Lecture 15

Authentication

ECE 422: Reliable and Secure Systems Design

UNIVERSITY OF ALBERTA

Instructor: An Ran Chen
Term: 2024 Winter

Schedule for today

- Key concepts from last class
- Authentication
    - Password-based authentication
    - Magic links
    - SMS-based authentication
    - Authenticator apps
        - TOTP
        - HOTP
    - Biometric authentication
    - Multi-factor authentication

The CIA triad

The CIA triad:

- Confidentiality: only the authorized user can access particular resources
- Integrity: ensure data are trustworthy, complete, and have not been modified by unauthorized parties
- Availability: ensure data are accessible when needed

Both security and reliability are concerned with these three concepts

- Difference: the presence or lack of a malicious adversary

Integrity

Integrity

- Ensure data are trustworthy, complete, and have not been modified by unauthorized parties

Methods to achieve integrity:

- Hashing: transforms any given data into fixed-size values
  - E.g., Comparing stored data
- Digital signature: verifies the authenticity of data
  - E.g., Emails, software application codes

Hash function

Hash function: transforms any given data into fixed-size values

- Deterministic
  - Same input = same hash value
- Irreversible
  - One-way function (input to hash)
  - The data is secure even if the hash function is public

Problem: hash collision may happen

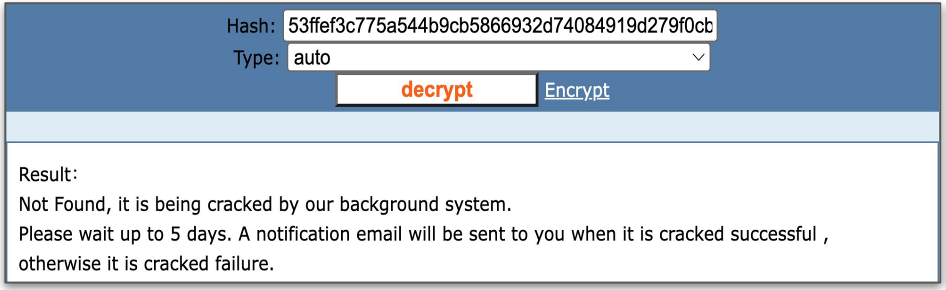
- Unavoidable by nature
- More possible inputs than outputs

Applications of hash function

- Digital signature
  - Creating a digital signature = Hash of the message + encryption with private key
- File integrity check
  - Compare hashes to verify it is the right file
  - E.g., verify file download
- Password storage
  - Store passwords as hashes
  - Implication 1: actual password is hidden
  - Implication 2: same password is stored as different hashes

Workaround for hash function?

- Password storage
  - Potential problem: reverse-engineering the password (e.g., by brute force)
- Brute force solution: SHA256 generation tool, SHA256 database
  - Input 1: ECE422!(hello*@
  - Hash: 53ffef3c775a544b9cb5866932d74084919d279f0cbab0687d11b53d1df8900e
  - Input 2: ECE422
  - Hash: b3af9c50da07cc8f7f7ed00f86b2c6ae7e41c75e5c84dce9b70c6ac8cf8454cc



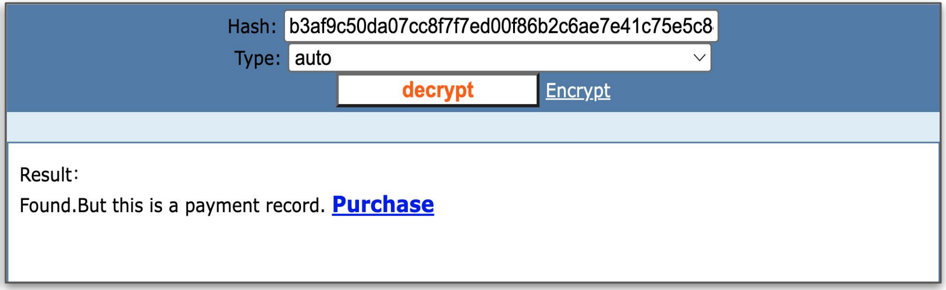
Hash: 53ffef3c775a544b9cb5866932d74084919d279f0cb

Type: auto

Result:

Not Found, it is being cracked by our background system.

