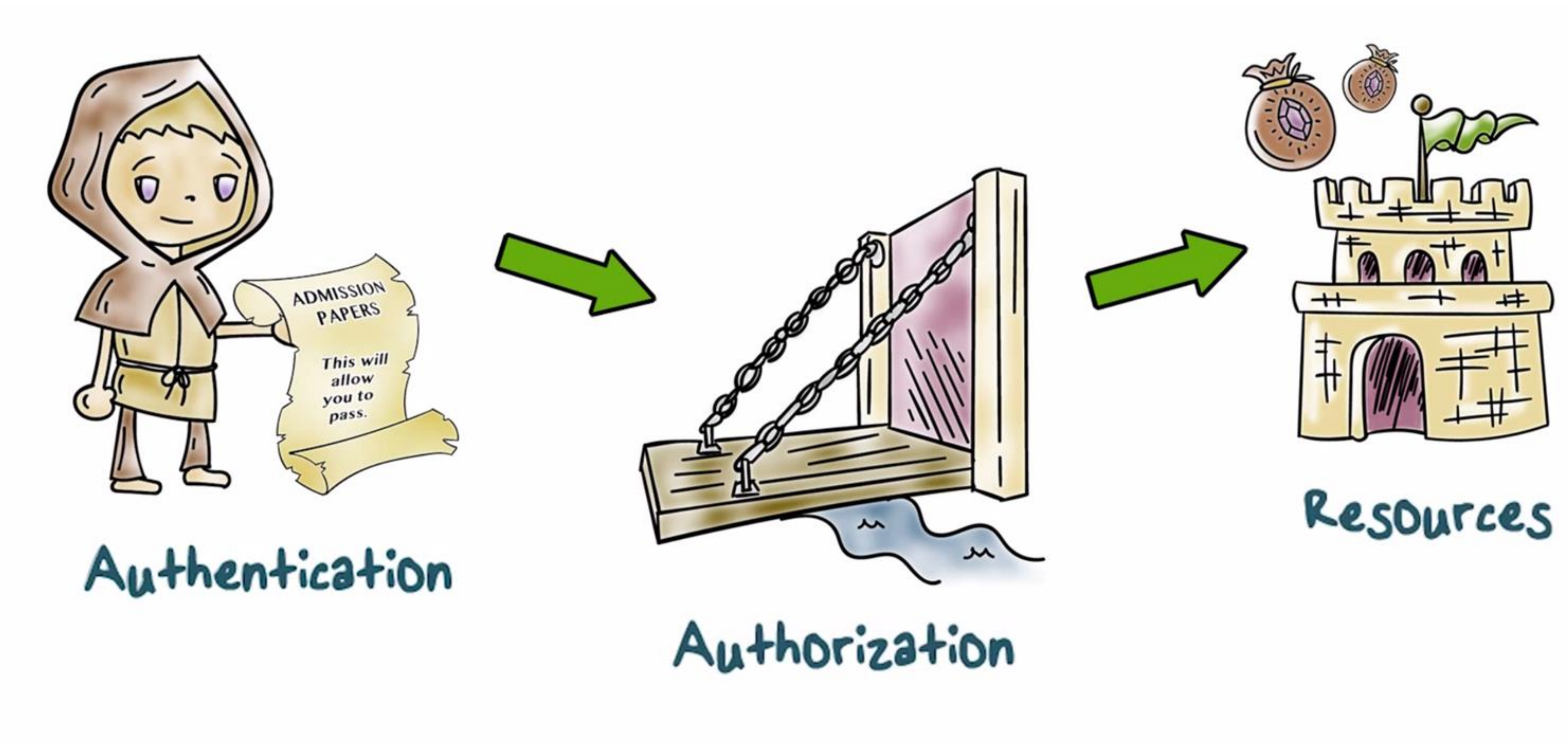
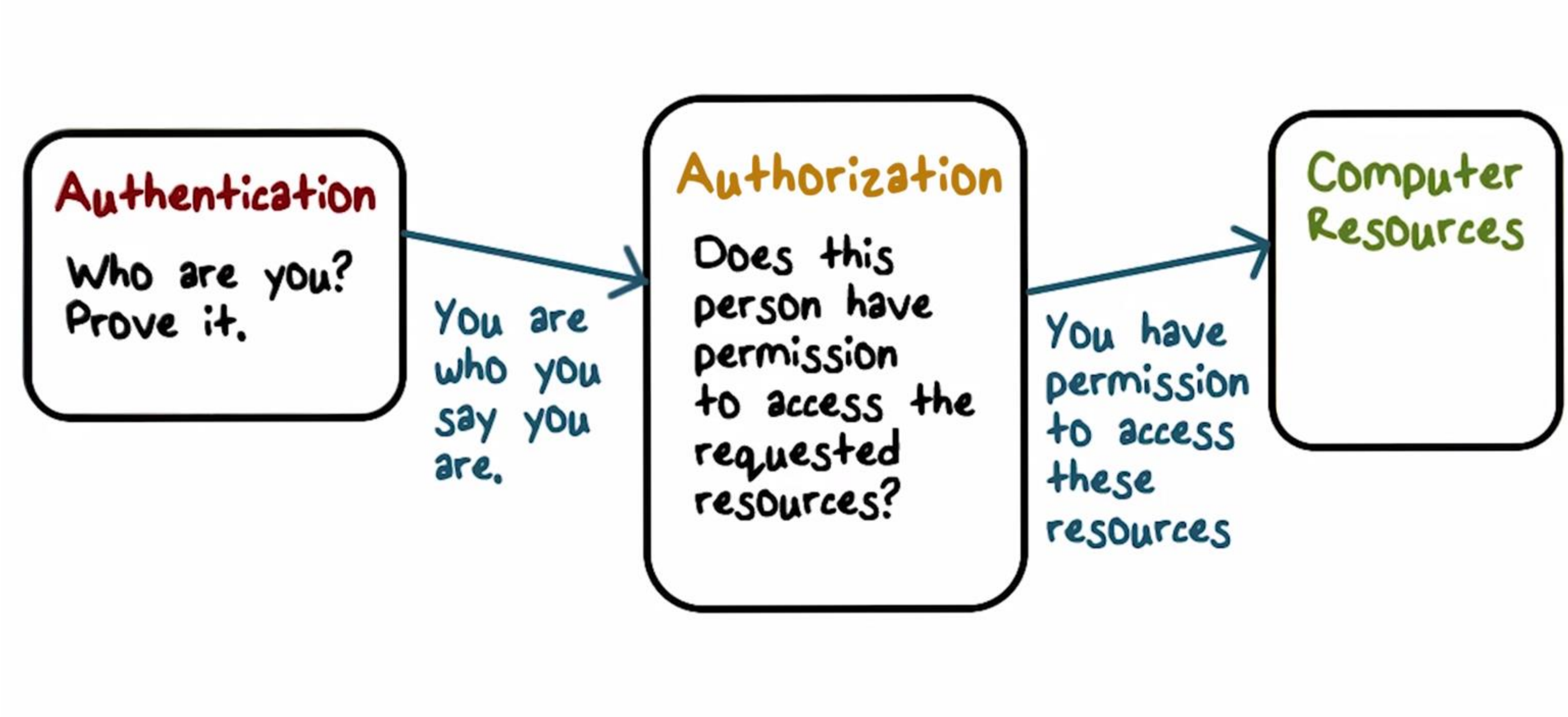
Authentication
Lesson Introduction

