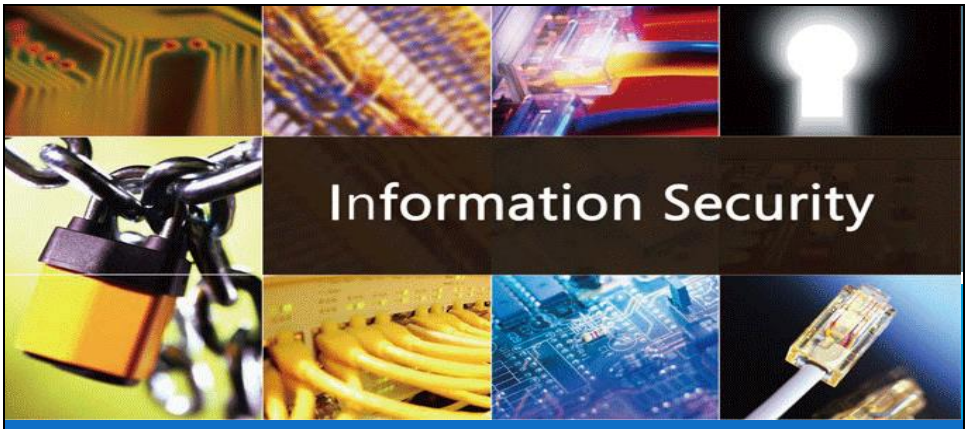


Authentication

Lecturer: Nguyễn Thị Thanh Vân – FIT - HCMUTE

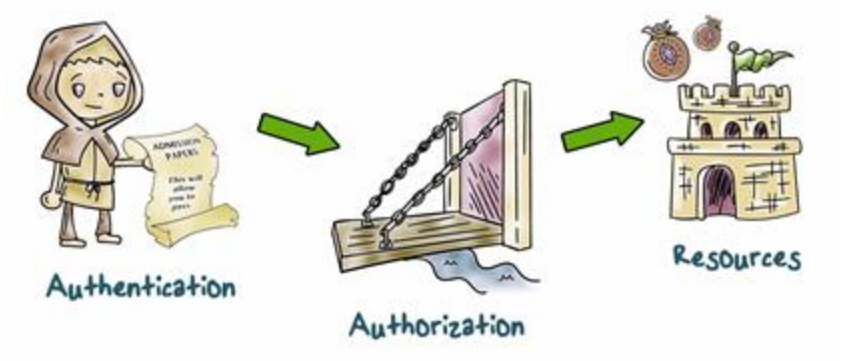
Objective

- 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

What is Authentication?

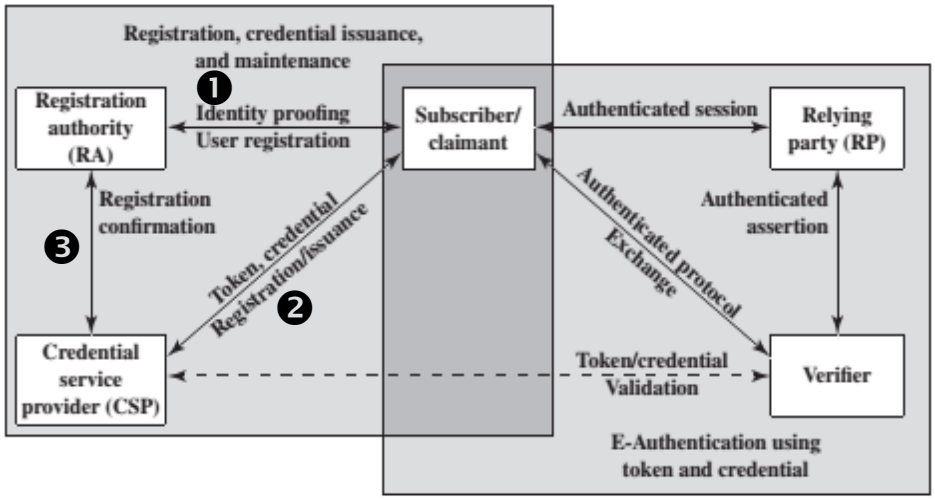


What is Authentication?