Please wait up to 5 days. A notification email will be sent to you when it is cracked successful , otherwise it is cracked failure.



Hash: b3af9c50da07cc8f7f7ed00f86b2c6ae7e41c75e5c8

Type: auto

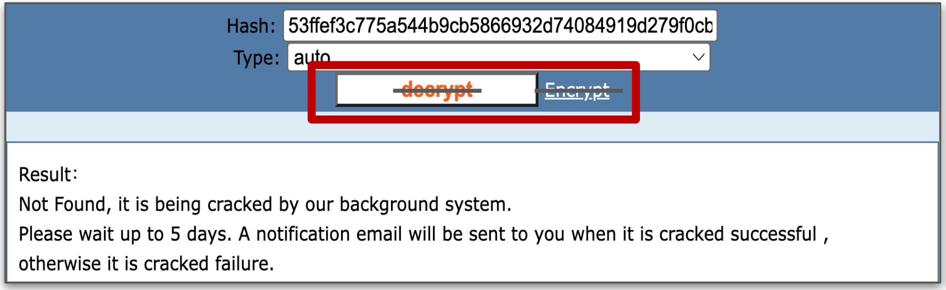
Result:

Found.But this is a payment record. **Purchase**

Workaround for hash function?

Note that hash function does not encrypt the data, it generates a hash using the input as a seed instead.

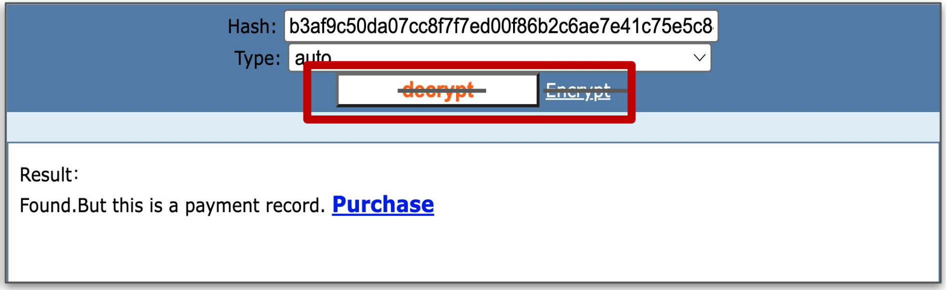
- Hashing: one-way function
- Encryption: two-way function



Hash: 53ffef3c775a544b9cb5866932d74084919d279f0cb

Type: auto

Result:
Not Found, it is being cracked by our background system.
Please wait up to 5 days. A notification email will be sent to you when it is cracked successful , otherwise it is cracked failure.



Hash: b3af9c50da07cc8f7f7ed00f86b2c6ae7e41c75e5c8

Type: auto

Result:
Found.But this is a payment record. **Purchase**

Example of hash function: SHA256

Example of hashing: SHA256

- Hash of 64 hexadecimal characters / 256-bit hashes
- Produces a total of 2^{256} hashes
- Hash collision: 1 out $(4.3\text{ billions})^8$

Input 1: “Hi ECE 422”

