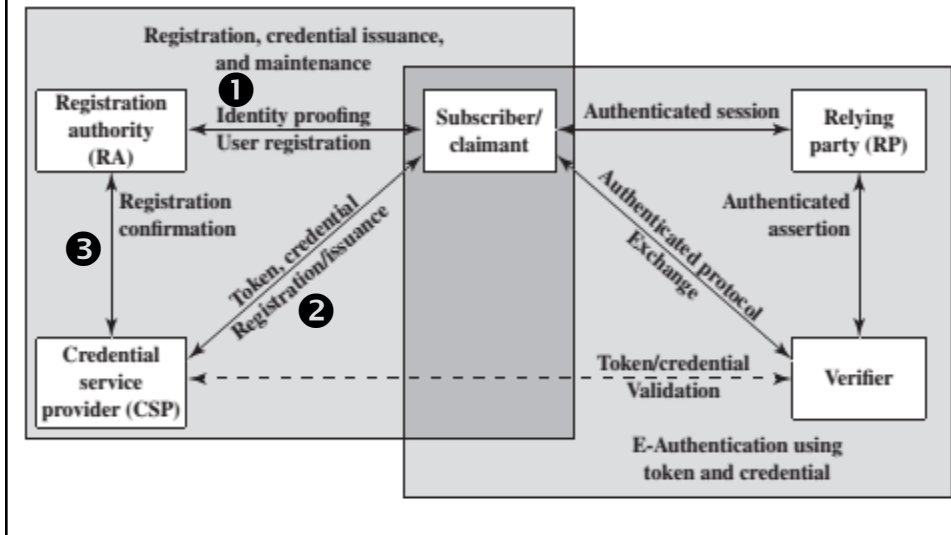
Check the correct answer from the choices.

An attacker correctly guesses Alice's password and logs in as her. Is this a case of...



- ☐ False negative
- ☐ True positive
- ☐ False positive
- ☐ True negative

Authentication Architectural Model



Authentication Quiz

Check the correct answer from the choices.

We now have personal devices that are not shared across multiple users. What threats motivate the use of authentication in such devices?

- ☐ Malware infection that may exfiltrate sensitive data
- ☐ Loss of theft of the device

The evolution of authentication technology



- ↻ 1961: Password (Fernando J. Corbató, MIT): storing plaintext passwords
- ↻ Late 1960s: password encryption (Robert Morris, Bell Labs.) hash of password
 - extremely difficult to crack. Hackers can build password scanners.
- ↻ 1980s: Dynamic Passwords
 - The passwords change based on factors such as time, location, or physical password updates.
 - Two dynamic password protocols: Time-based one-time (OTP) and HMAC based OTP.
- ↻ Late 1990s: Public Key Infrastructure
 - Transport Layer Security protocol - TLS
 - Late 1990s, Taher Elgamal - an engineer at Netscape - developed Secure Sockets Layer (SSL)

05/03/2025

11

The evolution of authentication technology



- ↻ 2000s: multi-factor authentication and single sign-on
- ↻ 2010s: Biometrics
 - In 2011, the Motorola ATRIX Android was the first mobile device to feature a fingerprint
 - Apple is behind the times with Touch ID technology. By 2017, Apple had a FaceID technology,
 - Biometric authentication technology provides a higher level of security and convenience
- ↻ Decades of 2020: Passwordless Authentication
 - use the authentication key (physical key, virtual key application on smartphones) then activate the biometric key for authentication.
 - Big technology trend

04/03/2025

12

Means of Authentication

Something the individual knows



Password
PIN,
Answer

Something the individual process



Smart card
Physical key
Token

Something the individual is (Static biometrics)



fingerprint
retina,
Face
iris

Something the individual does (Dynamic biometric)



Voice, gait
Handwriting
Typing rhythm

04/03/2025

13

Means of Authentication

🔗 GOTPass: users employ “images and a one-time numerical code” in order to secure password.

- o using patterns and images instead of letters and numbers
- o the generated digits random code



04/03/2025

14

Authentication Methods

- ☞ Authentication: Verifies user access to the operating system
- ☞ Physical authentication:
 - Allows physical entrance to company property
 - Magnetic cards and biometric measures
- ☞ Digital authentication: verifies user identity by digital means
- ☞ Digital certificates: identifies and verifies holder of certificate
- ☞ Digital token (security token):
 - Small electronic device
 - Displays a number unique to the token holder;
 - Uses a different password each time
- ☞ Digital card: Also known as a security card or smart card
 - Similar to a credit card; uses an electronic circuit instead of a magnetic strip
 - Stores user identification information
- ☞ Kerberos:
 - Developed by MIT
 - Uses tickets for authentication purposes

15

Authentication Methods (continued)

- ☞ Lightweight Directory Access Protocol (LDAP):
 - Developed by the University of Michigan
 - A centralized directory database stores:
 - Users (user name and user ID)
 - Passwords
 - Internal telephone directory
 - Security keys
 - Efficient for reading but not suited for frequently changing information
- ☞ NT LAN Manager (NTLM):
 - Developed and used by Microsoft
 - Employs a challenge/response authentication protocol
- ☞ Public Key Infrastructures (PKI):
 - User keeps a private key
 - Authentication firm holds a public key
 - Encrypt and decrypt data using both keys

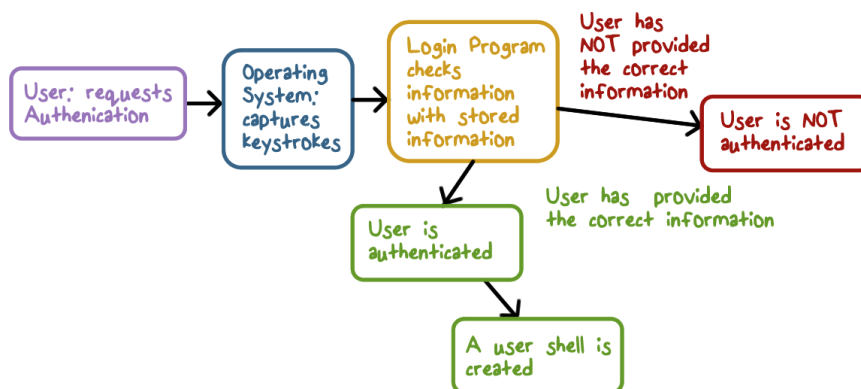
16

Authentication Methods (continued)

- ✎ RADIUS: used by network devices to provide a centralized authentication mechanism
 - **RADIUS provides:** Authentication, Authorization, Accounting
- ✎ Secure Socket Layer (SSL): authentication information is transmitted over the network in an encrypted form
- ✎ Secure Remote Password (SRP):
 - Password is not stored locally
 - Invulnerable to brute force or dictionary attacks

17

How is Authentication Implemented?



Risk Assessment for User Authentication

- Assurance level: the degree of confidence
 - Level 1:** Little or no confidence in the asserted identity's validity.
 - Level 2:** Some confidence in the asserted identity's validity.
 - Level 3:** High confidence in the asserted identity's validity
 - Level 4:** Very high confidence in the asserted identity's validity.
- Potential impact: potential impact on organizations r individuals should there be a breach of security
 - Low: adverse effect on organizational operation
 - Moderate: serious adverse effect
 - High: severe or catastrophic adverse effect
- areas of risk.: mapping between the potential impact and the appropriate level of assurance

Risk Assessment for User Authentication

- areas of risk.