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

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

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)

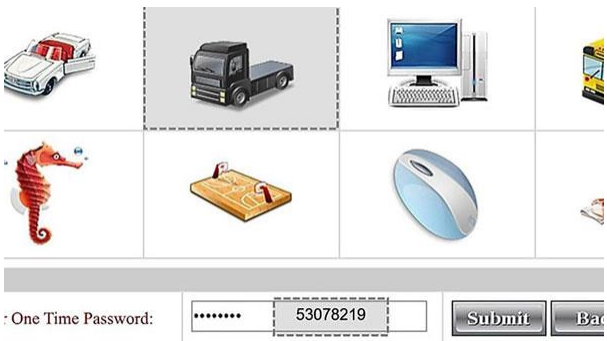
fingerprint
retina,
Face
iris

Something the individual does (Dynamic biometric)

Voice,
Handwriting
Typing rhythm

Means of Authentication

- GOTPass: users employ "images and a one-time numerical code" in order to secure password.
  - using patterns and images instead of letters and numbers
  - the generated digits random code



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

11

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

12

Authentication Methods (continued)

- RADIUS: used by network devices to provide a centralized authentication mechanism
- 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

13

How is Authentication Implemented?

Login Attacks Quiz

Check the correct answer from the choices.

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

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

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.

	Assurance Level Impact Profiles			
Potential Impact Categories for Authentication Errors	**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

Means of Authentication

- **Password-Based Authentication**
  - The Vulnerability of Passwords
    The Use of Hashed Passwords
    Password Cracking of User-Chosen Passwords
    Password File Access Control
    Password Selection Strategies
- **Token-Based Authentication**
- **Biometric Authentication**

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.

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.

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.

Password Popularity Quiz

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

- ☐ 123456
- ☐ password
- ☐ letmein
- ☐ abc123
- ☐ 111111
- ☐ 696969
- ☐ 123123
- ☐ batman
- ☐ qwerty
- ☐ 123456789

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 Authentication

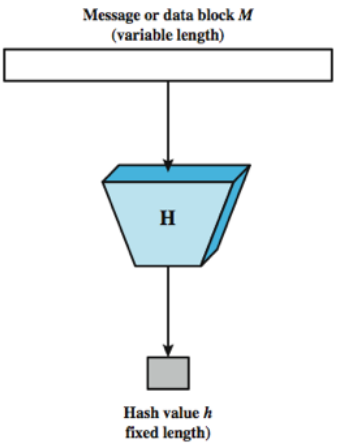
How do we check the password supplied with a user id?

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

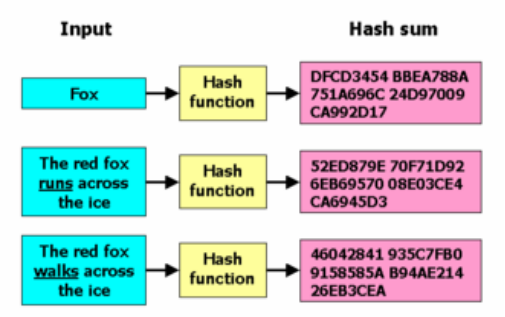
The Use of Hashed Passwords

Hash Functions



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*

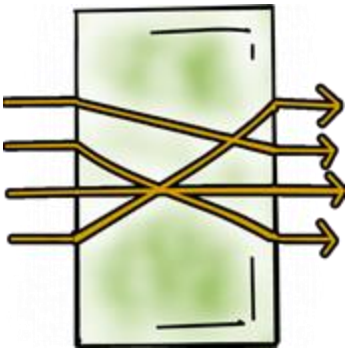


Hash function Requirement

- Variable input size
- Fixed output size
- Efficiency: H (M) is easily calculated with arbitrary M
- For any given value h, it is difficult to find M such that H(M) = h
  - One-way function
- For any M1, it is very difficult to find M2#M1 such that H(M2) = H(M1)
  - collision resistant: weak
- Very difficult to find any pair (M1, M2) such that H (M1) = H(M2)
  - collision resistant: Strong