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

What is Authentication?



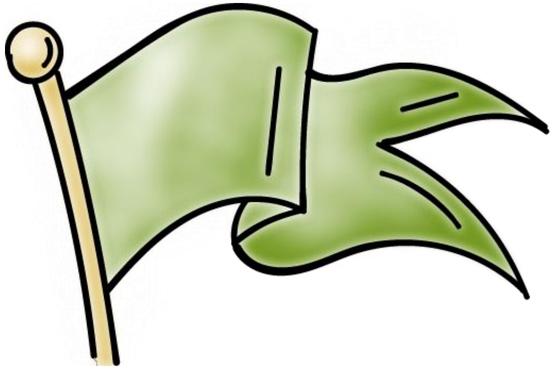
What is Authentication?


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

What is Authentication?

- OS (TCB) needs to know **who makes a request** for a protected resource
- A process that makes the request does it **on behalf of a certain user**, subject or principal
- Authentication helps us answer the question: **on whose behalf the requesting process runs?**
- Includes claims about an identity and verification of the claimed identity of **the user who wants to gain access to system and resource**

Authentication Goals



User/principal associated with an identity should be able to successfully authenticate itself

- Availability
- No false negatives

User/principal not associated with the identity should not be able to authenticate itself

- Authenticity
- No false positives

Authentication Quiz

Check the correct answer from the choices.

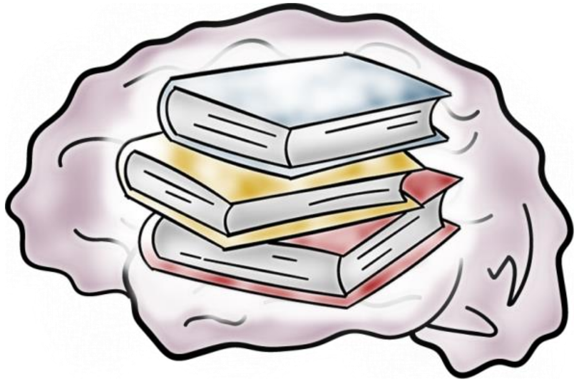
We now have personal devices that are not shared across multiple users. What threats motivate the use of authentication in such devices?

□ Malware infection that may exfiltrate sensitive data

□ Loss of theft of the device

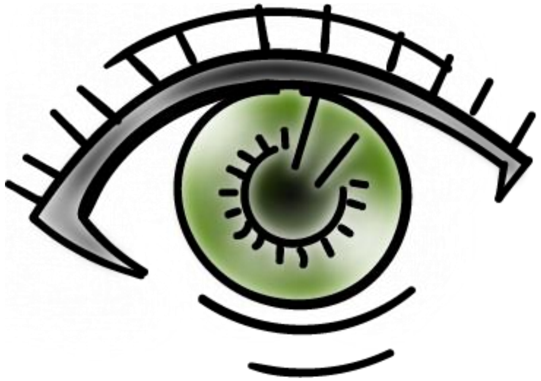
How is Authentication Implemented?

