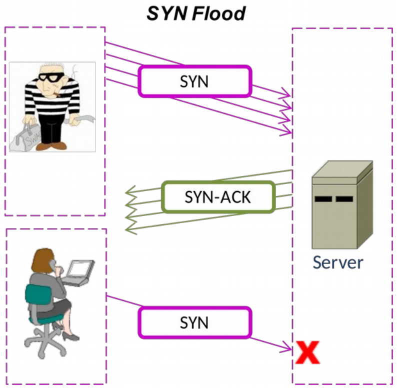
WE BUILD FOR THE FUTURE

Physical Security



CISSP®

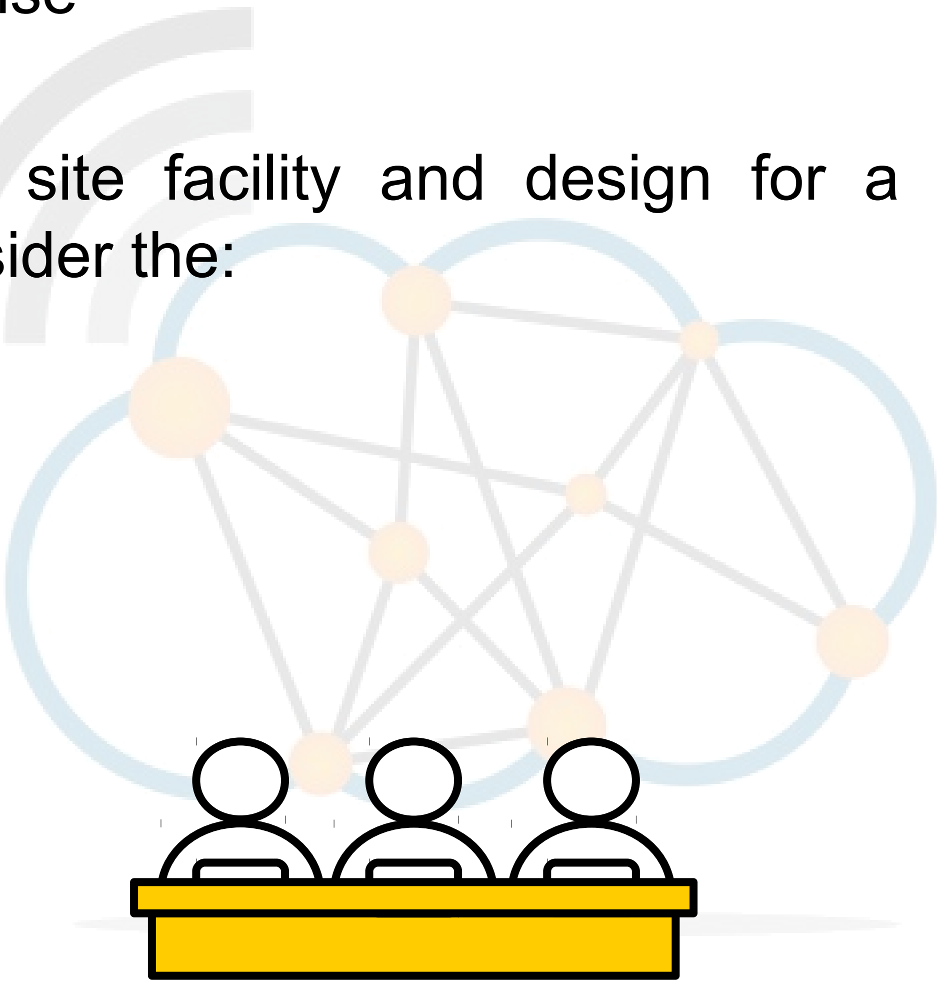
Diarmuid Ó Briain
CEng, FIEI, FIET, CISSP

diarmuid@obriain.com

Site facility and design

- Group exercise

- In terms of site facility and design for a small Data Centre, consider the:
  - Location
  - Threats



Site & Facility Design

- Location
  - Emergency Services
  - Hazards and threats
  - Adjacency to services
    - Power
    - Fibre
    - Height for radio
    - Water

- Threats
  - Fire
  - Water and flooding
  - Storms
  - Vandalism
  - Sabotage
  - Explosions
  - Building failure, collapse
  - Utility failure and continuity
  - Equipment failures
  - Access
  - Strikes

Secure Facility Plan

- Planning process:
  - What are we securing against?
  - What levels of security do we need and are we willing to provide?
- List of threats.
- Systematically relate the company applications with all the possible threats to it.
  - A Database Server will require, hardware, software, power, temperature control.
  - Critically analyse any dependencies for this server, what if the electricity goes down, what if the hardware overheats.

Physical Security Controls

- Physical Group
  - Walls
  - Fences
  - Gates
  - Locks
  - Lighting
  - Guards
  - Guard dogs

- Administrative Group
  - Site Management
  - Personnel Access Controls
  - Security Training
  - Procedures in the event of security breaches

- Technical Group
  - Intrusion detection systems
  - Alarms
  - CCTV
  - Fire detection
  - Fire Suppression

Server rooms

- Enclosed
- Restricted
- Protected rooms
- Mission critical equipment in controlled environment
  - Temperature
  - Humidity.
- Fire detection and extinguishing systems
  - Halon type oxygen displacement.

Work areas

- Designed to prevent shoulder surfing.
  - Shoulder surfing
    - Act of gathering info by watching a monitor and keyboard.
- The level of access an employee has should determine the work area they have.
- High level access employees work area not in proximity of level access employees.

Physical Access Controls - Fence

Physical Access Controls - Fence

- First line of defence.
- Fence guidelines;

– 1 metre	Deter casual trespassers
– 2 meters	Hard to climb easily
– 2.5 meters	Delay determined intruders

- Planning laws in locality.
  - May impact the type or look of the fence in plan.
- A grass or gravel clearway deter vehicles from parking.
- Bollards.

Physical Access Controls - Fence

- Access points
  - These points can be a weakness in the first layer of defence.
  - By their nature gates provide access through the fence and therefore should be afforded the appropriate management.

Intrusion detection devices

- Photoelectric beams
- Ultrasonic
- Passive infrared
- Microwave
- Pressure sensitive pads

- The use of intrusion detection systems can be mixed.
- Trigger audio or silent alarms or drown the area in light.
-
- Consideration; the triggering of alarms by non intruders i.e. animals and birds.

Light

- **Continuous Lighting**
  - Fixed lights should be installed 2.5 metres above ground.
  - Light on the ground should be at least 2 lumens.
- **Motion sensitive/trip lighting**
  - Sensor activated light can be both a good security deterrent and a cost effective alternative to continuous lighting.
- **Standby lighting**
  - Lights that come on in the event of power failure.
- **Exit lighting**
  - Lights to indicate the exit points.

Closed Circuit Television (CCTV)

CCTV equipment may be used to observe parts of a process from a central control room; when, for example, the environment is not suitable for humans.