Potential Impact Categories for Authentication Errors	Assurance Level Impact Profiles			
	1	2	3	4
Inconvenience, distress, or damage to standing or reputation	Low	Mod	Mod	High
Financial loss or organization liability	Low	Mod	Mod	High
Harm to organization programs or interests	None	Low	Mod	High
Unauthorized release of sensitive information	None	Low	Mod	High
Personal safety	None	None	Low	Mod/ High
Civil or criminal violations	None	Low	Mod	High

Common Means of Authentication

✎ Password-Based Authentication

- ✎ The Vulnerability of Passwords
- ✎ The Use of Hashed Passwords
- ✎ Dynamic Passwords

✎ Token-Based Authentication

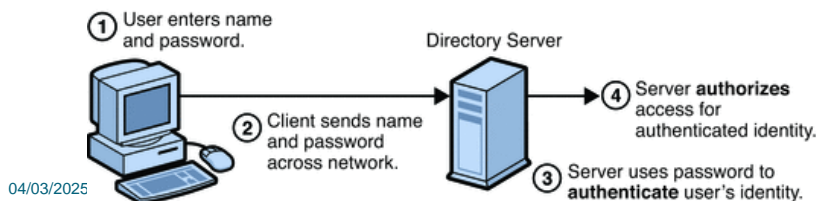
✎ Biometric Authentication

✎ Passwordless authentication

21

Password-Based Authentication

- ✎ The password systems defense against intruders
- ✎ Systems require: user provide name or ID + password
 - all multiuser systems,
 - network-based servers,
 - Web-based e-commerce sites,
 - and other similar services
- ✎ The password serves to authenticate the ID of the individual logging on to the system.



04/03/2025

22

The Vulnerability of Passwords

1. Offline dictionary attack:

- ☞ A hacker gain access to the system password file.
- ☞ Compares the password hashes against hashes of commonly used passwords.

2. Specific account attack:

- ☞ Attacker targets a specific account & submits password guesses until the correct password is discovered.

3. Popular password attack / Against single user:

- ☞ The attacker chooses a popular password and tries it.
- ☞ Attacker attempts to gain knowledge about the account holder and system password policies and uses that knowledge to guess the password.

04/03/2025

23

The Vulnerability of Passwords

4. Workstation hijacking:

- ☞ The attacker waits until a logged-in workstation is unattended.

5. Exploiting user mistakes:

- ☞ User is more likely to write it down passwords, because it is difficult to remember.

6. Exploiting multiple password use.

- ☞ Similar password for a many applications

7. Electronic monitoring:

- ☞ If a password is communicated across a network to log on to a remote system, it is vulnerable to eavesdropping.

04/03/2025

24

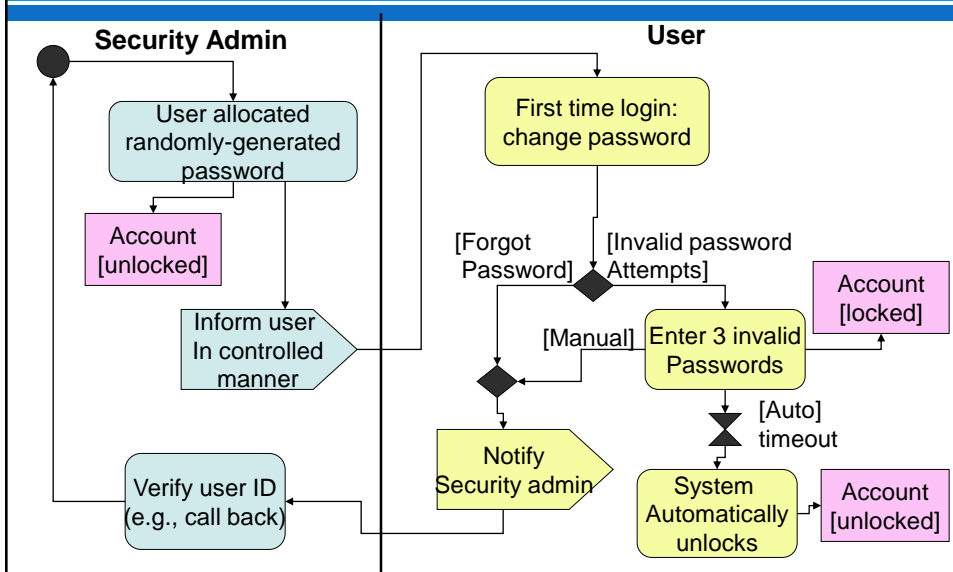


Password Popularity Quiz

Check which passwords made the top 10 most common passwords for 2014:

<input type="checkbox"/> 123456	<input type="checkbox"/> 696969
<input type="checkbox"/> password	<input type="checkbox"/> 123123
<input type="checkbox"/> letmein	<input type="checkbox"/> batman
<input type="checkbox"/> abc123	<input type="checkbox"/> qwerty
<input type="checkbox"/> 111111	<input type="checkbox"/> 123456789

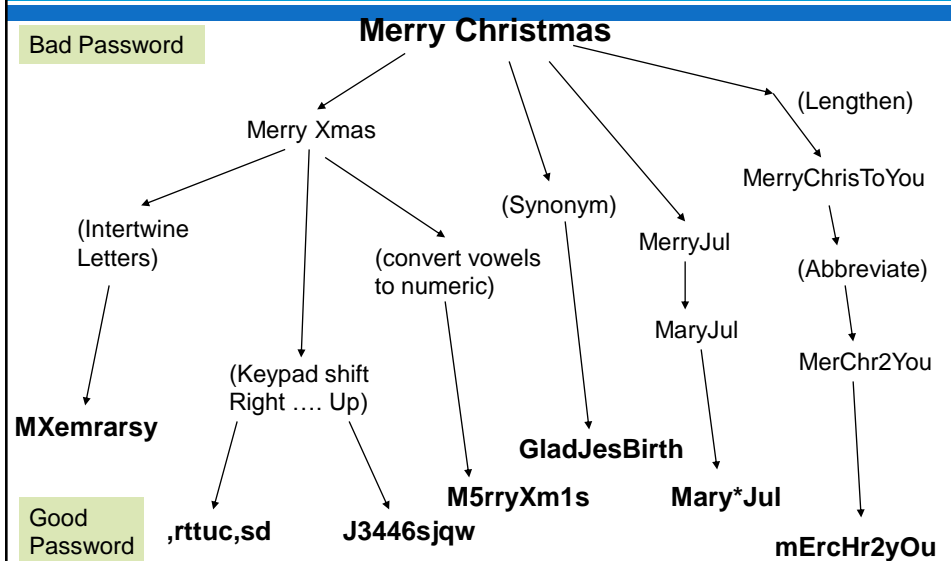
Recommended Password Allocation



Password Rules

- ↻ One-way encrypted using a strong algorithm
- ↻ Never written down and retained near terminal or in desk
- ↻ should be changed every 30 days, by notifying user in advance
- ↻ A history of passwords should prevent user from using same password in 1 year
- ↻ Passwords should be ≥ 8 (better 12) characters, including 3 of: alpha, numeric, upper/lower case, and special characters
- ↻ Passwords should not be identifiable with user, e.g., family member or pet name
- ↻ Four basic techniques are in use:
 - User education
 - Computer-generated passwords
 - Reactive password checking
 - Complex password policy