Three basic methods:



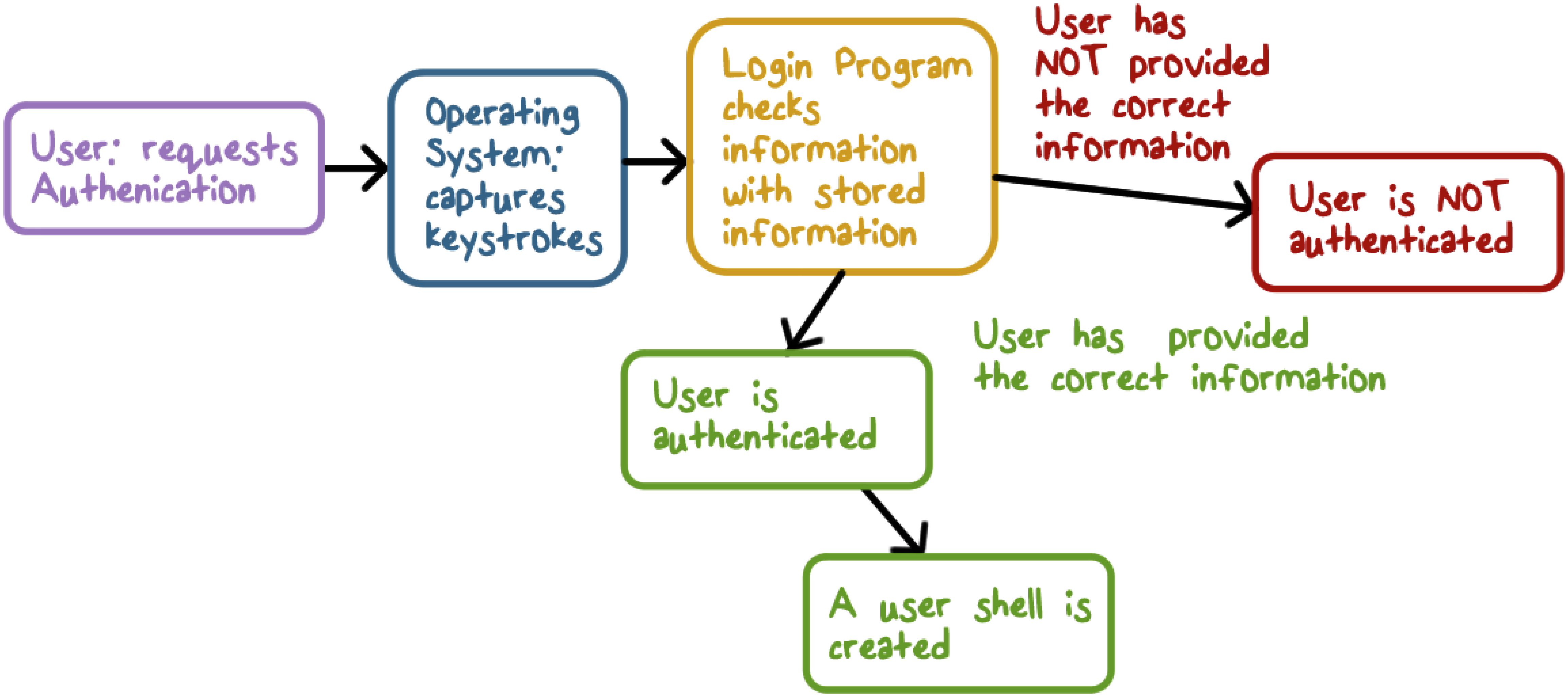
- Something a user **knows**

- Something a user **has**



- Something a user **is**

How is Authentication Implemented?


User: requests Authenication
Operating System: captures keystrokes
Login Program checks information with stored information
User has NOT provided the correct information
User is NOT authenticated
User has provided the correct information
User is authenticated
A user shell is created

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 positive

□ True positive

Implementation Quiz

Check the correct answer from the choices.

A number of online banking systems send a limited lifetime PIN to your smartphone for you to be able to authenticate yourself to the bank. Is this an example of...

□ Something you have

□ Something you are

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

Importance of a Trusted Path

Hardware/OS must provide a trusted path:

- Windows CNTL-ALT-DEL
- Keyboard and display must have trusted paths to OS
- Special kind of display under OS control
- Do users pay attention?

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

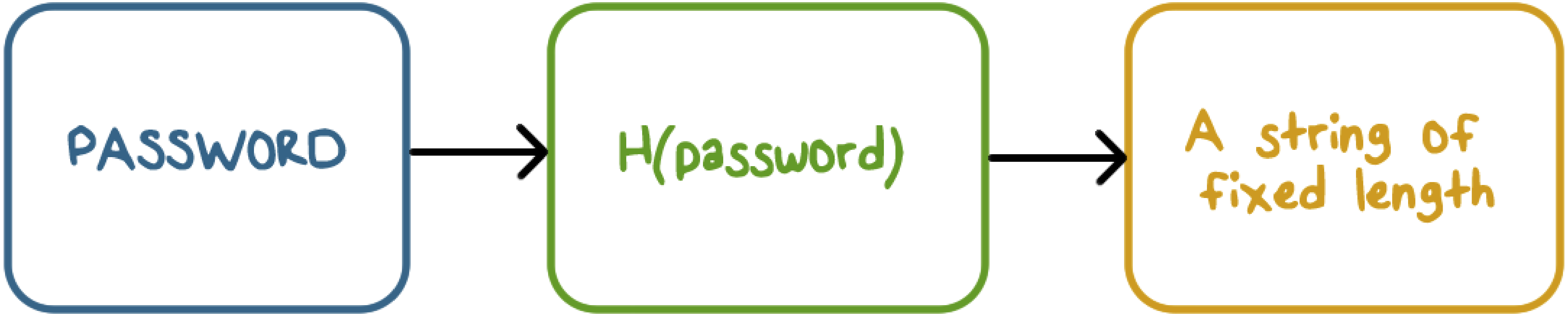
How do we check the password supplied with a user id?