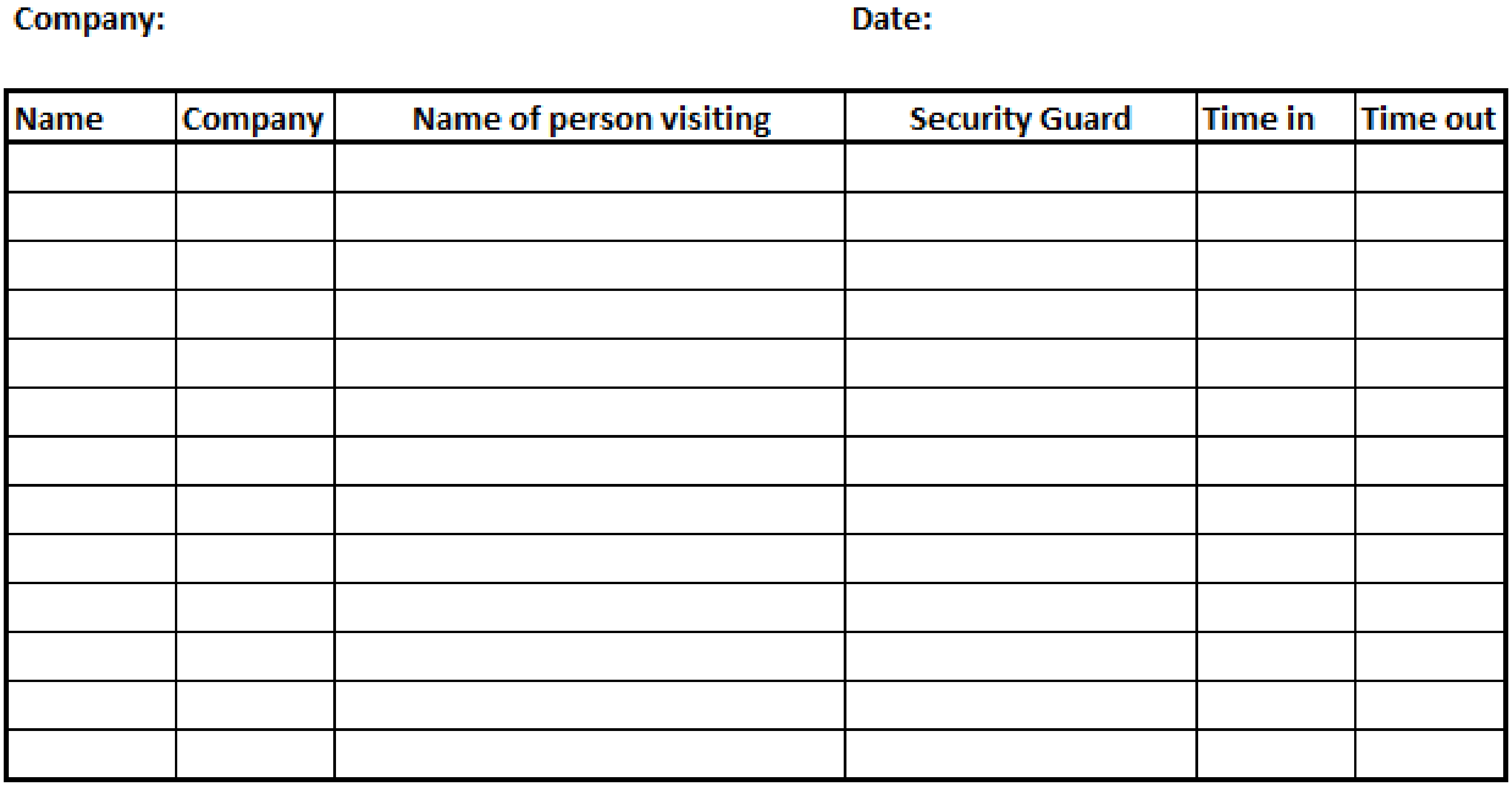
- Points to consider when installing CCTV systems:
  - The ability to **detect** an object.
  - The ability to **recognise** a detected object.
  - The ability to **identify** object details.

Security Guards

- A security guard:
  - Privately and formally employed person who is paid to protect property, assets, and people.
  - Is uniformed, overt and visible presence as a deterrent.
  - Practice the;
    - ***Detect***
    - ***Deter***
    - ***Observe***
    - ***Report***
  - Call on the civil police when necessary.
  - Perform access control at building entrances and vehicle gates.

Access Logs

- Maintained either in paper form though more commonly in electronic form to record the comings and goings of non employees.



Company: **Date:**

Name	Company	Name of person visiting	Security Guard	Time in	Time out

Perimeter Security - Doors

- Doors
  - Panels and glass protected against being kicked in or knocked out.
  - Install metal lining on exterior wooden doors to resist drilling or sawing.
  - Secure double doors with heavy duty, multiple-point, long flush bolts.
  - Make sure the frame is as strong as the door.
  - All exterior doors should be;
    - Constructed of steel, aluminium alloy, or solid-core hardwood
    - Minimum 1.5 mm steel on side and rear doors.
  - Door frames should be securely fixed to the walls.
  - Glass doors should have burglar-resistant glass installed.
  - Doors should be secured with a minimum of 3 hinges.
  - Doors should be clearly lit.
  - Emergency doors should be clearly marked.
  - Doors provide entry and exit for emergencies like power failure.
  - Doors should have the same fire rating as the walls.

Perimeter Security - Locks

- Exterior swinging doors should have a minimum 25 mm deadbolt lock, 25 mm throw bolt with a hardened insert, and free turning steel or brass tapered-cylinder guard.
- Steel strike plates should be used on aluminium door frames.
- Outside hinges should have non-removable hinge pins.
- Electronic/Electrical Locks connected to an access control system, advantages which include:
  - Key control, where keys can be added and removed without re-keying the lock cylinder.
  - Fine access control, where time and place are factors.
  - Transaction logging, where activity is recorded.

Electronic lock authentication methods

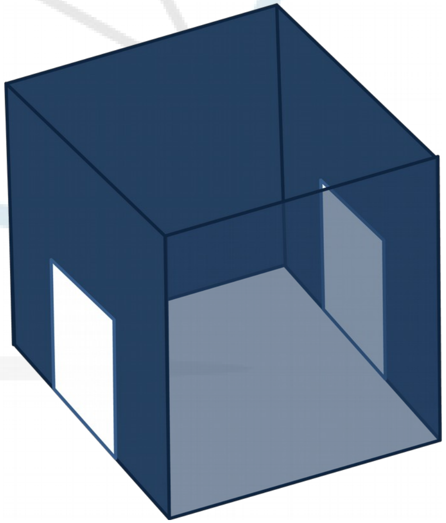
- Numerical codes, passwords and passphrases
- Security tokens
  - Cards.
- Biometrics
  - Fingerprint
  - Retinal scanning
  - Iris scanning
  - Voice print identification.

Padlocks

- The most common assaults on padlocks are made with bolt cutters or pry bars.
- Quality padlocks should have the following features:
  - Laminated or solid body case.
  - Hardened steel shackle with a minimum diameter of 8 mm.
  - A double locking mechanism providing "heel and toe" locking, and at least 5 pin tumblers in the cylinder.

Turnstiles (Baffle gate) or Man-trap

- Allows one person to pass at a time.
- Can enforce one-way traffic.
- Restrict passage to people with a security pass.
- Patrons to enter single-file, so security have a clear view.
- With mantraps when alarm, all doors lock
  - Suspect trapped between the doors in the "dead-space".



Windows

- **Windows**
  - Light, ventilation, and visibility, but not easy access.
  - **Locks**
    - Cannot be reached and opened by breaking the glass.
  - **First floor windows**
    - Protected with burglar-resistant glass, bars, grilles, grates.
  - **Plate Glass**
    - Most common type of glass found in windows. It tends to shatter in shards when broken or subject to an explosion, a safety hazard.
  - **Tempered Glass**
    - Processed by controlled thermal or chemical treatments to increase its strength compared with normal glass.
    - Does not shatter into shards when broken.
  - **Polycarbonate Glass**
    - Thermoplastic polymer moulded to look like glass and is the toughest glazing available.

