User Authentication and Identity Management

Authentication

RFC 4949 defines user authentication as follows:

- **Identification Step**: Presenting an identifier to the security system. (Identifiers should be assigned carefully, because authenticated identities are the basis for other security services, such as access control service.)

- **Verification Step**: Presenting or generating authentication information that corroborates the binding between the entity and the identifier.

User Identification

- I could have the user identifier tbakker.
- This information needs to be stored on any server or computer system that I wish to use and could be known to system administrators and other users.
- A typical item of authentication information associated with this user ID is a password, which is kept secret.
- If no one is able to obtain or guess my password, then the combination of my user ID and password enables administrators to set up Alice's access permissions and audit her activity.

User Identification

- Identification is the means by which a user provides a claimed identity to the system;
- User authentication is the means of establishing the validity of the claim.

User Identification

- Usernames - Most commonly used means of claiming an identity
- Certificates - Stored on the system or paired with a storage device or token
- Tokens - Physical devices which may generate a code or present a certificate
- SSH Keys - Cryptographic representations of identity that replace usernames and passwords
- Smartcards -Contactless or physical chip reader-capable. May generate key-pairs as well.

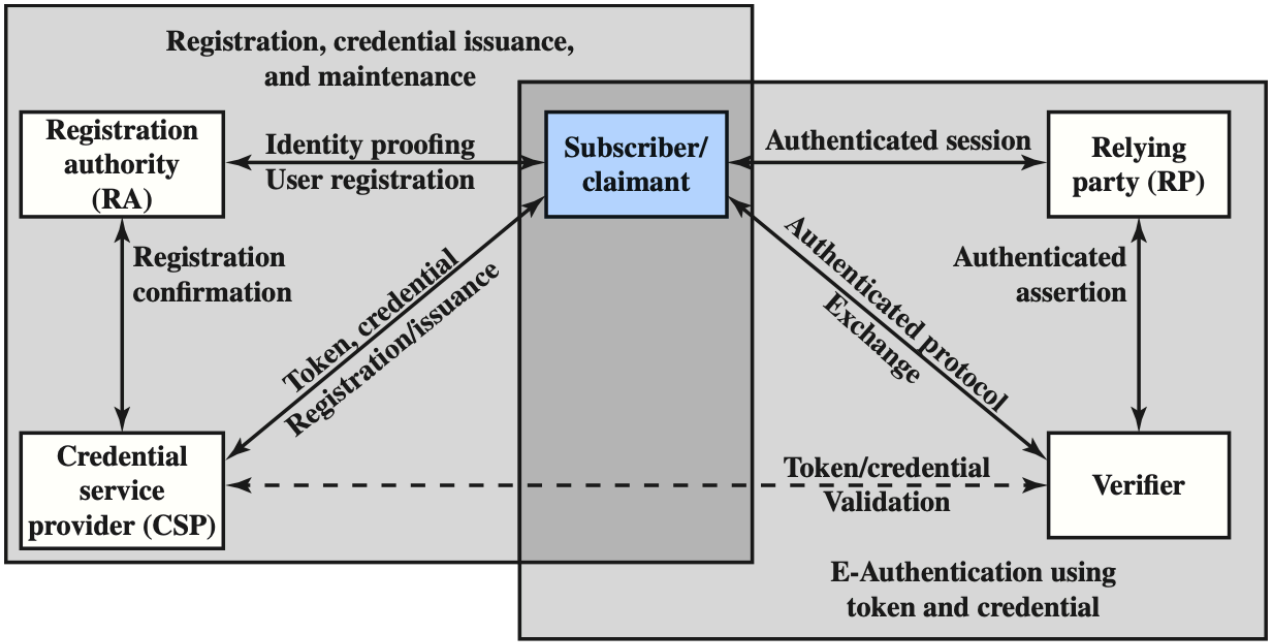
Electronic Authentication

- NIST SP 800-63-2 (Electronic Authentication Guideline, August 2013) defines electronic user authentication as the process of establishing confidence in user identities that are presented electronically to an information system

- Systems can use the authenticated identity to determine if the authenticated individual is authorized to perform particular functions

Electronic User Authentication

SP 800-63-2 defines a general model for user authentication that involves a number of entities and procedures.



Electronic User Authentication

Step 1: An applicant applies to a registration authority (RA) to become a subscriber of a credential service provider (CSP).

Step 2: The CSP then engages in an exchange with the subscriber.