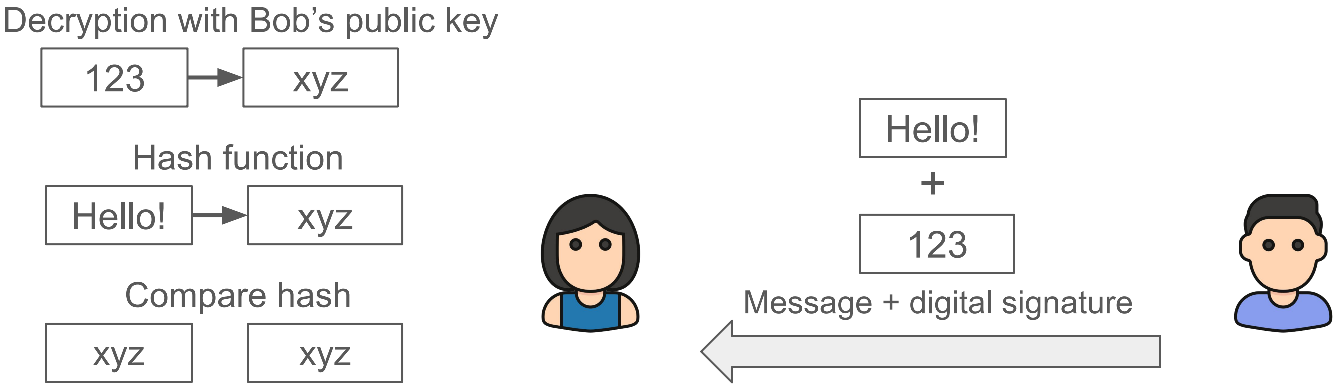
SHA256 hash:

```
911fe59b33e0cf049ba953138c05178c9ffd4
e57a0bd43be4c88cbf39dd7959a
```

Digital signature

Digital signature verifies the authenticity of the sender through hashing and decryption. For example:

- Alice uses Bob’s public key to decrypt the message.
- Alice create a hash of the message by herself.
- Alice verifies whether the hash matches what Bob sends.



Decryption with Bob’s public key

123 → xyz

Hash function

Hello! → xyz

Compare hash

xyz xyz

Hello!

+

123

Message + digital signature

Confidentiality

Confidentiality

- Only the authorized user can access particular resources

Methods to achieve confidentiality:

- Encryption: encoding/decoding of the plaintext
  - E.g., Symmetric/asymmetric encryption
- Access controls: restricted access
  - E.g., Our library website
- Authentication: credentials check
  - E.g., Mobile authentication for faculty and staff

UoA's Information Services & Technology

Schedule for today

- Key concepts from last class
- Authentication
  - Password-based authentication
  - Magic links
  - SMS-based authentication
  - Authenticator apps
    - TOTP
    - HOTP
  - Biometric authentication
  - Multi-factor authentication

Identification vs authentication vs authorization

Identification happens when a user claims an identity.

- Username, student ID card, CCID

Authentication provides access control for systems by checking to see if a user's credentials match the credentials in a database.

- Username + password, smart card, driver license + fingerprint
- Something the user knows/has/is

Authorization provides access to different resources based on the user identity.

- Admin privileges, student account access, library resources

Question

Q1) What happens when a user’s password has been verified?

A. Identification

B. Authentication

C. Authorization

D. Identity verification

Authentication

- Password-based authentication
  - Username + password
- Magic links
  - Links through email or mobile device
- SMS-based authentication
  - Text messages
- Authenticator apps
  - Push notifications, or one-time password (OTP)
- Biometric authentication
  - Biometric data (e.g., fingerprint and face recognition)
- Multi-factor authentication (MFA)
  - Two or more independent authentication factors

Password-based authentication

In password-based authentication, the user enters the right credentials to gain access to the system.

Use case:

- Enter the email address and password in the login page
- Check against the hashed (and salted) password in the database
- If they match, the user is granted access

Security risks:

- Can be stolen or guessed
- People forget passwords

Password storage

Salting is a technique to protect passwords stored in databases by adding characters before hashing.

- Stored password = Hash (password + salt)

Example:

- Password: ECE422
- Salt: !(hello*@
- Password + salt: ECE422!(hello*@
- Hash: 53ffef3c775a544b9cb5866932d74084919d279f0cbab0687d11b53d1df8900e

Magic link

In magic link authentication, the user leverages URLs with embedded tokens to gain access to the system.

Use case:

- Enter the email address in the login page
- Receive an email with a (magic) link
- Click on the link to login

Security risks:

- As secure as the email account
- Rely on the email service providers

Example of magic link in practice

On the login page:

- The user sends the email address to the server.

