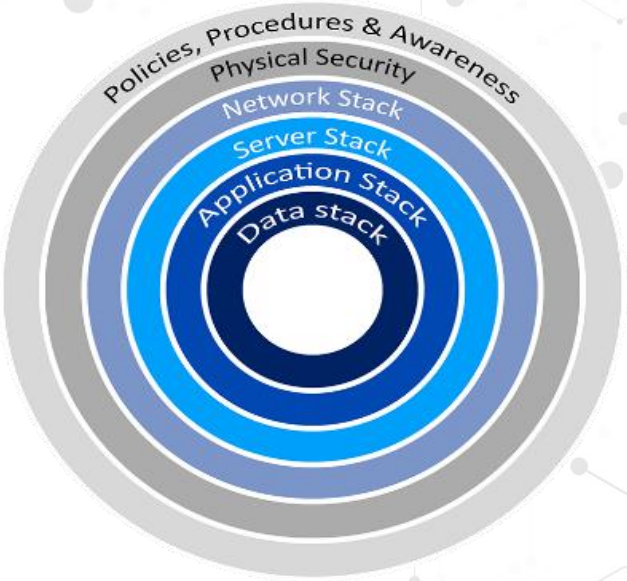
Welcome to the Fifth CBK Domain:

- **In this domain we cover:**
  - Physical and logical assets control.
    - The logical and physical controls we implement.
  - Identification and authentication of people and devices.
    - How we identify and authenticate our authorized users.
  - Identity as a service (e.g., cloud identities).
  - Third-party identity services (e.g., on-premise).
  - Access control attacks.
    - Common attacks, and how we mitigate them with defense in depth.
  - Identity and access provisioning lifecycle (e.g., provisioning review).

This chapter focuses on how we identify our assets, the platforms we use for them, how we provide authorized access and prevent unauthorized access to the assets and the asset and identity lifecycle. CBK 5 makes up 13% of the exam questions.

- **Access Control:**
  - Our **Access Control** is determined by our policies, procedures, and standards.
  - This outlines how we grant access whom to what:
    - We use least privilege, need to know, and we give our staff and systems exactly the access they need and no more.
  - Access control spans all the layers of our defense in depth model, different permissions are granted to different subjects depending on their need to access the systems or data and that adheres to the procedures for that area.
  - We covered some of the physical parts of access control in Domain 3's Physical Security, how we use fences, locks, turnstiles, bollards, ...
  - On the logical side we do this by implementing the access security models we talked about in Domain 1, how we Identify, Authenticate, Authorize our subjects and how we keep them Accountable (IAAA).
  - We never use group logins or accounts; they have no accountability.



IAAA Access Management:

- **Identification:**
  - Your name, username, ID number, employee number, SSN etc.
- **Authentication:**
  - Should **always** be done with Multifactor Authentication!
    - **Something you know - Type 1** Authentication (passwords, pass phrase, PIN etc.).
    - **Something you have - Type 2** Authentication (ID, Passport, Smart Card, Token, cookie on PC etc.).
    - **Something you are - Type 3** Authentication (and Biometrics) (Fingerprint, Iris Scan, Facial geometry etc.).
  - Newer and less commonly used authentication factors:
    - **Somewhere you are - Type 4 Authentication:** IP/MAC Address.
    - **Something you do - Type 5 Authentication:** Signature, Pattern unlock.
- Multi-factor authentication requires authentication from 2 or more categories.
  - Card and Pin, fingerprint and password qualify, but password and username does not (both are something you know).
- **Something you know - Type 1 Authentication:**
  - Passwords, pass phrase, PIN etc., also called Knowledge factors.
  - The subject uses these to authenticate their identity, if they know the secret, they must be who they say they are.
  - This is the most commonly used form of authentication, and a password is the most common knowledge factor.
  - The user is required to prove knowledge of a secret in order to authenticate.
  - Variations include both longer ones formed from multiple words (a passphrase) and the shorter purely numeric PINs (personal identification number) commonly used for cash machines (ATM's).
  - It is the weakest form of authentication and can easily be compromised.
  - Secret questions like "Where were you born?" are poor examples of a knowledge factor, it is known by a lot of people and can often be researched easily.
    - Sarah Palin had her email account hacked during the 2008 US Presidential campaign using her secret questions. Since she used basic ones (high school and birthday, …) the hackers could easily find that information online, he reset her password with the information and gained full control of her email account.

- **Passwords:**
  - It is always easier to guess or steal passwords than it is to break the encryption.
  - We have password policies to ensure they are as secure as possible.
    - They should contain minimum length, upper/lower case letters, numbers and symbols, they should not contain full words or other easy to guess phrases.
    - They have an expiration date, password reuse policy and minimum use before users can change it again.
    - Common and less secure passwords often contain:
      → The name of a pet, child, family member, significant other, anniversary dates, birthdays, birthplace, favorite holiday, something related to a favorite sports team, or the word "password".
      → Winter2017 is not a good password, even if it does fulfil the password requirements.
  - **Key Stretching** – Adding 1-2 seconds to password verification.
    - If an attacker is brute forcing a password and needs millions of tries it will become an unfeasible attack.
  - **Brute Force Attacks** (Limit number of wrong logins):
    - Uses the entire key space (every possible key), with enough time any ciphertext can be decrypted.
    - Effective against all key based ciphers except the one-time pad, it would eventually decrypt it, but it would also generate so many false positives the data would be useless.
  - **Dictionary Attacks** (Limit number of wrong logins, do not allow dictionary words in passwords):
    - Based on a pre-arranged listing, often dictionary words
    - Often succeed because people choose short passwords that are ordinary words and numbers at the end.
  - **Rainbow Tables Attacks** (Limit number of wrong logins, Salts):
    - Pre-made list of plaintexts and matching ciphertext.
    - Often Passwords and matching Hashes a table can have 1,000,000's of pairs.

