CompTIA Security+ Notes Part 2

Physical Security
- Measures taken to protect tangible assets from any harm
- Fencing and bollards
    - Bollards
        - Short posts
    - Fences
        - Separate areas
- Brute force attacks
- Surveillance system
- Access control vestibule
    - Double door system
- Piggybacking
- Tailgating
- Door Locks
- Access badge cloning

Fencing and bollards
- Primitive yet effective
- Fence
    - Structure that encloses area using interconnected panels or posts
    - Can be ugly or decorative and still secure
    - Provides visual deterrent
    - Establish physical barrier against unauthorized entry
    - Delays intruders allowing security a longer reaction window
    - Vulnerable to attack themselves
        - Intruder can climb over it
        - Wire fences can be cut
        - People can dig underneath it
- Bollards
    - Robust short vertical designed to redirect vehicular traffic
    - Permanent or temporary
    - Creates physical barrier protecting pedestrians
    - Physical reminder for intruders to not enter
    - Some can be appealing-looking
        - Look like giant plant pots
        - Target red balls
    - They are not invulnerable to attack
        - Some tamper or try to remove it
- Fences prevent people bollards prevent vehicles

Attacking with brute force
- Attack where access is gained from trying all possibilities until breaking through
- Can take a lot of time

- Forcible entry
    - Getting unauthorized access by physically breaking or bypassing barriers
    - Glass cutting
    - Breaking windows
    - Select reinforced or laminated windows
    - Doors can be kicked in
    - Use high strength doors with deadbolts and solid frame door
    - Fences can be climbed
    - Put barbed wire on top of fence
- Tampering with sec devices
    - Manipulating sec devices to create and exploit new vulnerabilities
    - Sensors can be painted and blinded, redirected
    - Have redundancy in security measures to make sure other systems stay in tact
- Confronting Sec Personnel
    - Direct confrontation or attack
    - Criminal and can be life threatening
    - Rigorous training and self defense
    - Backup available
- Ramming barriers with vehicles
    - Brute force with vehicle to ram a barrier
    - Bollards or reinforced barriers to dissipate a vehicle energy

Surveillance Systems

- Maintain safety and security
- Help detect and respond to potential threats
- Observe and report activities
- Can be a security guard
- 4 categories
    - Video surveillance
        - Motion detection
        - Night vision
        - Facial recognition
        - Remote access
        - Real time feedback
        - Ability to review
        - Wired solutions
        - Wireless solutions
            - Subject to interference
        - CCTV (closed circuit TV)
            - Indoor and outdoor
            - Pan-tilt-zoom
                - Move camera to better detect intrusions
            - Entrances and exits to critical infrastructure
                - Data center
                - Telecommunication closets

            - Entrance and exits
    - Security Guards
        - Flexible and adaptable
        - Reassure staff
    - Lighting
        - Crucial
        - Deters criminals
        - Improve performance and quality
        - Alert system
    - Sensors
        - Respond to external stimulus and converts to a readable signal
        - 4 types
            - IR
                - Changes in IR radiation triggers
                - Effective in dark
                - Changes in environmental heat such as from warm bodies
            - Pressure
                - Specified min amnt of weight
                - Embedded into floor
            - Microwave
                - Emits pulses and measures reflections off of moving objects
                - High sensitivity
            - Ultrasonic
                - Measures reflection of waves off of moving objects

Bypassing Surveillance

- Visual Obstruction
    - Simple yet effective
    - Blocks line of sight
    - Spray painting
    - Tape
    - Balloons
    - Umbrellas
- Blinding cameras
    - Overwhelms sensors permanent or temporary
    - Sudden burst of light
- Interfere with acoustics
    - Sensors listen to environment
    - Intruders play loud music
    - Frequencies to jam signals
- EMI (electromagnetic interference)
    - Jam signals surveillance systems rely on
- Physical environment attack
    - Temperature decrease or increase to trick sensor

        - Power box tampering
        - Attacker starts fire to distract and possibly damage equipment
        - Crude but effective
        - Require attacker to be close
- Modern systems are configured with countermeasures
    - Tamper alarms
    - Backup power
    - Encrypt frequencies
        - Guards against jamming and eavesdropping attacks
- Update and refine your systems

Access Control Vestibules

- Double door system elec control and only one opens at a time
- Controlled space to authenticate for access
- Combined with other measures
- How they work
    - First to outer door
    - Door locks behind and traps them
    - Identity must be verified before inner door opens
- Provides a controlled environment
- Prevents piggy backing
    - Person with access allows another without it to enter a secure area with them
    - Instigated with social engineering techniques
- Tailgating
    - Following someone with access to secure area without consent
    - Following another in a turnstile door
- Authorized personnel have a badge typically
    - RFID
    - NFC
    - Magnetic strips
    - Provide detailed info about the user that can be cross referenced for verification
    - Can be programmed with different levels of access in an organization
    - Access badge uses are logged
- Security guard
    - Visual deterrent
    - Assistance
    - Check identity
    - Response in case of a breach
- Access control vestibules, badges, guards

Door Locks

- Perimeter defenses become useless once the individual enters the building or secured area
- Secure entryways restricting and regulating access to a space or property
- Not all are created equal
    - Simple padlocks are nothing to a skilled attacker

        - Padlocks have basic pin and tumbler system not secure
        - Many generic door locks are no better either
    - Complex door locks provide better protection
    - Can be configured so each person has their own number
        - Allows to log who comes in and when
    - NFC from smart phone can act as a key
    - Biometrics
        - Rely on physical characteristics to verify ID
        - Inherence factor
        - Fingerprint
        - Retinal scanner
        - Face scanner
    - Some challenges to biometric sensors
        - False acceptance rate (FAR)
            - Rate at which the wrong person is let in by the sensor
            - Higher sensitivity = higher rejections
        - False rejection rate
            - Sensor denies the right user but set to too sensitive
        - Equal Error Rate (ERR) or Crossover error rate (CER)
            - Balance between FAR and FRR
            - The lower the CER, the better the lock
    - Many modern locks combine multiple auth factors
    - Cipher lock
        - Mechanical lock with push buttons
        - Cost more than traditional office lock
    - Vulnerability moment occurs when unauthorized individual enters a secured space within an organization
    - Multiple auth methods in one increases sec posture

Access Badge Cloning

- RFID (radio frequency identification)
- NFC (near Field Communication)
- Refers to copying data from card onto another device
    - Unauthorized
- 4 steps
    - Scanning
        - Attacker holds reader to capture data from card and store it
        - 2-10 inches depending on equipment and type of card
    - Data Extraction
        - Data is extracted from scan
    - Writing to new card
        - Specialized writing tools to transfer data to another card or device
    - Using cloned access badge
        - Attacker can gain access
- There is an ease of execution

- Large use in compromising physical security
- Ability to be stealthy
- How can you stop
    - Implement advanced encryption in card based auth systems
    - MFA (multi factor auth)
    - Regularly update sec protocols
    - Educate users
    - Users implement shielded wallets or sleeves
    - Monitor and audit access logs