Creating a Good Password



Admin & Login ID Rules

- ☞ Restrict number of admin accounts
 - should never be locked out, whereas others are
 - Login IDs should follow a confidential internal naming rule
- ☞ Admin password:
 - should only be known by one user
 - can be kept in locked cabinet in sealed envelope, where top manager has key
- ☞ Common accounts: Guest, Administrator, Admin should be renamed
- ☞ Session time out should require password re-entry

Single Sign On

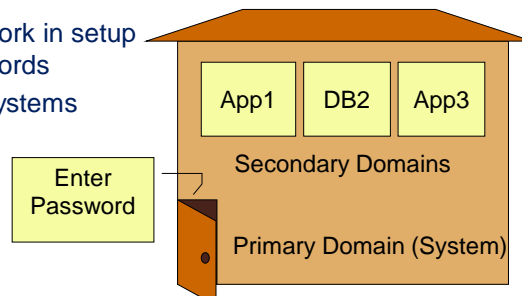
Single Sign On (SSO) is the ability for a user to enter the same id and password to logon to multiple applications within an enterprise.

Advantages

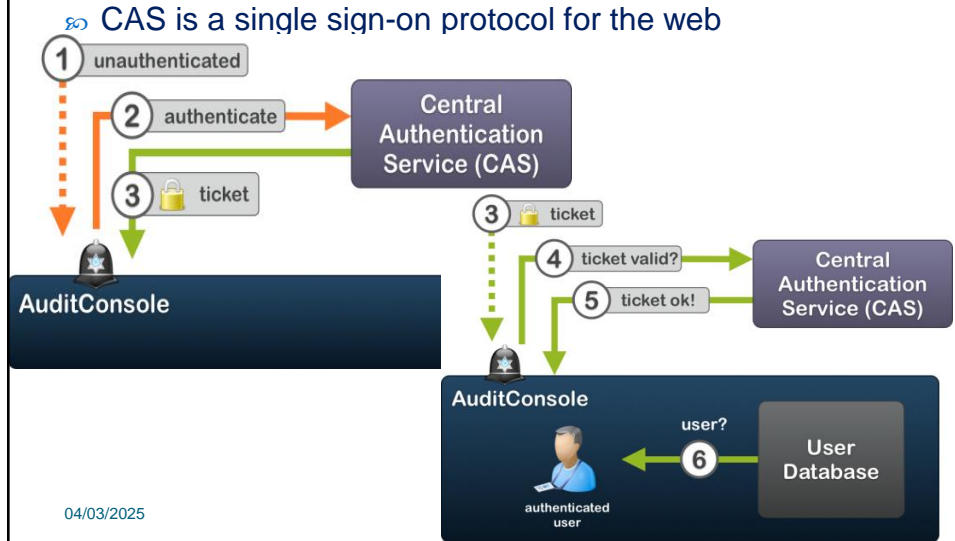
- ☞ One good password replaces lots of passwords
- ☞ IDs consistent throughout system(s)
- ☞ Reduced admin work in setup & forgotten passwords
- ☞ Quick access to systems

Disadvantages

- ☞ Single point of failure -> total compromise
- ☞ Complex software development due to diverse OS
- ☞ Expensive



Central Authentication Service (CAS)



Implementing Password Authentication

How do we check the password supplied with a user id?

Method 1 - store a list of passwords, one for each user in the system file.

- The file is readable only by the root/admin account
- What if the permissions are set incorrectly?
- Why should admin know the passwords?
- If security is breached, the passwords are exposed to an attacker.

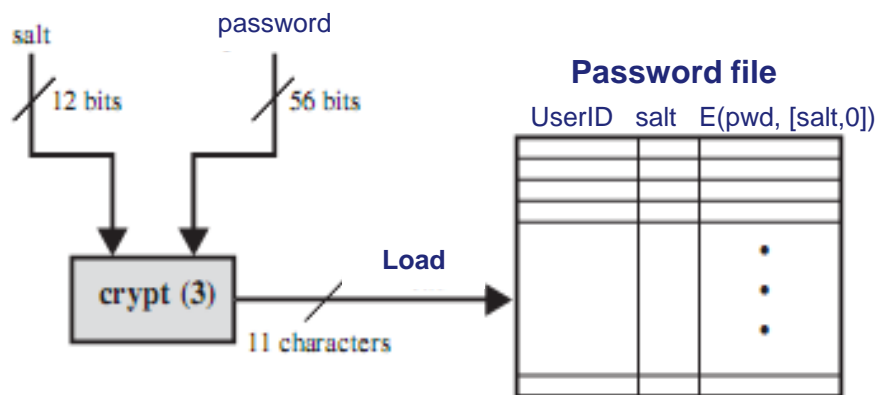
Implementing Password Authentication

How do we check the password supplied with a user id?

Method 2 - do not store passwords, but store something that is derived from them

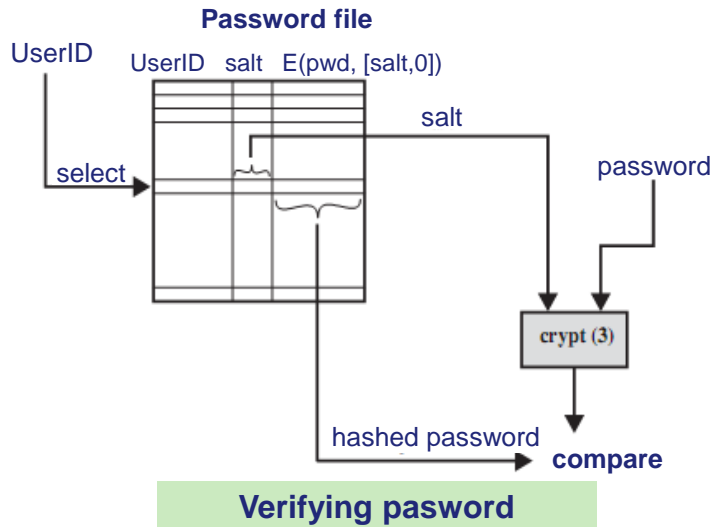
- Use a one-way hash function and store the result
- The password file is readable only for root/admin