On the server-side:

- The database checks if the email exists.
- The application generates a link embedding a login token and stores the token in the database.
- The application sends the user an email with the link.

Example of magic link in practice

Within the email:

- The user clicks on the link.

On the server-side:

- The application verifies the token and grants user the access.

Short message services (SMS)

In SMS authentication, the user provides a code that is sent to their phone as proof of identify.

Use case:

- Login with username and password
- An SMS code sent to the phone
- Enter the SMS code into the login interface

Security risks:

- Phishing messages
- SMS messages can be intercepted

Schedule for today

- Key concepts from last class
- Authentication
    - Password-based authentication
    - Magic links
    - SMS-based authentication
    - Authenticator apps
        - TOTP
        - HOTP
    - Biometric authentication
    - Multi-factor authentication

Authenticator apps

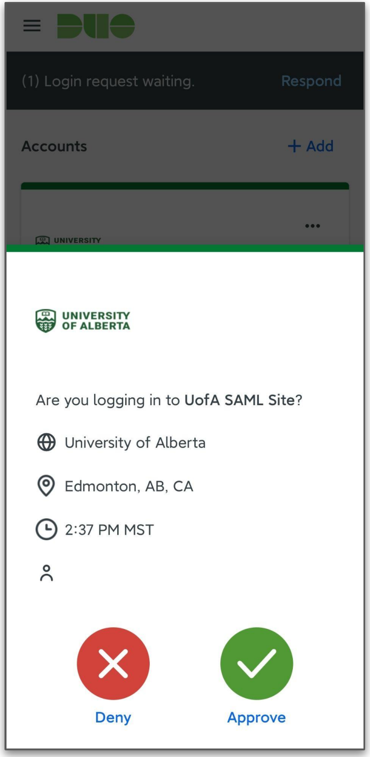
An authenticator app allows users to prove their identity through a specialized application.

- Usually on a mobile device
- Notifies users every time there is an attempt to log in
- Allows users to deny access, stopping the attacker in their tracks

Two common forms of authentication:

- Push notification
- One-time password (OTP)

Push notification



(1) Login request waiting.

Are you logging in to **UofA SAML Site**?

University of Alberta

Edmonton, AB, CA

2:37 PM MST

In push notification, the user approves a notification that is sent to their mobile device as proof of identify.

Use case:

- Login with username and password
- A notification sent to the mobile device
- Approve in the application

Security risks:

- Applications can be vulnerable
- Third-party applications can have access

One-time password (OTP)

Authenticator apps can also leverage one-time password to verify the identity of the user.

- Generally used within 2FA and MFA systems

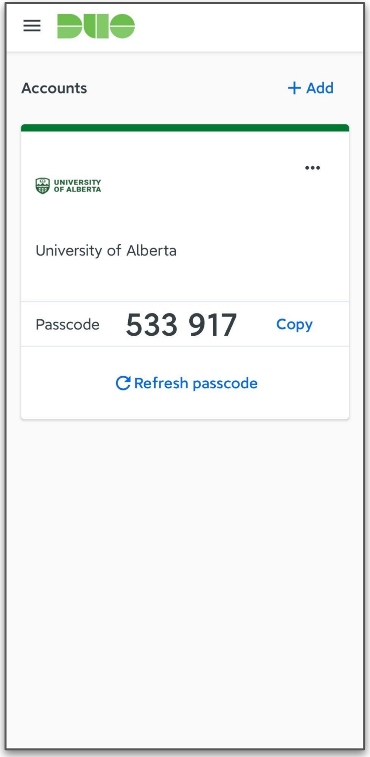
Example of OTP:

- Time-based one-time passwords (TOTP)
  - Passcode valid within a set interval of time
  - Input: secret key + time
- HMAC-based one-time passwords (HOTP)
  - Passcode that can only be used once
  - Input: secret key + counter

TOTP

Time-based one-time password (TOTP) uses a public algorithm to generate the one-time password.

