Access Controls Objectives

* IAAA
  + Identification
  + Authentication
    - Type 1 (Knowledge)
    - Type II (Possession)
    - Type III (Biometrics)
  + Authorization
  + Accounting - accountability, tracking activities
* Single Sign On
* Access Control Models - MAC, DAC
* Access Control Methods
* Access Control Administration - central vs decentralized
* Data Emanation

Authentication and Identity Management

* Identification: Making a claim. I claim to be xxx
* Authentication allows users to support the claim of their identity. P/W, smart card, biometric means, etc
* Identity and access management
  + Services, policies, procedures for managing a digital identity provisioning
* Security controls (including management) be sure we are under legal compliance. Sarbanes oxley - accounting, auditing
  + SOC: IT dept must keep records

Credential management

* Exploits
  + MITM (man in the middle) and traffic hijacking
  + Unauthorized access
  + Privilege escalation
* Solutions - strong authentication methods. Multi factor authentications. Smart cards.
  + Certificates
  + Single sign on - gives access to all resources on the domain. Problem is "keys to the kingdom".

Core Security Requirements

* Authorization
  + Confirms that an authenticated entity has the privileges and permissions necessary
  + CRUD Operations (Create, Read, Update, Delete). Based on least privilege
  + Access Control Models
    - DAC: Discretionary Access Control
    - MAC: Mandatory Access Control
    - RBAC: Role Based Access Control
    - RuBAC: Rules Based Access Control - firewalls, filters. Follow if/then logic. If traffic is coming from xyz, then allow.
  + Examples of authorization requirements
    - Access to highly sensitive information will be restricted to users with Secret or Top Secret clearance
    - Unauthenticated users will only have read permission to public access pages
    - Only those with admin credentials will be able to modify files
* Accountability (and auditing go hand in hand)
  + Trace an action to a subject; auditing
  + Must include the following:
    - Identity of subject
    - The Action
    - Object on which the action was performed
    - Timestamp
    - Examples of accountability requirements
      * All failed logon attempts will be logged with Timestamp and source IP address
      * Audit logs should not overwrite previous events. They should append to previous entry and alert admin when space becomes limited
      * You can hash audit logs to ensure integrity
      * Audit logs must be retained for one year
* Authorization
  + Examples of authorization requirements:
    - Access to highly sensitive information will be restricted to users with Secret or Top Secret clearance
    - Unauthenticated users will only have read permission to access public pages
    - Only those with admin credentials will be able to modify files

Access Control Models: the degree of security we want our systems to have

* From the TCSEC (Trusted Computer System Evaluation Criteria - Orange Book)
  + DAC (Discretionary Access Control). Almost all client, and many server based systems, use DAC for its ease of use and sharing capabilities.
    - Security of an object is at the owner's discretion
    - Access is granted through an ACL
    - Commonly implemented in commercial products and all client based systems
    - This is an Identity based system. User account bound to you.
  + MAC (Mandatory Access Control). More secure than DAC. Used by Gov't. The heart of MAC are the use of LABELS
    - Data owners cannot grant access
    - OS makes the decision based on a security **label** system
    - Subject's label must dominate the object's label. I cant access anything above my level. I dominate my level and below.
    - Users and data are given a clearance level (confidential, secret, top secret etc)
    - Rules for access are configured by the security officer and enforced by the OS.
* Established Later
  + RBAC (Role based Access Control)
    - Used to deal with privilege/authorization creep
    - Sometimes referred to as Non-discretionary access control because the owner of an object does not control access.
    - Each role as a set of rights and permissions which cannot be changed (without security admins involvement).
    - Based on functions within an organization.

Proving your identity

* Type 1: Something you know
* Type 2: Something you have
* Type 3: Something you are (biometrics)
* Type 4: something you do
* Type 5: somewhere you are
* Type 1: Something you know
  + Passwords/Passphrases/Cognitive Password.
    - Cognitive p/w: what was your first pets name, high school.
    - This info is out there on social media
  + Best practices
    - No less than 8 characters
    - Change on a regular basis (aging)
      * Max age: 30 days
      * Min age: enforce min age so they cant keep changing their p/ws until they cycle to their old one
    - Enforce p/w history (cant reuse)
    - Consider brute force and dictionary attacks.
      * Complex p/ws can overcome this
    - Ease of cracking cognitive p/w
    - Graphic image
    - Enable clipping levels and respond accordingly.
      * Clipping levels reduce admin overhead. PRIMARY GOAL
      * Lock acct after 3 bad p/w attempts
      * How I respond to a violation of clipping levels is to prevent p/w guessing
* Type 2: Something you have (you can touch)
  + Token devices: one time password generators
    - P/W used once then no longer valid
      * Reduces vulnerability associated with sniffing passwords
      * Simple device to implement
      * Can be costly
      * Users can lose or damage
      * Two types: synchronous and asynchronous
        + Synchronous token device: RSA SecurID

Rely upon synchronizing with authentication server. Frequently time based but could be event based (1st, 2nd, login etc)

If damaged, or battery fails, must be re-synchronized.