A Strong hash function: satisfied all 6 reqs (weak: 5 reqs)

Hash Functions & Threats



- We **assume a one-way property** for hash functions
- If we **know common passwords**, we can determine their hash
- For dictionary and offline attacks, we have the **hash values and plenty of time** *to test* for matches

Attacks on Hash function

- two categories of attacks on hash functions:
  - Brute-force attack:
    - depend only on bit length of the hash value (not specific algorithm)
    - Attack to: One-way function; collision resistant - weak

    wishes to find a value y such that H(y)=h, try 2m-1 values
    - Attack to: collision resistant - strong

    wishes to find 2 messages: x,y, that yield H(y)=H(x), try 2m/2 values
  - Cryptanalysis:
    - based on weaknesses in a particular cryptographic algorithm.
    - require a cryptanalytic effort greater than or equal to the BF effort

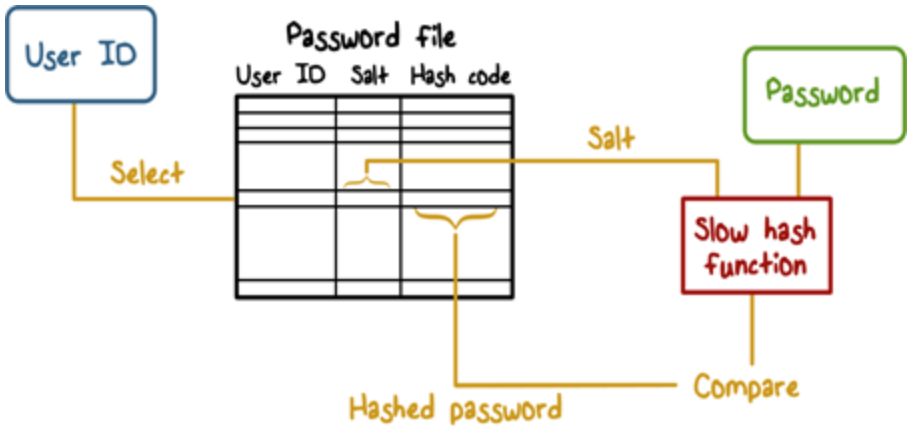
Threat Modeling of the Password Method

- **Guessing the password** for a given user allows impersonation
- **Impersonating** a real login program
- **Keylogging** to steal a password

Brute Force Guessing of Passwords

- Publicly available software can do **10^8 MD5 hashes/sec on a GPU**
- Six random upper case/lower case/digits then 62^6 possible passwords, **about *10 minutes***
- Eight random characters increases it to about **six days**
- **Passwords are not really random**
- **To reduce the work** required for a brute force attack:
  - Try the popular passwords first
  - Create a rainbow table
- **What if two users pick the same password?**
  - **Add a random salt** before hashing
  - **Store the salt** with the hashed value
  - **Check** by using the salt with the typed password

Brute Force Guessing of Passwords



Problems with Passwords

- As password length and complexity increases, **usability suffers**
- Phishing and social engineering – **users do not authenticate who is asking for a password**.
- Once a password is stolen, **it can be used many times**
  - This is why there are policies that say passwords be changed frequently
- **Humans have a hard time remembering** lots of passwords. Usable passwords are easy to guess.