- Generate unique passcodes based on the current interval of time
- Time interval is generally 30 seconds
- No delivery of the one-time passcode is required
  - Generation algorithm shared ahead of time
- One-time passcode generated through a shared secret key and the current time



Accounts

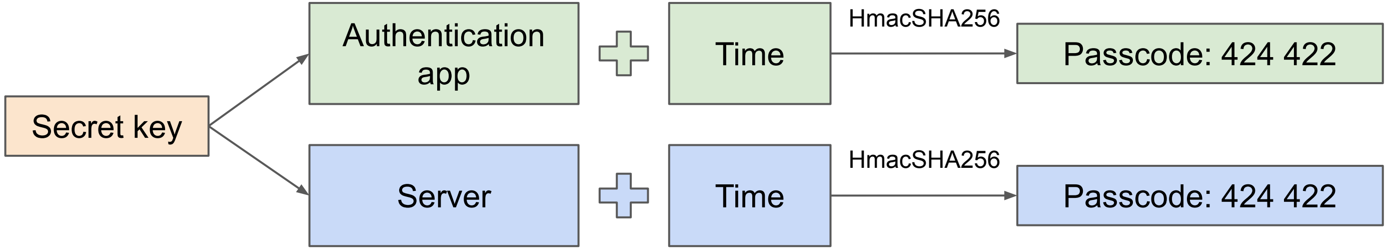
University of Alberta

Passcode 533 917

TOTP algorithm

Algorithm behind TOTP:

- Both the user application and the server generates the passcode based on the current time and secret key.
- Typical generation algorithm: HMAC-SHA-1 and HMAC-SHA-2
  - E.g., HmacSHA256, a hash-based message authentication code (HMAC) function
  - HMAC takes as input: (time + secret key)



Example of TOTP in practice

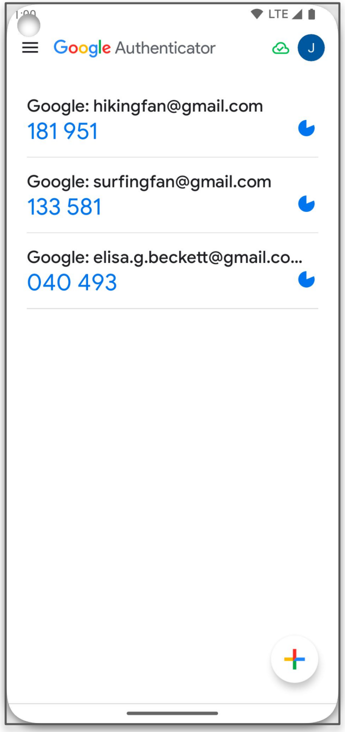
When the user installs the application:

- Time synchronization via the Network Time Protocol (NTP)
  - NTP is designed for sending time over the Internet (accurate to a few milliseconds)
- Share a unique secret key

When the user authenticates:

- The user uses the key and time to generate the passcode
- The user sends the passcode to the server
- The server computes the passcode and compares
- If the passcode matches, then the user gains access

HOTP



Google Authenticator

Google: hikingfan@gmail.com
181 951

Google: surfingfan@gmail.com
133 581

Google: elisa.g.beckett@gmail.co...
040 493

Google Authenticator

HMAC-based one-time passwords (HOTP) also uses a public algorithm to generate the one-time password.

- Generate unique passcodes based on the current counter
- Counter is a variable stored on the server and the application, increases each time a passcode is generated.
- No delivery of the one-time passcode is required
  - Generation algorithm shared ahead of time
- HMAC takes as input: (counter + secret key)

Example of HOTP in practice

When the user installs the application:

- Share a unique secret key

When the user authenticates:

- The user uses the key and counter to generate the passcode
- The user sends the passcode to the server
- The server computes the passcode and compares
- If the passcode matches, then the user gains access
- The server synchronizes on the counter