UNIX Password Scheme

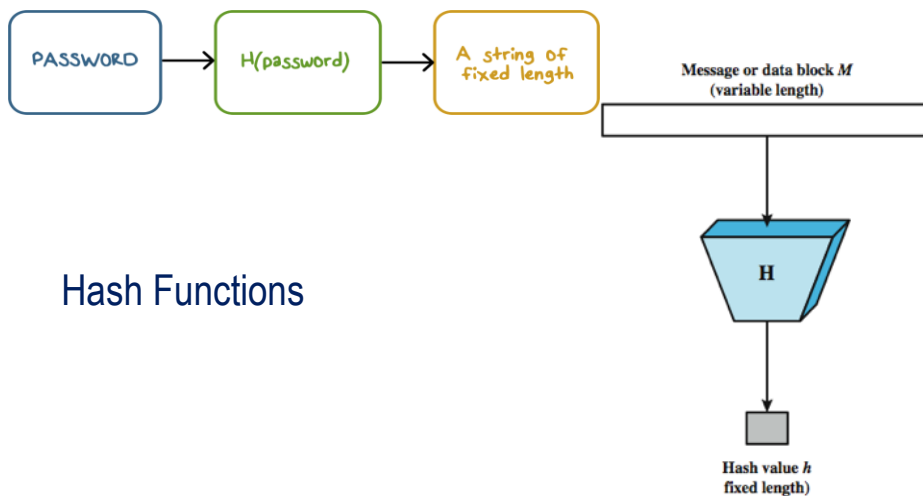


Loading password

UNIX Password Scheme



The Use of Hashed Passwords

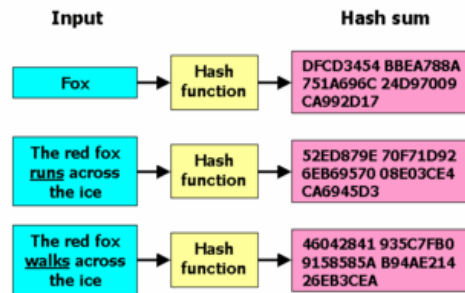


What is Hash Functions

- A hash function maps a *variable-length* message into a *fixed-length* hash value, or message digest

$$h = H(M)$$

- The *principal object*:
 - data integrity*



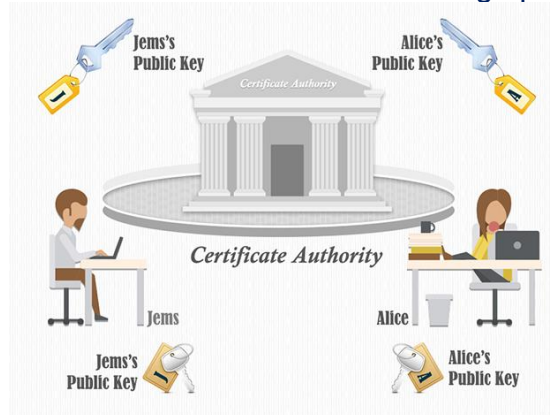
- Problems: hackers could build programs to brute-force guess passwords. To combat this, computer scientists came up with dynamic passwords.

04/03/2025

37

Public Key Infrastructure

- PKI is a mechanism for a third party (CA - Certificate authority) to provide and authenticate the identities of parties involved in the information exchange process.



04/03/2025

38

Public Key Infrastructure

Every PKI must include:

- Certificate authority () = Issuer of digital certificates (including signing)
- Registration authority () = Verifier of identities requesting digital certificates
- Central directory = Where keys are stored
- Certificate management system = Structure for operations, such as accessing stored certifications
- Certificate policy = Statement of PKI requirements

04/03/2025

39

Dynamic Passwords

Two dynamic password protocols:

- **TOTP** = Time-based OTP where the uniqueness of the OTP is generated based on the current time.
- **HOTP** = **HMAC-based** OTP where the uniqueness of the OTP is generated based on the hash of the previous password.

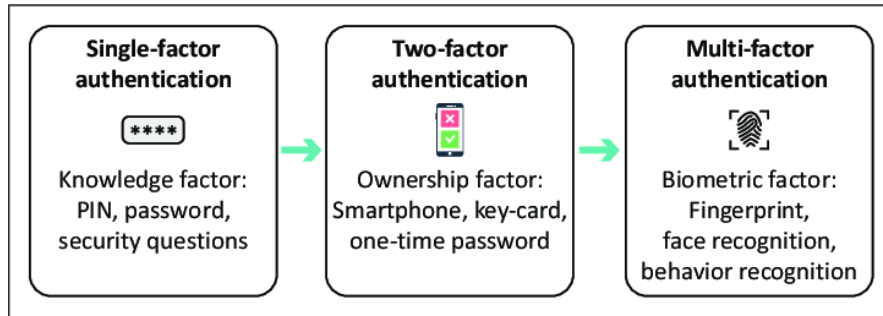


- These passwords change based on variables, like location, time, or a physical password update (like a FOB).
- They remove any risk of and solve the problem caused when users have the same password in many places.
- It's very common for dynamic passwords to be used in conjunction with regular passwords as a form of two-factor authentication (**2FA**).
- Multi-factor authentication (**MFA**) a little later, but it's important to note that it did appear as early as the '80s

04/03/2025

40

Multi-factor authentication



04/03/2025

41

Means of Authentication

🔗 Password-Based Authentication

- 🔗 The Vulnerability of Passwords
- 🔗 The Use of Hashed Passwords
- 🔗 Dynamic Passwords
- 🔗

🔗 Token-Based Authentication

🔗 Biometric Authentication

🔗 Passwordless authentication

42

Token-Based Authentication

Operation



Token Types:

- Card
- Token

04/03/2025

43

Memory Cards

- ✎ Memory cards can store only a simple security code (not process data).
- ✎ The bank card: a magnetic stripe on the back.
- ✎ Using memory card:
 - Alone
 - + PIN
- ✎ Among the potential drawbacks
 - **Requires special reader:** increases the cost hardware and software.
 - **Token loss:** determine the PIN to gain unauthorized access
 - **User dissatisfaction:** use for computer access

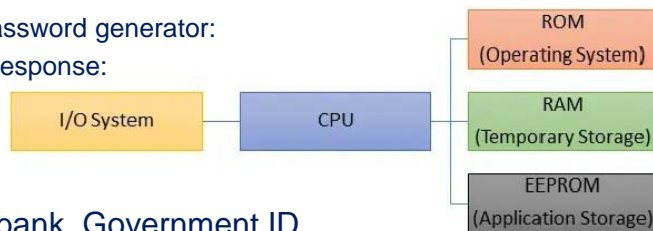


04/03/2025

44

Smart Cards

- ☞ Has own processor, memory, I/O ports
 - Wired or wireless access by reader
 - May have crypto co-processor
 - ROM, EEPROM, RAM memory
- ☞ Executes protocol to authenticate with reader/computer
 - Static:
 - Dynamic password generator:
 - Challenge-response:



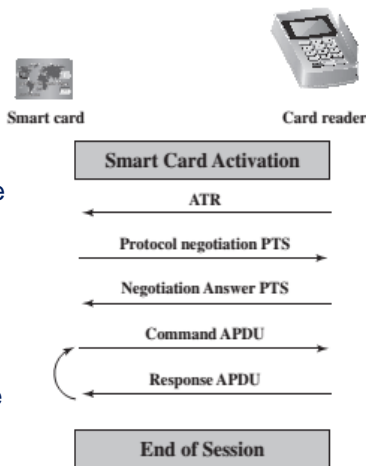
- ☞ Application: bank, Government ID...

