User Authentication

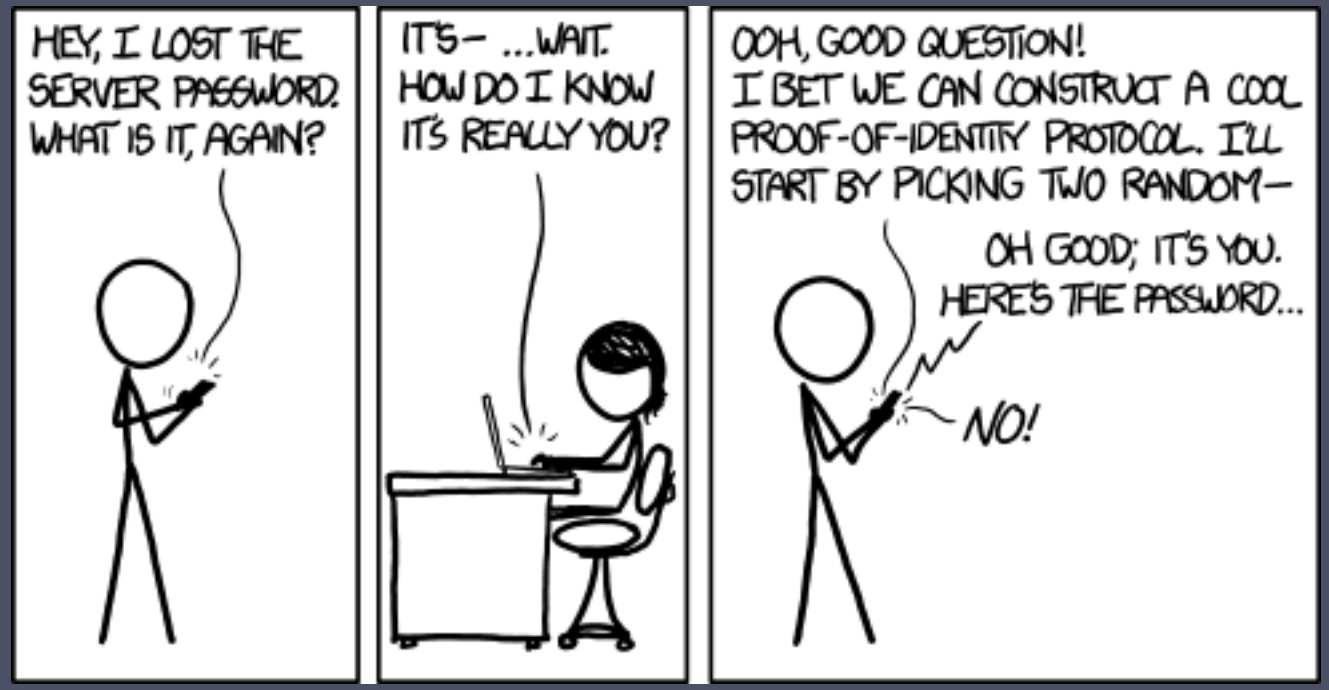
Introduction to Computer Security

Naercio Magaia and Imran Khan

Contents

- Digital user authentication principles
  - A model for digital user authentication
  - Means of authentication
  - Risk assessment for user 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
  - Smart cards
  - Smartphones
  - Electronic identity cards
- Biometric authentication
  - Physical characteristics used in biometric applications
  - Operation of a biometric authentication system
  - Biometric accuracy
- Federated Identity Management
  - Identity Management
  - Federated Identity

How do you know who you're talking to?



Source https://xkcd.com/1121/

System Identity and Authentication

- An ***identity*** on a system is typically a unique identifier
- All actions on a system are associated with at least one identity
- This identifier will be used to check what actions a user can perform – ***Access Control***
- This identifier will be associated with the records in log files - ***Accountability***

- The process by which a user, whether human or software, is associated with an identity is ***User Authentication***
- To authenticate, the user is typically required **to show evidence** that they are who they claim
- This evidence is the ***factor***

User identity attributes

The four factors 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

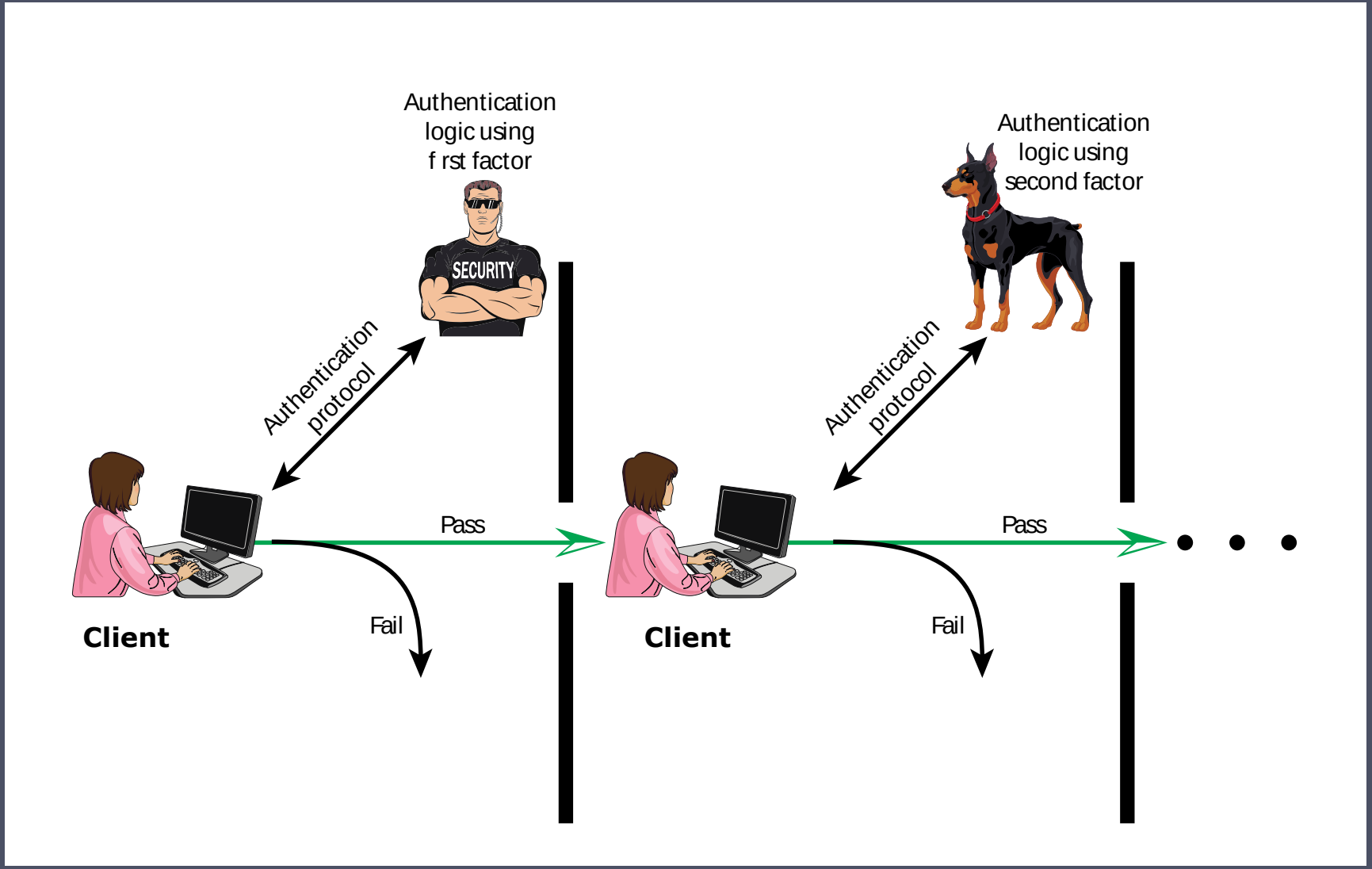
Something the individual is (static biometrics)