Problems with Passwords

Sys Administrators:

- Never store passwords in the clear
- Store only hashed values generated with a random salt and limit access to them
- Avoid general purpose fast hash functions

Users:

- Use password managers

Password File Access Control

- The hashed passwords are kept in a separate file from the user IDs, referred to as a **shadow password file**.
- Special attention is paid to making the shadow password file protected from unauthorized access.
- Vulnerabilities:
  - Exploit a software vulnerability in the OS to bypass the access control system long enough to extract the password file.
  - An accident of protection might render the password file readable
  - Use the same password on other machines in other protection domains
  - Access to this backup enables the attacker to read the password file.
  - Collecting user IDs and passwords is through sniffing network traffic.

Password Selection Strategies

- Four basic techniques are in use:
  - User education
  - Computer-generated passwords
  - Reactive password checking
  - Complex password policy

Token-Based Authentication

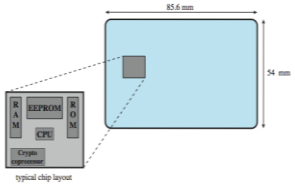
- You must have them
- May require additional hardware (e.g., readers)
- How does it implement authentication (challenge/response)
- Cost and misplaced trust (RSA SecureID master key breach)
- Types:
  - Memory card
  - Token

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

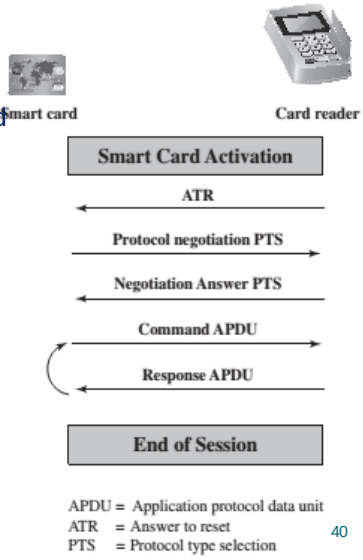
Smart Cards

- 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:
- Also have USB dongles



Smart Card/Reader Exchange

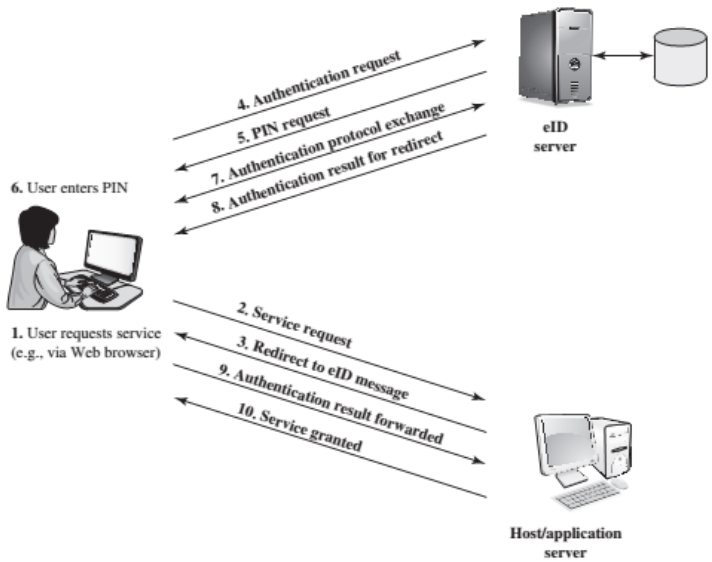
- Each time the card is inserted
  - a reset is initiated (clock value)
  - the card responds (the parameters and protocols).
  - The terminal may be able to change the protocol used and other parameters via a protocol type selection (PTS) command.
  - The cards PTS response confirms the protocols and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