Environment and Safety - Power

- Power problem terms:
  - **Fault** – This is a momentary loss of power
  - **Blackout** – Complete loss of power
  - **Sag** – Lowering of the power supply voltage
  - **Brownout** – Prolonged period of low voltage
  - **Spike** – Momentary increase in voltage
  - **Surge** – Prolonged period of high voltage
  - **Noise** – A continuous power fluctuation
  - **Transient** – A short period of noise
  - **Ground** – Electrical earth
  - **Clean** – Continuous non fluctuating power
  - **Inrush** – Surge of voltage given initially after a device is connected to a power source

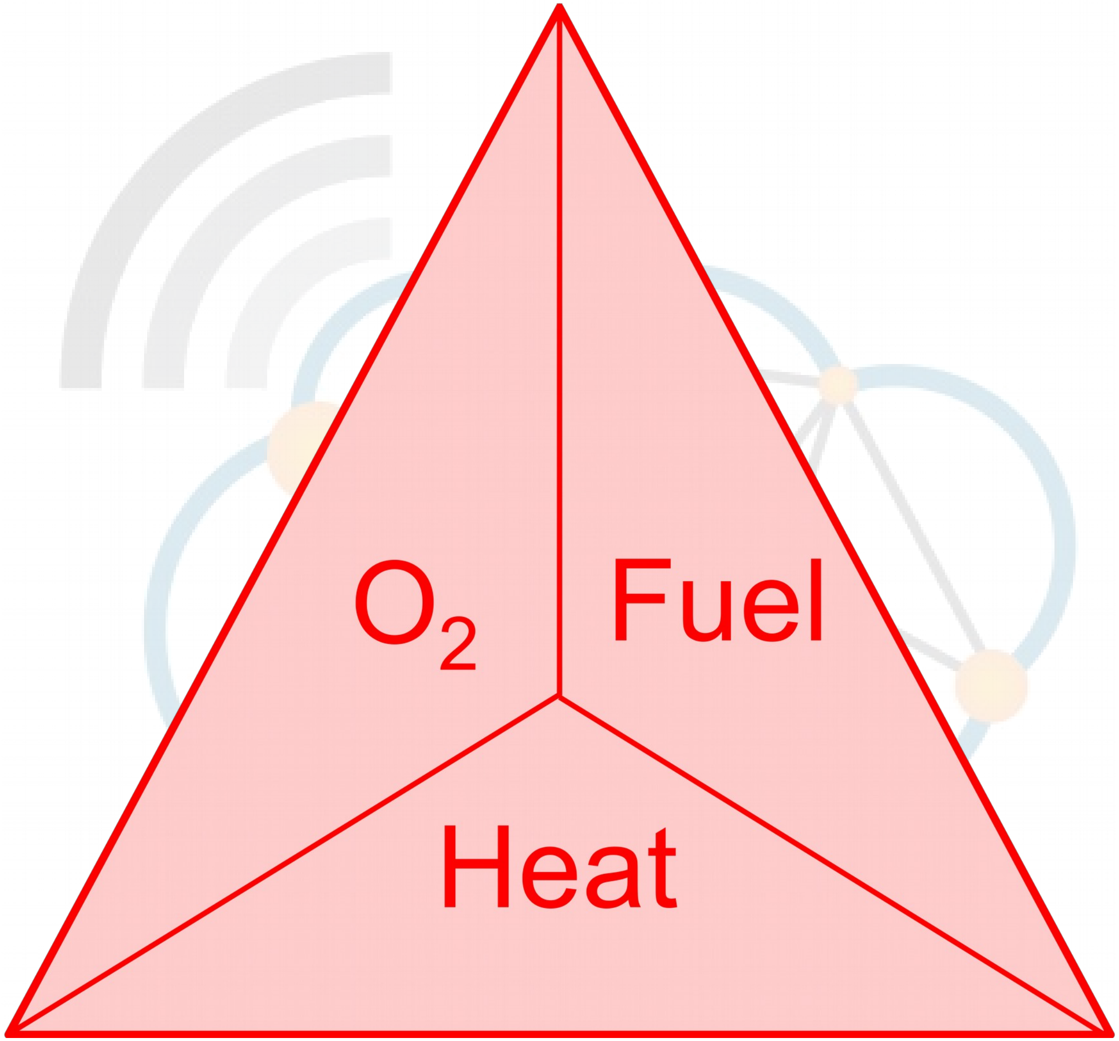
Uninterruptible Power Supply (UPS)

- Battery backup, emergency power source.
- Unlike generator provides instantaneous power.
- On-battery runtime can be relatively short 5 – 15 minutes being typical for smaller units
  - Sufficient to allow time to bring an auxiliary power source on line, or to properly shut down the protected equipment.

Water and Fire

- A fire develops typically in four stages, and fire detectors are designed to detect some characteristic effect of one or more of these stages:
  - **Incipient stage**
  - **Smouldering/smoke stage**
  - **Flame stage**
  - **Heat stage**

Water and Fire – Fire triangle



Fire management in data centres and labs

- Water ? electronic equipment ?
- Halon 1301 Gas was used in such environments.
  - Damage the ozone layer.
- The Montreal Protocol of 1987, limited the production of Halon 1301 to roles like aircraft emergency equipment where another alternative did not exist.
- Halon 1301 replaced
  - Argon
  - Inergen.

Fire management in data centres and labs

- **Halocarbon gases**
  - Remove heat from the fire.
  - Evacuation necessary before the release of these agents.
  - Lower storage space requirement compared to inert gasses.
  - Fast fire suppression time (10 sec).
  - Must be very near point of use (max 30M).
  - More expensive than inert gasses.
- **Inert gases**
  - Lower the oxygen concentration in the room.
  - Perform more effectively in rooms that aren’t well sealed.
  - More gas required than Halocarbon gasses.
  - These can be piped long distances (100 – 200M) to a room and still retain their effectiveness.

Pre-action sprinklers

- Pre-action sprinkler systems also are an option.
- Water no retained in pipes which reduces the risk of leaks:
  - Valve located outside keeps water from entering
  - Smoke detector triggers and temperature threshold must be reached before water flows
  - Two trigger events reduces risk of an accidental leak.

Water threat

- Water damage is a threat in itself.
  - Information systems
  - Paper records.
- Water detection sensors that can trigger an alarm.
- Raised floors to allow time for a water threat to be reacted to are common
  - though these are also used for conduits to carry room power and network cabling.
- Water threats are another reason to place such rooms above ground level.

Heating, Ventilating, and Air Conditioning

- Temperature and humidity control.
- Positive Pressure:
  - Ensures that should there be any leakage it will be out and thus prevent any unwanted air in
  - Monitoring of air pressure by alarm system
  - Should the pressure change suddenly it is an indication of the possibility of unauthorised access.