- Fingerprint, retina, face

Something the individual does (dynamic biometrics)

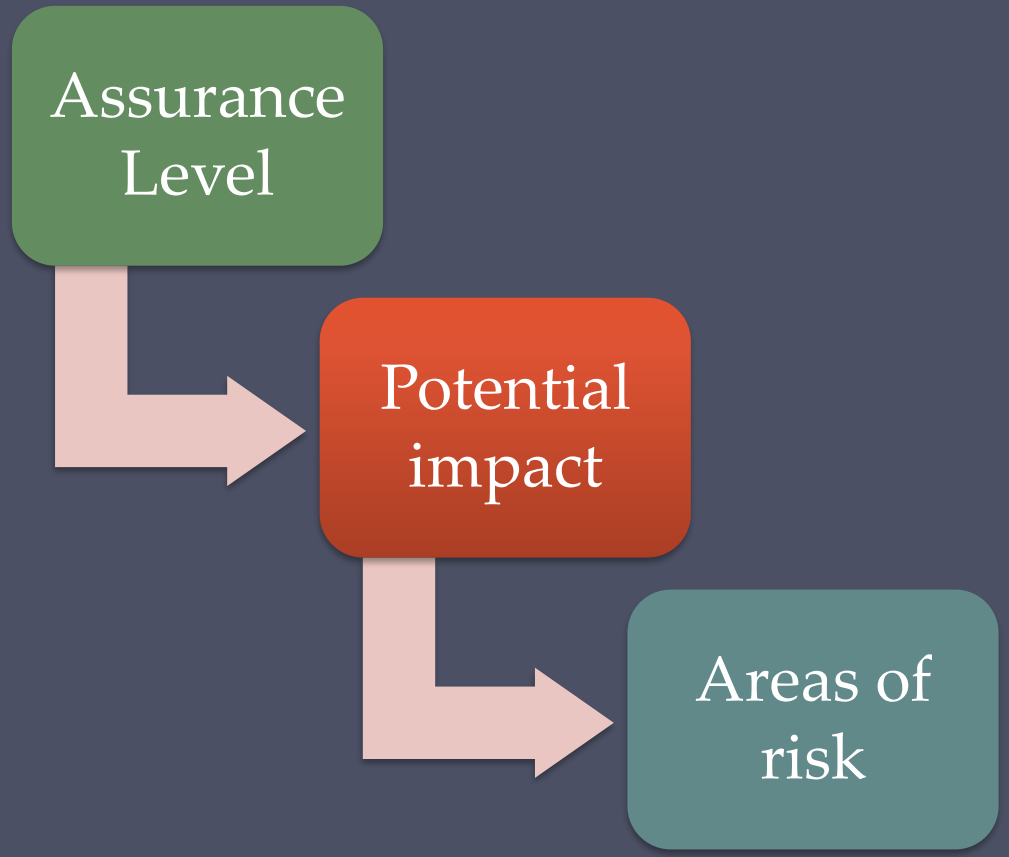
- Voice pattern, handwriting, typing rhythm

Multifactor Authentication



Risk Assessment for User Authentication

- There are three separate concepts:



Assurance Level

Describes an organization's **degree of certainty** that a user has presented a credential that refers to his or her identity

More specifically is defined as:

The degree of confidence **in the vetting process used to establish the identity of the individual** to whom the credential was issued

The degree of confidence that **the individual who uses the credential** is the individual to whom the credential was issued

Four levels of assurance

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

- FIPS 199 defines three levels of potential impact on organizations or individuals should **there be a breach of security**:
  - Low
    - An authentication error could be expected to have **a limited adverse effect** on organizational operations, organizational assets, or individuals
  - Moderate
    - An authentication error could be expected to have **a serious adverse effect**
  - High
    - An authentication error could be expected to have **a severe or catastrophic adverse effect**

Maximum Potential Impacts for Each Assurance Level

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
	Low	Mod	Mod	High
Financial loss or organization liability	None	Low	Mod	High
Harm to organization programs or interests	None	Low	Mod	High
Unauthorized release of sensitive information	None	None	Low	Mod/ High
Personal safety				
Civil or criminal violations	None	Low	Mod	High

An example risk assessment: For each system, examine the likely effect of an authentication error to the organization; this will then determine how much assurance is needed for authentication

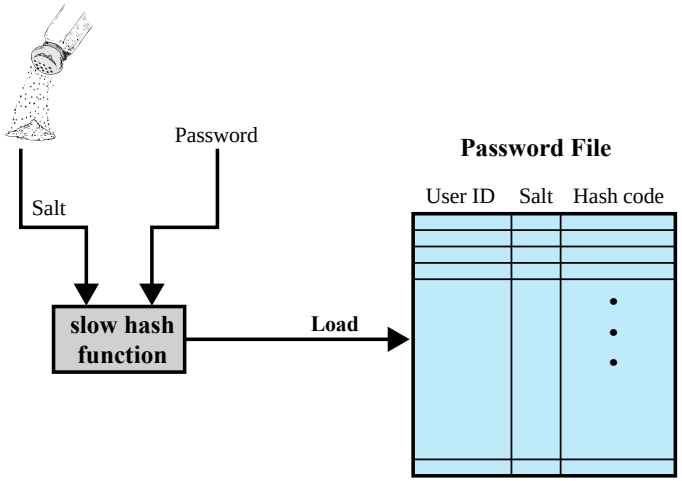
Password-Based Authentication

- Widely used line of defense against intruders
  - User provides name/login and password
  - System compares password with the one stored for that specified login
  - If passed, user is represented by their identity or user ID within the runtime
- The user ID is the token identifying the user in the system:
  - Determines that the user is authorized to access the system
  - Determines the user's privileges
  - Is used in discretionary access control
  - Used as part of the logging entry for logged actions

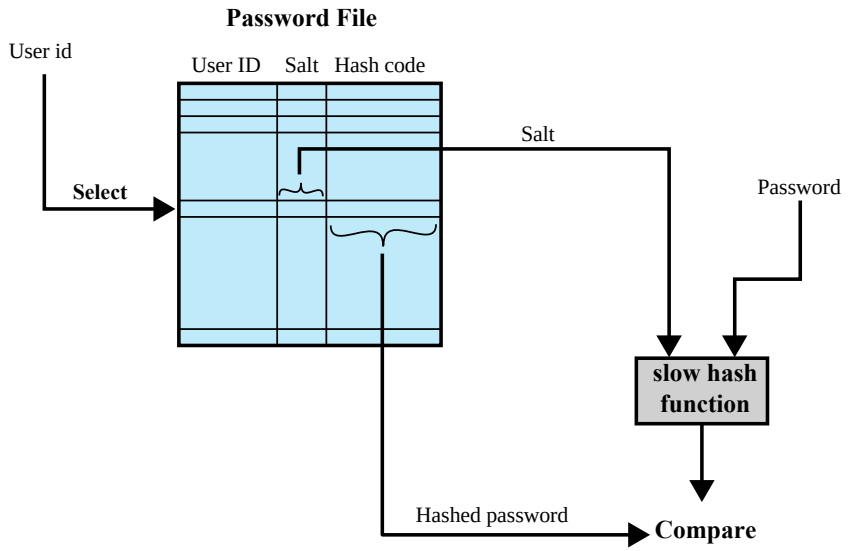
Password Storage

- Passwords need to be stored in the system
  - Should they be stored as the actual password?
  - No! When attackers **get the file/table** containing the passwords, no more security
- Can passwords be stored encrypted, e.g., by a Secure Hash Algorithm?
  - Hash function applied to password after entry and compared to hashed value in the file.
  - Prevents casual password scavenging, but…
- Dictionary Attacks
  - Attacker gets a dictionary, and applies hash function to each entry
  - Most passwords are single words, so attacker can search through password file to match entries
  - Attacker can apply **common password addition rules** to generate further match possibilities, such as numbers at the end, punctuation at the end, 1337 speak
- Salt
  - Using a **random number prefix** on the password reduces the effectiveness of dictionary attacks