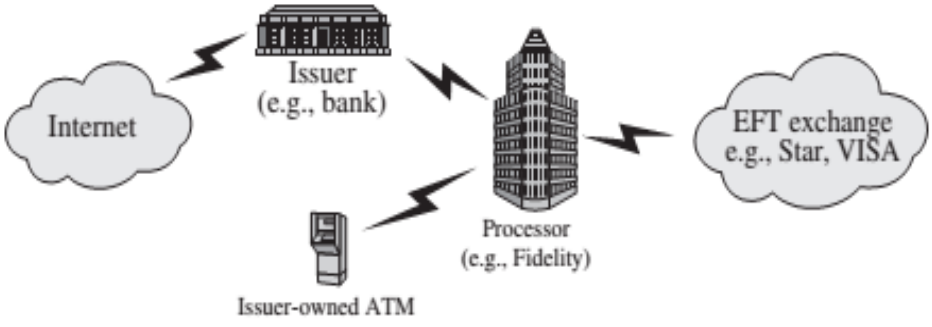
Electronic Identity Cards

- 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

User authentication eID

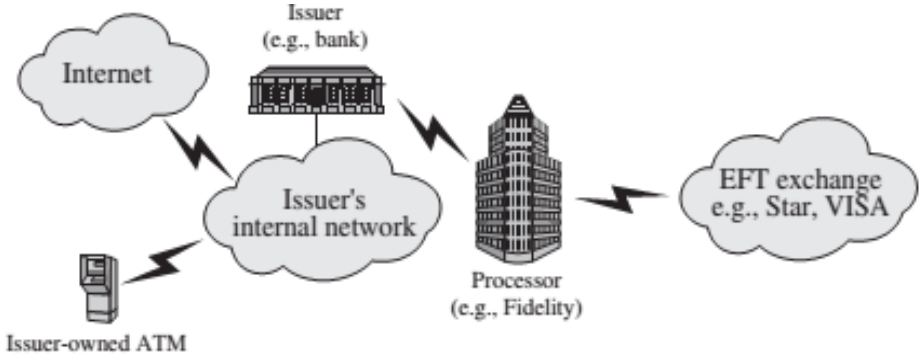


Ex, ATM architectures



(a) Point-to-point connection to processor

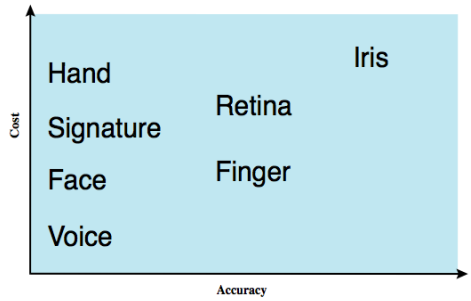
Ex, ATM architectures



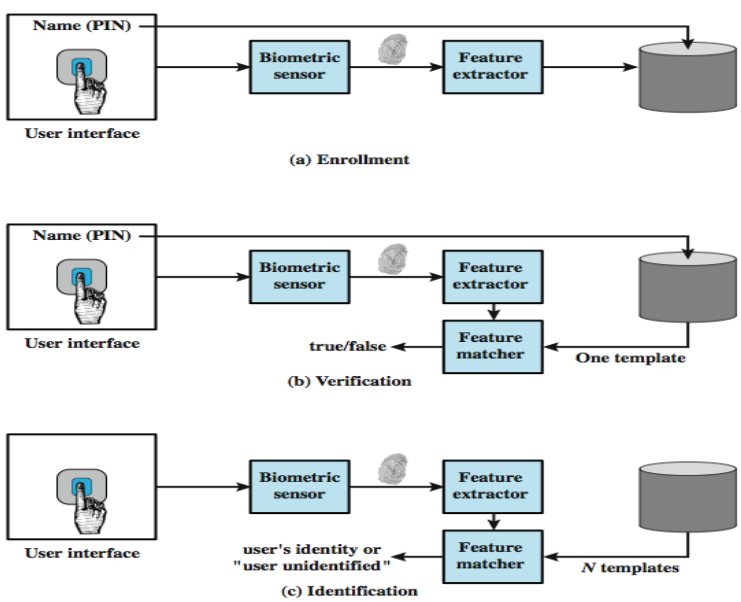
(b) Shared connection to processor

Biometric authentication

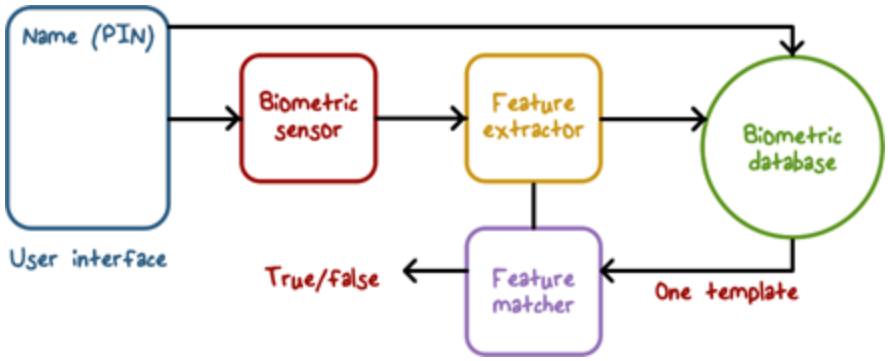
- based on pattern recognition.
- more complex and expensive.



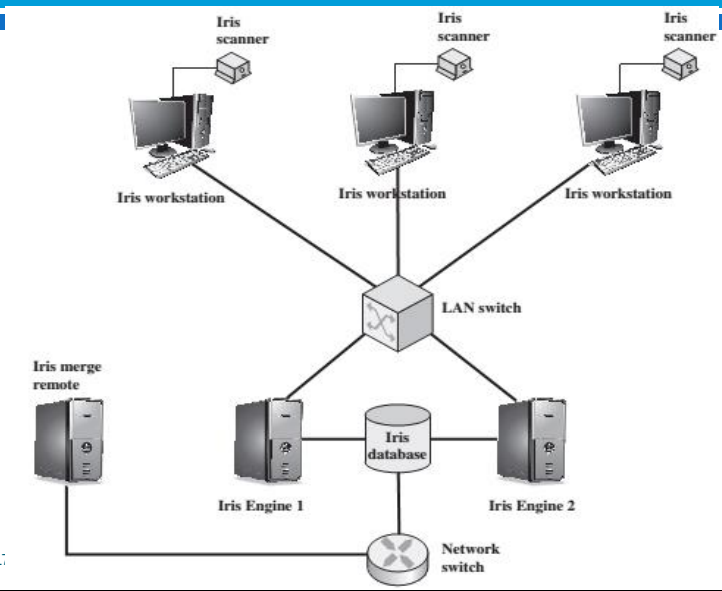
Operation of a Biometric Authentication System



Implementing Biometric Authentication