- **Keylogging (Keystroke Logging):**
  - A keylogger is added to the user's computer and it records every keystroke the user enters.
  - **Hardware**, attached to the USB port where the keyboard is plugged in.
    → Can either call home or needs to be removed to retrieve the information

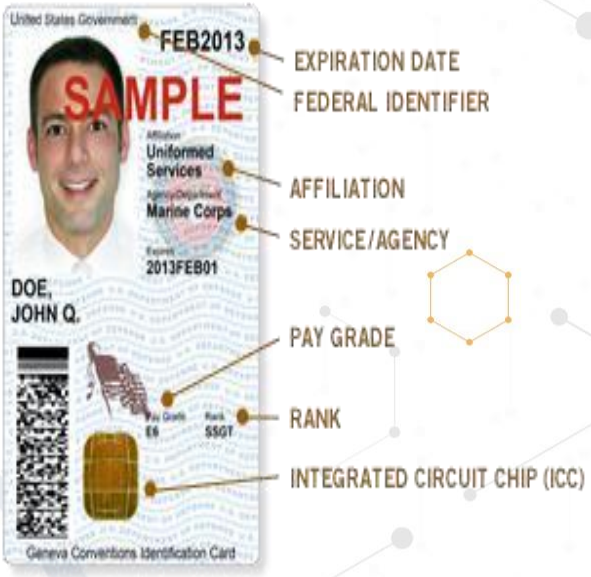
  - **Software**, a program installed on the computer.
    → The computer is often compromised by a trojan, where the payload is the keylogger or a backdoor.
    → The keylogger calls home or uploads the keystrokes to a server at regular intervals.
- **Salt (Salting):**
  - Random data that is used as an additional input to a one-way function that hashes a password or passphrase.
  - Salts are very similar to nonce.
  - The primary function of salts is to defend against dictionary attacks or a pre-compiled rainbow table attack.
- **Nonce** (arbitrary number that may only be used once):
  - It is often a random or pseudo-random number issued in an authentication protocol to ensure that old communications cannot be reused in replay attacks.
  - They can also be useful as initialization vectors and in cryptographic hash function.
- **Clipping Levels:** Clipping levels are in place to **prevent administrative overhead**.
  - It allows authorized users who forget or mistype their password to still have a couple of extra tries.
  - It prevents password guessing by locking the user account for a certain timeframe (an hour), or until unlocked by an administrator.
- Many systems store a cryptographic hash of passwords.
  - If an attacker can get access to the file of hashed passwords guessing can be done off-line, rapidly testing candidate passwords against the true password's hash value.
  - This will circumvent the clipping levels, stealing is always easier than decrypting it.
- Some access systems store user passwords in plaintext, they are used to compare user log on attempts.

        - We need to secure every link in the chain, attackers will go for the weakest one, it is often people, but can just as well be our systems.
    - **Password Management:**
        - We covered some password requirements, here are the official recommendations by the U.S. Department of Defense and Microsoft.
            - Password history = set to remember 24 passwords.
            - Maximum password age = 90 days.
            - Minimum password age = 2 days (to prevent users from cycling through 24 passwords to return to their favorite password again).
            - Minimum password length = 8 characters.
            - Passwords must meet complexity requirements = true.
            - Store password using reversible encryption = false.

- **Something you have - Type 2 Authentication:**
    - ID, passport, smart card, token, cookie on PC, these are called Possession factors.
        - The subject uses these to authenticate their identity, if they have the item,
        - they must be who they say they are.
        - Simple forms can be credit cards, you have the card, and you know the pin, that is multifactor authentication.
        - Most also assume a shared trust, you have your passport, it looks like you on the picture, we trust the issuer, so we assume the passport is real.

    - **Single-Use Passwords:**
        - Having passwords which are only valid once makes many potential attacks ineffective, just like one-time pads.
        - While they are passwords, it is something you have in your possession, not something you know.
        - Some are one-time-pads with a challenge-response or just a pin or phase sent to your phone or email you need to enter to confirm the transaction or the login.
        - Most users find single use passwords extremely inconvenient.
        - They are widely implemented in online banking, where they are known as TANs (Transaction Authentication Numbers).
        - Most private users only do a few transactions each week, the single-use passwords has not led to customers refusing to use it.
        - It is their money; they actually care about keeping those safe.

- **Smart Cards and Tokens** (contact or contactless):
  - They contain a computer circuit using an ICC (Integrated Circuit Chip).
  - **Contact Cards** - Inserted into a machine to be read.
    - This can be credit cards you insert into the chip reader or the DOD CAC (Common Access Card).
  - **Contactless Cards** - can be read by proximity.
    - Key fobs or credit cards where you just hold it close to a reader.
    - They use a RFID (Radio Frequency Identification) tag (transponder) which is then read by a RFID Transceiver.