Access Control

Diarmuid Ó Briain
CEng, FIEI, FIET, CISSP

diarmuid@obriain.com

Access Controls

- Group exercise

- Discuss these access controls

Group 1

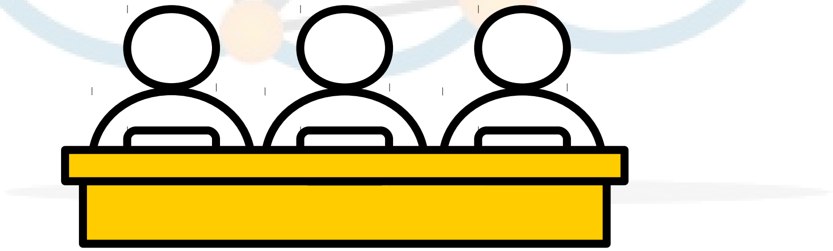
- Preventive
- Deterrent
- Detective

Group 2

- Corrective
- Recovery
- Compensation
- Directive

Group 3

- Administrative
- Logical / technical
- Physical



Access Controls

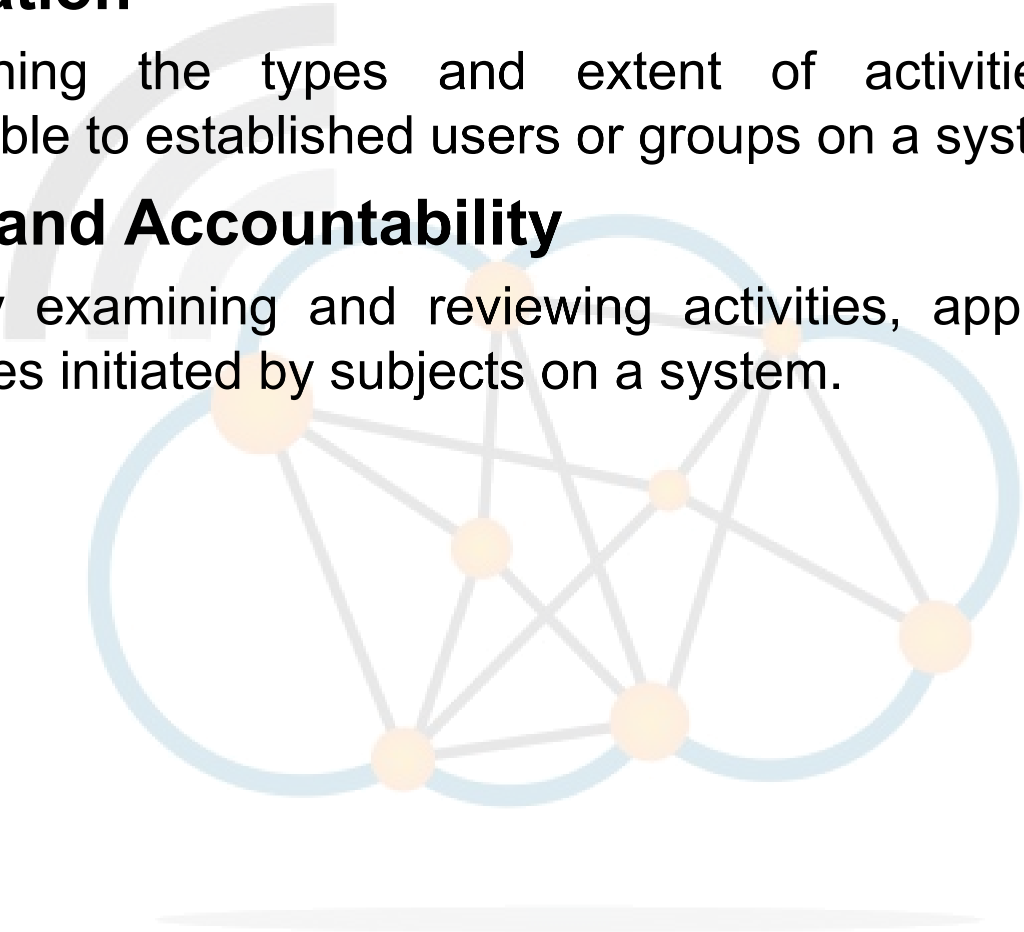
- **Preventive**
  - Stop unwanted or unauthorised activity from occurring.
- **Deterrent**
  - Discourages the violation of security policies.
- **Detective**
  - Discovers unwanted or unauthorised activity.
- **Corrective**
  - Restore systems to a known-good state.
- **Recovery**
  - Repair and restore critically damaged capabilities, functions and resources.
- **Compensation**
  - Operational requirements, utilisation criteria, personnel supervision, monitoring and work procedures.
- **Directive**
  - Confines and controls the actions of subjects.
- **Administrative**
  - Policies and procedures.
- **Logical** or **technical**
  - Hardware and software mechanisms.
- **Physical**
  - Structural barriers.

Access Control in a Layered Environment

- **Layered / Defence in depth**
  - The use of several forms of access control.
- **Identification**
  - Subject authentic, accredited and held accountable.
- **Authentication**
  - This is the process of verifying that a given identity is valid.
    - Type 1 – “Something you know”, i.e. Password
    - Type 2 – “Something you have”, i.e. Token
    - Type 3 – “Something you are”, i.e. Biometric
    - “Something you do”
    - “Somewhere you are”
    - Multi-factor Authentication.

Access Control in a Layered Environment

- **Authorisation**
  - Determining the types and extent of activities that are permissible to established users or groups on a system.
- **Auditing and Accountability**
  - Formally examining and reviewing activities, applications and processes initiated by subjects on a system.



Identification and Authentication techniques

- **Identification**
  - Subject must provide an identity to a system to start the Authentication, Authorisation and Accountability process.
  - The Identity correlates an authentication factor with a subject:
    - Typing a username
    - Swiping a Smart Card
    - Waving a Token Device
    - Speaking a Phrase
    - Positioning Face, Hand or Finger for camera/scanner.
- **Authentication**
  - Authentication verifies the Identity of a Subject, thus Identification and Authentication are always a two step process, one useless without the other.

Passwords

- Poor security mechanism for the following reasons:
  - Users typically use passwords they can easily remember
  - Random generated passwords are difficult to remember so the Subject tends to write them down
  - Passwords are easily shared, written down, forgotten
  - Passwords are easily stolen through observation, recording, playback, social engineering and security database theft
  - Passwords often transmitted in clear or shrouded in simple to break encryption
  - Short passwords can be discovered quickly by brute force attacks.

Password selection

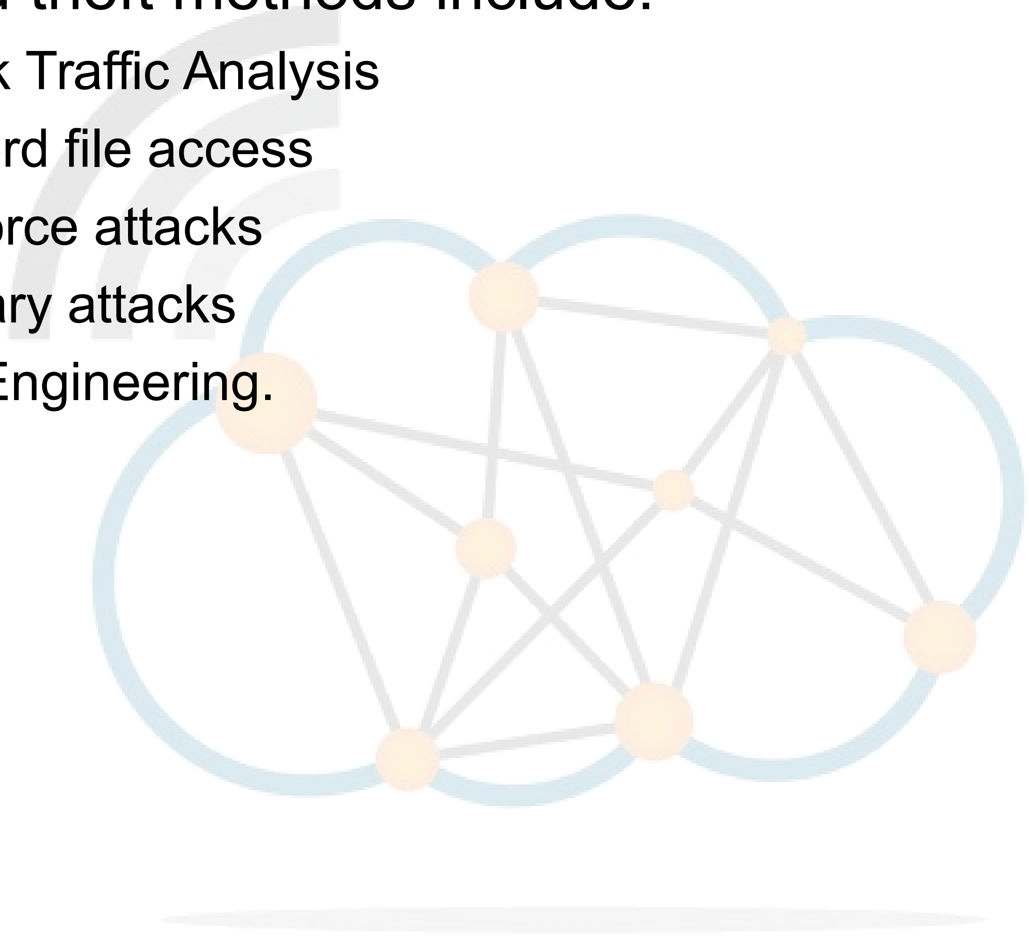
- Passwords are broken into two groups:
  - Static
    - Always remain the same
  - Dynamic
    - One-time passwords, single-use passwords
    - Cognitive password
    - What is your date of birth?
    - What is your first pet’s name?
    - What is your mother’s maiden name?