Depending on the details of the overall authentication system, the CSP issues some sort of electronic credential to the subscriber.

The credential is a data structure that authoritatively binds an identity and additional attributes to a token possessed by a subscriber, and can be verified when presented to the verifier in an authentication transaction.

Electronic User Authentication

Step 3: Once a user is registered as a subscriber, the actual authentication process can take place between the subscriber and one or more systems that perform authentication and, subsequently, authorization.

The party to be authenticated is called a claimant and the party verifying that identity is called a verifier.

Electronic User Authentication

Step 4: When a claimant successfully demonstrates possession and control of a token to a verifier through an authentication protocol, the verifier can verify that the claimant is the subscriber named in the corresponding credential. The verifier passes on an assertion about the identity of the subscriber to the relying party (RP).

Authentication Methods

- Something You Have - A key, an ATM card, a Token
- Something You Know - A username, a password
- Something Your Are:
  - Something the individual is (static biometrics): fingerprints, retina patterns, veins in palm
  - Something the individual does (dynamic biometrics): voice pattern, handwriting characteristics, and typing rhythm, walking gait

Risk Assessment for User Authentication

- Assurance Level, Potential Impact, and Areas of Risk.

- An assurance level describes an organization's degree of certainty that a user has presented a credential that refers to his or her identity.

    1. 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.
  - A Reddit post
- Level 2: Some confidence in the asserted identity's validity.
  - At this level, some sort of secure authentication protocol needs to be used,

Four Levels of Assurance

- Level 3: High confidence in the asserted identity's validity. This level is appropriate to enable clients or employees to access restricted services of high value but not the highest value.
  - Multi-Factor Authentication
- Level 4: Very high confidence in the asserted identity's validity. This level is appropriate to enable clients or employees to access restricted services of very high value or for which improper access is very harmful
  - Multi-Factor Authentication and In-Person Registration

Potential Impact

- 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.

Areas of Risk

- Low: At worst, an insignificant or inconsequential unrecoverable financial loss to any party, or at worst, an insignificant or inconsequential organization liability.

- Moderate: At worst, a serious unrecoverable financial loss to any party, or a serious organization liability.

- High: severe or catastrophic unrecoverable financial loss to any party; or se- vere or catastrophic organization liability.

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

- The table indicates that if the potential impact is low, an assurance level of 1 is adequate.
- If the potential impact is moderate, an assurance level of 2 or 3 should be achieved.
- And if the potential impact is high, an assurance level of 4 should be implemented.

Password-Based Authentication

- Name or identifier (ID) and a password.
- The ID determines whether the user is authorized to gain access to a system.
- The ID determines the privileges accorded to the user.
- The ID is used in what is referred to as discretionary access control.

Vulnerability of Passwords

- Offline dictionary attack: Typically, strong access controls are used to protect the system's password file.
- An attacker obtains the system password file and compares the password hashes against hashes of commonly used passwords. If a match is found, the attacker can gain access by that ID/password combination.
- Countermeasures include controls to prevent unauthorized access to the password file, intrusion detection measures to identify a compromise, and rapid reissuance of passwords should the password file be compromised.

Vulnerability of Passwords

- Specific account attack: The attacker targets a specific account and submits password guesses until the correct password is discovered.
- The standard countermeasure is an account lockout mechanism, which locks out access to the account after a number of failed login attempts.

Vulnerability of Passwords

- Popular password attack: A variation of the preceding attack is to use a popular password and try it against a wide range of user IDs.
- A user's tendency is to choose a password that is easily remembered; this unfortunately makes the password easy to guess.
- Countermeasures include policies to inhibit the selection by users of common passwords and scanning the IP addresses of authentication requests and client cookies for submission patterns.

Vulnerability of Passwords

- Popular password attack: A variation of the preceding attack is to use a popular password and try it against a wide range of user IDs.
- A user's tendency is to choose a password that is easily remembered; this unfortunately makes the password easy to guess.
- Countermeasures include policies to inhibit the selection by users of common passwords and scanning the IP addresses of authentication requests and client cookies for submission patterns.

Passwords

- Passwords are problematic because of social factors.
  - Worst is the default. Many times never changed.
  - weak password - easily guessed
  - strong password - combination of upper and lower case, symbols, numbers

Passwords

- In 2006, a survey of 34,000 MySpace passwords revealed that the most common were "password1", "abc123", "myspace1", and "password"

Password Authentication from a Human Factors Perspective: Results of a Survey among End-Users by Peter Hoonakker, Nis Bornoe and Pascale Carayon

Vulnerability of Passwords

- Password guessing against single user: The attacker attempts to gain knowledge about the account holder and system password policies and uses that knowledge to guess the password.