UNIX Password Scheme

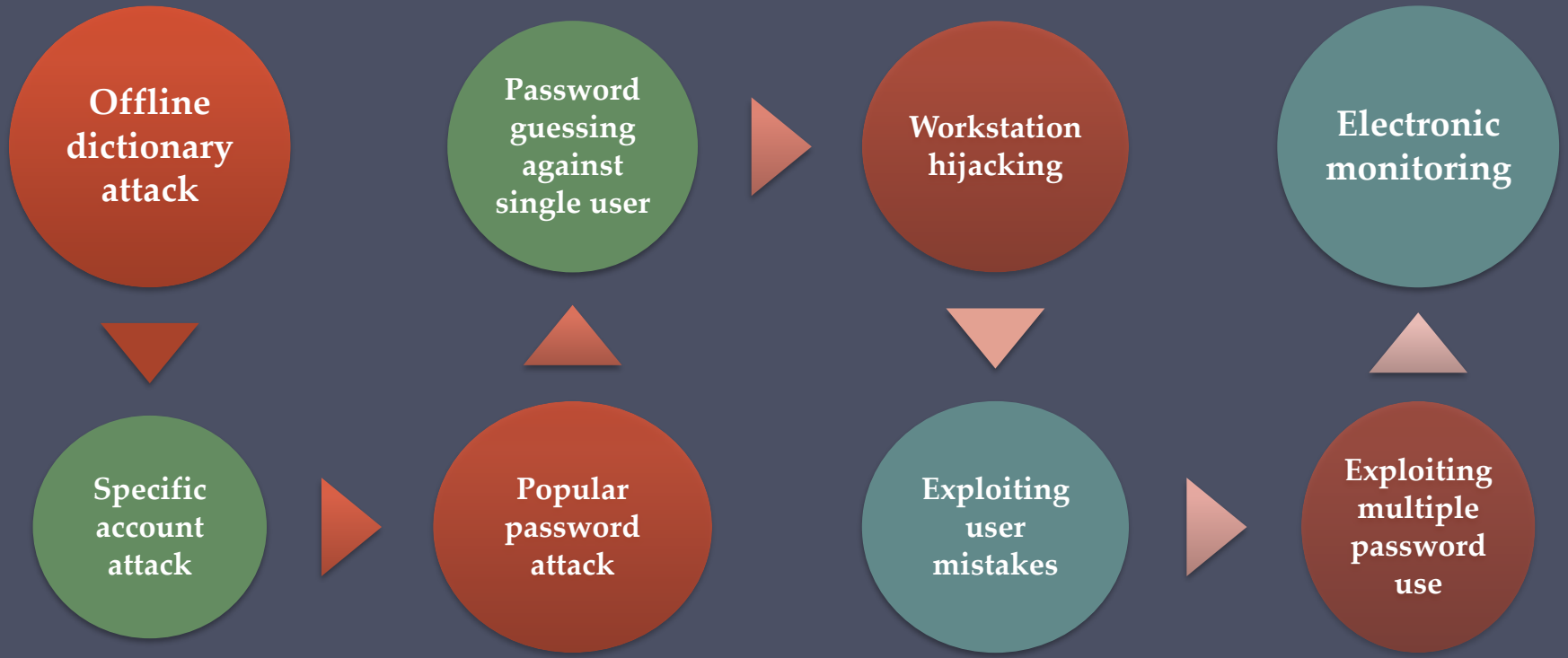


(a) Loading a new password

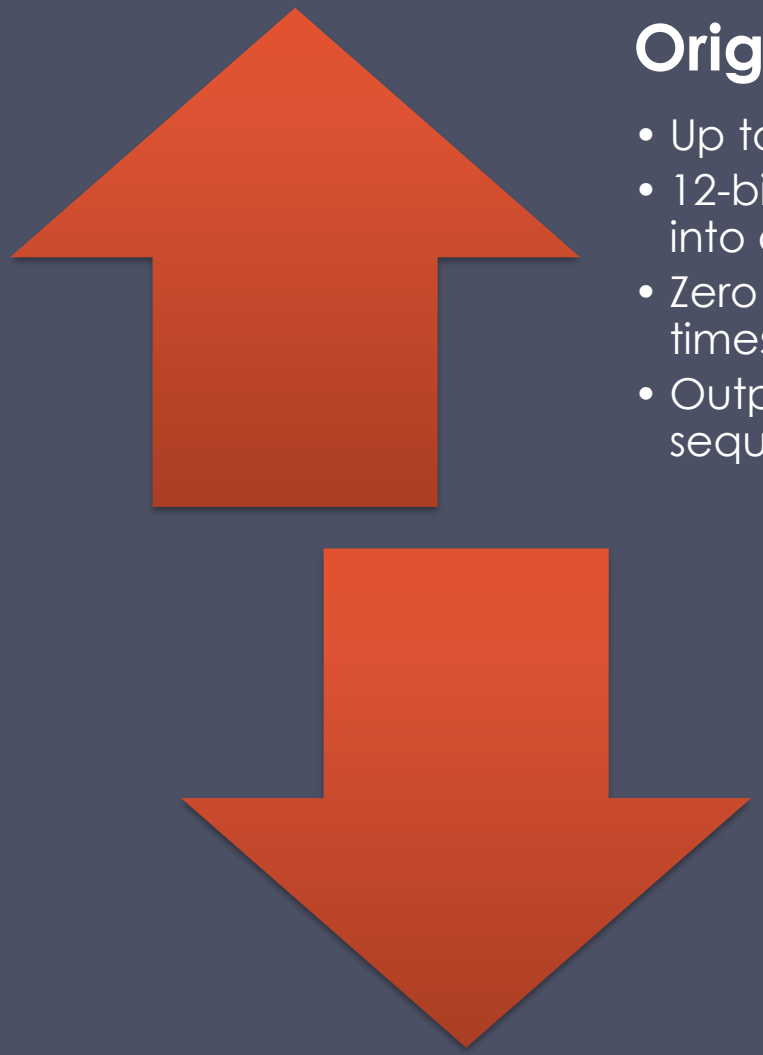


(b) Verifying a password

Password Vulnerabilities



UNIX Implementation



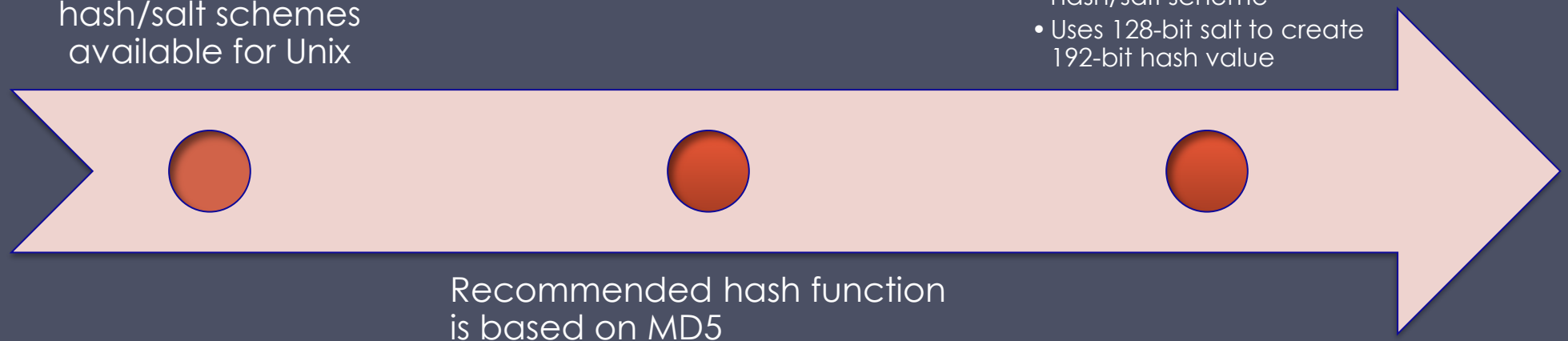
Original scheme

- Up to eight printable characters in length
- 12-bit salt used to modify DES encryption into a one-way hash function
- Zero value repeatedly encrypted 25 times
- Output translated to 11 character sequence

Now regarded as inadequate

- Still often required for compatibility with existing account management software or multivendor environments

Improved Implementations



Much stronger hash/salt schemes available for Unix

Recommended hash function is based on MD5

- Salt of up to 48-bits
- Password length is unlimited
- Produces 128-bit hash
- Uses an inner loop with 1000 iterations to achieve slowdown

OpenBSD uses Blowfish block cipher-based hash algorithm called Bcrypt

- Most secure version of Unix hash/salt scheme
- Uses 128-bit salt to create 192-bit hash value

Password Cracking

Dictionary attacks

- Develop a large dictionary of possible passwords and try each against the password file
- Each password must be hashed using each salt value and then compared to stored hash values

Rainbow table attacks

