Chapter 2

Identity and access management

horizontal line

# AAA

Authentication, authorization and accounting (tracking user activity through logs.)

Identification is claiming the identity, and authentication is proving the identity. Authorisation is providing access, and accounting is logging activity.

## Authentication factors

**Something you know**

Password, or PIN. Weakest form of authentication.

**Password complexity:** Strong passwords have uppercase, lowercase, number and special characters, and are at least 14 length.Keyspace is the combination of different characters, calculated by noOfPossibleCharsUsed^Length. E.g. 6 length password containing only lowercase = 26^6.

However, extra long passwords are less secure, since you are likely to forget them.

**Password expiration policy** forces users to regularly change passwords.

When **resetting passwords,** it is important to verify user identity. With manual password reset, it is better to use a temporary password that expires on first use.

**Group policy:** Used to manage multiple users and computers in a domain, and use Group policy object (**GPO**) to apply settings to all users.

Group policy is implemented on a domain controller within a domain. Can be used to create password policies, implement security changes such as firewall configuration.

**Password policy:** Policies such as length, amount of chars etc can be enforced using a technical control such as a technical password policy within a GPO.

If you set minimum password age to 1 day, and set password history to 24, it deters users from changing their password constantly (24 times) until they get their old password back.

**Account lock policy**: If user enters wrong password too many times, then they are locked out. Lockout threshold is max no of times an incorrect password can be entered, and lockout duration is length of time they are locked out for.

**Changing default passwords:** Changing default name and password of admin accounts is more secure.

**Something you have**

Something you can physically hold

**Smart card**: Embedded with **microchip** and **certificate(**holding user’s private key which is matched to public key on system via PKI - public key infrastructure**)**, which allows use for a complex encryption key. Provides Confidentiality, integrity, non repudiation and authentication.

**CAC**: Common access card. Includes picture of user and other readable info. Used by US DoD, to gain access to locations and login to computer systems.

**PIV**: Personal identity verification, used by federal agencies, and similar to CAC.

If they are used with PIN, it provides dual authentication (something you have and something you know). They include embedded certificates used with digital signatures and encryption.

**Token/key fob:** Electronic device with LCD displaying a number, which a server knows. It is a one time, rolling password. This is entered on a website to authenticate. Dual factor (something you have, something you know)

**HOTP/TOTP:** Hash-based message authentication code (HMAC) uses a hash key and crypto key, and is used to create HMAC-based OTPs (HOTP).

HOTP algorithm combines a secret key and a counter, and uses HMAC to create a hash, which is converted to HOPT.

HOPT remains active until it is used, so someone can shoulder surf and steal it.

TOPT: Time based one time password, uses a timestamp instead of a counter, and expire within 30 sec.

HOTP AND TOTP are open source and cheap!

**Something you are**

Uses biometrics to identify, and is the strongest form of authentication. User registers with system, and their info is linked to their identity.

**Biometric methods:**

1. **Fingerprint scanners**: Store fingerprints
2. **Retina scanner:** uses pattern of blood vessels at back of eye for recognition. They can identify medical issues, and you need to have physical contact with the scanner.
3. **Iris scanner:** Capture pattern of iris for recognition. Used in border control. Can take picture from up to 10 inches away, avoiding physical contact.
4. **Voice recognition:** Use speech recog to identify different acoustic features and patterns
5. **Facial recognition:** Identify people based on facial features. Can be affected by lighting. However, some systems use IR which can operate in diverse lights.

**Biometric errors:**

1. **False acceptance:** Incorrect identification of unauthorized user as authorised.
2. **False rejection:** Incorrectly rejects authorized user

CER: Crossover error rate is the point where FAR meets FRR. Lower CER indicates more accurate system.

**Something you do**

Actions you take, e.g. gestures on a screen such as drawing line pattern. Also includes behavioural biometrics, which is the typing pattern of an individual, such as speed, and dwell time which is the duration a key is pressed for.

**Somewhere you are**

Geolocation is most commonly used, using IP. However, this can easily be spoofed using a VPN.

For an organisation, MAC address of a system can be used for identification, so a user can only log in through one specific computer.