- Countermeasures include training in and enforcement of password policies that make passwords difficult to guess. Such policies address the secrecy, minimum length of the password, character set, prohibition against using well-known user identifiers, and length of time before the password must be changed.

Worst Password Ideas

- Pet names
- A notable date, such as a wedding anniversary
- A family member's birthday
- Your child's name
- Another family member's name
- Your birthplace
- A favorite holiday
- Something related to your favorite sports team
- The name of a significant other
- The word "Password"

Vulnerability of Passwords

- Workstation hijacking: The attacker waits until a logged-in workstation is unattended.
- The standard countermeasure is automatically logging the workstation out after a period of inactivity. Intrusion detection schemes can be used to detect changes in user behavior.

Vulnerability of Passwords

- Exploiting user mistakes: If the system assigns a password, then the user is more likely to write it down because it is difficult to remember. This situation creates the potential for an adversary to read the written password.

- Countermeasures include user training, intrusion detection, and simpler passwords combined with another authentication mechanism.

Vulnerability of Passwords

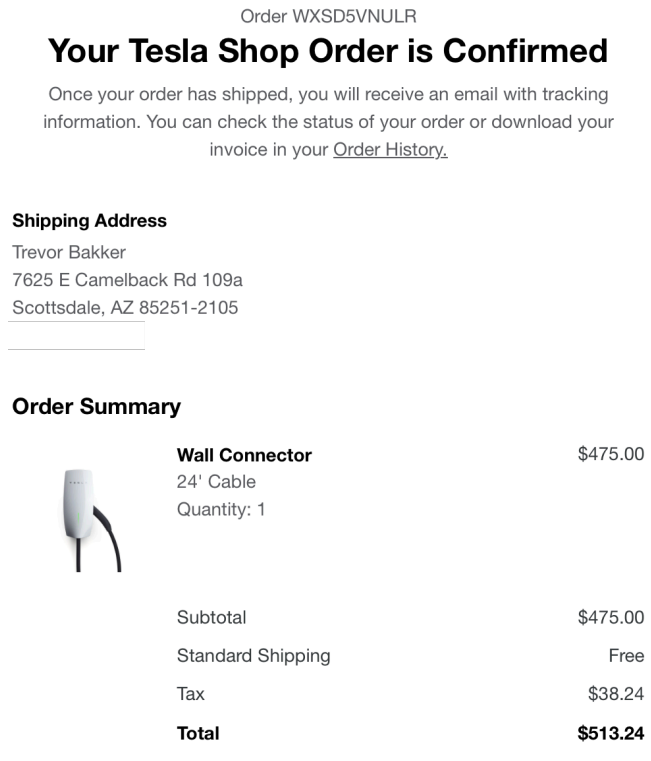
- The easier a password is for the owner to remember generally means it will be easier for an attacker to guess.
- However, passwords which are difficult to remember may also reduce the security of a system because
  - users might need to write down the password
  - users will need frequent password resets
  - users are more likely to re-use the same password.
  - Similarly, the more stringent requirements for password strength, e.g. "have a mix of uppercase and lowercase letters and digits" or "change it monthly", the greater the degree to which users will subvert the system.

Vulnerability of Passwords

- Exploiting multiple password use: Attacks can also become much more effective or damaging if different network devices share the same or a similar password for a given user.
- Countermeasures include a policy that forbids the same or similar password on particular network devices.

My Password Re-use cost me $1,026 (Temporarily)

- 8/14/23 - My personal email was Spam Bombed
- Over 2,000 email an hour in an attempt to hide two fraudulent purchases using my Tesla account
- Use Two-Factor and a Password Manager



Order WXSD5VNULR

Your Tesla Shop Order is Confirmed

Once your order has shipped, you will receive an email with tracking information. You can check the status of your order or download your invoice in your Order History.