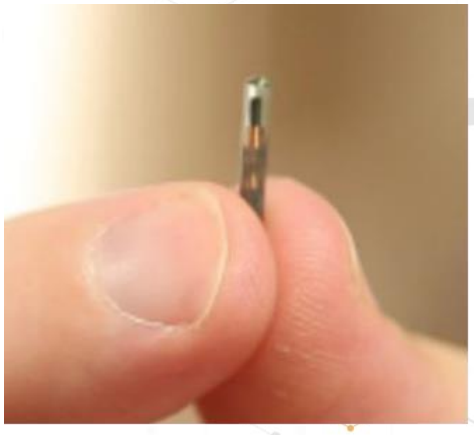


- **Magnetic Stripe Cards:**
  - Swiped through a reader, no circuit.
  - Very easy to duplicate.
- **Tokens:**
  - HOTP and TOTP can be either hardware or software based.
  - Cellphone software applications are more common now.
    - **HOTP (HMAC-based One-Time Password):**
      → Shared secret and incremental counter, generate code when asked, valid till used.
    - **TOTP (Time-based One-Time Password):**
      → Time based with shared secret, often generated every 30 or 60 seconds,
      synchronized clocks are critical.

TOTP tokens
Hardware
Software

- A Wisconsin company Three Square Market (32M) is offering to implant tiny radio-frequency chips in its employees.

- They say the employees are lining up for the technology.
- Employees who have the rice-grain-sized RFID chip implanted between their thumb and forefinger can then use it "to make purchases in their break room micro market, open doors, login to computers, use the copy machine,"
- "The chip is not trackable and only contains information you choose to associate with it," the company said, "This chip does not have GPS capabilities."
- I would never do this; I understand they save 5 seconds at the copier.
    - I just have an innate skepticism when companies say, “We can’t, or we won’t use this for anything else than intended”.
    - History proves they rarely do just that.

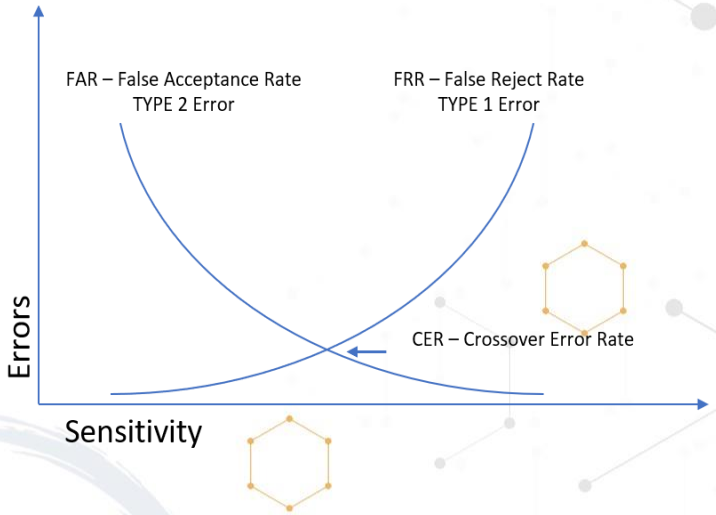


RDFI chip to make access easier.

- **Something you are - Type 3 Authentication (Biometrics):**
    - Fingerprint, iris scan, facial geometry etc., these are also called realistic authentication.
        - The subject uses these to authenticate their identity, if they are that, they must be who they say they are.
        - Something that is unique to you, this one comes with more issues than the two other common authentication factors.
        - We can allow unauthorized people into our facilities or systems if we accept someone by mistake. (False Accept)
        - We can prevent our authorized people from entering our facilities if we refuse them by mistake. (False Reject).

Fingerprint reader, with keypad. This is multifactor authentication.

- Errors for Biometric Authentication:
  - **FRR (False rejection rate) Type 1 error:**
    - Authorized users are rejected.
    - This can be too high settings - 99% accuracy on biometrics.
  - **FAR (False accept rate) Type 2 error:**
    - Unauthorized user is granted access.
    - This is a very serious error.

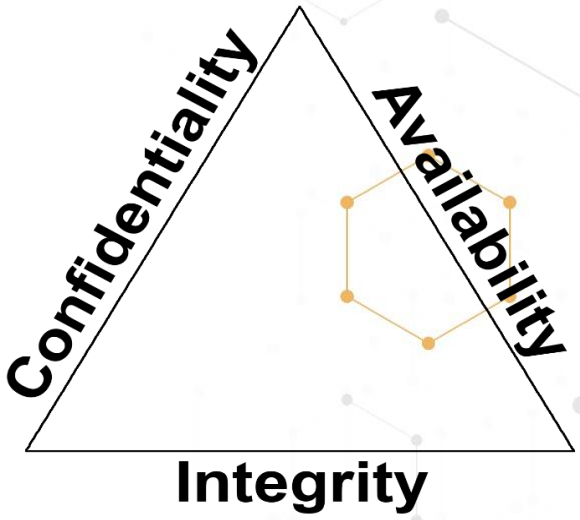


  - We want a good mix of FRR and FAR where they meet on the graph is the **CER (Crossover Error Rate)**, this is where we want to be.
- Biometric identifiers are often categorized as physiological and behavioral characteristics.
  - **Physiological Characteristics** uses the shape of the body, these do not change unless a drastic event occurs.
    - Fingerprint, palm veins, facial recognition, DNA, palm print, hand geometry, iris recognition, retina, and odor.
  - **Behavioral Characteristics** uses the pattern of behavior of a person, these can change, but most often revert back to the baseline.
    - Typing rhythm, how you walk, signature and voice.
- We also need to respect and protect our employee's privacy:
  - Some fingerprint patterns are related to chromosomal diseases.
  - Iris patterns could reveal genetic sex, retina scans can show if a person is pregnant or diabetic.
  - Hand vein patterns could reveal vascular diseases.
  - Most behavioral biometrics could reveal neurological diseases, etc.
- Issues with Biometric Authentication:
  - While passwords and smart cards should be safe because you keep them a secret and secure, biometrics is inherently not and something others can easily find out.
  - Attackers can take pictures of your face, your fingerprints, your hands, your ears and print good enough copies to get past a biometric scan.