- Pre-compute tables of hash values for all salts
- A mammoth table of hash values
- Can be countered by using a sufficiently large salt value and a sufficiently large hash length

Password crackers exploit the fact that people choose easily guessable passwords

- Shorter password lengths are also easier to crack

John the Ripper

- Open-source password cracker first developed in in 1996
- Uses a combination of brute-force and dictionary techniques

Modern Approaches

- Complex password policy
  - Forcing users to pick stronger passwords
- However, password-cracking techniques have also improved
  - The processing capacity available for password cracking has increased dramatically (e.g., GPUs)
  - The use of sophisticated algorithms to generate potential passwords (e.g., standard Markov modeling techniques from natural language processing)
  - Studying examples and structures of actual passwords in use

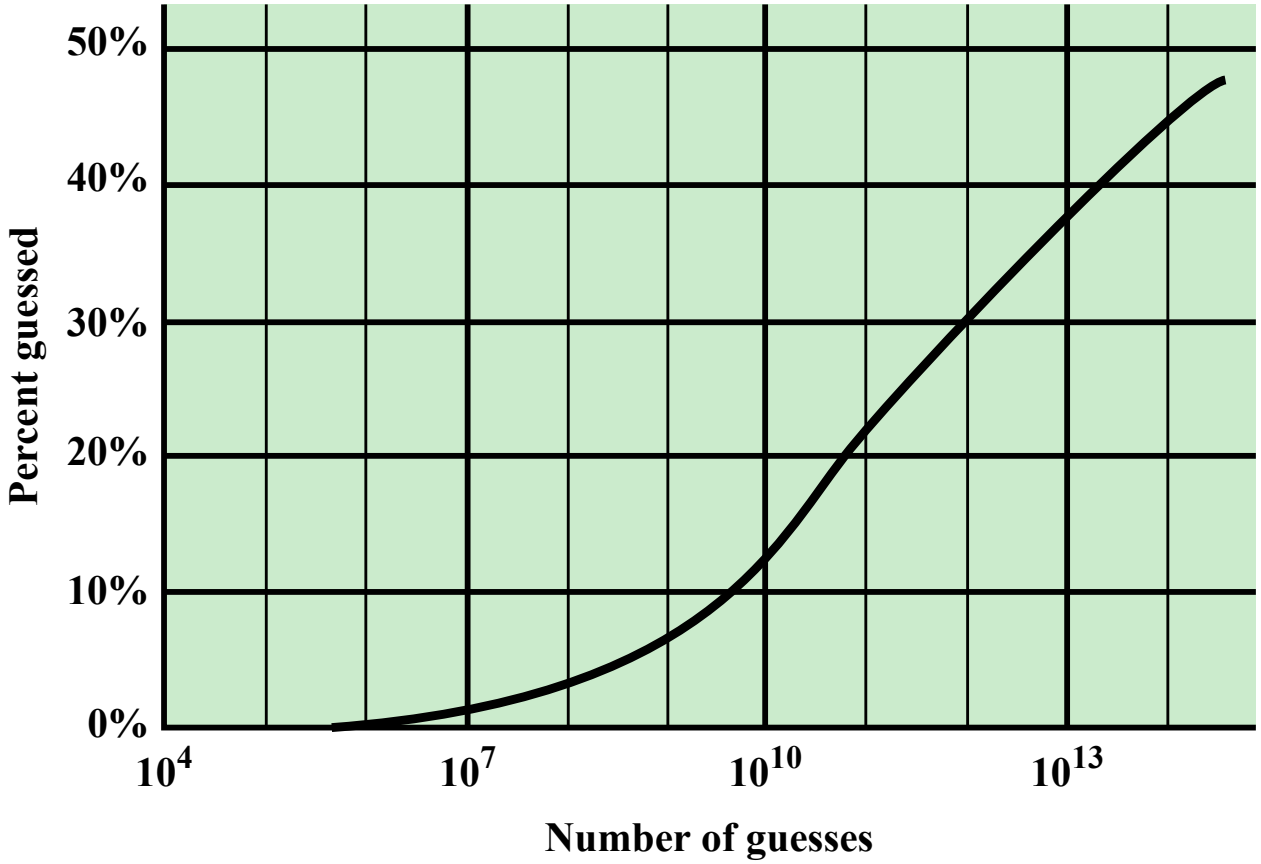


Figure 3.4 The Percentage of Passwords Guessed After a Given Number of Guesses

Password Selection Strategies

User education

Users can be told the importance of using **hard to guess** passwords and can be **provided with guidelines** for selecting strong passwords

Computer generated passwords

Users have trouble remembering them. Password managers can help.