Password policies

- Password policies should at a minimum force:
  - Change the password regularly, minimum and maximum age
  - Password characters should be dictated by the object during creation.
    - Not all letters
    - No number or letter sequences
    - Does not contain the Identification name
    - Minimum length
    - Mix of letters and numbers, upper and lower case
    - No password reuse.

Password security

- Password theft methods include:
  - Network Traffic Analysis
  - Password file access
  - Brute-force attacks
  - Dictionary attacks
  - Social Engineering.



Biometrics

- Uniquely recognising humans based upon one or more intrinsic physical or behavioural traits.
  - Fingerprints.
  - Face scans.
  - Iris Scans
    - Coloured area around pupil.
  - Retina scans
    - Pattern of blood vessels in back of eye
    - Most unacceptable by subjects as it can determine medical conditions (pregnancy, blood pressure) and it also blows air into the subjects eye.
  - Palm scans (Palm Topography).
  - Hand geometry.
  - Signature dynamics
    - Recognition of how a subject signs a set of characters.
  - Keystroke patterns (keystroke dynamics)
    - Flight time
    - Dwell time.

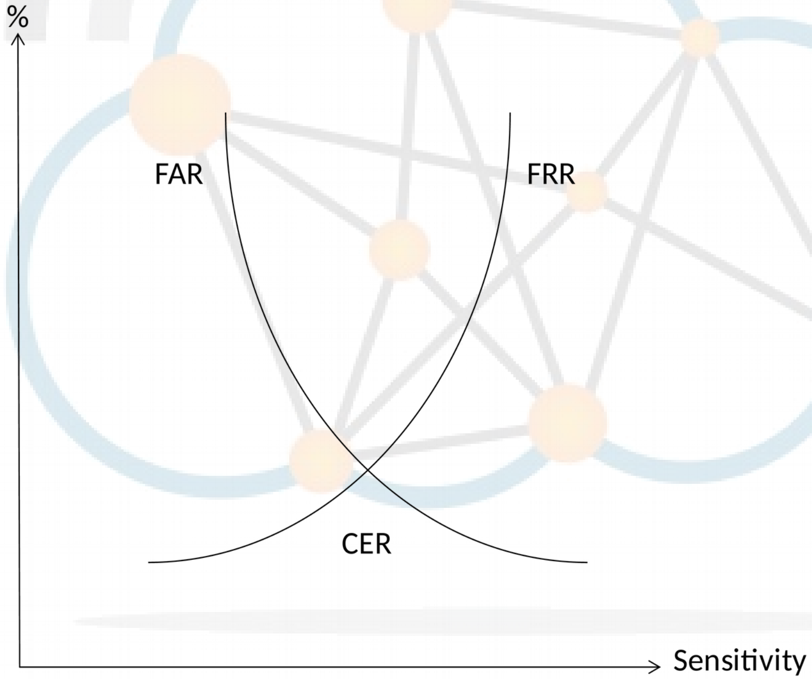
Biometric factor ratings

Errors can occur with biometrics and are categorised as follows:

- **Type 1**
  - Valid subject is not authenticated
  - False Rejection Rate (FRR)
    - Percent of valid inputs which are incorrectly rejected.
- **Type 2**
  - Invalid subject authenticated
  - False Acceptance Rate (FAR)
    - Percent of invalid inputs which are incorrectly accepted.

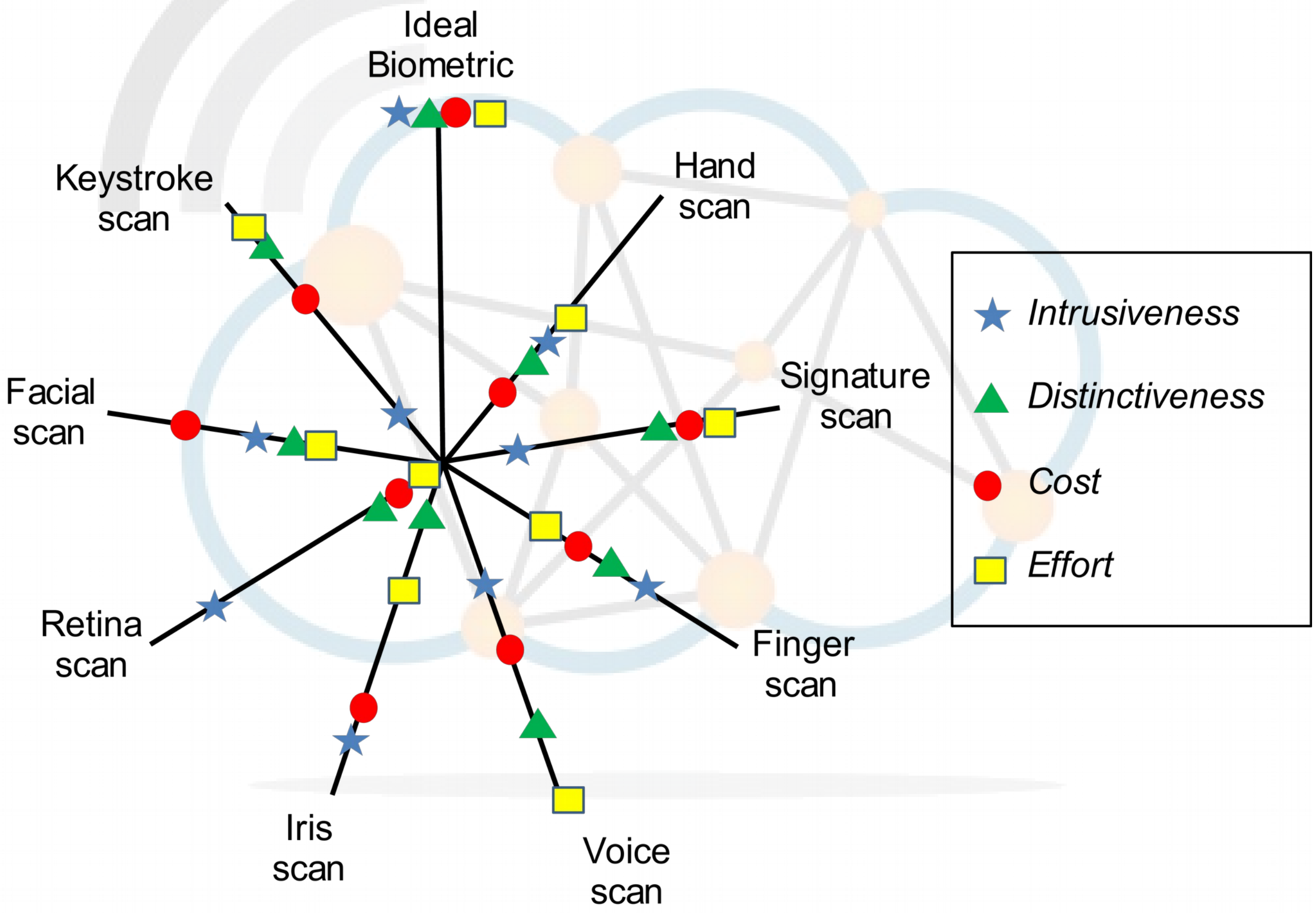
Biometric factor ratings

- Crossover Error Rate (CER) is point of intersection between FRR and FAR.
- The lower the CER rate the more accurate is the system.



