## Seven Categories of access controls

Divided by function or purpose

1. Preventative - prevent the potential for attack by restricting user activity, applying limits and restrictions
2. Deterrent - applying access controls can discourage incidents because users are forced into accountability via identification and authentication. Also A/C policies may specify potential punishment
3. Detective - access controls provide visibility into the environment. Logs can be kept of identification, authentication and authorization activities. Can be evidence gathering, or a real-time alert system.
4. Corrective - if a security event occurs, the access control mechanism can be used to enact corrective measures to reduce, avoid or eliminate the threat.
5. Recovery - after an event which affects access controls (such as system outage, attack, project changes, administrative gaps) access controls should be accurately reinstated and return to normal operational mode.
6. Compensating - when the existing capabilities of the system do not adequately enforce the security policy, further measures can be introduced. May be administrative, technical or physical in nature.
7. Directive – policies and procedures to guide good behaviour

## How Access Controls are implemented

* System access controls should be implemented to reduce the potential damage or loss of system data.
* **Administrative controls** consist of an organization's system security policy, supervision of users, and security-awareness training.
* **Logical controls**, also known as technical controls, restrict system access using techniques such as access control lists (ACL), encryption, and smart cards.
* **Physical controls** are restrictions to control system access, such as alarms, security guards, and locking doors to restrict access to system hosts and server rooms.

## Authentication

* Type 1 – something you know, password, pass phrase
* Type 2 – something you have, swipe card, token
* Type 3 – something you are, biometrics
* Example: ATM and PIN – ATM card is type 2,  
  PIN is type 1.
* remember: they are increasing order of strength

### Passwords

* insecure: human nature, transmission and storage, easily broken, inconvenient, refutable
* protective measures: length, complexity, aging, history, limited attempts (clipping level), lockout duration, limited time periods
* good practice: mixed case, replac3 le44er5 with num6er5, use first letters form a nonsense phrase or song
* “Stop! In the name of love!” = S!Itn0L
* Brute force attack: try all passwords
* Dictionary attack: strategically pick passwords to try

### Biometrics

Strongest to weakest

* palm scan, hand geometry
* iris scans – examine pattern on color portion of the eye
* retina scans – pattern of blood vessels in back of the retina
* fingerprint
* voice verification
* face scans
* signature dynamics
* keystroke patterns

**Zephyr chart** is used to compare biometrics based on cost, effort, intrusiveness, and distinctiveness

**Crossover Error Rate**

* FRR (Type 1) error: False Failure Rate
* FAR (Type 2) error: False Acceptance Rate
* CER: Crossover Error Rate
* the sensitivity level (eg 1.5%) where FFR = FAR
* type 1 has only 1 letter that is not an F: “R” (F**RR**)
* type 2 has 2 letters that are not an F: “A” and “R” (F**AR**)

## Types of Access Control Policies

* Centralized, one server is responsible for granting or denying access to all clients
* RADIUS – Remote Authentication Dial-in User Service, authenticates and authorized dial-up users (PPP and SLIP)
* TACACS – Terminal Access Controller Access Control System, client/server protocol mainly for authenticating remote users,
* TACACS+ includes two-factor user authentication, CISCO proprietary
* Diameter – more flexible, works with IPSEC if encryption is required
* Decentralized, access control decisions are left to those closer to the data and resources, usually the functional managers.

### Access Control Models

**Discretionary Access Control (DAC)**

* Access control decisions left to the owner of the object. For example, users have the ability to set sharing permissions for files and folders in their own accounts.
* Commonly uses Access Control Lists (ACL)

**Mandatory Access Control (MAC)**

* Operating system has final say about access.
* Based on security labels, and user’s security clearance

**Role Based Access Control (RBAC)**

* Also called non-discretionary access control
* Content dependent
* Context dependent

**Kerberos**

* 1. User logs into a Kerberos client using the KDC Authentication Service (AS).
  2. The KDC sends a ticket granting ticket (TGT) to the client.
  3. User sends a request access a Kerberos principal (e.g. a server) – request is sent to the TGS on the KDC.
  4. TGS generates a client/server session key, and a service ticket (ST). These are sent back to the client.
  5. Client sends the service ticket to Kerberos principal.
  6. Principal verifies the service ticket.

User can now use the requested service (principal)

### Other Single Sign on Mechanisms

* Kerberos is a symmetric (secret) key algorithm
* Krypto Knight – peer to peer authentication with KDC, symmetric key
* SESAME – secure European system for apps in a multi-vendor environment
* LDAP – Lightweight Directory Access Protocol, MS Active Directory, and other directory services

### Accountability

Audit logs

IDS – Intrusion Detection System

IPS – Intrusion Prevention System

### Network Denial of Service Attacks

* DoS: consume bandwidth to bring target network to a halt
* DDoS: distributed denial of service, uses many computers (Zombies) to target victim

**Syn Flood**

* TCP/IP uses a three-way handshake
* syn, syn/ack, ack
* problem is when resources are committed before handshake is complete

**Session Hijacking / Spoofing**

* Attacker changes the TCP packet so it appears to be from a trusted source

**Smurf DoS**

* ICMP flood attack
* spoof the broadcast of ping messages (that is, the ICMP echo command) sending the reply to the victim
* Fraggle DoS uses UDP packets in the same way.

**Teardrop DoS Attack**

* fragmented TCP/IP data (“teardrops”) with invalid length and fragmentation offset fields in IP headers of sequential packets
* target system gets confused

**Land DoS**

* Attacker sends a forged SYN request, with the server’s own address as the return address

## Intrusion detection systems

* A **signature-based intrusion detection system** uses accumulated knowledge to determine if an attack occurs. The accumulated knowledge is known as signatures. These signatures contain the different types of situations that could be considered as an attack. When an attack matches the information within a signature, the intrusion detection system will take the required actions to protect the network.
* **Network-based intrusion detection** systems are used to detect changes in activity on your network.
* **Host-based intrusion detection systems** are used to detect changes in activity on a host.
* The **Statistical anomaly-based intrusion detection** system learns as it performs its day-to-day tasks. It will determine the normal day-to-day activities, and if the values change drastically, it could mean that an intrusion is occurring.