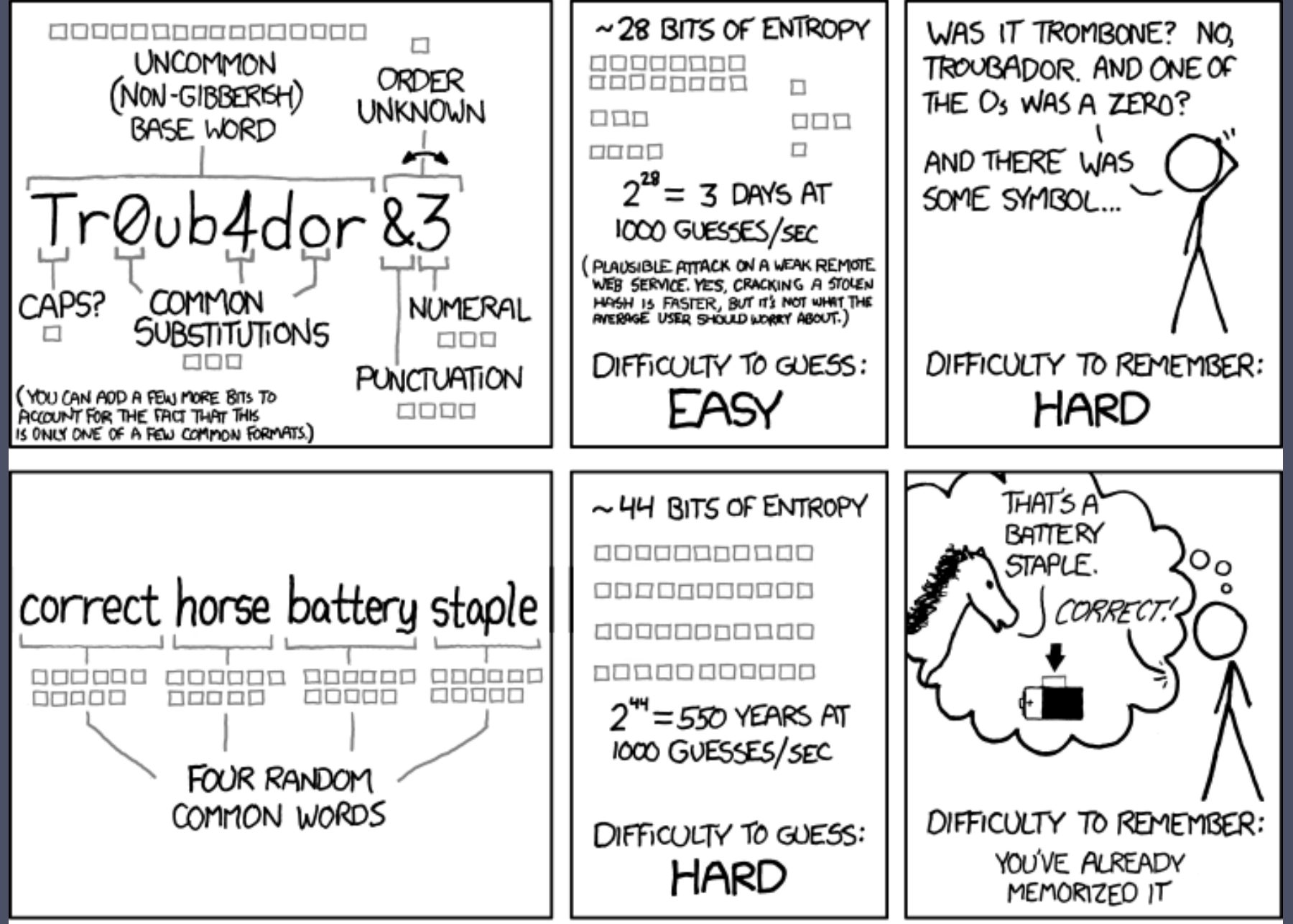
Reactive password checking

System periodically runs its own password cracker to **find guessable passwords**

Complex password policy

User is **allowed to select their own password**; however, the system checks to see if the password is allowable, and if not, rejects it

Goal is to **eliminate guessable passwords** while allowing the user to select a password that is memorable



https://xkcd.com/936/

Memory Cards

- Can store but do not process data
- The most common is the magnetic stripe card
- Can include an internal electronic memory
- Can be used alone for physical access
  - Hotel room
  - ATM
- Provides significantly greater security when combined with a password or PIN
- Drawbacks of memory cards include:
  - Requires a special reader
  - Loss of token
  - User dissatisfaction

Smart Tokens

- Physical characteristics:
  - Include an embedded microprocessor
  - A smart token that looks like a bank card
  - Can look like calculators, keys, small portable objects
- User interface:
  - Manual interfaces include a keypad and display for human/token interaction
- Electronic interface
  - A smart card or other token requires an electronic interface to communicate with a compatible reader/writer
  - Contact and contactless interfaces
- Authentication protocol:
  - Classified into three categories:
    - Static
    - Dynamic password generator
    - Challenge-response

Smart Cards

- Most important category of smart token
  - Has the appearance of a credit card
  - Has an electronic interface
  - May use any of the smart token protocols
- Contain:
  - An entire microprocessor
    - Processor
    - Memory
    - I/O ports
- Typically include three types of memory:
  - Read-only memory (ROM)
    - Stores data that does not change during the card's life
  - Electrically erasable programmable ROM (EEPROM)
    - Holds application data and programs
  - Random access memory (RAM)
    - Holds temporary data generated when applications are executed

Electronic Identity Cards (eID)

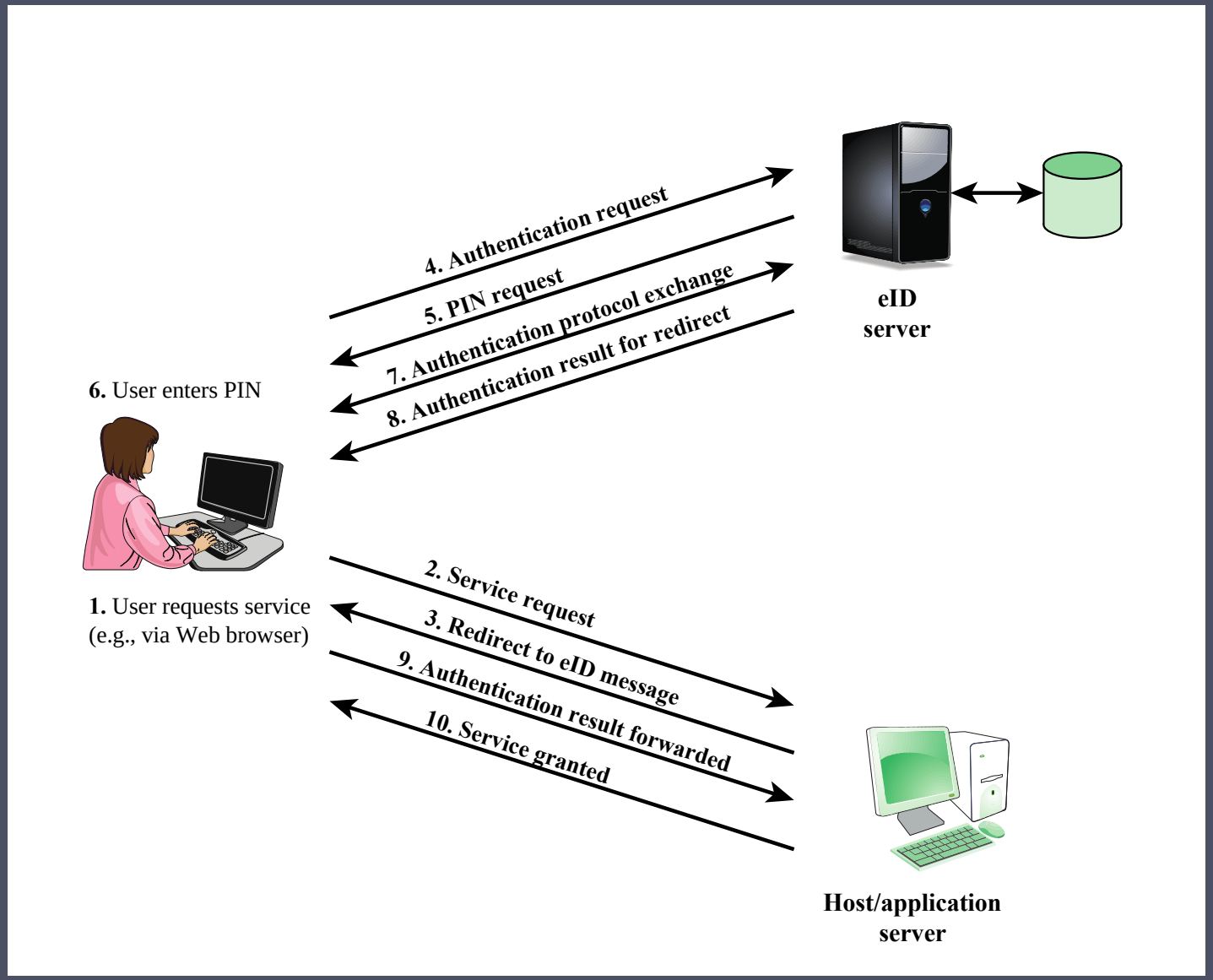
Use of a smart card as a national identity card for citizens