## Authentication services

**Kerberos**

Network authentication protocol within a microsoft windows active directory, providing mutual authentication to prevent man in the middle and replay attacks (attacker attempts to impersonate user after intercepting data). Here are the requirements needed for it to work properly:

1. **Method of issuing tickets for authentication:** key distribution centre (KDC) issues ticket granting tickets (TGT). KDC packages user credentials within a ticket, which authenticate users when they want to access a resource.
2. **Time synchronisation:** Requires all systems to be synchronised within 5 mins of each other, so it can timestamp tickets, ensuring they expire correctly. Prevents replay attacks; if attacker intercepts data, then timestamp limits time attacker can use a ticket for.
3. **Database of users:** Database of users

KDC issues a TGT, so when a user tries to access a resource, they are provided a ticket for that resource after they present the TGT.

## NTLM

New technology LAN manager is a suite of protocols providing authentication, integrity and confidentiality within windows, using a Message Digest algorithm to check credentials. It has 3 versions:

1. NTLM: MD4 hash of passwords (MD4 has been cracked)
2. NTLMv2: Creates HMAC MD5 hash, composed of user credentials and other details
3. NTLM2: Adds mutual authentication, where server also authenticates with client.

We should use Negotiate, which automatically selects the most secure protocol available.

## LDAP and LDAPS

Lightweight Directory Access Protocol specifies formats and methods to query directories, used by windows.

Active directory: Directory of objects and provides single location for object management. Queries to AD are in LDAP format.

LDAP Secure (LDAPS) uses encryption to protect LDAP transmissions. Client and server establish Transport Layer Security (TLS), which encrypts data.

## Single sign on

Only need to login once → more secure because user is less likely to forget credentials.

Creates a secure token for entire session, and the SSO system uses this token to authenticate.

If attacker gains credentials, attacker gets access to multiple resources.

Does not provide authorisation! Only authentication

## SSO and transitive trusts

Transitive trust creates indirect trust relationship. Domains use transitive trusts for SSO. Without transitive trust, multiple accounts are needed for authentication.

## SSO and SAML

Security assertion markup language (SAML) is an XML based data format for SSO. SAML is used as an identity management system if 2 systems trust each other. SAML defines 3 roles:

1. **Principle**: A user, requesting an identity from identity provider
2. **Identity provider**: Creates, maintains and manages identity
3. **Service provider**: Provides service to principles, by redirecting them to obtain an identity.

## SAML and authorisation

XML based standard used to exchange authentication and authorisation info between different parties. SAML provides SSO for web apps.

## SSO and federation

Federated database provides central authentication in a nonhomogenous environment, allowing authentication from different environments e.g. different os/networks.

**Shibboleth**: Open source and free, with open SAML libraries

## OAuth and openID Connect

**OAuth**: You can use the same account that has been created with google/fb etc, so you can do things like pay a website with paypal.

**OpenID Connect:** Works with OAuth 2.0, and allows verification without handling credentials.

**Managing accounts**

**Least privilege**

A technical control; specifies which resources a user can access to perform a specific function

**Need to know**

Users are granted access to info that is necessary to perform a function.

**Account types**

* End user accounts: Standard user accounts
* Privileged accounts: Additional rights over a standard user account
* Guest accounts: Grants limited access without creating a new account.
* Service accounts: When apps or services need to run under the context of an account. It is a regular account, but used by a service or app. They are not managed, so if the password expires then nothing can be done, as a user is not managing the account! One solution is to remove the password policy for that account.

**Admins using 2 accounts**

One regular account, and one privileged account. Regular account is better for everyday use because if it is compromised, privilege escalation attack is prevented.

**Standard naming convention is used for company accounts**

**Prohibiting shared and generic accounts**

If multiple users share a single account, you cannot implement basic authorisation controls.

**Disablement policies**

Disabling is preferred over deletion, because it retains encryption and security keys allowing files to be decrypted after disabling. Also ensures data associated with account remains available

Disabling is commonly used for:

* Terminated employee: So disgruntled ex employees can't do anything
* Leave of absence
* Delete account: Inactive for a long time

**Recovering accounts**

* To enable a disabled account: Reset a first time use password, and give control of the account to someone else
* Recover a deleted account: Detailed procedure followed for this!

