Though passwords are most widely used method of authentication, far from most reliable method.

Other methods of authentication also have problems.

Something the entity has also problematic if thing you have easily lost or taken away from user.

Biometric methods of authentication also have problems.

Solving password problems

If part of problem is users are required to choose and remember too many passwords to be able to cope with requirements one puts on them ,maybe can reduce burden of remembering with aid of technology.

Password rememberers ,password managers and keyrings and single sign on -different ideas

1) browser based password rememberers

When you type password into web interface, browser will notice field is password field and offer to remember it for you and also what system the password is for.

Then when you return to website browser can automatically insert password into field.

Weak strategy if anyone can ever access browser you use ,since they gain access to variety of services in your name.

If browser not programmed to handle password field well, possible password can be revealed.

A similar phenomenon is those who are running server side service offer to “remember you” once you have logged in.

Next time u return to website server will automatically authenticate you so you can avoid the password dialogue.

Normal method of doing this – plant a cookie with browser containing data service provider thinks is sufficient to identify you.

Not secure as it has been known for some sites to save your username and password in clear in a cookie to save you from retyping them.

Password managers and keyrings

Improvement on browser based password rememberers.

System wide password manager that can fill in remembered passwords over variety of applications.

These tools are designed to be cryptographically well protected, unlocked by a single password, or other authentication mechanism.

Private keys and certificates may also be kept by such a scheme.

If tool – well implemented, passwords decrypted kept in primary memory for shortest time to limit opportunities for malicious tool to search for sensitive data.

This tool often implemented to link to authentication method used to identify you to system, once logged in your system maybe extra vulnerable.

There are ways to limit the vulnerability, by invoking tools that time-out inactive sessions.

Cloud based password managers – now more common.

Adds extra level of convenience that entering a password in one device can allow password to be stored in cloud and then retrieved for any other device using the same service.

Single sign on

Example - Kerberos

Systems where there are no separate passwords to several different systems, but user authenticates to central authority who verifies authentication to other dependent services.

Single sign on puts great demands on security of single authentication that gives us right to access several different services.

Kerberos careful to never use term password, preferring passphrase.

Authentication formats for single sign on are often based on more complex authentication formats than just something the entity knows.

Federated ID’s

Similar in function to single sign on but identity maybe trusted across several organizations.

Ex – Bank ID

One time passwords

Using a password once, once used password invalidated.

Multi -factor authentication

uses 2 different forms of authentication to validate identity.

Ex- mechanism that asks for password , then asks user to enter sequence of numbers sent to smartphone.

What the entity knows and what the entity has

Widespread use of phones encouraged this. Many banks use it.

Challenge response

Single sign-on, these are systems where there are no separate passwords to several different systems, but the user authenticates to a central authority who then verifies your authentication to other dependent services. This means that services have to be specifically adapted to allow any one of these models of cooperative authentication.

Note how single sign-on puts great demands on the security of the single authentication that gives us the right to access several diverse services. To propose one small example - Kerberos documentation is careful to never use the term password, preferring pass phrase, thereby encouraging users not to create the same kinds of problems one commonly sees in passwords for this one, critical authentication.

Federated ID is similar in function to single sign-on but where the identity may be trusted across several organisations. Things can become complex here, for example when different organisations have different policies on what are sufficient factors to identify an entity, and yet hope to collaborate on the authentication.

A completely different take on securing passwords is one-time passwords. As the name implies, this involves using a password once, but once used that password is invalidated.

Biometrics – automated measurements of biological and behavioural features that identify a person.

Because biometrics are measurements of the characteristics of the individual, people are tempted to believe that attackers cannot pose as authorized users on systems that use biometrics. Several assumptions underlie this belief.

A close-up of a document

Description automatically generated

Multifactor authentication uses 2 different forms of authentication to validate identity.

Ex – Asks for a password (what the entity knows) and then asks to enter a sequence of digits sent to a smartphone (what the entity has).