- It is possible to copy fingerprints from your high-resolution social media posts if you do a peace sign like the one on the right here.
- How you type, sign your name and your voice pattern can be recorded, also not too difficult to cheat biometrics if it is worth the effort.
- Some types are still inherently more secure, but they are often also more invasive.

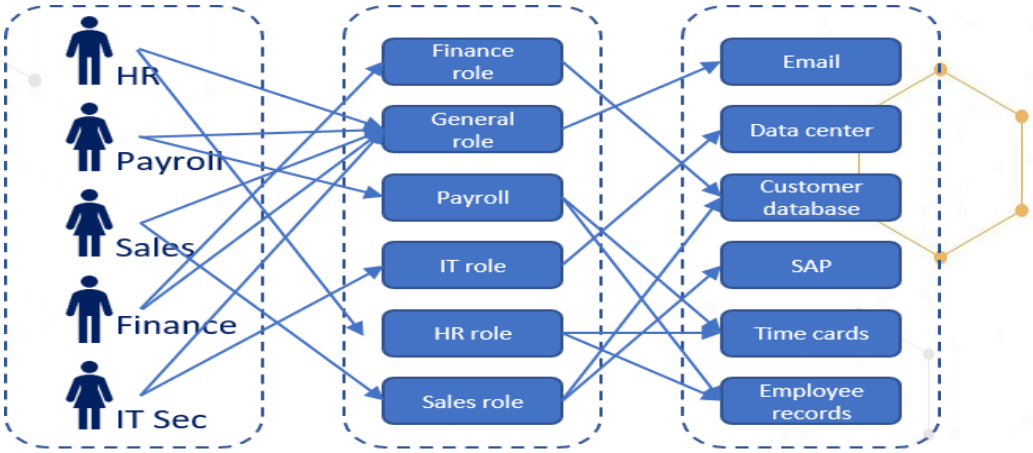
- Issues with Biometric Authentication:
  - Lost passwords and ID cards can be replaced with new different ones, biometrics can't.
  - Which should make us question even more the mass collection of biometric data.
    - When Home Depot loses 10 million credit card numbers it is bad, but they can be reissued.
    - The US Office of Personnel Management got hacked and lost 5.6 million federal employees' fingerprints.
    - The FBI has a database with 52 million facial images and Homeland Security and U.S. Customs and Border Patrol is working on adding the iris scans and 170 million foreigner fingerprints to the FBI's database.
    - The compromises of the future will have much more wide-reaching ramifications than the ones we have seen until now.

- **Authorization:**
  - We use Access Control models to determine what a subject is allowed to access.
  - What and how we implement depends on the organization and what our security goals are, type can often be chosen dependent on which leg of the CIA Triad is the most important one to us.
  - If it is **Confidentiality,** we would most likely go with Mandatory Access Control.
  - If it is **Availability,** we would most likely go with Discretionary Access Control.
  - If it is **Integrity,** we would most likely go with Role Based Access Control or Attribute Based Access Control.
  - There technically is also RUBAC (Rule Based Access Control), it is mostly used on firewalls with IF/THEN statements but can be used in conjunction with the other models to provide defense in depth.

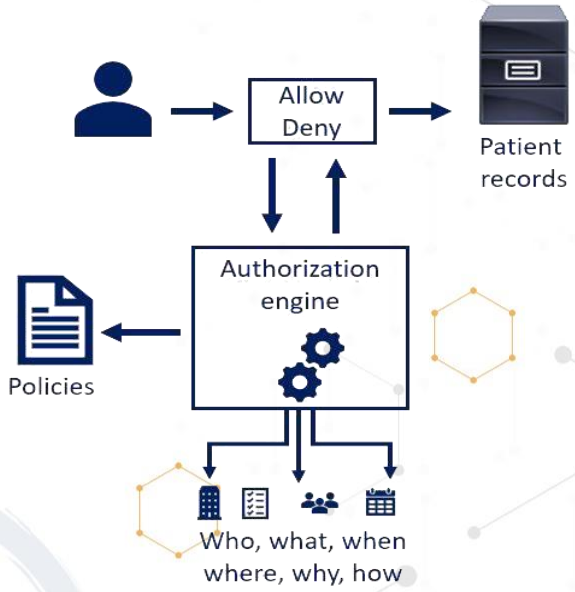


- **DAC (Discretionary Access Control) -** Often used when Availability is most important:
  - Access to an object is assigned at the discretion of the object owner.
  - The owner can add, remove rights, commonly used by most OS's'.
  - Uses DACL's (Discretionary ACL), based on user identity.
- **MAC (Mandatory Access Control) -** Often used when Confidentiality is most important:
  - Access to an object is determined by labels and clearance, this is often used in the military or in organizations where confidentiality is very important.
  - **Labels**: Objects have Labels assigned to them; the subject's clearance must dominate the object's label.
    - The label is used to allow Subjects with the right clearance access them.
    - Labels are often more granular than just "Top Secret", they can be "Top Secret – Nuclear".
  - **Clearance**: Subjects have Clearance assigned to them.
    - Based on a formal decision on a subject's current and future trustworthiness.
    - The higher the clearance the more in depth the background checks should be.