Shipping Address

Trevor Bakker
7625 E Camelback Rd 109a
Scottsdale, AZ 85251-2105

Order Summary

	Wall Connector 24' Cable Quantity: 1	$475.00
	Subtotal	$475.00
	Standard Shipping	Free
	Tax	$38.24
	Total	**$513.24**

Vulnerability of Passwords

- Electronic monitoring: If a password is communicated across a network to log on to a remote system, it is vulnerable to eavesdropping.
- Simple encryption will not fix this problem, because the encrypted password is, in effect, the password and can be observed and reused by an adversary.

Vulnerability of Passwords

- Despite the many security vulnerabilities of passwords, they remain the most commonly used user authentication technique, and this is unlikely to change in the foreseeable future

Why Keep Using Passwords?

- Techniques the utilize client-side hardware, such as fingerprint scanners and smart card readers, require the implementation of the appropriate user authentication software to exploit this hardware on both the client and server systems.

- Physical tokens, such as smart cards, are expensive and/or inconvenient to carry around, especially if multiple tokens are needed.

Why Keep Using Passwords?

- Schemes that rely on a single sign-on to multiple services create a single point of security risk.

Okta Hacks

- Okta, Inc. is an American identity and access management company based in San Francisco.
- They provide Single Sign-On for 100 million registered users and 17,000 companies

Okta Hacks

- In early October 2023, Okta was notified of a breach resulting in hackers stealing HTTP access tokens from Okta's support platform by BeyondTrust.
- Okta denied the incident for a number of weeks, but later recognized that a breach had occurred.
- Customers impacted by the Okta breach included Caesars Entertainment, MGM Resorts International, 1Password and Cloudflare.
- On November 29th, 2023, it was known that the security incident affected all Okta customers

Okta Hacks

- Caesars paid out a ransom worth $15 million to a cybercrime group that managed to infiltrate and disrupt its systems.

- MGM, which owns more than two dozen hotel and casino locations around the world as well as an online sports betting arm, reported on September 11 that a “cybersecurity issue” was affecting some of its systems, which it shut down to “protect our systems and data.” For the next several days, reports said everything from hotel room digital keys to slot machines weren’t working.

Okta Hacks

- Cloudflare ailed to rotate one service token and three service accounts (out of thousands) of credentials that were leaked during the Okta compromise.
- On Thanksgiving Day, November 23, 2023, Cloudflare detected a threat actor on a self-hosted Atlassian server.
- From November 14 to 17, a threat actor did reconnaissance and then accessed the internal wiki (which uses Atlassian Confluence) and bug database (Atlassian Jira).

Okta Hacks

- Nov. 15th - The threat actor accessed Jira tickets about vulnerability management, secret rotation, MFA bypass, network access, and even response to the Okta incident itself.

- The wiki searches and pages accessed suggest the threat actor was interested in all aspects of access to the systems: password resets, remote access, configuration, the use of Salt

Okta Hacks

- Nov. 16 - The threat actor used the Smartsheet credential to create an Atlassian account that looked like a normal Cloudflare user. They added this user to a number of groups within Atlassian so that they'd have persistent access to the Atlassian environment should the Smartsheet service account be removed.

Okta Hacks

- Nov. 17 - During this period, the attacker took a break from accessing Cloudflare systems (apart from apparently briefly testing that they still had access) and returned just before Thanksgiving.

Okta Hacks

- Nov. 22nd — Since the Smartsheet service account had administrative access to Atlassian Jira, the threat actor was able to install the Sliver Adversary Emulation Framework, which is a widely used tool and framework that red teams and attackers use to enable “C2” (command and control), connectivity gaining persistent and stealthy access to a computer on which it is installed.

Okta Hacks

- Over the next day, the threat actor viewed 120 code repositories (out of a total of 11,904 repositories). Of the 120, the threat actor used the Atlassian Bitbucket git archive feature on 76 repositories to download them to the Atlassian server