Biometric usage, acceptance & cost

- Zephyr analysis chart shows the relation between ideal biometrics and most popular biometric technologies.



Tokens

There are four types of token:

- **Static** Tokens
  - Swipe card, disk, USB RAM Key or a physical key.
- **Synchronous dynamic** password tokens
  - Device that generates new passwords at fixed time intervals.
  - Subject enters generated password with PIN and passphrase/password.
- **Asynchronous dynamic** password tokens
  - Device that generates new passwords on the occurrence of an event
  - Press a key on the token and the server for example, advances next password
  - Subject enters generated password with PIN and passphrase/password.
- **Challenge-response** tokens
  - Passwords are generated by the token in response to instructions from the object.

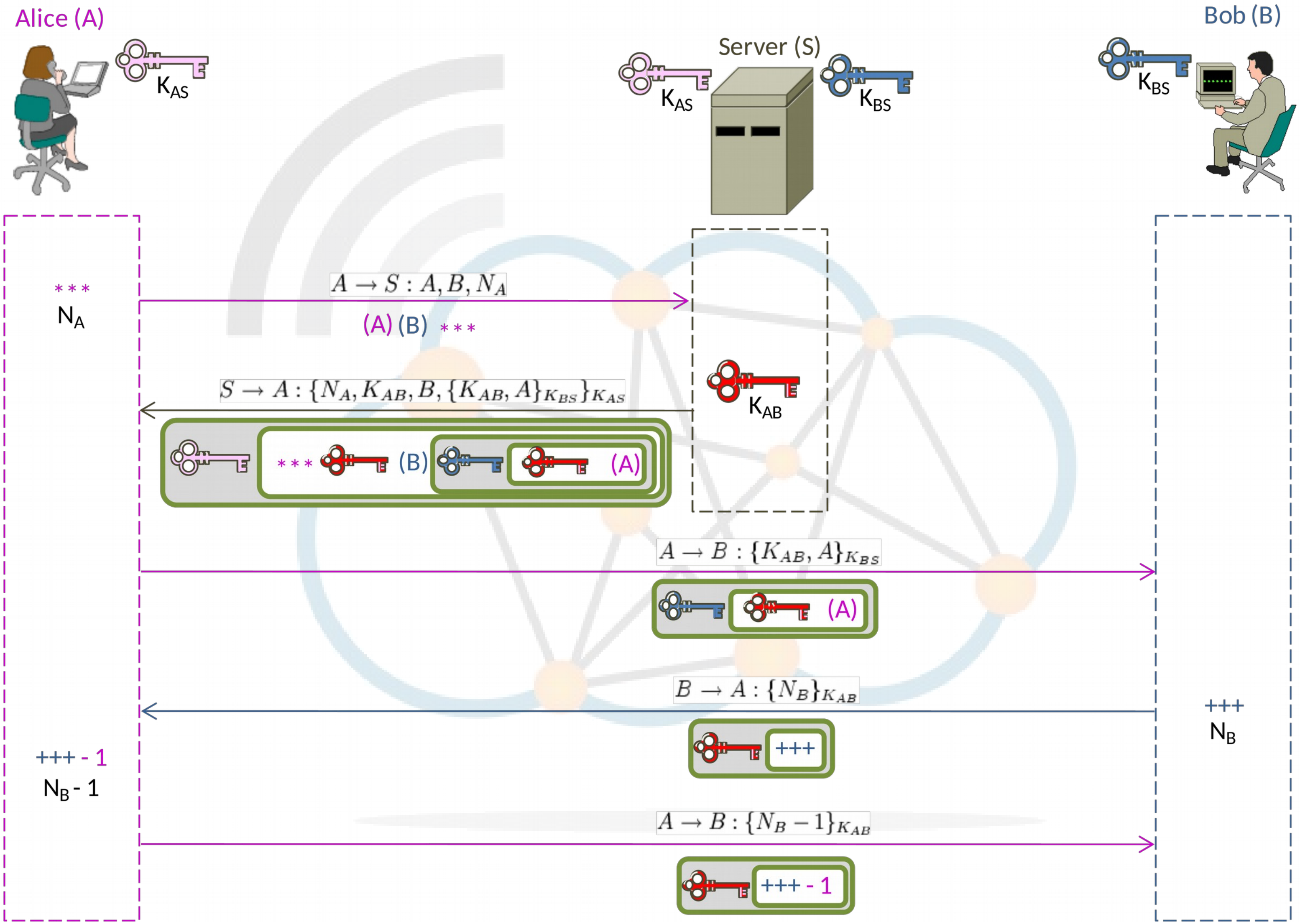
Tickets

Single Sign On (SSO), this means is a mechanism where multiple applications use one place to authenticate.

A very common example of this will be Google, a single login permits access to Gmail, Google Calendar and other Google applications.

Google uses Security Assertion Markup Language (SAML) Single Sign-On (SSO) service.

Needham-Schroeder Symmetric Key Protocol



$A \rightarrow S : A, B, N_A$

$S \rightarrow A : \{N_A, K_{AB}, B, \{K_{AB}, A\}_{K_{BS}}\}_{K_{AS}}$

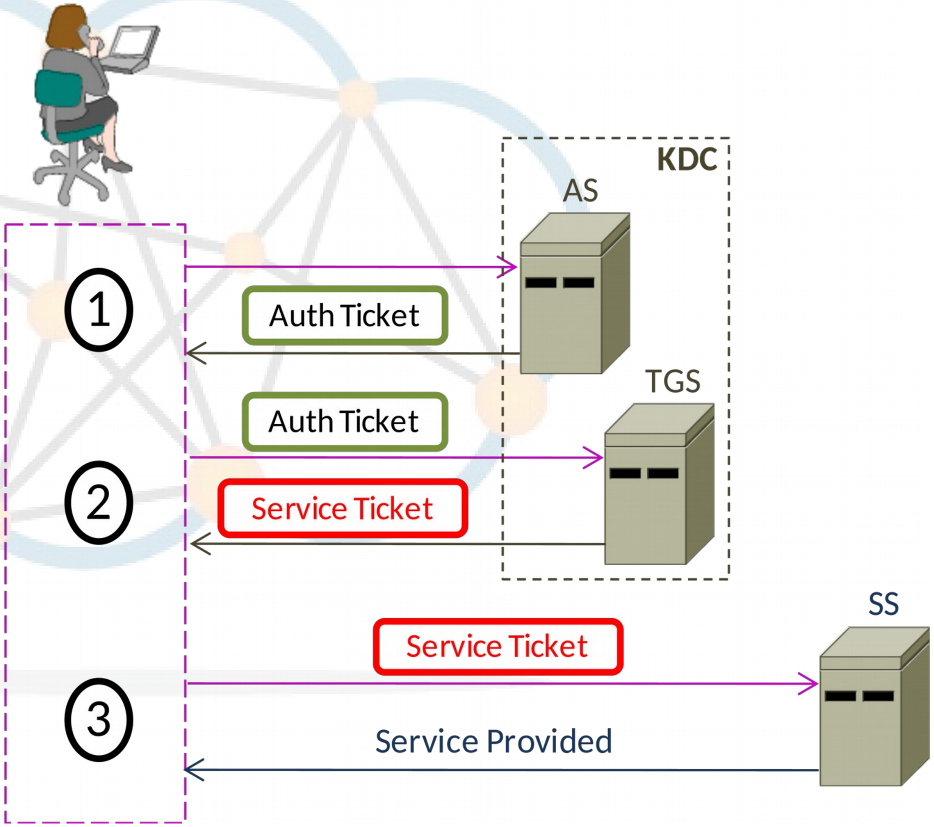
$A \rightarrow B : \{K_{AB}, A\}_{K_{BS}}$

$B \rightarrow A : \{N_B\}_{K_{AB}}$

$A \rightarrow B : \{N_B - 1\}_{K_{AB}}$

Kerberos

- Kerberos is a computer network authentication protocol, which allows nodes communicating over a non-secure network to prove their identity to one another in a secure manner.