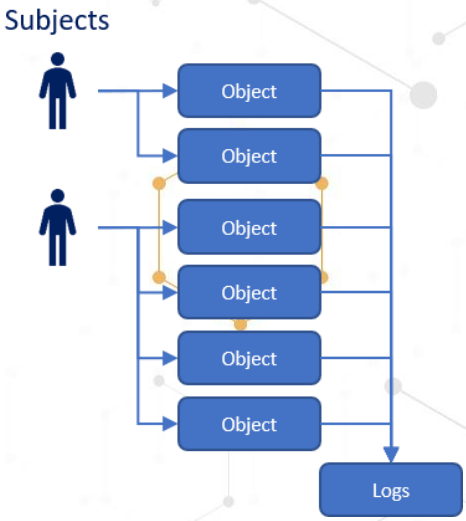
- **RBAC (Role-Based Access Control) -** Often used when Integrity is most important:
  - Policy neutral access control mechanism defined around roles and privileges.
  - A role is assigned permissions, and subjects in that role are added to the group, if they move to another position they are moved to the permissions group for that position.
  - It makes administration of 1,000's of users and 10,000's of permissions much easier to manage.
  - The most commonly used form of access control.
  - If implemented right it can also enforce separation of duties and prevent authorization/privilege creep.
    - We move employees transferring within the organization from one role to another and we do not just add the new role to the old one.



- **ABAC (Attribute-Based Access Control):**
- Access to objects is granted based on subjects, objects, AND environmental conditions.
  - Attributes could be:
    - *Subject* (user) – Name, role, ID, clearance, etc.
    - *Object* (resource) – Name, owner, and date of creation.
    - *Environment* – Location and/or time of access, and threat levels.
  - Expected to be used by 70% of large enterprises within the next 5 years, versus around 20% today.
  - Can also be referred to as policy-based access control (PBAC) or claims-based access control (CBAC).

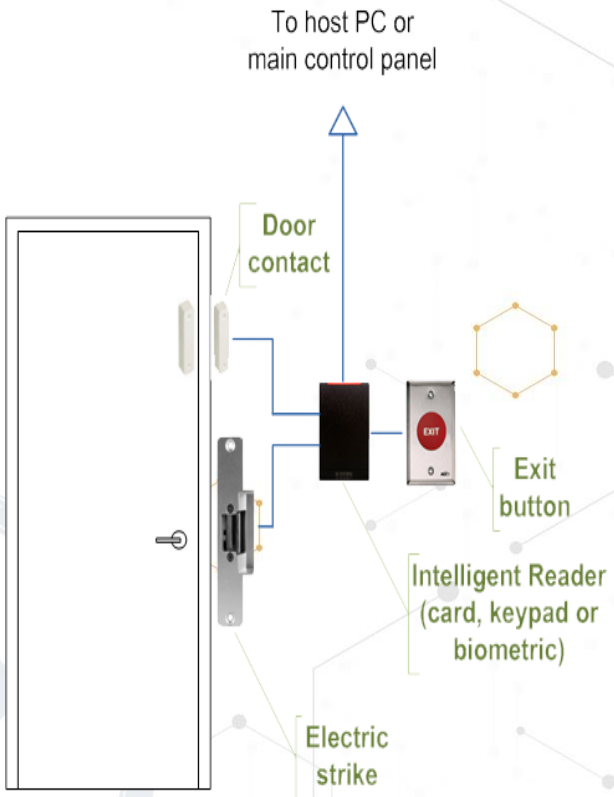


- **Context-Based Access Control:**
  - Access to an object is controlled based on certain contextual parameters, such as location, time, sequence of responses, access history.
  - Providing the username and password combination followed by a challenge and response mechanism such as CAPTCHA, filtering the access based on MAC addresses on wireless, or a firewall filtering the data based on packet analysis are all examples of context-dependent access control mechanisms.
- **Content-Based Access Control:**
  - Access is provided based on the attributes or content of an object, then it is known as a content-dependent access control.
  - In this type of control, the value and attributes of the content that is being accessed determine the control requirements.
  - Hiding or showing menus in an application, views in databases, and access to confidential information are all content-dependent.
- **Accountability** (often referred to as Auditing):
  - Traces an Action to a Subject's Identity:
    - Proves who performed given action, it provides non-repudiation.
    - Group or shared accounts are never OK, they have zero accountability.
    - Uses audit trails and logs, to associate a subject with its actions.