Ex: General Iris Scan Site Architecture for UAE System



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**

Multi-factor Authentication Quiz

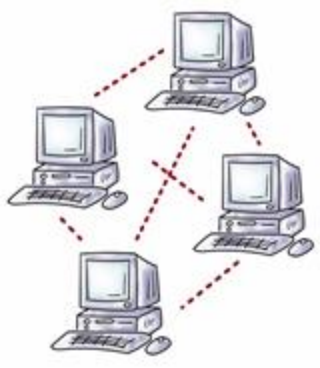
A multi-factor authentication method will likely reduce false negative. Choose one:

☐ True

☐ False

Other Authentication Methods

Authentication over a network:

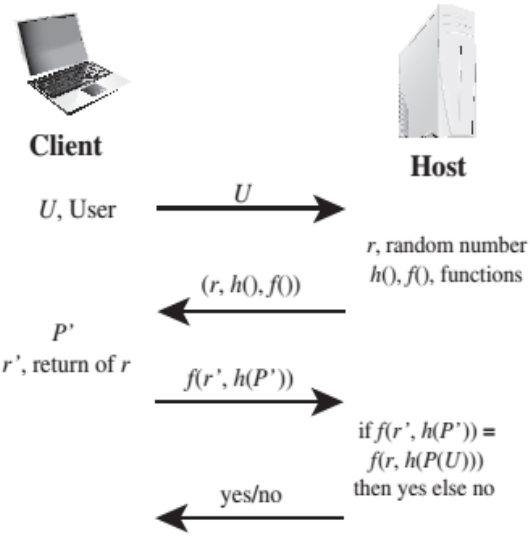


- Do we always have a trusted path to the OS we need to authenticate to?
  - **Remote services**
- Network authentication **introduces new problems**
- Need crypto to secure network communication
- **Other attacks** (man-in-the-middle)