TOTP vs HOTP

- OTP expiration
  - TOTP only valid for a period of time until they expire
  - HOTP valid until usage, no time expiration
- Convenience
  - TOTP must be used before expiration
  - HOTP request anytime, use them later
- Security
  - TOTP is more secure, time as a moving factor
  - HOTP is vulnerable to brute force attacks

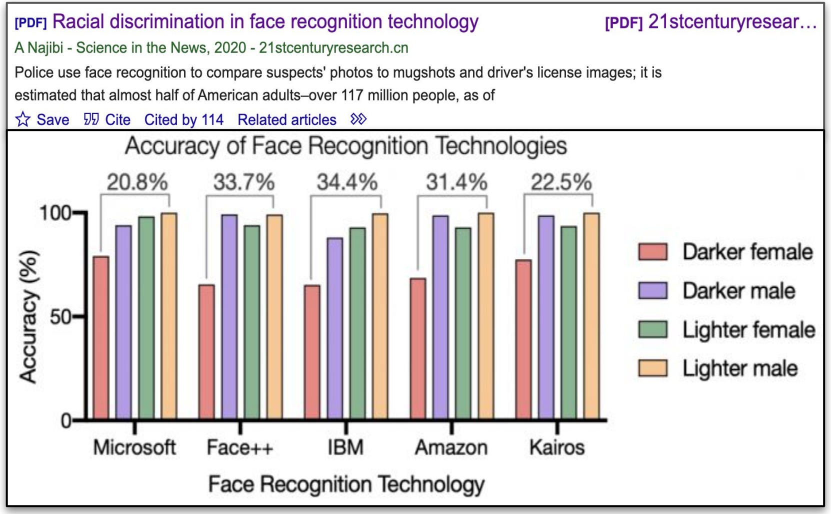
Schedule for today

- Key concepts from last class
- Authentication
  - Password-based authentication
  - Magic links
  - SMS-based authentication
  - Authenticator apps
    - TOTP
    - HOTP
  - Biometric authentication
  - Multi-factor authentication

Biometric authentication

Examples of biometric authentication:

- Facial recognition
  - ○ Accuracy of facial recognition can depend on age, race and gender.
- Fingerprint
  - ○ Nearly 99% accuracy
- Retina recognition
  - ○ Used in government and military organization
- Voice recognition
  - ○ Noisy environment can be a problem



[PDF] Racial discrimination in face recognition technology [PDF] 21stcenturyresear…

A Najibi - Science in the News, 2020 - 21stcenturyresearch.cn

Police use face recognition to compare suspects' photos to mugshots and driver's license images; it is estimated that almost half of American adults–over 117 million people, as of

☆ Save 99 Cite Cited by 114 Related articles »

Multi-factor authentication (MFA)

Multi-factor authentication (MFA) requires two or more factors to verify user's identify.

- Knowledge factor: Something only the user knows
    - Password, PIN code
- Possession factor: Something only the user has
    - Access card, key, authorized device
- Biologically factor: Something only the user is
    - Physical trait: fingerprint, retinal pattern
    - Behavioral process: voice recognition, keystroke dynamics

Multi-factor authentication (MFA)

- Location factor: Some location information the user should have
    - IP address, geolocation
- Time factor: Some time information the user should have
    - Weekdays, hours

Authentication

- Password-based authentication
  - Username + password
- Magic links
  - Links through email or text messages
- SMS-based authentication
  - Text messages
- Authenticator apps
  - Push notifications, or one-time password (OTP)
- Biometric authentication
  - Biometric data (e.g., fingerprint and face recognition)
- Multi-factor authentication (MFA)
  - Two or more independent authentication factors

Multi-factor authentication (MFA)

Q1) An example of multi-factor authentication is a username and password.

A. True

B. False

Q2) Which one of the following does NOT help upgrade the security of a current password-based authentication system to a multi-factor authentication system?

A. Access card

B. Retinal scan

C. Authenticator apps

D. Security questions

TODOs

- Demo sessions will be held in DICE 11-242 instead.
- Review session next Friday