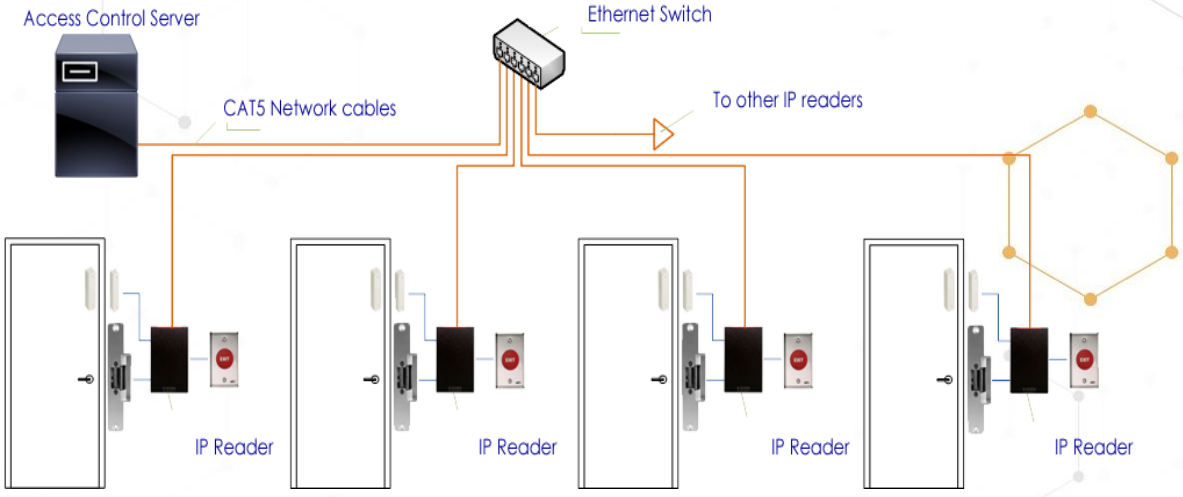


Access Control:

- **Access Control Systems:**
  - We can use centralized and/or decentralized (distributed) access control systems, depending on which type makes the most sense.
    Both options provide different benefits.
  - Access control decisions are made by comparing the credential to an access control list.
  - This look-up can be done by a host or server, by an access control panel, or by a reader.
  - Most common is hub and spoke with a control panel as the hub, and the readers as the spokes.
  - Today most private organizations use Role Based Access Control (RBAC).
    - You are in Payroll you get the payroll staff access and permissions, if you move to HR, you lose your payroll access and get HR access assigned.

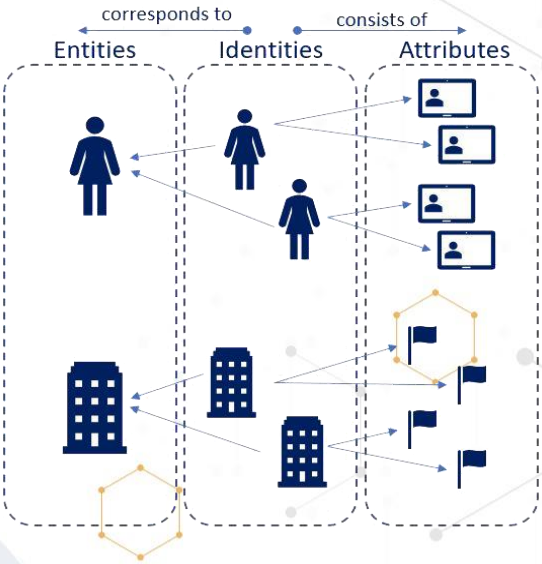


  - Normal systems are much larger, but you get the idea from this drawing how they would connect.
  - In a perfect world, access control systems should be physically and logically segmented from the rest of our IP Network, in reality it is most often segmented logically with VLANs, but in many cases not even that.



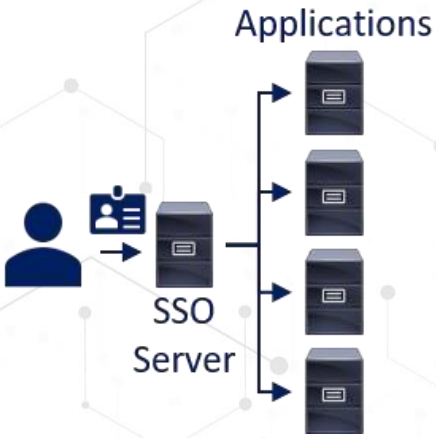
- **Centralized Pro's** (Decentralized Con's):
  - All systems and locations have the same security posture.
  - Easier to manage: All records, configurations and policies are centralized and only configured once per policy.
    - Attackers look for the weakest link in our chain, if a small satellite office is not following our security posture, they can be an easy way onto our network.
  - It is more secure, only a few people have access and can make changes to the system.
  - It can also provide separation of duties, the local admin can't edit/delete logs from their facility.
  - SSO can be used for user access to multiple systems with one login.
- **Centralized Con's** (Decentralized Pro's):
  - Traffic overhead and response time, how long does it take for a door lock to authenticate the user against the database at the head office?
  - Is connectivity to the head office stable, is important equipment on redundant power and internet?
- **Hybrid:**
  - Centrally controlled; access lists for that location are pushed to a local server on a daily/hourly basis; local administrators have no access.
  - We must still ensure that the local site follows the organization's security posture in all other areas.
- **Just-In-Time (JIT) Access Control:**
  - Allows us to use third-party websites without checking if all of our employees have accounts on those sites.
  - Users log in on a third-party site, and on their first visit, the JIT system confirms the employee with our systems and creates the user account on their systems, most commonly using SAML.
- **OpenID Connect (OIDC)/Open Authorization:**
  - Adds an identity layer to OAuth 2.0, allowing 3rd party applications or sites to verify the identity of a user.
  - You can use your Google or Facebook account to log into 1000s of other sites.
- **Risk-Based Access Control:**
  - Access decisions are made based on risk assessment.
  - Done using machine learning, which analyzes behavioral and contextual data analytics to calculate risk for each access.