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

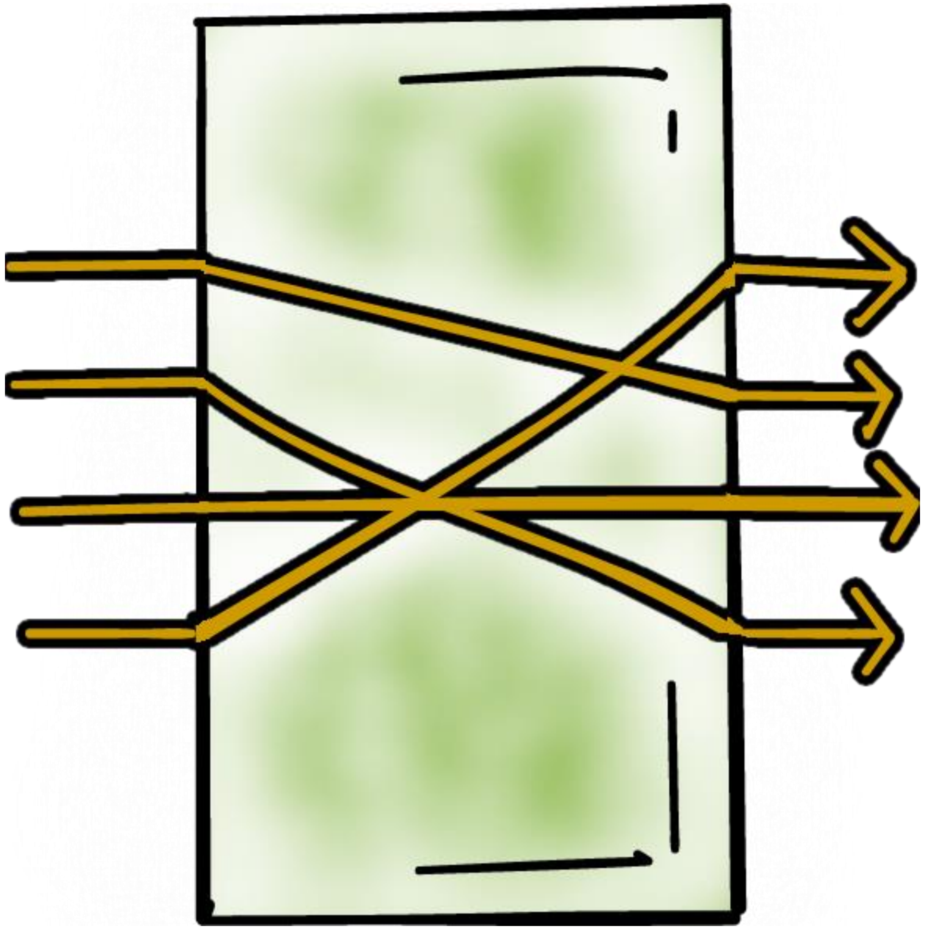
- Use a one-way hash function and store the result

- The password file is readable only for root/admin

Hash Functions



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

Password Quiz

If we do not have a trusted path between a user and the system, what problem may occur. Check the correct answer(s):

□ User is not able to log into the system

□ User may provide the password to a malicious program

Hashed Passwords Quiz

In the past, hashed passwords were stored in a publicly readable file /etc/passwd. **Why were shadow password files added** instead of making/etc/passwd file readable only to privileged users?

□ Shadow files are more efficient to access

□ There is other public information in /etc/passwd file that various utilities need

Hash Function Characteristics Quiz

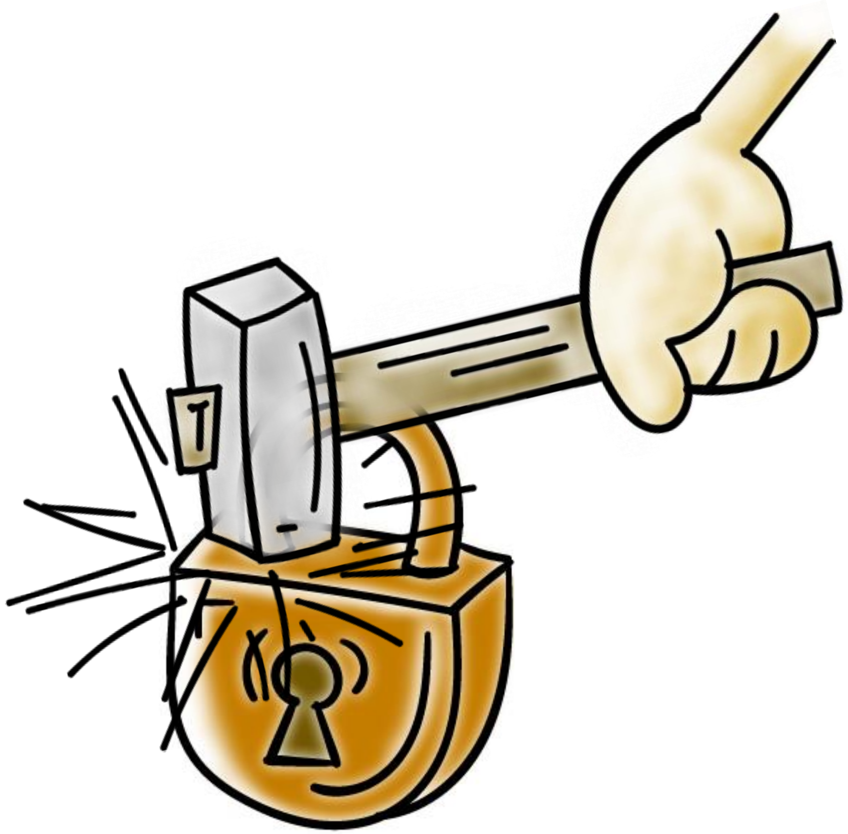
The hash function used for computing hashed password values should meet the following requirements. Check the correct answer(s):