Can serve the same purposes as other national ID cards, and similar cards such as a driver's license, for access to government and commercial services

Can provide **stronger proof of identity** and can be used in a wider variety of applications

In effect, is a smart card **that has been verified by the national government** as valid and authentic – around 3.6 billion wordwide

User Authentication with eID



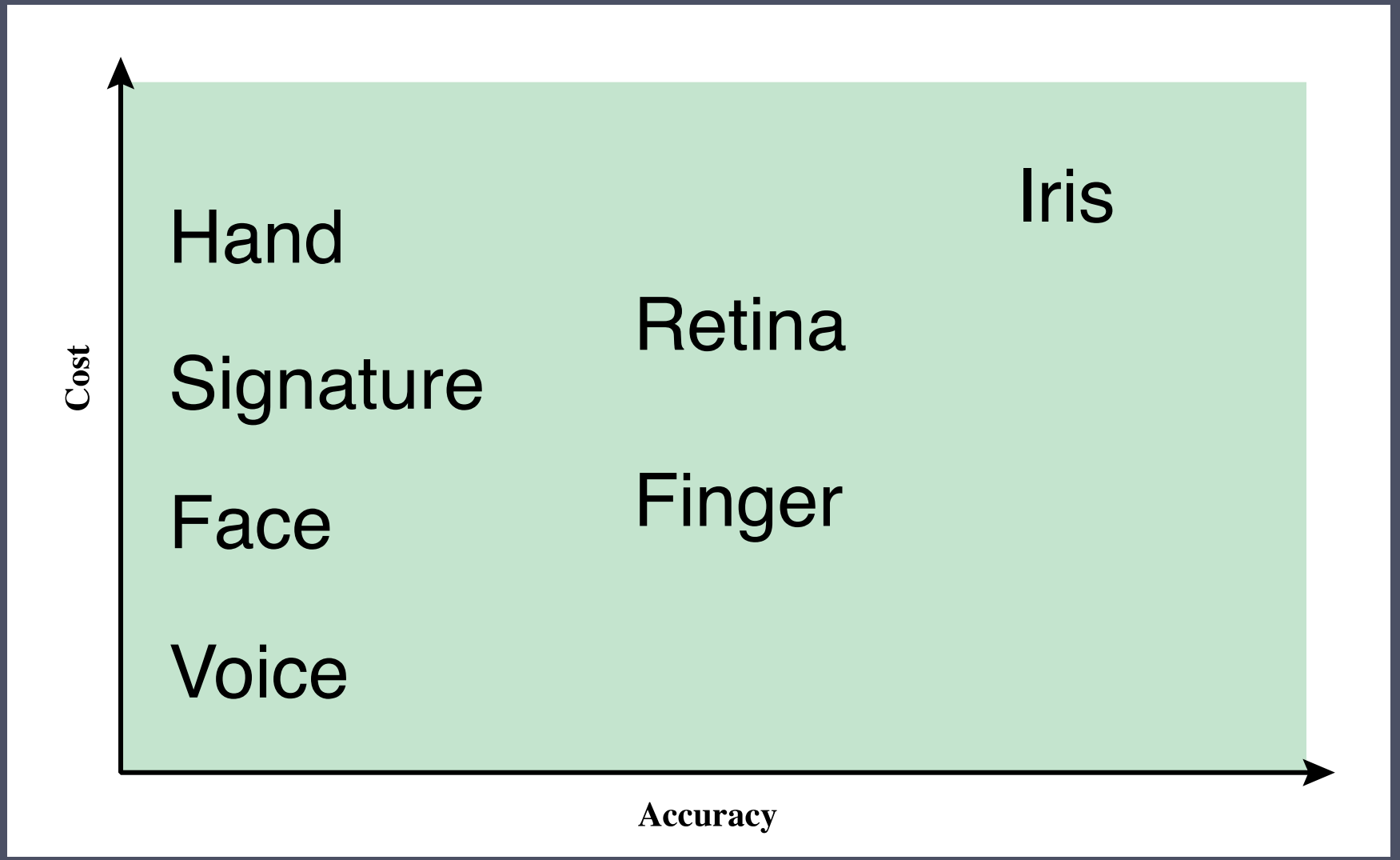
SmartPhones

- Physical characteristics:
  - Open market for software applications
  - Standard user interface experience
  - In 2023, 6.9 billion smartphone subscriptions worldwide
  - By Oct. 2024, 71.85% Android, 27.6% Apple
- Authentication protocol:
  - Can utilize directly for two factor authentication, by SMS or other mechanisms
  - Install Authenticator apps
- We will discuss more in Internet authentication