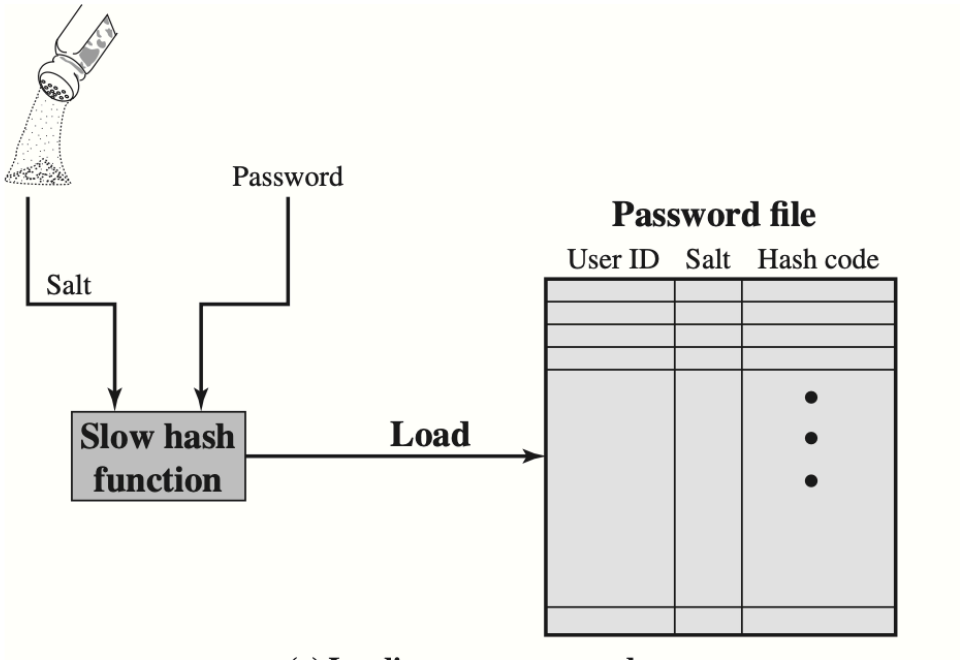
- Nov. 23 - Cloudflare security was notified of the threat actor's presence and began to shut down thae access.

Why Keep Using Passwords?

- Automated password managers that relieve users of the burden of knowing and entering passwords have poor support for roaming and synchronization across multiple client platforms, and their usability had not be adequately researched.

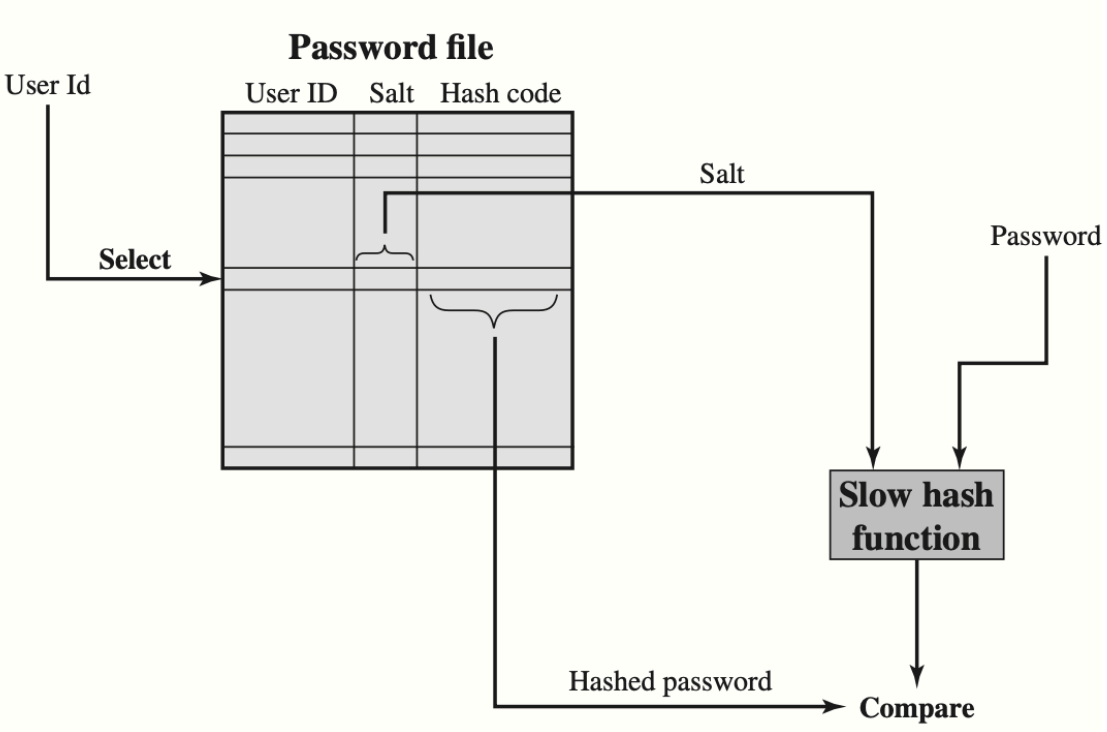
All Passwords Should be Salted

- Before hashing, a password is combined with a fixed-length salt value



All Passwords Should be Salted

- When a user attempts to log in the salt is added to the user password, hashed, and checked against the stored hashed value



Salting

- The salt serves three purposes:

1. It prevents duplicate passwords from being visible in the password file. Even if two users choose the same password, those passwords will be assigned different salt values. Hence, the hashed passwords of the two users will differ.

