- Authentication Methods
    - Directory services
        - Keep all of an organizations usernames and passwords in a single database
            - Also contains computers, printers, and other devices
    - Large distributed Database
        - Constantly replicated
    - All authentication requests reference this directory
        - Each user only needs one set of credentials
        - One username and password for all services
    - Access via Kerberos or LDAP
- Federation
    - Provide network access to others
        - Not just employees - Partners, suppliers, customers, etc.
        - Provides SSO and more
    - Third parties can establish a federated network
        - Authenticate and authorize between the two organizations
        - Login with your FB credentials
    - The third parties must establish a trust relationship
        - And the degree of the trust
- Attestation
    - Prove the hardware is really yours
        - A system you can trust
    - Easy when its just your computer
        - More difficult when there are 1,000
    - Remote attestation
        - Devices provides an operational report to a verification server
        - Encrypted and digitally signed with the TPM
        - An IMEI or other unique hardware component can be included in the report
- Short message service (SMS)
    - Text messaging
        - Includes more than text these days
    - Login factor can be sent via SMS to a predefined number
        - Provide username and password
        - Phone receives an SMS
        - Input the SMS code into the login form
    - Security issues exist
        - Phone number can be reassigned to a different phone
        - SMS can be intercepted
- Push notifications
    - Similar process to an SMS notification
        - Authentication factor is pushed to a specialized app
        - Usually on a mobile device

    - Security challenges
        - Applications can be vulnerable
        - Some push apps send in the clear
    - Still more secure than SMS
        - Multiple factors are better than one factor
- Authentication Apps
    - Pseudo-random token generators
        - A useful auth factor
    - Carry around a physical hardware token generator
        - Where are my keys again?
    - Use software based token generator on your phone
        - Powerful and convenient
- TOTP
    - Time based one time password algorithm
        - Use a secret key and the time of day
        - No incremental counter
    - Secret key is configured ahead of time
        - Timestamps are synchronized via NTP
    - Timestamp usually increments every 30 seconds
        - Put in your username, password and TOTP code
    - One of the most common OTP methods
        - Google, Facebook, Microsoft
- HOTP
    - One time passwords
        - Use them once, and never again
        - Once a session, once each auth attempt
    - HMAC-based One time password algorithm
        - Keyed hash message authentication code (HMAC)
        - The keys are based on a secret key and a counter
    - Token based auth
        - The hash is different every time
    - Hardware and software tokens available
        - You'll need additional tech to make this work
- Phone call
    - A voice call provides the token
        - The computer is talking to you
        - Your code is “1 6 2 5 1 7”
    - Similar disadvantages to SMS
        - Phone call can be intercepted or forwarded
        - Phone number can be added to another phone
- Static codes
    - Authentication factors that dont change
        - You just have to remember
    - Personal Identification Number (PIN)

        - Your secret numbers
    - Can also be alphanumeric
        - A password or passphrase
- Smart cards
    - Integrated circuit card
        - Contact or contactless
    - Common for credit cards
        - Also used for access control
    - Must have physical card to provide digital access
        - A digital certificate
    - Multiple factors
        - Use the card with a PIn or fingerprint

- Biometric Factors
    - Fingerprint scanner
        - Phones, laptops, door access
    - Retinal scanner
        - Unique capillary structure in the back of the eye
    - IRIS scanner
        - Texture, color
    - Voice Recognition
        - Talk for access
    - Facial recognition
        - Shape of the face and features
- Gait Analysis
    - Identify a person based on how they walk
    - Many unique measurements
- Veins
    - Vascular scanners
    - Match the blood vessels visible from the surface of the skin
- Biometric acceptance rates
    - False acceptance rate (FAR)
        - Likelihood that an unauthorized user will be accepted
            - Not sensitive enough
    - False rejection rate (FRR)
        - Likelihood that an authorized user will be rejected
            - Too sensitive
    - Crossover error rate (CER)
        - Defines the overall accuracy of a biometric system
        - The rate at which FAR and FRR are equal
        - Adjust sensitive to equalize both values

- AAA framework (Authentication, Authorization, Accounting)
    - Identification

        - This is who you claim to be
        - Usually your username
    - Authentication
        - Prove who you say you are
        - Password and other authentication factors
    - Authorization
        - Based on your identification and authentication, what access do you have?
    - Accounting
        - Resources used: login time, data sent and received, logout time
- Cloud vs On Premises authentication
    - Cloud based security
        - Third party can manage the platform
        - Centralized platform
        - Automation options with API integration
        - May include additional options (for a cost)
    - On premises authentication system
        - Internal monitoring and management
        - NEed internal expertise
        - External access must be granted and managed
- Multi factor authentication
    - Factors
        - Something you know
        - Something you have
        - Something you are
    - Attributes
        - Somewhere you are
        - Something you can do
        - Something you exhibit
        - Someone you know
- Something you know
    - Password
        - Secret word/phrase, string of chars
        - Very common authentication factor
    - PIN
        - Personal identification number
        - Not typically contained anywhere on a smart card or ATM card
    - Pattern
        - Complete a series of patterns
        - Only you know the right format
- Something you have
    - Smart card
        - Integrates with devices
        - May require a PIN

    - USB Token
        - Certificate is on the USB device
    - Hardware or software tokens
        - Generates pseudo-random authentication codes
    - Your phone
        - SMS a code to your phone
- Something you are
    - Biometric authentication
        - Fingerprint, iris scan, voice print
    - Usually stores a mathematical representation of your biometric
        - Your actual fingerprint isnt usually saved
    - Difficult to change
        - You can change your password
        - You can't change your fingerprint
    - Used in very specific situations
        - Not fool proof
- Somewhere you are
    - Provide a factor based on your location
        - The transaction only completes if you are in a particular geography
    - IP address
        - Not perfect, but can help provide more info
        - Works with IPv4, not so much with IPv6
    - Mobile device location services
        - Geolocation to a very specific area
        - Must be in a location that can receive GPS information or near an identified mobile or 802.11 network
        - Still not a perfect identifier or location
- Something you can do
    - A personal way of doing things
        - You're special
    - Handwriting analysis
        - Signature comparison
        - Writing techniques
    - Very similar to biometrics
        - Close to something you are
- Something you exhibit
    - A unique trait, personal to you
    - Gait analysis - the way you walk
    - Typing analysis - the way you hit enter key too hard
- Someone you know
    - A social factor
    - Its not what you know
    - Web of trust
    - Digital signature