- **Identity and Access Provisioning:**
  - We can have multiple identities per entity and each identity can have multiple attributes.
    - I can be staff, alumni, and enrolled student at a college.
    - As staff I could have access to different areas and data than I would as alumni and student.
    - Companies can have the same, they can be the parent company, then smaller companies under the parent umbrella, all with different attributes.



- **Identity and Access Provisioning Lifecycle:**
  - This is a suggested lifecycle example from "Identity Management Design Guide with IBM Tivoli Identity Manager".
  - You obviously don't have to implement it verbatim but find a clear policy that works for your organization.
    - Life cycle rules provide administrators with the ability to define life cycle operations to be executed as the result of an event. Life cycle rules are especially useful in automating recurring administrative tasks.
      - Password policy compliance checking.
      - Notifying users to change their passwords before they expire.
      - Identifying life cycle changes such as accounts that are inactive for more than 30 consecutive days.
      - Identifying new accounts that have not been used for more than 10 days following their creation.
      - Identifying accounts that are candidates for deletion because they have been suspended for more than 30 days.
      - When a contract expires, identifying all accounts belonging to a business partner or contractor's employees and revoking their access rights.

- **Federated Identity:**
  - How we link a person's electronic identity and attributes across multiple distinct identity management systems.
  - **FIDM (Federated Identity Management):**
    - Having a common set of policies, practices and protocols in place to manage the identity and trust into IT users and devices across organizations.
    - **SSO** is a subset of federated identity management, it only uses authentication and technical interoperability.
  - Technologies used for federated identity include SAML, OAuth, OpenID, Security Tokens, Microsoft Azure Cloud Services, Windows Identity Foundation...
    - **SAML (Security Assertion Markup Language):**
      - An XML-based, open-standard data format for exchanging authentication and authorization data between parties.
      - The single most important requirement that SAML addresses is web browser SSO.
  - **SSO (Single Sign-on):**
    - Users use a single sign-on for multiple systems.
    - Often deployed in organizations where users have to access 10+ systems, and they think it is too burdensome to remember all those passwords.
    - SSO have the same strong password requirements as normal single system passwords.
    - If an attacker compromises a single password they have access to everything that user can access.



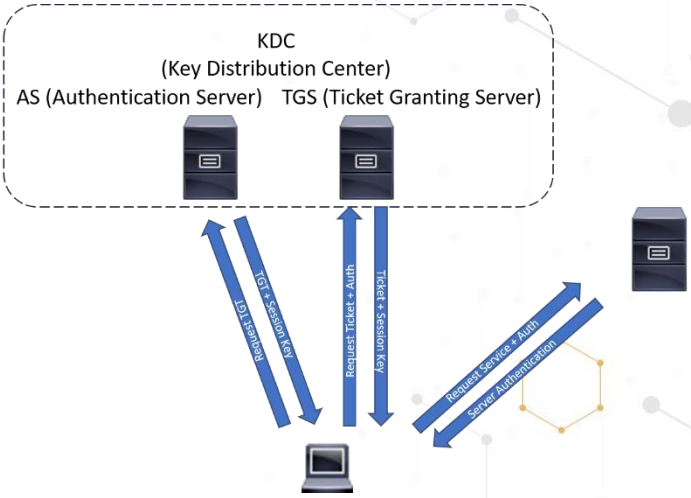
  - **Super Sign-on:**
    - One login can allow you to access many systems and sites.
    - Social media logins are common super sign-ons, if an account is compromised an attacker can often access multiple other sites or systems, the social media account is linked all the other systems.

- **IDaaS (Identity as a Service):**
  - Identity and access management that is built, hosted and managed by a third-party service provider.
  - Native cloud based IDaaS solutions can provide SSO functionality through the cloud, Federated Identity Management for Access Governance, Password Management, ...
  - Hybrid IAM solutions from vendors like Microsoft and Amazon provide cloud-based directories that link with on-premises IAM systems.

Access Control - Authentication Protocols:

- Communications or cryptographic protocols designed to transfer authentication data between two entities.
- They authenticate to the connecting entity (often a server) as well as authenticate itself (often a server or desktop) by declaring the type of information needed for authentication as well as syntax.
- It is the most important layer of protection needed for secure communication between networks.
- **Kerberos:**
  - Authentication protocol that works on the basis of tickets to allow nodes communicating over a non-secure network to prove their identity to each other in a secure manner.
  - The protocol was named after the character Kerberos (or Cerberus) from Greek mythology, the three-headed guard dog of Hades.
  - It is based on a client–server model and it provides mutual authentication both the user and the server verify each other's identity.
  - Messages are protected against eavesdropping and replay attacks.
  - Builds on **symmetric** keys and requires a trusted third party, and can optionally use PKI during certain phases of authentication.
  - Uses UDP port 88 by default, used in Active Directory from Windows 2000 and onwards, and many Unix OS's.
    - **Pros:** Easy for end users, centralized control and easy to administer.
    - **Cons:** Single point of failure, access to everything with single password.

1. Send TGT request sending only plaintext user ID.
2. Sends session key encrypted with user's secret key + TGT encrypted with TGS secret key.
3. TGT + Service request encrypted with the client/TGS session key.
4. Client to server ticket encrypted with server's secret key + client/session key encrypted with the client/TGS session key.



5. Client/session key encrypted with the client/TGS session key + new authenticator encrypted with the client/server session Key.
6. Timestamp authentication Client/Server Session Key.