Authentication Server (AS)
Ticket Granting Server (TGS)
Service Server (SS)

Access Control Techniques

- Discretionary Access Controls (DAC)
- Mandatory Access Controls (MAC)
- Role-based Access Control (RBAC)
  - Permissions to perform certain operations are assigned to specific roles
  - RBAC is attractive to organisations with a high rate of turnover.
- Lattice-based Access Control (LBAC)
  - Complex access control based on the interaction between any combination of objects (such as resources, computers, and applications) and subjects
  - Subjects are only allowed to access an object if the security level of the subject is greater than or equal to that of the object.

Centralised Access Control

- Advantages
  - Managed by small team or individual
  - Administrative overhead is low
  - Single changes impact the complete system.
- Disadvantages
  - Single point of failure
  - If elements cannot access centralised access control system then subjects cannot access objects.

Centralised Access Control - RADIUS

- Remote Access Dial-in User Service (RADIUS)
  - Centralised Authentication, Authorisation, and Accounting (AAA) management for computers to connect and use a network service
  - Developed by Livingston Enterprises, Inc., in 1991 as an AAA protocol and later became IETF standard
  - Client/server protocol that runs in the application layer, using UDP as transport
  - RADIUS serves three functions:
    - Authenticate users or devices before granting them access to a network
    - Authorise users or devices for certain network services
    - Account for usage of services.
- Diameter
  - Successor to RADIUS however a lot of the features of Diameter have been included in upgrades of RADIUS
  - Uses Reliable transport protocols TCP or SCTP instead of UDP.

Centralised Access Control - TACACS

- Terminal Access Controller Access Control System (TACACS)
  - Remote authentication protocol that is used to communicate with an authentication server commonly used in UNIX networks
  - Uses TCP for transport.
- TACACS+
  - TACACS+ is based on TACACS, but, in spite of its name, it is an entirely new protocol which is incompatible with any previous version of TACACS
  - Whereas RADIUS combines authentication and authorisation in a user profile, TACACS+ separates the two operations.

De-centralised Access Control

- Advantages
  - No single point of failure.
- Disadvantages
  - Large administrative overhead
  - Maintaining homogeneity becomes difficult.
- A domain is a realm of trust created were a collection of subjects and objects share a common security policy.
- Between these domains a security bridge called a trust can be established to allow subjects in one to access objects in the other.

Access Control Administration

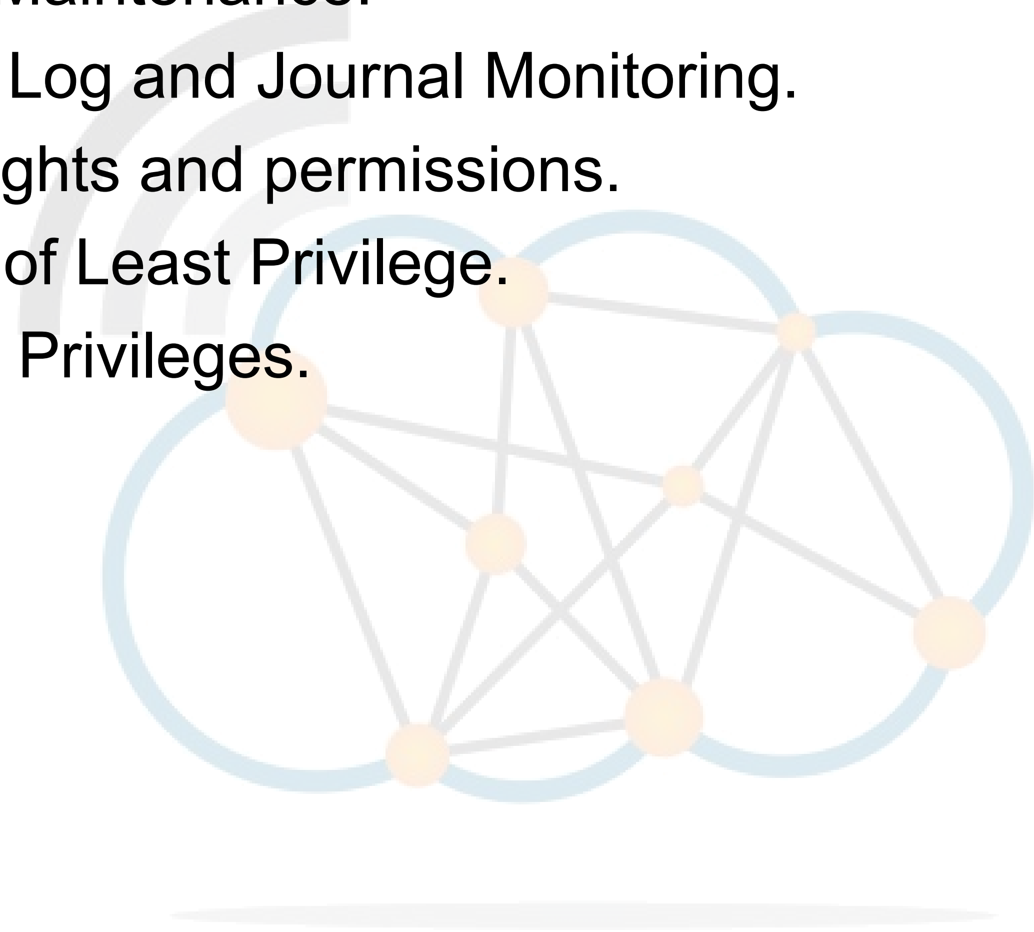
- Responsibilities
  - User Account Management.
  - Activity Tracking.
  - Access rights and permission management.
- User Accounts
  - **User** (Subject)
  - **Owner**
    - Responsibility for classification and labelling an Object.
  - **Custodian**
    - Responsibility of properly storing and protecting Objects.