04/03/2025

45

Smart Card/Reader Exchange

- ☞ Each time the card is inserted
 - a reset is initiated (clock value)
 - the card responds (the parameters and protocols).
 - The terminal may be able to change the protocol used and other parameters via a protocol type selection (PTS) command.
 - The cards PTS response confirms the protocols and parameters to be used.
 - The terminal and card can now execute the protocol to perform the desired application.



APDU = Application protocol data unit

ATR = Answer to reset

PTS = Protocol type selection

46

04/03/2025

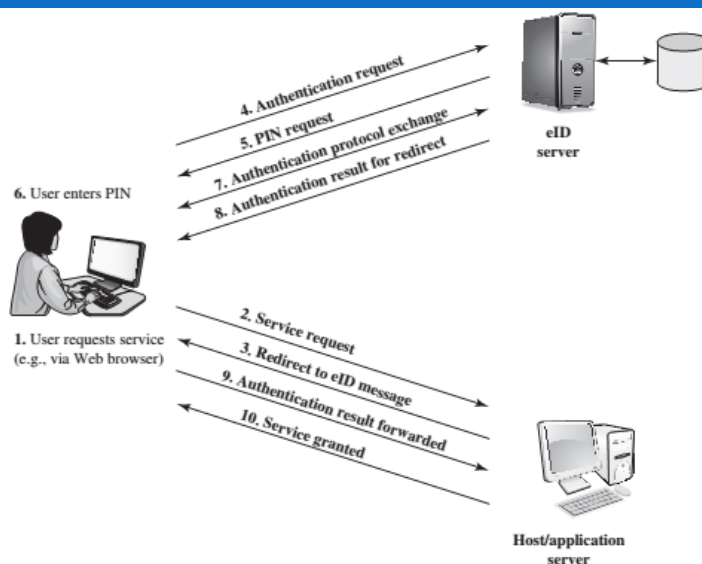
Electronic Identity Cards

- ∞ A smart card as a national identity card for citizens
- ∞ A national electronic identity (eID)
 - national ID cards
 - driver's license
- ∞ an eID card has been verified by the national government as valid and authentic.
- ∞ Functions:
 - **ePass**: stores a digital representation of the cardholder's identity. (electronic passport)
 - **eID**: stores an identity record that authorized service can access
 - **eSign**: stores a private key and a certificate verifying the key

04/03/2025

47

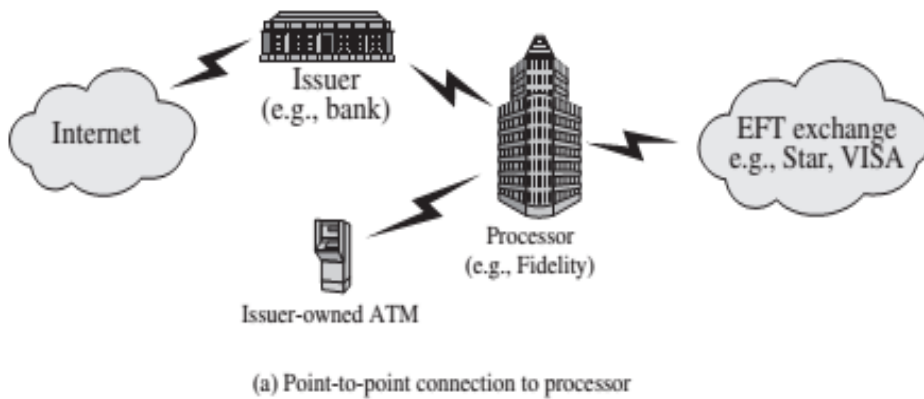
User authentication eID



04/03/2025

48

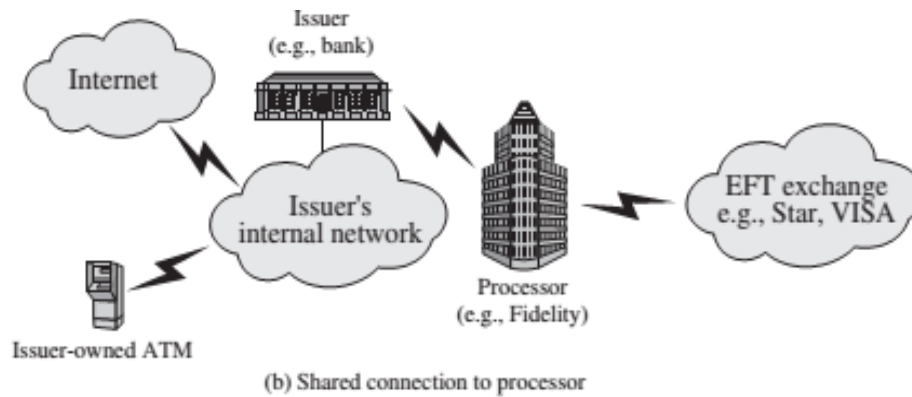
Ex, ATM architectures



04/03/2025

49

Ex, ATM architectures



04/03/2025

50

Means of Authentication

☞ Password-Based Authentication

- ☞ The Vulnerability of Passwords
- ☞ The Use of Hashed Passwords

☞ Token-Based Authentication

☞ Biometric Authentication

51

Biometric Authentication

☞ Advantages of biometric systems:

- Avoid remembering long passwords, losing tokens
- Unique and uncopyable
- Systems and resources become more secure from unauthorized access
- Trusted, standard feature in smart mobile devices

☞ Static, Dynamic



05/03/2025

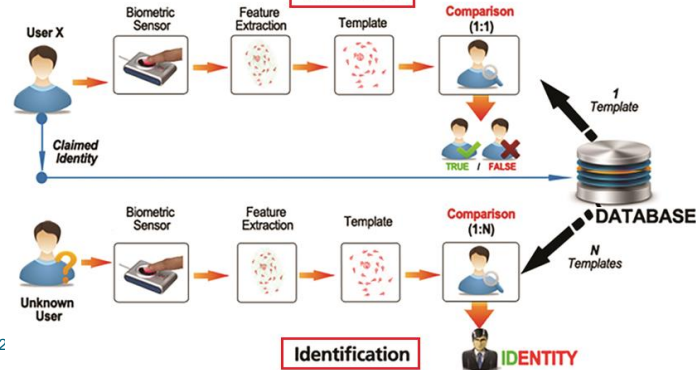
52

Operations of a Biometric Authentication System

Enrollment



Verification



04/03/2

53

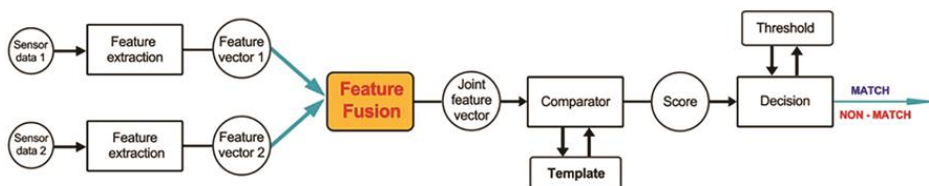
Biometrics: Single factor, Multiple factor

Single factor biometrics.

