Define Authenticator

- A generic description for a hardware or software based means that produces secret based strings for authentication

Hardware Tokens

- USB, chip-cards
- Intended to securely store secrets and generate digital tokens from them in challenge-response authentication protocols

Password Generators

- Commercial form of one-time passwords
- Device specific secret and computes passcode output similar to OTP’s
- The passcode is a function of this secret and a TVP challenge

Authentication: Where you are

- Your location (geolocation, gps, …)

Authentication: What you know

- Include things you remember mentally (passwords, PINS, passphrases)

Authentication: What you are

- Physical biometrics (fingerprints, etc)

Authentication: What you have

- A computer or hardware token physically possessed, often holding a cryptographic secret or hard to replicate properly (ie. RFID card)

Lamport Hash Chain

- Technique for generating OTP's using weak secret
- Start with random secret seed w, user A can authenticate server B using a sequence of one-time-passwords, such that H is a one way hash function, t is an integer, hash chain of order t:

$$w, H(w), H(H(w)), \ldots, H^t(w)$$

First OTP is $H^t(w)$ then $H^t - 1(w)$...

Lambert Hash Chain: Weak to small n attack

The attacker impersonates the server, when the client tries to authenticate, the man-in-the-middle queries with n. The client answers with hash^n(password), the attacker can calculate hash^m(password) for any m>n

Lambert Hash Chain: Attacker knows t

- Attacker knows t and knows what run is approaching, then the attacker knows the number of times that the secret was hashed which gives them verifiable text to guess w (the secret)

The One-Time Password Challenge

- How to pre share lists of one time passwords between the party to be authenticated (claimant) and the verifier

One Time Passwords

- Passwords valid for a single use only

Secret Questions for password recovery: pros and cons

Cons: space of potential answers is small, information is publicly available (social media), peoples answers change

Pros: High usability, easy to implement

Memory aids for passkeys:

The first letters of words in a relatively long sentence

Password Derived Cryptographic Keys - Passkeys

- Must be strong because they are subject to offline attacks and require high guessing resistance

Defensive Measures: MAC on password

addresses offline guessing, stolen hashfile no longer useful

Defensive Measures: Pepper

addresses offline guessing, increases time per guess

Defensive Measures: Iterated Hashing

addresses offline guessing, increases time per guess

Defensive Measures: Salts

address pre-computed dictionaries

Defensive Measures: blacklisting

addresses online guessing, disallow most common, or simple passwords

Defensive Measures: Rate Limiting

addresses online guessing, locks a user out after n attempts

User Authentication: Defensive Measures

- Rate Limiting
- Blacklisting
- Salt
- Iterated Hashing
- Pepper
- MAC on Password

Probability of correctly guessing a password

$q = GT/R$ where

R = the password space

G = the number of guesses per one time unit (guessing rate)

T = amount of time units

Targeted vs Trawling Scope

- Targeted: attack specific pre-identified users
- Trawling: break into any account, by trying many or all accounts

System assigned passwords: Definition + pros and cons

- A randomly generated password
- Pros: It eliminates password bias, and minimizes guessability
- Cons: It decreases usability, user have a hard time remembering random strings

Slowing down attackers: Salts vs Peppers vs Iterated Hashing

- Iterated hashing: by a factor of k (where k is the number of times the password is hashed)
- Salting: 2^t (where t is the length of the salt)
- Peppering: 2^R-1 (where R is the keyspace of the salts)

Define Iterated Hashing

The password is hashed k times. It is used to slow down attackers because an attacker must also perform the hashing k times in order to get the password.

Define Pepper or Secret Salt

A pepper is like a regular salt except it is not stored. To verify the password for an account the system tries all salts in a deterministic order.

Define Password Salt

A password salt is a random k-bit value that is concatenated with the password before hashing. The salt is stored in plaintext. Prevents the usage of rainbow tables.

Disadvantages of Passwords

- Can be guessed very easily
- Finite keyspace
- User behaviour is predictable (non-uniform password distribution)

Advantages of Passwords:

- Simple, easy to use and learn
- Free, require no physical device to carry
- Can be replaced if lost
- Quick login times

Password Capture Prevention

- Prevent with encrypted traffic, educating the public

Define Password Capture

An attacker intercepts or observes passwords directly

Bypassing Authentication Interface Prevention

Prevent with up to date software, regular security testing

Define Bypassing Authentication Interface

gaining unauthorized access to software vulnerabilities or design flaws

Defeated Password Recovery Prevention

Prevent with recovery questions

Define Defeated Password Recovery

attacker abuses password recovery mechanism to make a new password for your account instead of stealing the old one

Offline Guessing Prevention

Salts, Peppers, iterated hashing, MAC on passwords

Define Offline Guessing

No per-guess interaction with the server is required

Online Guessing Prevention

Prevent with: rate limiting - setting a limit on the number of guesses before lockout

Define Online Guessing

Guesses are sent to legitimate server

Authentication Signals

- Checking IP addresses of devices associated with previous logins
- Browser cookies, and device fingerprinting

Biometric Authentication: Physical

- Parts of a person that uniquely define them (ie. facial recognition, fingerprints)

Biometric Authentication: Behavioral

- The way a person acts
- Behavioral patterns
- Call-patterns, typing speed

Biometric Authentication: Mixed

- A combination of physical characteristics and actions (ie. voice recognition)

Define Failure to Enroll (FTE)

- Users are unsuccessful in registering for the template (ie. some people have no fingerprints or hard-to-read fingerprints)

Define Failure to Capture (FTC)

- How often the system is unable to get a sufficient sample to proceed

Define False Acceptance Rate (FAR)

- Rate at which invalid signatures are accepted

Define False Rejection Rate (FRR)

- Rate at which valid signatures are rejected

Define Equal Error Rate (ERR)

The point at which FAR=FRR

- Not really used in practice, only really useful for simple point comparisons of protocols - system with lower ERR is better

Identification vs Authentication

Authentication: confirms the authenticity of a user's identity

Identification: determines the user's identity from a population

Factors for Evaluating Biometrics Modularity: Universality

- Do all users have this characteristic?

Factors for Evaluating Biometrics Modularity: Distinguishability

Do the characteristics differ enough across users to distinguish them

Factors for Evaluating Biometrics Modularity: Invariance

- Stability of the characteristics over time

Factors for Evaluating Biometrics Modularity: Ease of Sampling

How are easily are samples obtained and measured?

Password Managers

Instead of remembering many different passwords user remembers one master password

Password Wallets:

- Tool manages existing collection of passwords
- Automatically selects password
- Passwords are stored in wallet are individually encrypted under a password derived from the master password
- Poorly designed tools leave them in plaintext

Derived Passwords

- Application of site specific passwords are derived from master password plus other information such as the target domain

Types of graphical password generators:

- Pure recall
- Cued Recall
- Recognition

Shannon Entropy:

Given by the formula $H = -\sum_{i} p_i log_b p_i$

where p_i is the probability of the character i appearing in the stream of characters in the message