Access Control Administration - Enrolment

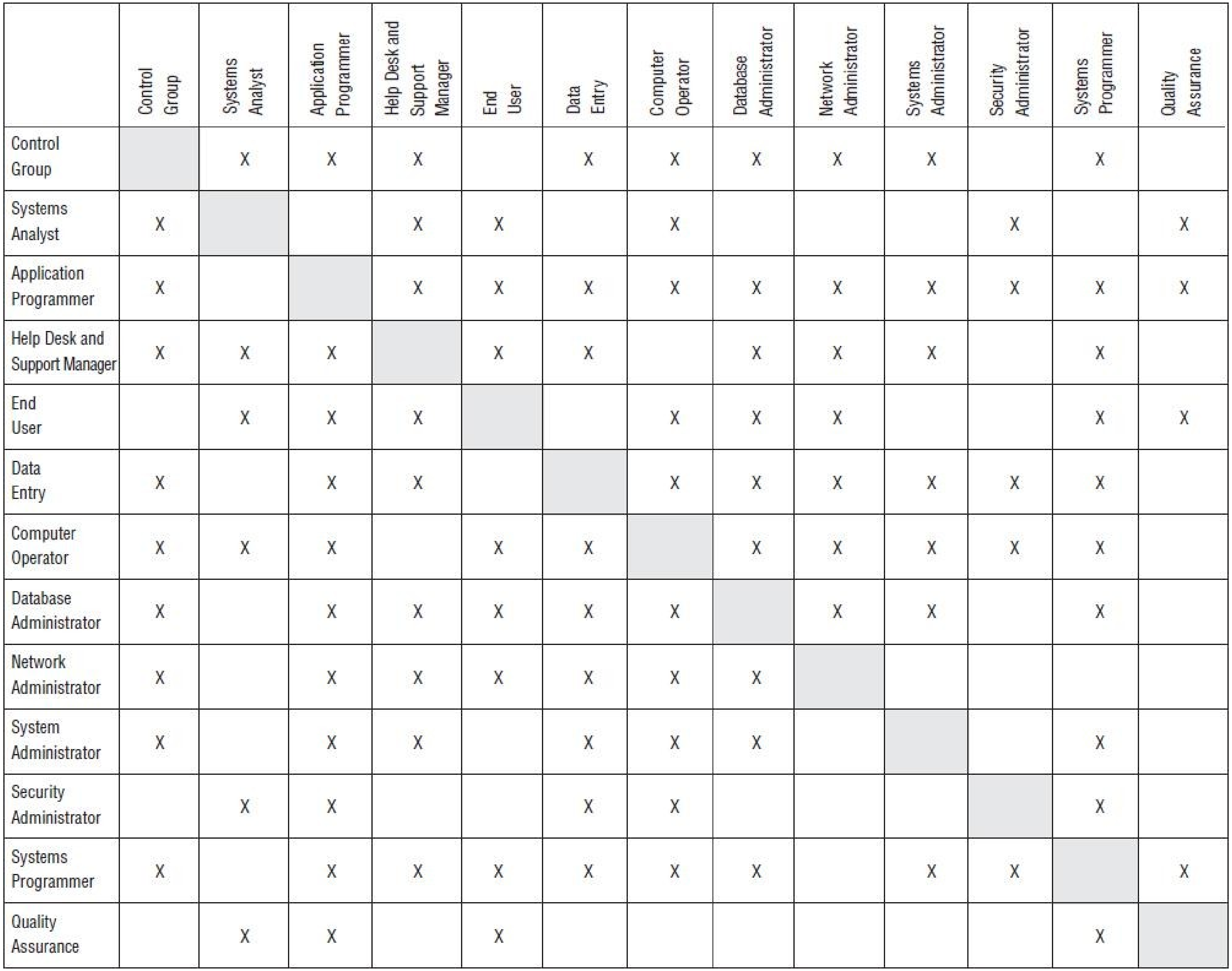
- **Enrolment** function of creating and amending user accounts protected through organisation policies.
- User Accounts cannot be created without HR department request on new-hire or promotion.
- Formal request from HR department:
  - User details
  - Security classification.
- Users/Security manager verify/approve the assignment.
- User training on the organisations security policies.
- User should sign a document agreeing to comply with the policies.

Access Control Administration

- Account Maintenance.
- Account, Log and Journal Monitoring.
- Access rights and permissions.
- Principle of Least Privilege.
- Creeping Privileges.



Separation of Duties (SoD)



	Control Group	Systems Analyst	Application Programmer	Help Desk and Support Manager	End User	Data Entry	Computer Operator	Database Administrator	Network Administrator	Systems Administrator	Security Administrator	Systems Programmer	Quality Assurance
Control Group		X	X	X		X	X	X	X	X		X	
Systems Analyst	X			X	X		X				X		X
Application Programmer	X			X	X	X	X	X	X	X	X	X	X
Help Desk and Support Manager	X	X	X		X	X		X	X	X		X	
End User		X	X	X			X	X	X			X	X
Data Entry	X		X	X			X	X	X	X	X	X	
Computer Operator	X	X	X		X	X		X	X	X	X	X	
Database Administrator	X		X	X	X	X	X		X	X		X	
Network Administrator	X		X	X	X	X	X	X					
System Administrator	X		X	X		X	X	X				X	
Security Administrator		X	X			X	X					X	
Systems Programmer	X		X	X	X	X	X	X		X	X		X
Quality Assurance		X	X		X							X	

Monitoring - Intrusion detection system (IDS)

- Sensors which generate security events.
- Console to monitor events and alerts and control the sensors.
- Central Engine that records events logged by the sensors in a database and uses a system of rules to generate alerts from security events received.

- **Host**-based IDS (HIDS).
- **Network**-based IDS (NIDS).

- Detection types
  - **Knowledge** (**Signature**) Based Detection
  - **Behaviour** (**Statistical anomaly**) Based Detection.

Monitoring – IDS tools

- Honey Pot
  - A trap set to detect, deflect, or in some manner counteract attempts at unauthorised use of information systems.
  - **Entrapment**
  - **Enticement**
    - A Honey Pot placed with open security vulnerabilities and services with known exploits is enticement
    - Perpetrator makes their own decision to perform the exploit.
  - **Entrapment**
    - If the honey pot actively solicits subjects to access it and then the owner charges them with unauthorised intrusion
    - Typically Illegal.

Vulnerability scanner

- Search for and map systems for weaknesses.
  1) Look for active IP addresses, open ports, OS's and any applications running.
  2) Create a report or move to the next step
  3) Attempt to determine the patch level of the OS or applications.
     - Can cause an exploit such as crash the OS or application.
  4) Attempt to exploit the vulnerability.
- Scanners may either be malicious or friendly. Friendly scanners usually stop at step 2 and occasionally step 3 but never go to step 4.

Vulnerability scanner types

- Port Scanner
  - NMAP.
- Network Scanner
  - OpenVAS, Metasploit.
- Web Application Security Scanner
  - OWASP Zed Attack Proxy (ZAP).
- Computer worm
  - Self-replicating computer program that replicates itself to other nodes.
  - Unlike a virus, it does not need to attach itself to an existing program.
  - Worms almost always cause at least some harm to the network, if only by consuming bandwidth, whereas viruses almost always corrupt or devour files on a targeted computer.

Penetration testing

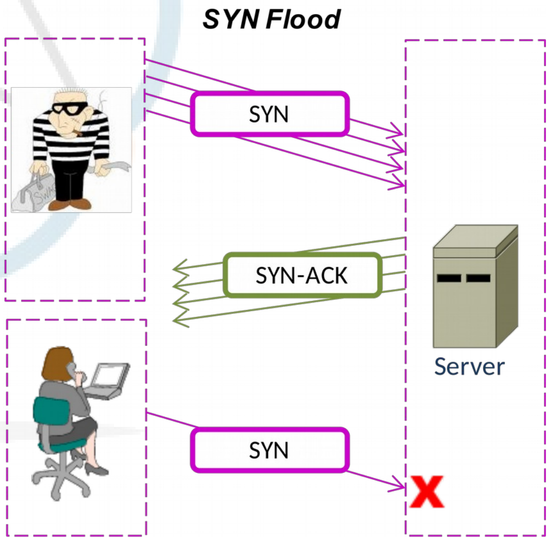
- Penetration testing is a method of evaluating security by simulating an attack, (Black Hat Hacker, or Cracker).
  - Active analysis of the system.
  - Analysis from the position of a potential attacker.
  - Active exploitation of security vulnerabilities.
- Security issues found are presented to the system owner together with an assessment of their impact and often with a proposal for mitigation or a technical solution.
- Penetration testing determines the feasibility of an attack and the business impact of a successful exploit
- It is a component of a full security audit.

Padded cell

- A padded cell is like a honey pot but is used for intruder isolation.
- When the IDS detects an intruder he/she is transferred to the padded cell.
- The padded cell has the look of an actual system but with fake programs and data, a simulated environment of sorts.

Methods of Attack

- Brute Force Attack.
- Dictionary Attack.
- Denial of Service (DoS) attacks
  - SYN Flood example.
- Distributed DOS (DdoS) attack.
- Smurf attack
  - Ping attack.
- Spoofing.
- Man in the middle Attack.
- Spamming.
- Sniffers.



Thank you