Limitations:

- Noise problem
- Variable biometric factor
- Successful impersonation by attackers

Multiple factor biometrics. Using Feature Fusion



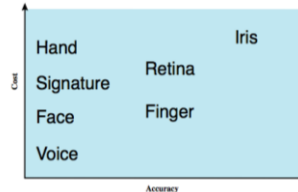
- Advantages: superior recognition performance
- Disadvantages: High cost, long processing time

05/03/2025

54

Biometric authentication

- ∞ based on pattern recognition.
- ∞ more complex and expensive.

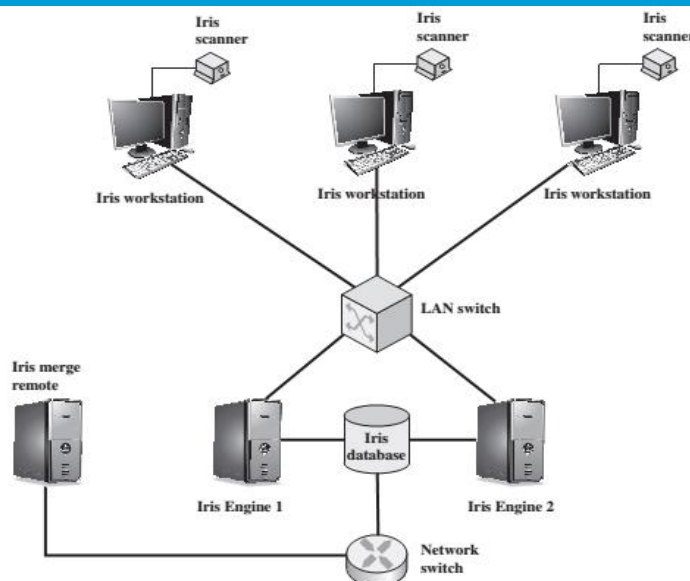


Characteristic	Fingerprints	Hand geometry	Retina	Iris	Face	Signature	Voice
Ease of use	High	High	low	Medium	Medium	High	High
Error incidence	Dryness, dirt, age	Hand injury	Glasses	Poor lighting	Lighting, age, glasses, hair	Changing signatures	Noise, colds, weather
Accuracy	High	High	Very high	Very high	High	High	High
User acceptance	Medium	Medium	Medium	Medium	Medium	Very high	High
Required security level	High	Medium	High	Very high	Medium	Medium	Medium
Long term stability	High	Medium	High	High	Medium	Medium	Medium

04/03/2025

55

EX: General Iris Scan Site Architecture for UAE System



04/03/2025

56

Other Authentication Methods

Multi-factor authentication

- Uses more than one method
- Type password but also send a code via SMS
 - It goes to your phone (something you have)
 - Gmail implements this
- ATM card and a PIN
- Other things like your location

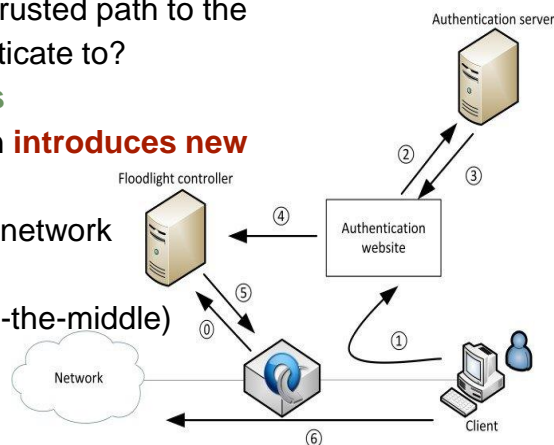


- Attacker must defeat both to compromise authentication

Other Authentication Methods

Authentication over a network:

- Do we always have a trusted path to the OS we need to authenticate to?
 - Remote services
- Network authentication **introduces new problems**
- Need crypto to secure network communication
- **Other attacks** (man-in-the-middle)



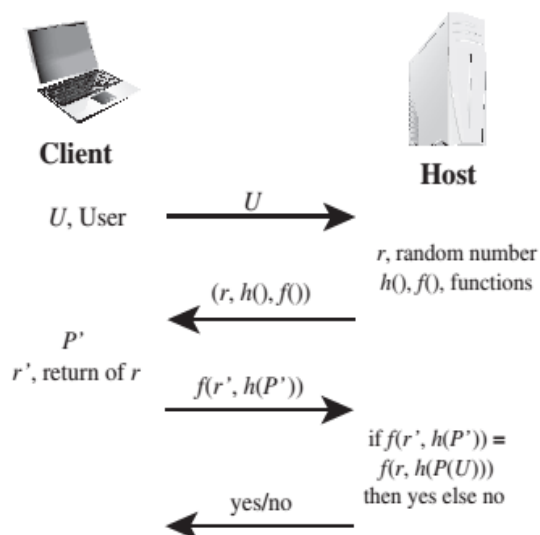
Remote user authentication

- ∞ More security threats with remote user authentication
 - an eavesdropper being able to capture a password
 - an adversary replaying an authentication sequence that has been observed
- ∞ Systems generally rely on some form of challenge-response protocol.
- ∞ Protocols:
 - Password Protocol
 - Token protocol
 - Biometric protocol