- **SESAME (Secure European System for Applications in a Multi-vendor Environment):**
  - Often called the successor to KERBEROS, it addresses some of the issues of Kerberos.
  - It uses PKI encryption (asymmetric), which fixed the Kerberos the plaintext storage of symmetric keys issue.
  - Uses a PAS (Privilege Attribute Server), which issues PACs (Privilege Attribute Certificates) instead of Kerberos' tickets**.**
  - Not widely used, Kerberos is widely used since it is natively in most OS's.

- **RADIUS (Remote Authentication Dial-In User Service):**
  - A networking protocol that provides centralized Authentication, Authorization, and Accounting management for users who connect and use a network service.
  - Widely used by ISP's (Internet service providers) and large organizations to manage access to IP networks, AP's, VPN's, Servers, 802.1x,...
  - Uses a client/server protocol that runs in the application layer and can use either TCP or UDP as transport.
  - Network access servers, the gateways that control access to a network, usually contain a RADIUS client component that communicates with the RADIUS server.
  - Uses UDP ports 1812 for authentication and 1813 for accounting, can use TCP as the transport layer with TLS for security.

Code	Assignment
1	Access-Request
2	Access-Accept
3	Access-Reject
4	Accounting-Request
5	Accounting-Response
11	Access-Challenge
12	Status-Server (experimental)
13	Status-Client (experimental)
255	Reserved

- **Diameter:**
  - Also provides centralized AAA (Authentication, Authorization, and Accounting) management for users who connect and use a network service.
  - Was intended as a replacement for RADIUS, but the use cases changed, and both now have different uses.
  - Diameter is largely used in the 3G space, RADIUS is used elsewhere.
  - Uses 32bit for the AVP field (4.2 billion AVPs), RADIUS uses 8bit and only has 256 possible AVPs.
  - Use SCTP (Stream Control Transmission Protocol) or TCP as default.
  - Not directly backwards compatible but provides an upgrade path for RADIUS.
  - One of the largest barriers to having Diameter replace RADIUS is that switches and Access Points typically implement RADIUS, but not Diameter. Uses SCTP or TCP.

- **TACACS (The Terminal Access Controller Access Control System):**
  - Centralized access control system requiring users to send an ID and reusable (vulnerable) passwords for authentication.
  - Uses TCP/UDP port 49.
  - TACACS has generally been replaced by TACACS+ and RADIUS.

- **TACACS+:**
  - Provides better password protection by using two-factor strong authentication.
  - Not backwards compatible with TACACS.
  - Uses TCP port 49 for authentication with the TACACS+ server.
  - Similar to RADIUS, but RADIUS only encrypts the password TACACS+, encrypts the entire data package.

- **PAP (Password Authentication Protocol):**
  - Authentication is initialized by client/user by sending packet with credentials (username and password) at the beginning of the connection.
  - One of the oldest authentication protocols, no longer secure. Credentials are sent over the network in plain text.

- **CHAP (Challenge-Handshake Authentication Protocol):**
  - Provides protection against replay attacks by the peer through the use of an incrementally changing identifier and of a variable challenge-value.
  - Requires the client and server know the plaintext of a shared secret, but it is never sent over the network.
  - Providing better security compared to PAP which is vulnerable for both these reasons.
  - Used by PPP (Point to Point Protocol) servers to validate the remote clients.

- CHAP periodically verifies the identity of the client by using a three-way handshake.
- The CHAP server stores plaintext passwords of each client, an attacker gaining access to the server can steal all the client passwords stored on it.

- **AD (Active Directory):**
  - Directory service that Microsoft developed for Windows domain networks.
  - Included in most Windows Server OS as a set of processes and services.
  - Originally it was only in charge of centralized domain management, as of Windows Server 2008, AD became an umbrella term for a broad range of directory-based identity-related services.
  - A server running Active Directory Domain Services (AD DS) is a domain controller,
  - The DC authenticates and authorizes all subjects in a domain, networks can have one or more domains.
  - Uses LDAP (Lightweight Directory Access Protocol) versions 2 and 3, Microsoft's version of Kerberos, and DNS.
  - Each domain can have a separate authentication process, users, network components and data objects.
  - Uses groups to control access by users to data objects, often used as a RBAC where roles are assigned to groups, where the group has access rights.
  - Can use Trust domains which allow users in one domain to access resources in another.
    - **One-way Trust:** One domain allows access to users on another domain, but the other domain does not allow access to users on the first domain.
    - **Two-way Trust:** Two domains allow access to users on both domains.
    - **Trusted Domain:** The domain that is trusted; whose users have access to the trusting domain.
    - **Transitive Trust:** A trust that can extend beyond two domains to other trusted domains in the forest.
    - **Intransitive (non-transitive) Trust:** A one way trust that does not extend beyond two domains.

- **What we covered in the Fifth CBK Domain:**
  - In this domain we covered:
    - How we identify, classify, and assign labels to our objects and clearance to our subjects, and the access control models and platforms we use for doing so.
    - How we provide authorized objects access and prevent unauthorized access.
    - The logical and physical controls we implement.
    - How we identify and authenticate our authorized users, how we use multifactor authentication and the strengths and weaknesses of each authentication factor.
    - We looked at IDaaS, SSO, and super sign-on.
    - Access control attacks and what we can do to mitigate them.
    - Identity and access provisioning lifecycle (e.g., provisioning review).