2. It greatly increases the difficulty of offline dictionary attacks. For a salt of length b bits, the number of possible passwords is increased by a factor of 2^b, increasing the difficulty of guessing a password in a dictionary attack.

3. It becomes nearly impossible to find out whether a person with passwords on two or more systems has used the same password on all of them.

Password Cracking

- The traditional approach to password guessing is to develop a large dictionary of possible passwords and to try each of these against the password file.

- This means that each password must be hashed using each available salt value and then compared with stored hash values. If no match is found, the cracking program tries variations on all the words in its dictionary of likely passwords.

SLOW

Rainbow Tables

- An alternative is to trade-off space for time by precomputing potential hash values.
- In this approach the attacker generates a large dictionary of possible passwords.
- For each password, the attacker generates the hash values associated with each possible salt value. The result is a mammoth table of hash values known as a rainbow table.

Rainbow Tables

- In 2003, Philippe Oechslin showed that using 1.4 GB of data, he could crack 99.9% of all alphanumeric Windows password hashes in 13.8 seconds. This approach can be countered using a sufficiently large salt value and a sufficiently large hash length.

https://iacr.org/archivecrypto2003/27290615/27290615.pdf

Password File

- One way to thwart a password attack is to deny the opponent access to the password file.
- Often, the hashed passwords are kept in a separate file from the user IDs, referred to as a shadow password file.
- A password protection policy must complement access control measures with techniques to force users to select passwords that are difficult to guess.

Password Selection

- When not constrained, many users choose a password that is too short or too easy to guess.
- At the other extreme, if users are assigned passwords consisting of randomly selected printable characters, password cracking is effectively impossible.
  - But it would be almost as impossible for most users to remember their passwords.

Password Selection

- Our goal, then, is to eliminate guessable passwords while allowing the user to select a password that is memorable.

Four basic techniques are in use:

1. User education
2. Computer-generated passwords
3. Reactive password checking
4. Complex password policy

These are not considered effective in the real world.

Password Selection

"Perhaps the best approach is the following advice: A good technique for choosing a password is to use the first letter of each word of a phrase. However, do not pick a well-known phrase like "An apple a day keeps the doctor away" (Aaadktda). Instead, pick something like "My dog's first name is Rex" (MdfniR) or "My sister Peg is 24 years old" (MsPi24yo).

Studies have shown that users can generally remember such passwords but that they are not susceptible to password guessing attacks based on commonly used passwords.

THE BOOK IS WRONG. Aaadktda will be in every rainbow table.

Password Selection

Computer-generated passwords also have problems.

If the passwords are quite random in nature, users will not be able to remember them. Even if the password is pronounceable, the user may have difficulty remembering it and so be tempted to write it down.

FIPS-181 defines one of the best-designed automated password generators.

The standard includes not only a description of the approach but also a complete listing of the C source code of the algorithm. T

The algorithm generates words by forming pronounceable syllables and concatenating them to form a word.

Password Selection

- A reactive password checking strategy is one in which the system periodically runs its own password cracker to find guessable passwords.
- The system cancels any passwords that are guessed and notifies the user.
- This tactic has a number of drawbacks.
  - It is resource intensive if the job is done right.
  - Passwords remain vulnerable until the reactive password checker finds them.

Password Selection

- Complex password policy, or proactive password checker. In this scheme, a user is allowed to select his or her own password.
- At the time of selection, the system checks to see if the password is allowable and, if not, rejects it.

Complex Password Rule Enforcement

- Bloom Filter - Filter based on rejecting words on a list.

I'm so furious at the textbook at this point I'm going to tell you what professionals believe about password policies.