04/03/2025

59

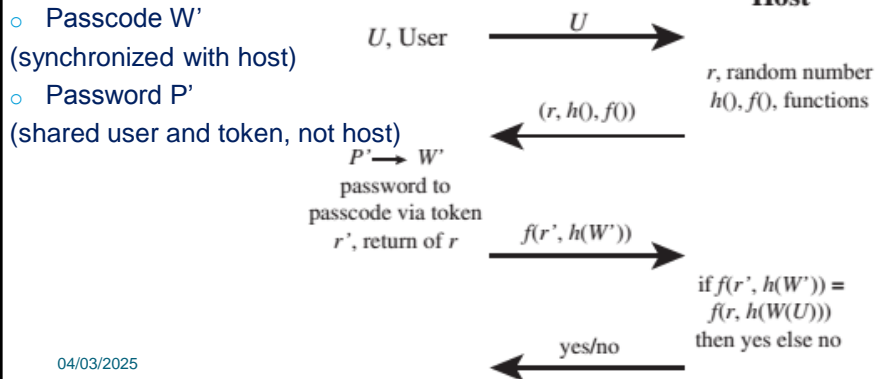
Password Protocol



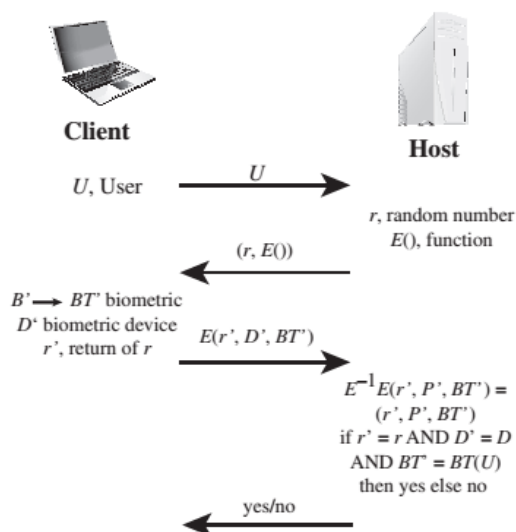
04/03/2025

60

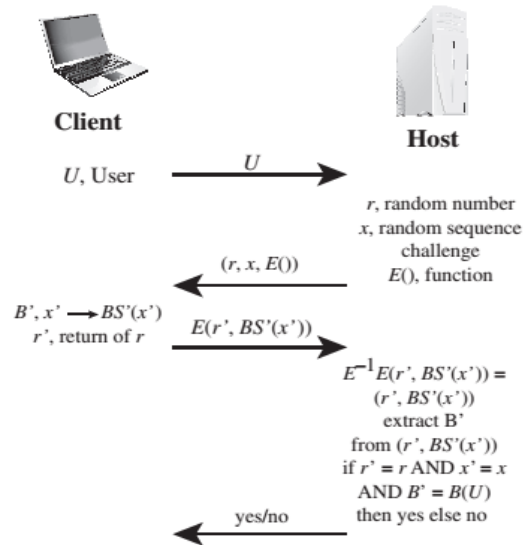
Token protocol



Static biometric protocol



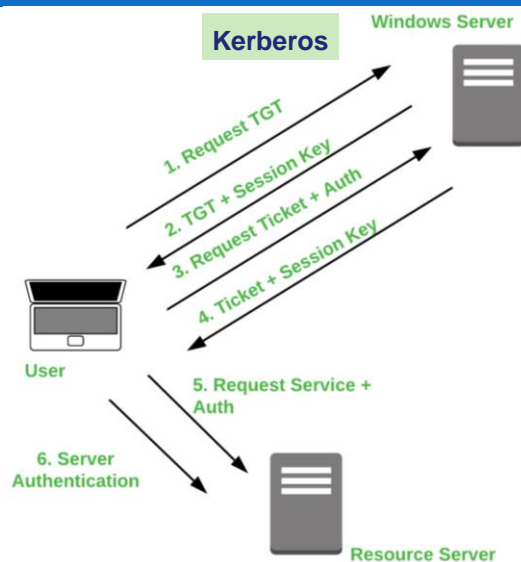
Dynamic biometric protocol



04/03/2025

63

Protocol: Kerberos

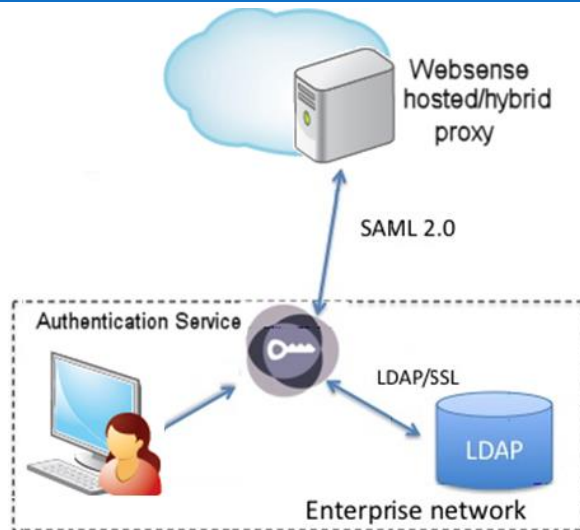


05/03/2025

64

Protocol: SAML

- Security Assertion Markup Language

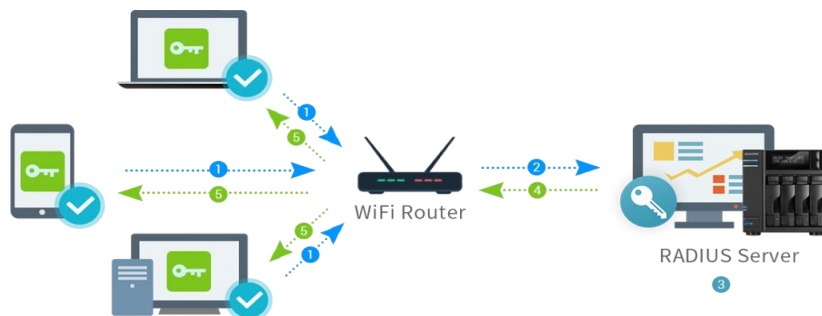


05/03/2025

65

Remote Authentication

RADIUS (Remote Authentication Dial-In User Service)



05/03/2025

66

Passwordless authentication

🔗 Evaluate Recognition and Risk Signals to skip Passwords

🔗 Passwordless authentication

- In the late 2010s () began to become known.
- However, it was not until the early 2020s that this technology was applied to many platforms.



05/03/2025

67

Passwordless authentication

🔗 Characteristic

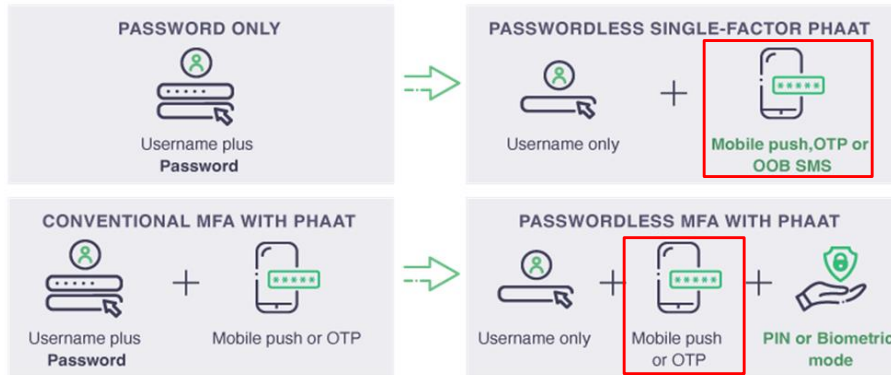
- use the authentication key (physical key, virtual key application on smartphones) then activate the biometric key for authentication.
- It is a big technology trend of the future because of outstanding benefits in enhancing security efficiency,
- a major trend that inevitably creates the future for secure strong authentication when most of the world's large corporations are developing and using this technology such as Apple, Microsoft, Samsung, Amazon.

04/03/2025

68

Passwordless authentication

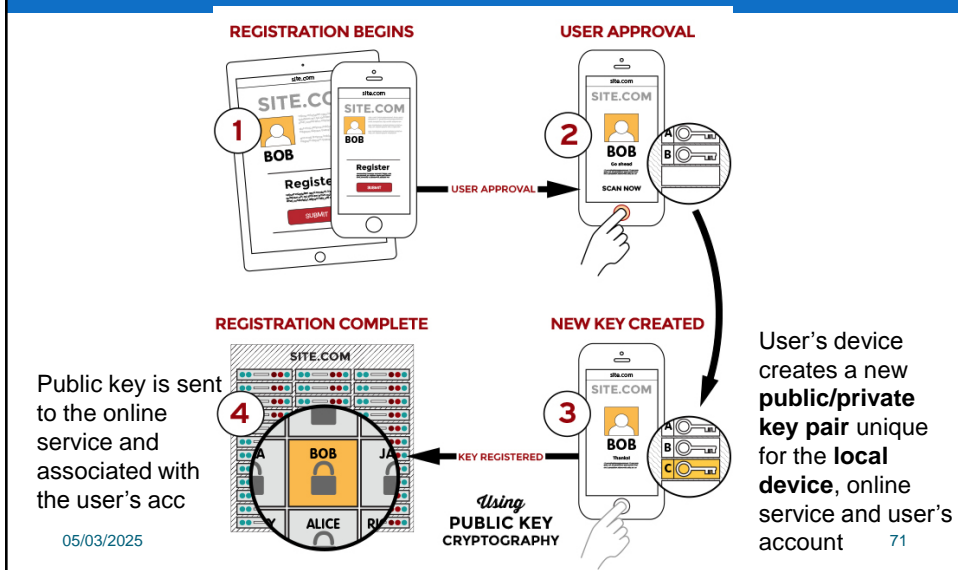
- Two mainstream methods for directly replacing password authentication.
 - The first is to use the phone-as-a-token (PHAAT) method.
 - Secondly, both single-factor and multi-factor authentication (MFA) can be modelled to authenticate without the use of passwords.
- Adopt Passwordless phone-as-a-token authentication:



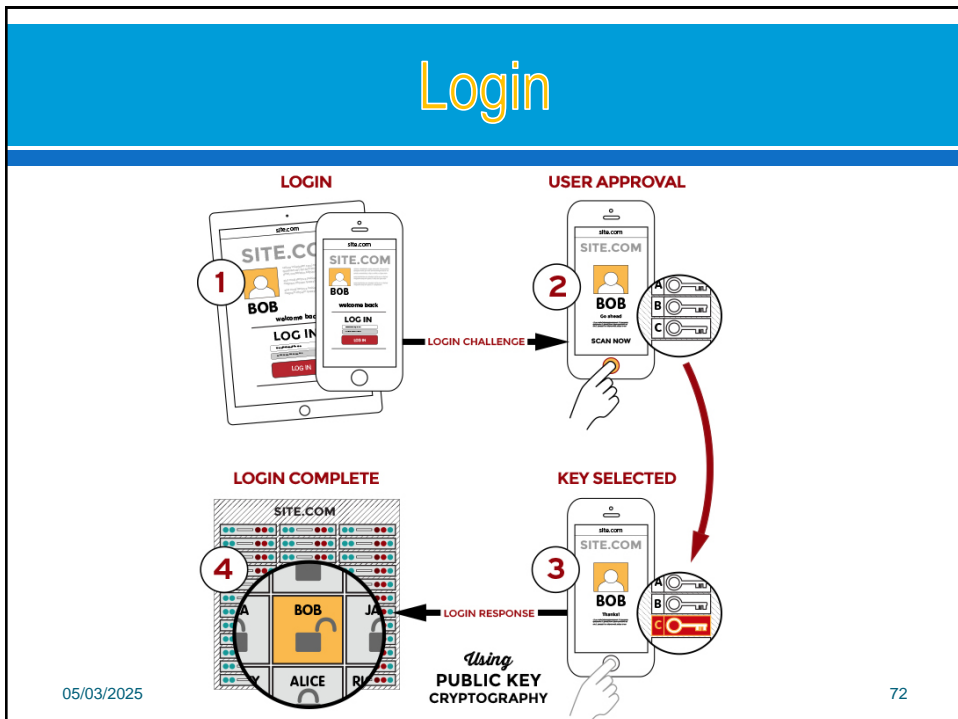
FIDO authentication

- Fast IDentity Online (Fast ID Online)
 - a set of technology-agnostic security specifications for strong **authentication**.
- FIDO2 – the new passwordless standard
 - Passwordless authentication using a hardware authenticator, eliminates the need for weak password-based authentication.
 - Two factor authentication using a hardware authenticator as an extra layer of protection beyond a password.
 - Multi-factor authentication using a hardware authenticator *and* a PIN or biometric, to meet high assurance requirements such as needed for financial transactions and ordering a prescription.

Registration



Login



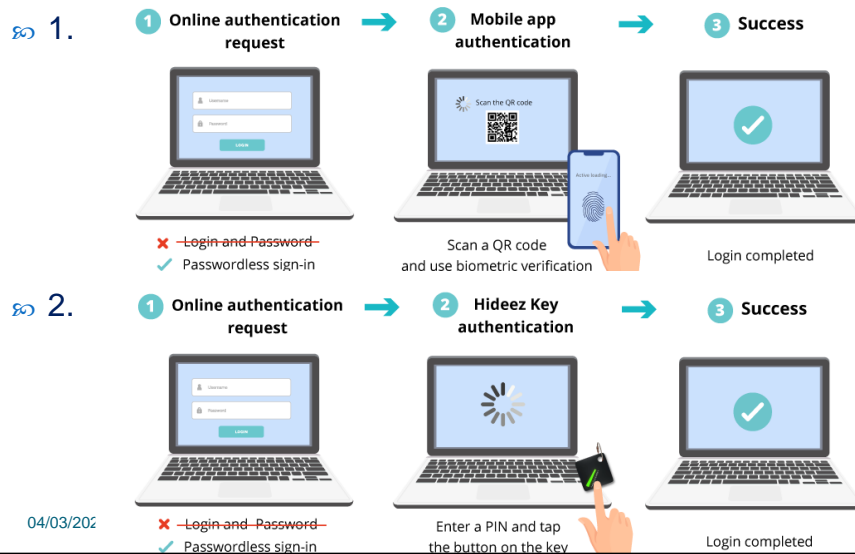
Passwordless authentication methods



05/03/2025

73

FIDO2 Authentication Use Cases



04/03/2025

Zero-trust security model

- ∞ Zero-trust: "never trust, always verify,"
- ∞ A security framework requiring all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data.
- ∞ Zero Trust assumes that:
 - there is no traditional network edge;
 - networks can be local,
 - in the cloud, or a combination or hybrid with resources anywhere
 - as well as workers in any location.

04/03/2025

75

Security Issues for User Authentication

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

04/03/2025

76

Security Issues for User Authentication

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
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

Authentication in IIS

- ✓ Anonymous Authentication: ko dùng username/pass
- ✓ Basic Authentication: Có dùng username/pass (plaintext)
- ✓ Digest Authentication: u/p có mã hóa
- ✓ Windows Authentication: Dùng kỹ thuật bấm (NTLM or Kerberos protocols) để xác nhận thông tin của users.
- ✓ Client Certificate Mapping Authentication

Server tạo ra các giấy Client Certificate và yêu cầu Client khi truy xuất tới Server thì phải gửi giấy chứng nhận.

- ✓ Forms Authentication

Cho phép user logon vào một form (html logon page) để chứng thực

- ✓ ASP.NET Impersonation Authentication

Có thể dùng ứng dụng ASP.NET dưới sự bảo mật khác với bảo mật mặc định của ASP.NET

LAB

- ☞ Install and configure IIS in Windows and use authentication types
- ☞ Install and configure Apache in Linux and use authentication types (digest and Basic)

04/03/2025

79

Summary

- Introduction
- Electronic User Authentication Principles
- Password-Based Authentication
- Token-Based Authentication
- Biometric Authentication
- Remote User Authentication
- Security Issues for User Authentication