□ Provide more efficient storage of password related information

□ Produce different hashed values for distinct passwords

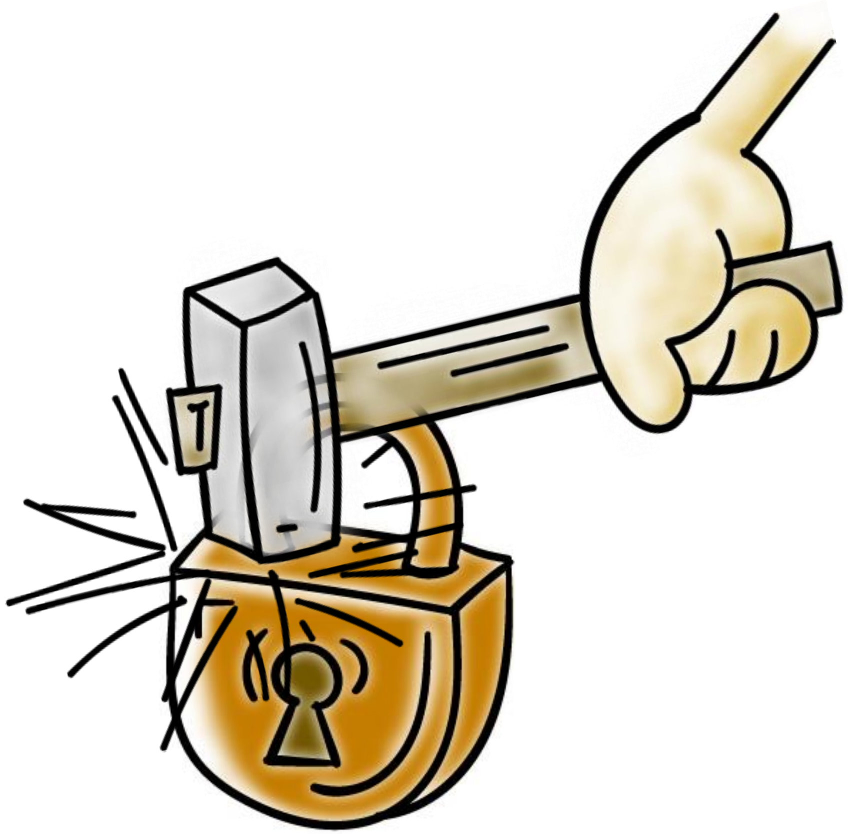
□ Its inverse should be very hard to compute

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**

Brute Force Guessing of Passwords

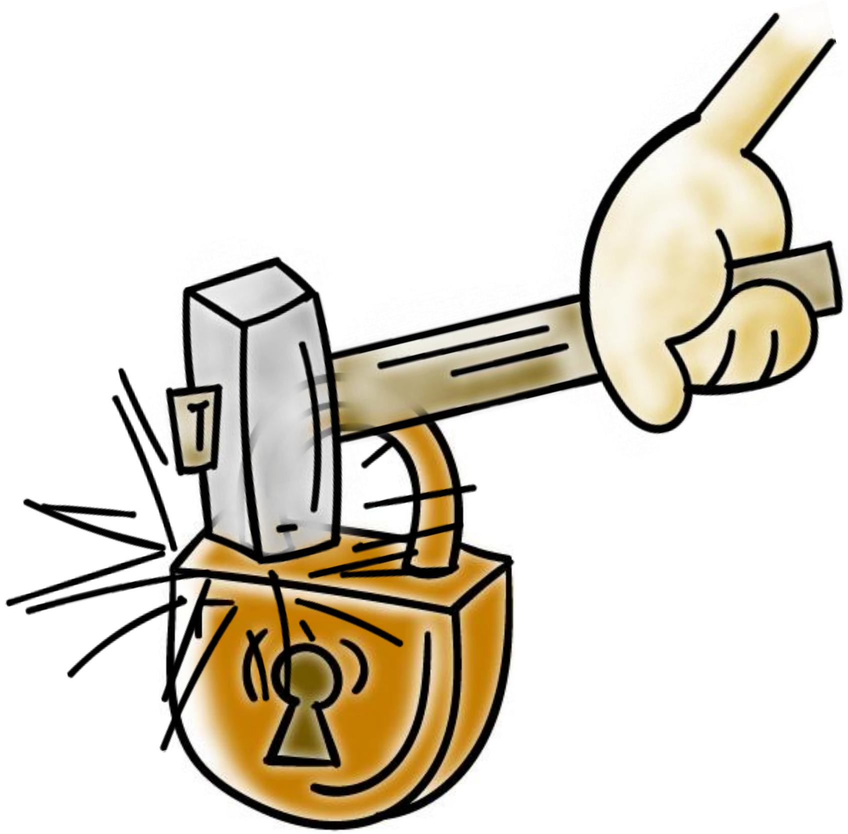


Passwords are not really random

To reduce the work required for a brute force attack:

- Try the popular passwords first
- Create a rainbow table

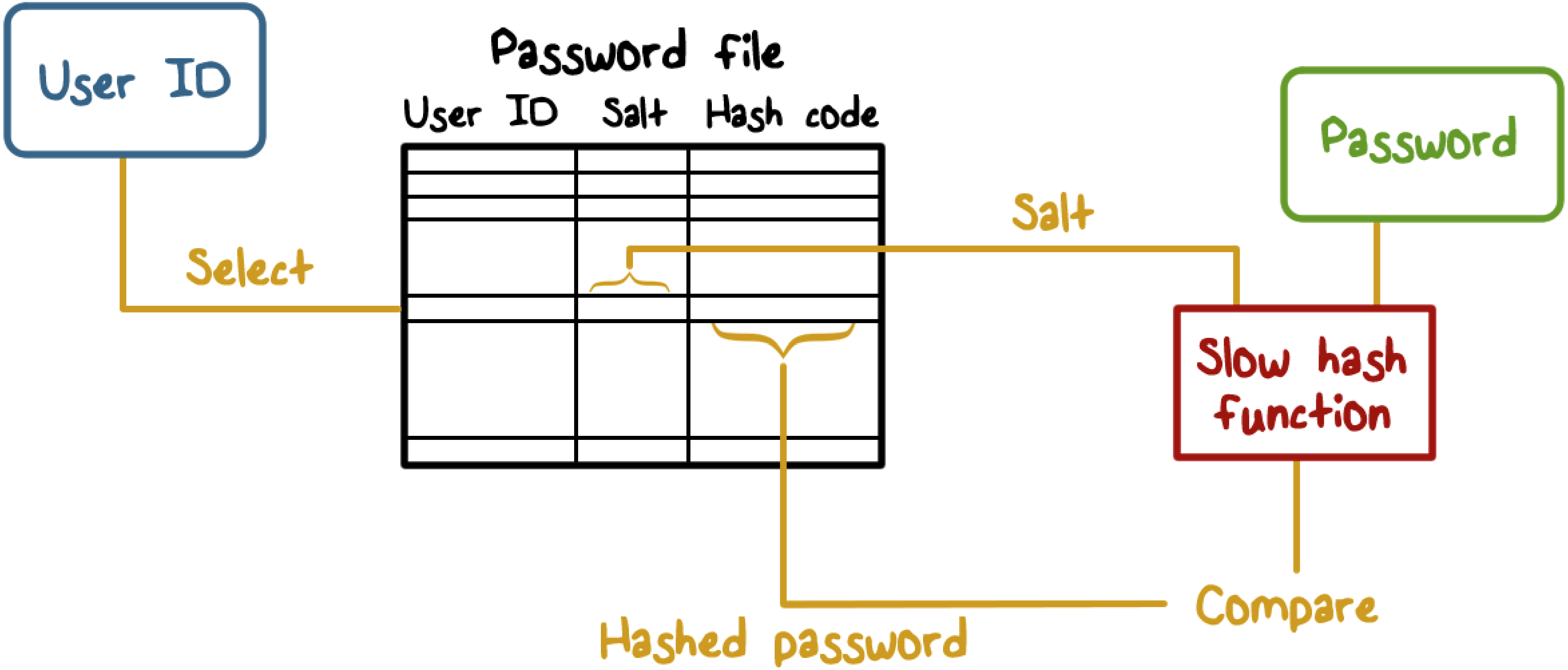
Brute Force Guessing of Passwords



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



Unique PINs Quiz

How many unique four digits PINs are possible?

Check the correct answer:

□ 1,000

□ 100,000

□ 10,000

□ 1,000,000

Brute Force Quiz

A randomly chosen password has six characters that include upper and lower case letters, digits (0-9) and 10 special characters (examples are +, ; etc.). In the worst case, how many attempts must a brute-force method make to determine a password when its hashed value is available?

Check the correct answer:

□ 6^{72} □ 62^{6} □ 72^{6}

Touch Screen Passwords Quiz

In smartphone touch screens, pattern based passwords are used to unlock the device. It is believed that such patterns are not random and there is a bias in where users start. This can be explained by ...

Check the correct answer(s):

□ Users often start at a random point but then fall back to a common pattern

□ There is bias in starting at a point near the top left of the screen

□ The ease of moving from current to next point introduces bias

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

Other Authentication Methods

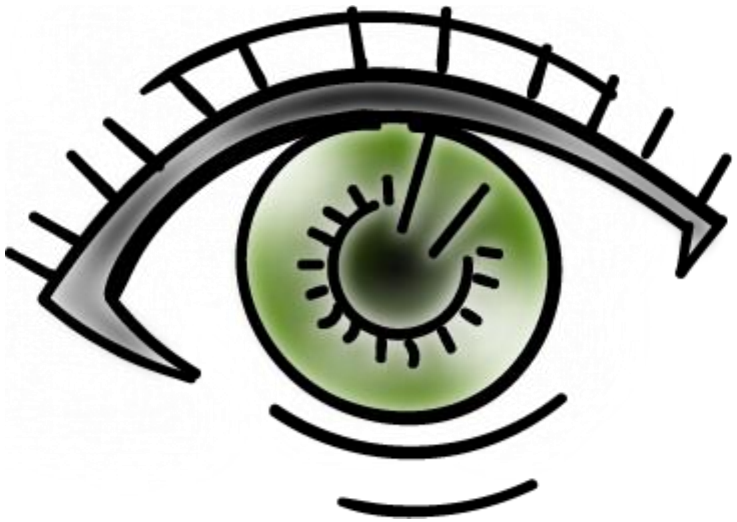
Something you have:

Tokens, smart cards

- 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)

Other Authentication Methods

Something You Are:

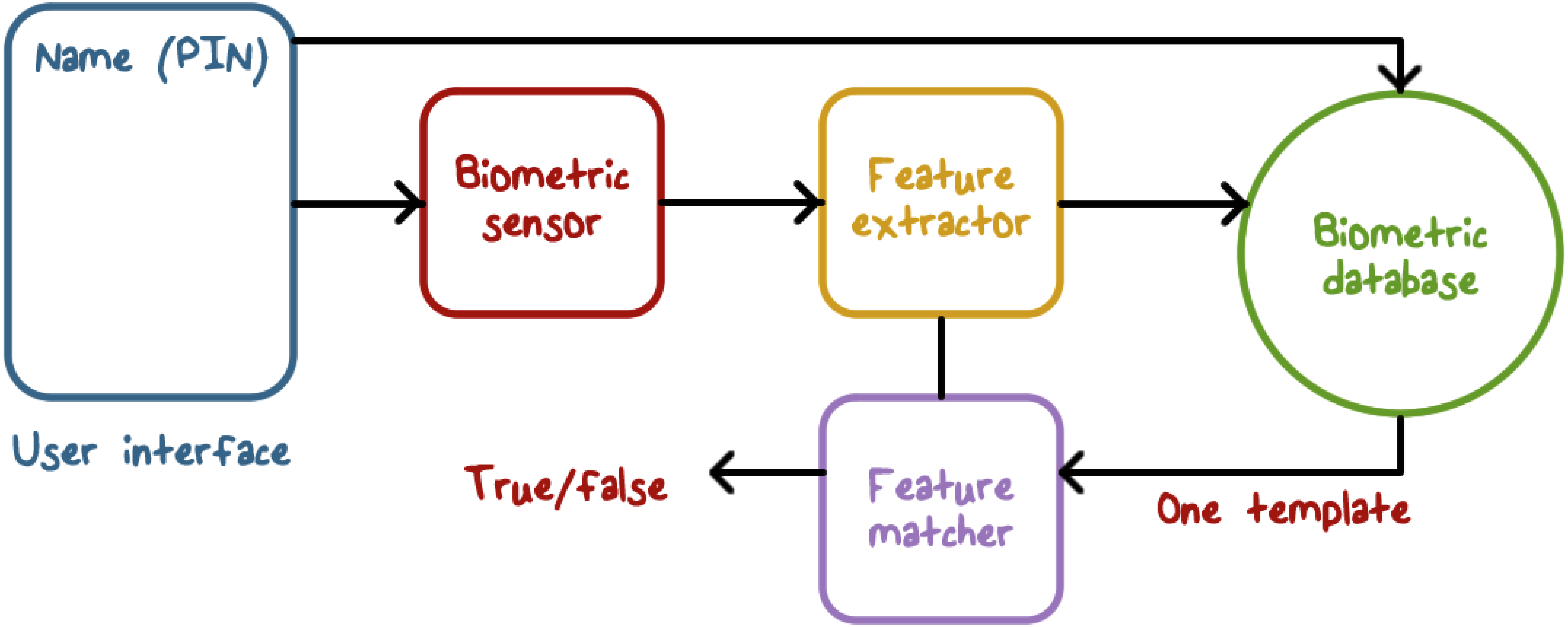


- **Various biometrics**
  - Fingerprints (finger swipes)
  - Keystroke dynamics
  - Voice
  - Retina scans

Do you get the same biometric measurement each time?

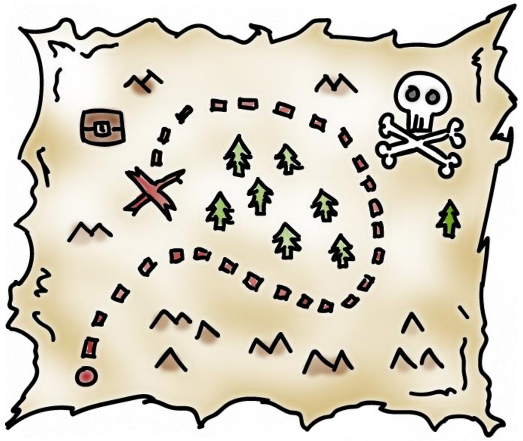
- Probability distribution or a range for feature values
- False positives and negatives