**Time of day restrictions specify when a user can login**

**Location based policies**

“Somewhere you are”

**Whitelisting**: We can identify a set of IP address that are acceptable

We can also restrict access based on MAC addresses, so a user can only login from one computer.

**Expiring accounts and recertification**

Useful for temporary accounts, if a company has hired someone on a fixed term basis.

**Account maintenance**

Done with scripts to automate process. Useful for disabling or deleting accounts automatically, and checking statuses of accounts.

**Credential management**

Helps users manage multiple credentials, while preventing unauthorised access.

**Comparing access control models**

Ensure that only authorised users gain access to resources.

Subjects: Users that access objects

Objects: Items that subjects access. Access control determines how a system grants users access to these resources

**Role-based access control**

Uses roles to manage rights and permissions for users, useful for users in a department that perform same functions.

* Administrator role: Complete access and control on everything
* Executives: Can access data across all projects, but cannot modify
* Project managers: Full control over their own projects
* Team members: Have little access outside the scope of their assigned tasks

**Establishing access with group based privileges**

Roles are implemented as groups. This reduces the administrative workload of access management, because one rule is needed for one group with several members.

**Rule-based access control**

Rules can be used in routers and firewalls, which use rules within Access Control lists (ACLs). Rules can also be used within apps.

**Dynamic rules**: IPSs can detect attacks, then modify rules to block traffic from an attacker by modifying ACLs

**Discretionary access control - Owner and objects**

Every object has an owner, e.g. NTFS (new tech file system) used in windows, which allows users to restrict access to files with permissions

**SIDs and DACLs:**

* **SID:** Security identifiers, used to Identify users and groups with a long string of chars
* **DACLs**: Discretionary Access Control List identifies who can access what. It is a list of Access Control Entries (ACEs) which are composed of a SID and permissions.

DAC is more flexible than MAC, which has predefined privileges, and the admin is required to make changes.

**Trojans:** If a trojan is downloaded on an admin account, the trojan can run those privileges.

**Mandatory access control - Labels**

Uses labels of objects and users to identify access by matching them.

It is used by Security-enhanced Linux (SELinux)

**Labels and Lattice:** Levels of security to classify users and data are defined in a lattice.

Access in MAC is restricted to a need to know basis

**Establishing access:** Admin establishes access, but only someone higher up can define access for subjects and objects. The process of defining access is multilayered.

**Attribute-based access control - Attributes**

Grants access based on attributes, and used by SDNs. Can enforce DAC and MAC

They usually have 4 statements:

* Subject: A user, and you can use any attribute such as role, group membership etc
* Object: resource that the user is trying to access.
* Action: What the user is trying to do
* Environment: Context of the access request, inc time, protocols etc

Uses attributes defined in policies to grant access to resources, and used in SDNs.

**ACRONYMS**

AAA: Authentication, authorisation, accounting

GPO: Group policy object. Applies setting to all users in a domain

CAC: Common access card. Includes picture and other details on a card

PIV: Personal identity verification. Similar to CAC

HMAC: Hash-based message authentication code.

HTOP: HMAC based OTP. one time password remains active indefinitely

TOTP: Time based OTP. Expires within 30sec

CER: Crossover error rate. Used to measure accuracy of biometric ID system

KDC: Key distribution centre. Packages user credentials within a TGT.

TGT: Ticket granting ticket. Allows access to other resources

NTLM: New technology LAN manager. Suite of protocols providing authentication

LDAP/LDAPS: Lightweight Directory Access Protocol (Secure). Specifies formats to query directories

SSO: Single sign on

SAML: Security assertion markup language. XML based data format for SSO, used in ID management systems

ACL: Access Control list. Defines rules for firewall

NTFS: New technology file system. Allows users to restrict access to files

SID: Security Identifiers. Identify users with a long string of chars

DACLs: Discretionary Access Control List. Identifies who can access what