Current Password Advice

- NIST 800-63
- https://pages.nist.gov/800-63-FAQ/

Token Based Authentication

- Objects that a user possesses for the purpose of user authentication are called tokens

Card Type	Defining Feature	Example
Embossed	Raised characters only, on front	Old credit card
Magnetic stripe	Magnetic bar on back, characters on front	Bank card
Memory	Electronic memory inside	Prepaid phone card
Smart Contact Contactless	Electronic memory and processor inside Electrical contacts exposed on surface Radio antenna embedded inside	Biometric ID card

Token Downsides

- Requires special reader: This increases the cost of using the token and creates the requirement to maintain the security of the reader's hardware and software.
- Token loss: A lost token temporarily prevents its owner from gaining system access. Thus there is an administrative cost in replacing the lost token. In addition, if the token is found, stolen, or forged, then an adversary now need only determine the PIN to gain unauthorized access.
- User dissatisfaction: Although users may have no difficulty in accepting the use of a memory card for ATM access, its use for computer access may be deemed inconvenient.

Biometric

- Facial characteristics: Facial characteristics are the most common means of human-to-human identification; thus it is natural to consider them for identification by computer.
- Fingerprints: Fingerprints have been used as a means of identification for centuries, and the process has been systematized and automated

Biometric

- Hand geometry: Hand geometry systems identify features of the hand, including shape, and lengths and widths of fingers.

- Retinal pattern: The pattern formed by veins beneath the retinal surface is unique and therefore suitable for identification.

Biometric

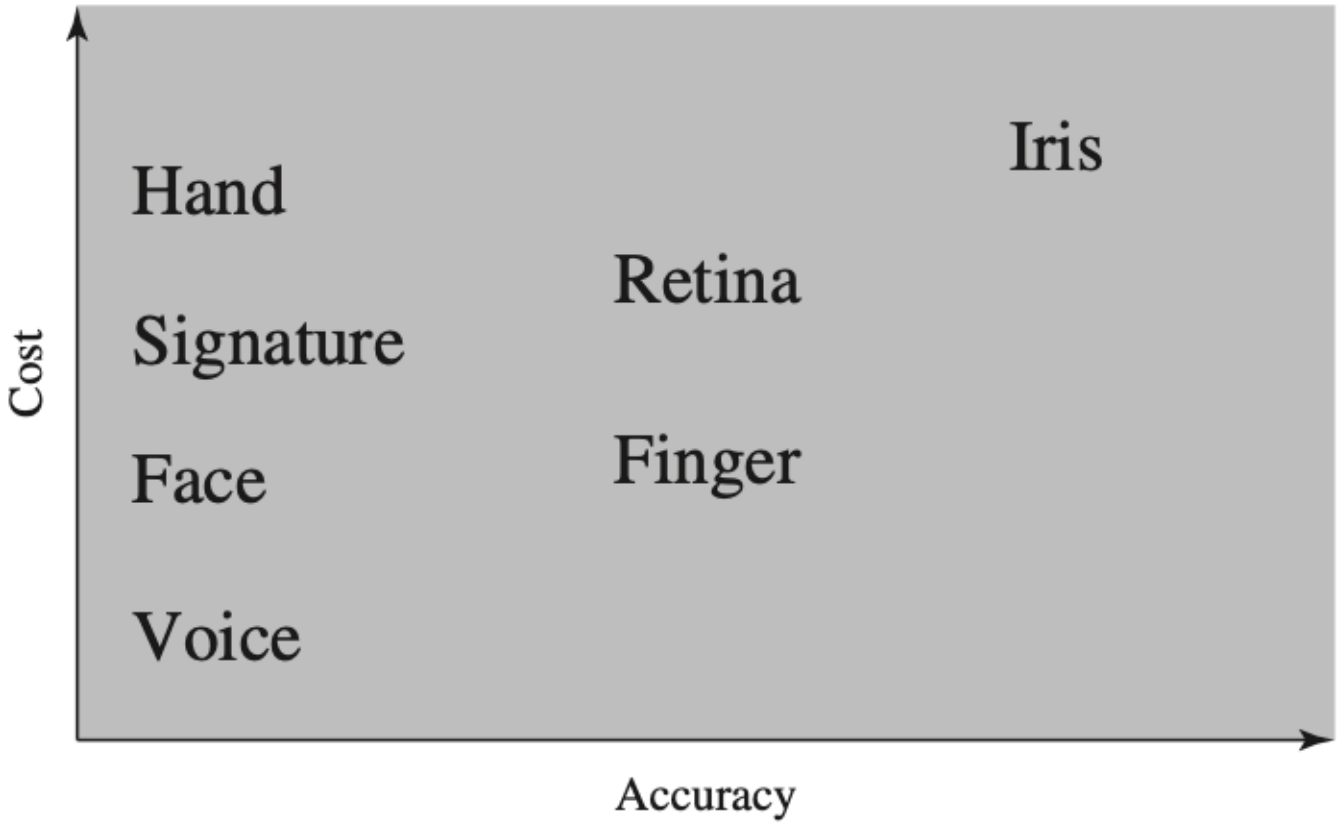
- Iris: Another unique physical characteristic is the detailed structure of the iris.