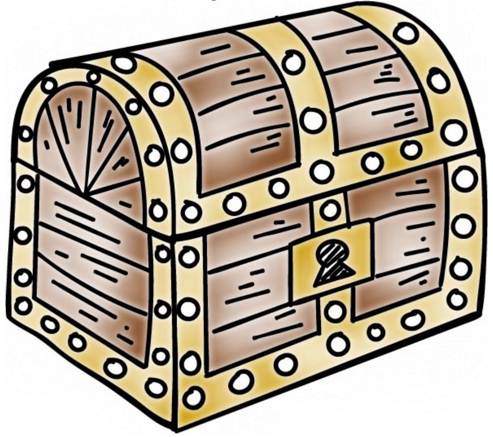
Implementing Biometric Authentication



Other Authentication Methods

Multi-factor authentication

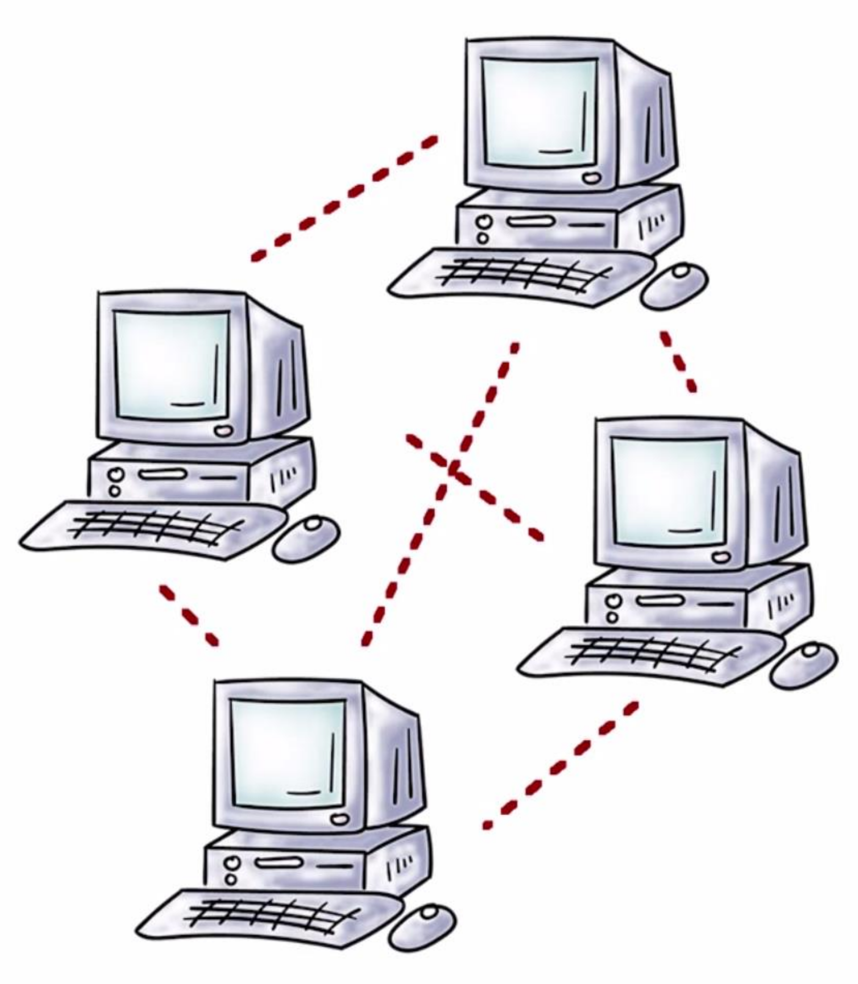




- Uses more than one method
- Type password but also send a code via SMS
  - It goes to your phone (something you have)
  - Gmail implements this
- ATM card and a PIN
- Other things like your location
- **Attacker must defeat both to compromise authentication**

Other Authentication Methods

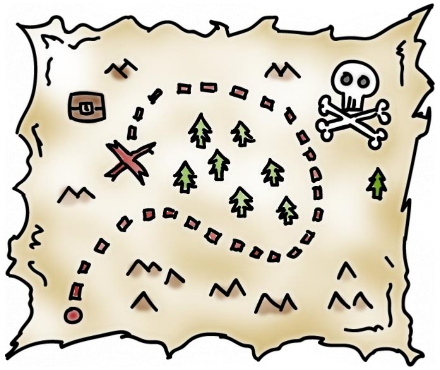
Authentication over a network:

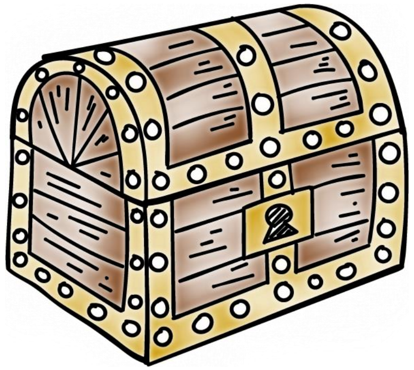


- Do we always have a trusted path to the OS we need to authenticate to?
    - Remote services
- Network authentication **introduces new problems**
- Need crypto to secure network communication
- **Other attacks** (man-in-the-middle)

Multi-factor Authentication Quiz

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





□ True

□ False

Chip and Pin Authentication Quiz

Although a “something you have” based authentication method avoids problems associated with passwords, it could also be prone to attacks. For example, read about chip and pin based authentication at the link listed in the instructor notes.

What is the main weakness that is illustrated here?

- □ Lost cards
- □ Cloning of cards
- □ Vulnerabilities in implementation

Biometric Authentication Quiz

Biometric authentication based on fingerprints can be hacked if an attacker can gain access to a user’s fingerprint.

For example, it has been demonstrated that the Apple’s Touch ID can be fooled with lifted fingerprints. See the link in the instructor’s note.

Can a similar attack be mounted if voice biometric authentication is used?

□ Yes □ No

Authentication
Lesson Summary

- Authenitcation is a **key requirement for securing access** to resources
- All methods present a **number of tradeoffs** that need to be balanced
- Understand how **various types of authentication is implemented**
- Security mindset requires that we do **careful threat modeling**