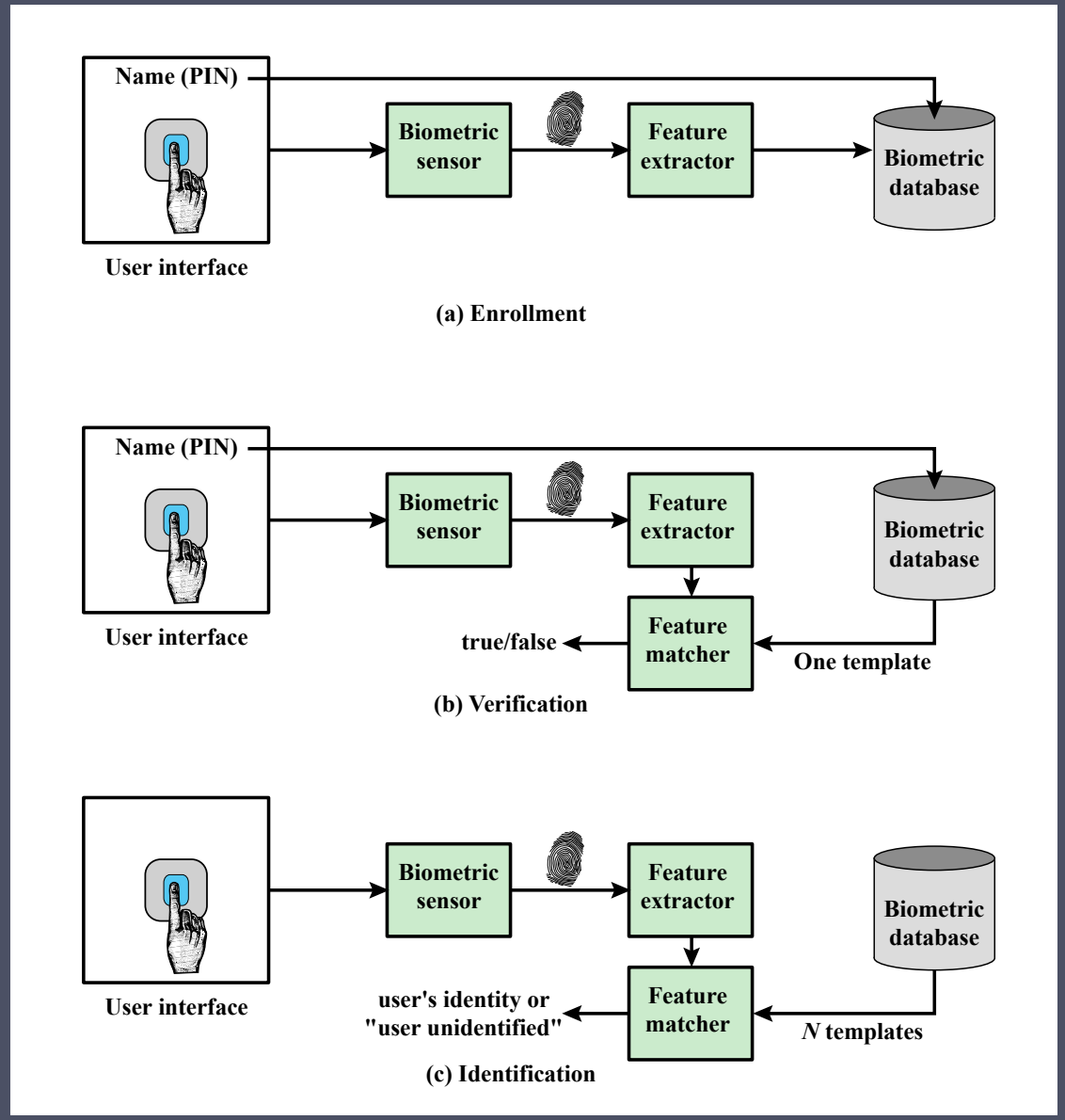
Biometric Authentication

- Attempts to authenticate an individual based on unique physical characteristics
- Based on pattern recognition
- Is technically complex and expensive when compared to passwords and tokens
- Physical characteristics used include:
  - Facial characteristics
  - Fingerprints
  - Hand geometry
  - Retinal pattern
  - Iris
  - Signature
  - Voice

Cost Vs Accuracy



A Generic Biometric System



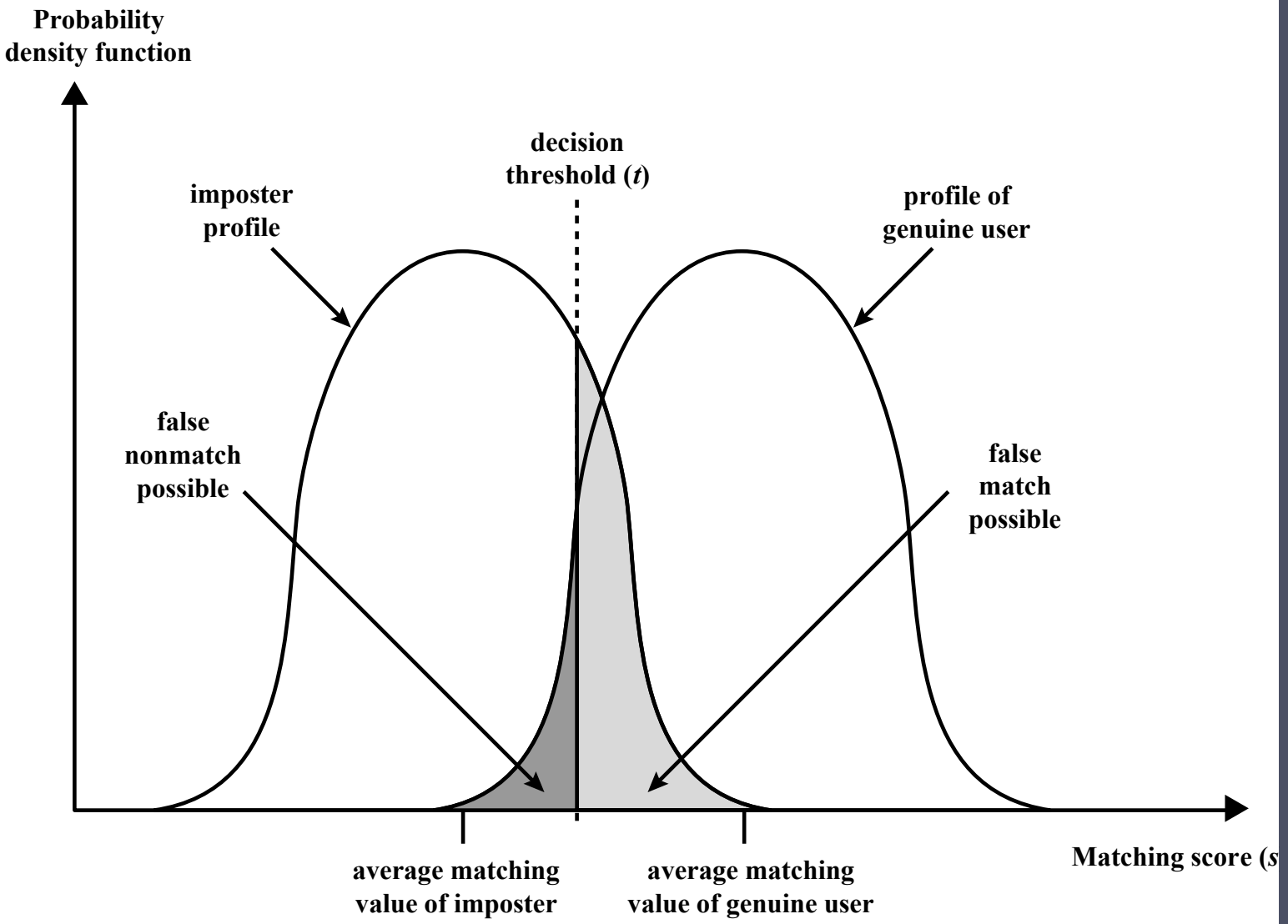


Figure 3.10 Profiles of a Biometric Characteristic of an Imposter and an Authorized Users In this depiction, the comparison between presented feature and a reference feature is reduced to a single numeric value. If the input value (*s*) is greater than a preassigned threshold (*t*), a match is declared.