Authentication server knows what p/w to expect based on time or event

* + - * + Asynchronous token devices: Challenge device

User logs in

Authentication returns a challenge to the user

User types challenge string into token device and presses enter

Token device returns a reply

Only that specific user's token device could respond with the expected reply

More complex than synchronous

May provide better protection against sniffing

* + Smart card: chip
    - More secure than memory cards
    - Can actually process information
    - Includes a microprocessor
    - Often integrated with PKI
    - Two types: contact and contactless
    - Attacks
      * Fault generation - manipulate environmental controls and measure errors in order to reverse engineer logic
      * Side channel attacks - measure the cards while they work
        + Differential power analysis - measure power emissions
        + Electromagnetic analysis - example frequencies emitted
      * Microprobing - using needles to vibrations to remove the outer protection on the cards circuits. Then tap into ROMS if possible or "die" ROMS to read the data
  + Memory card: easy to counterfeit
    - Holds information, does not process it. Usually not encrypted.
    - A memory card holds authentication info, usually you'll want to pair with a PIN…why?
    - A cred card or ATM card is a type of memory card, so is key/swipe card
    - Usually insecure, easily copied
  + Hardware key (house key)
  + Cryptographic key
  + Certificate
  + Cookies - when you use a new comp you get the message that the bank doesn’t recognize the computer. That is because the cookie is gone
* Type 3: Something you are
  + Biometrics
    - Static: should not significantly change over time. Bound to a users physiological traits
      * Fingerprint, hand geometry, iris, retina, etc
    - Dynamic: based on behavioral traits
      * Voice, gait, signature, keyboard cadence, etc
      * Even though these can be modified temporarily, they are very difficult to modify for any significant length of time.
    - Concerns
      * Accuracy
        + Type 1 error: false rejection - a legit user is barred from access. Caused when a system identifies too much information, this causes excessive overhead.
        + Type 2 error: false acceptance - an imposter is allowed access. This is a security threat and comes when a system doesn’t evaluate enough information
        + As FRR goes down, FAR goes up and vice versa
        + The level at which the two meet is called CER (Crossover Error Rate). The lower the number, the more accurate the system.
        + Iris scans are the most accurate
      * User acceptance
        + Many people feel biometrics are intrusive: retina scans can reveal health care information
        + Time for enrollment and verification can make users resistant
      * Cost/benefit analysis: very costly, unwieldy technology. Costs are coming down but some technologies still remain prohibitive
      * No way to revoke biometrics

Access Control Methods

* Rule-based access control: uses specific rules that indicate what can and cannot transpire between subject and object.
  + Also called non-discretionary which means they are compulsory. Purely enforced.
  + "if x then y" logic: firewalls and routers
  + Before a subject can access and object, it must meet a set of predefined rules
    - Ex/ if a user has proper clearance, and its between 9am-5pm then allow access (context-based)
  + However, it does not have to deal specifically with identity/authorization
    - May only accept email attachments 5M or less
* Constrained user interfaces: restrict user access by not allowing them to see certain data or have certain functionality (see slides)
  + Views - only allow access to certain data (canned interfaces)
  + Restricted shell - like a real shell but only with certain commands (like Cisco's non-enable mode)
  + Menu - similar but more "GUI"
  + Physically constrained interface - show only certain keys on a keypad/touchscreen - like an ATM. The difference is you are physically constrained from accessing them.
    - Hidden columns in excel
    - Front end user interfaces (no access to databases).
* Content dependent access control: access determined by the type of data. A closet with cleaning tools inside - who should have the key? A folder with accounting info inside - who should have access?
  + Example: email filters that look for specific things like "confidential", "SSN", images.
  + Web proxy servers may be content based
* Context dependent access control: system reviews a situation then makes a decision on access.
  + A firewall is a great ex; if a session is established, then allow traffic to proceed.
  + In a web proxy, allow access to certain body imagery of previous web sessions are referencing medical data, otherwise deny access.