- Signature: Each individual has a unique style of handwriting and this is reflected especially in the signature, which is typically a frequently written sequence. However, multiple signature samples from a single individual will not be identical.

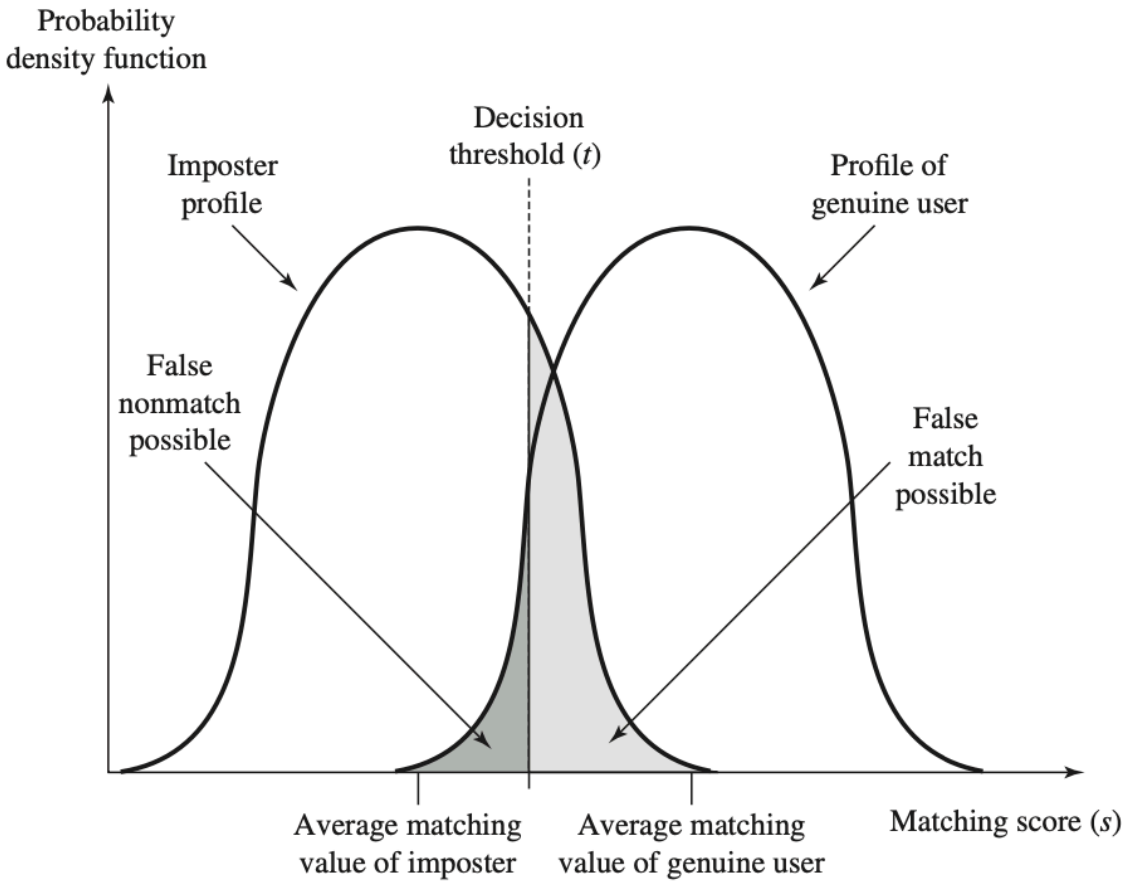
Biometric

- Voice: Voice patterns are more closely tied to the physical and anatomical characteristics of the speaker.

Biometric


Iris
Hand
Retina
Signature
Finger
Face
Voice
Cost
Accuracy

Biometric


Probability
density function
Decision
threshold (t)
Imposter
profile
Profile of
genuine user
False
nonmatch
possible
False
match
possible
Average matching
value of imposter
Average matching
value of genuine user
Matching score (s)

Attacks Against Authenticators

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
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