Remote user authentication

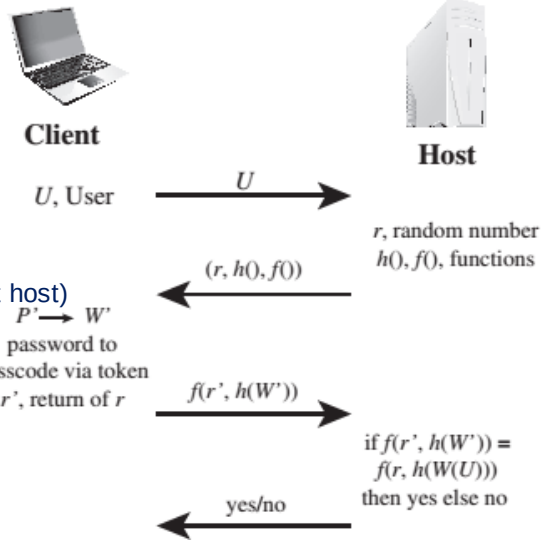
- More security threats with remote user authentication
  - an eavesdropper being able to capture a password
  - an adversary replaying an authentication sequence that has been observed
- Systems generally rely on some form of challenge-response protocol.
- Protocols:
  - Password Protocol
  - Token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

Password Protocol

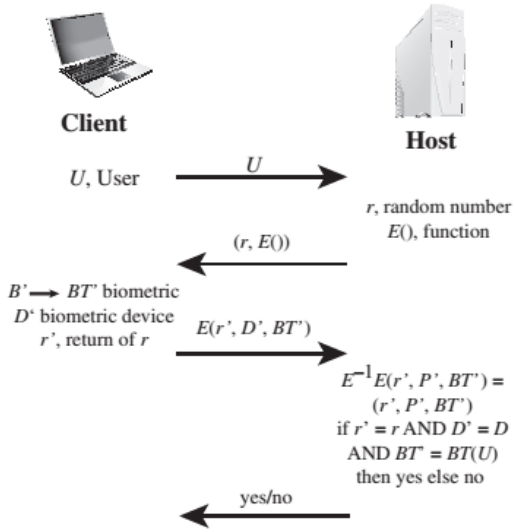


Token protocol

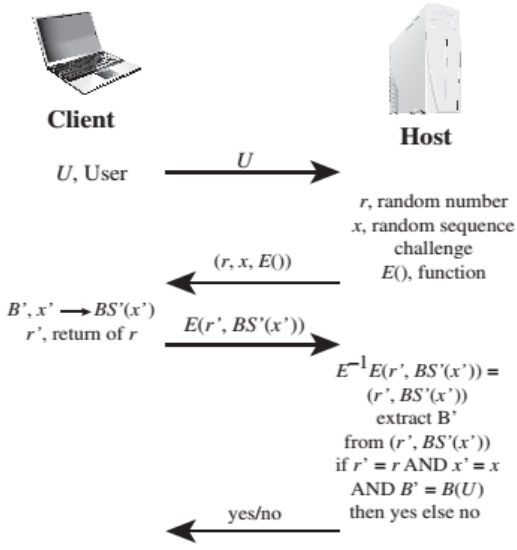
- Passcode W' (synchronized with host)
- Password P' (shared user and token, not host)



Static biometric protocol



Dynamic biometric protocol



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

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
Lesson Summary

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

Q & A