Remote User Authentication

- Authentication over a network, the Internet, or a communications link is more complex
- Additional security threats such as:
  - Eavesdropping, capturing a password, replaying an authentication sequence that has been observed
- Generally, rely on some form of a challenge-response protocol to counter threats
- We will return to this in a later lecture for *oauth* and other approaches

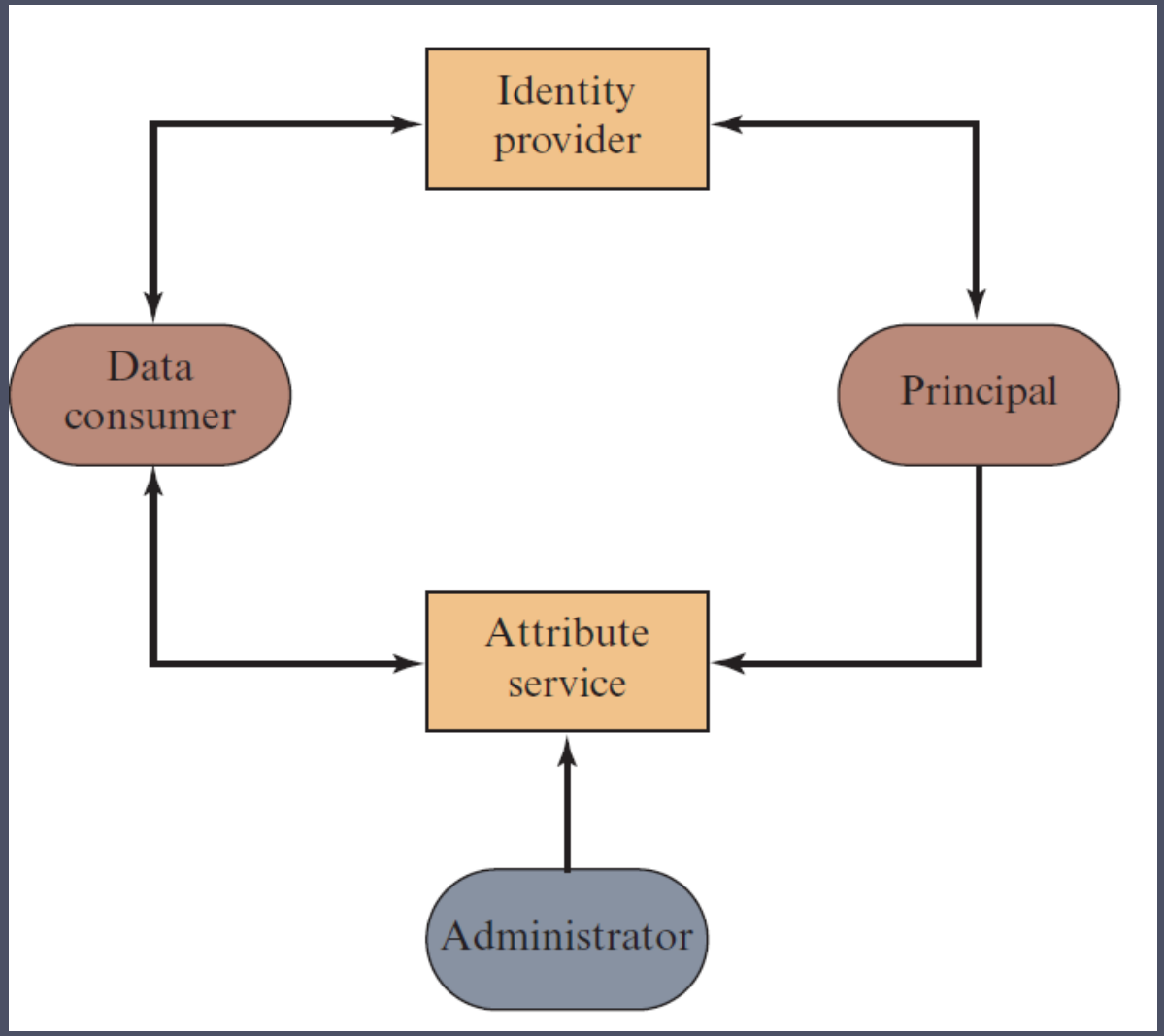
Federated Identity Management

- Relatively new concept dealing with the use of a common identity management scheme across multiple enterprise and numerous applications and supporting many users
- Services provided include:
  - Point of contact
  - SSO protocol services
  - Trust services
  - Key services
  - Identity services
  - Authorization
  - Provisioning
  - Management

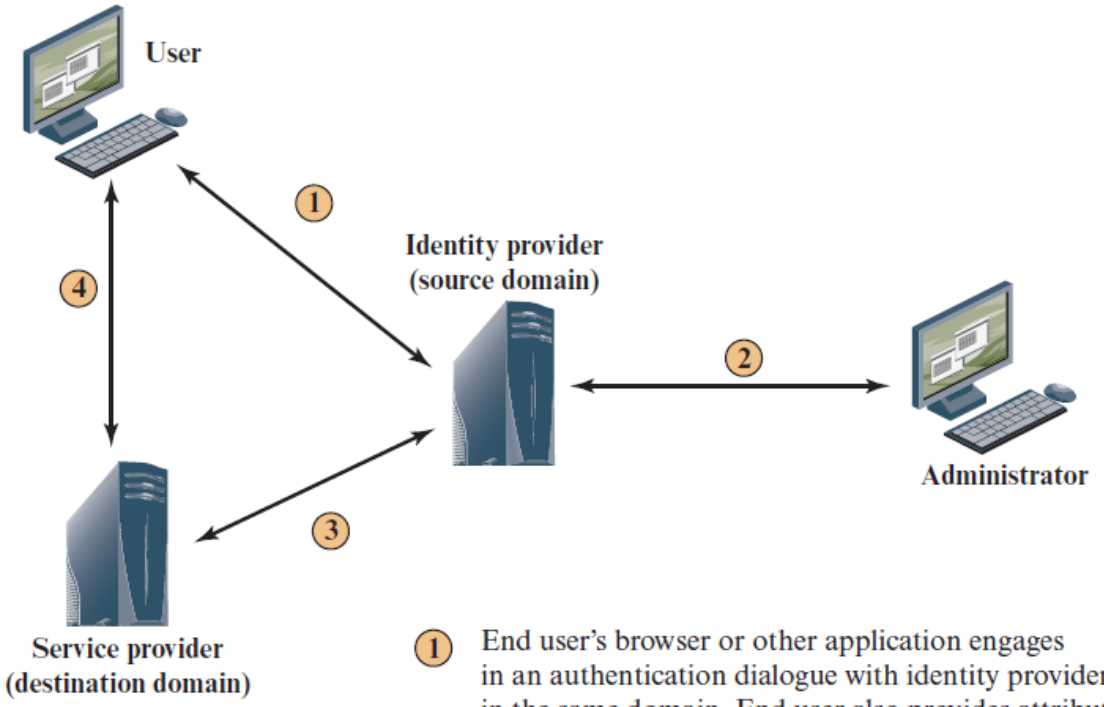
Identity Management

- A centralized, automated approach to provide enterprise-wide access to resources by employees and other authorized individuals
- The focus of identity management is defining an identity for each user (human or process), associating attributes with the identity, and enforcing a means by which a user can verify identity
- The central concept of an identity management system is the use of **single sign-on** (SSO)
- SSO enables a user to access all network resources after a **single authentication**

Generic Identity Management Architecture



Federated Identity Operation



1. End user's browser or other application engages in an authentication dialogue with identity provider in the same domain. End user also provides attribute values associated with user's identity.
2. Some attributes associated with an identity, such as allowable roles, may be provided by an administrator in the same domain.
3. A service provider in a remote domain, which the user wishes to access, obtains identity information, authentication information, and associated attributes from the identity provider in the source domain.
4. Service provider opens session with remote user and enforces access control restrictions based on user's identity and attributes.

Summary

- Digital user authentication principles
  - A model for digital user authentication
  - Means of authentication
  - Risk assessment for user 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
  - Smart cards
  - Smartphones
  - Electronic identity cards
- Biometric authentication
  - Physical characteristics used in biometric applications
  - Operation of a biometric authentication system
  - Biometric accuracy
- Federated Identity Management
  - Identity Management
  - Federated Identity