Access Control

Ed Crowley CISSP

Spring '05

1

Topics

- Access control models
  - MAC, DAC, and NDAC
- Access control types
- Authentication Methods
  - Passwords
  - Tokens
- Identification Methods
  - Biometrics
- Passwords and attacks
- Kerberos and other SSOs
- Auditing and Monitoring
- Intrusion Detection
- Object reuse

Access Control Systems

- Specify how users, systems, and processes interact.
- Include procedures that:
  - Identify users and processes
  - Process and log access requests
  - Grant or deny access
  - Monitor system access
- Specifies what users and processes :
  - Can do
  - Can access

Access Controls

- Components could be
  - Hardware (physical) and/or
  - Software (logical).
- Pertain to both:
  - Distributed and
  - Centralized systems.
- Three possible purposes
  1. Prevent
  2. Detect
  3. Recover

Typical Goals

- Maintain confidentiality and integrity
  - Prevent unauthorized utilization, modification, or denial of service. (i.e. maintain data and system confidentiality, integrity, and availability.)
  - Provide Auditing Services
    - Users
    - Processes
    - Resources
- Maintain availability
  - Utilize appropriate fault tolerance and recovery processes.

Context

- Effective access control requires a secure physical infrastructure and a secure computer base.
- Specific goals dependent on specific environment.

Related Integrity Goals

- Internal and external data consistency.
  - Internal consistency assures that data is consistent with itself.
    - For example, changes in computer inventories are congruent with purchase orders.
  - External consistency ensures that data stored in the database is consistent with the real world.
    - For example, computer inventory records are congruent with physical computer inventories.
    - Requires a method for comparing computer and physical inventories.

Access

Access

- A specific type of interaction between a subject and an object that results in the flow of information from one to the other.

Subject

- An active entity, generally in the form of a person, process, or device, that causes information to flow among objects or changes the system state. Technically, a process/domain pair.
- *From the Aqua Book (NCSC-TG-004-88)*

Object

Object

- Passive entity that contains or receives information.
  - Access to an object potentially implies access to the information it contains.
- Examples of objects include: records, blocks, pages, segments, files, directories, directory trees, and programs, as well as bits, bytes, words, fields, processors, video displays, keyboards, clocks, printers, and network nodes.
- *From the Aqua Book (NCSC-TG-004-88)*

Planning Considerations (TVR)

- Threat
  - Any circumstance or event with the potential to cause harm...
- Vulnerability
  - A weakness in system security procedures, system design, implementation, internal controls, etc., that could be exploited to violate system security policy.
    - *From NCSC-TG-004, the Aqua Book.*

Vulnerability Sources

- Physical
- Natural
- System
- Tempest (RF)
- Human
- Many more …

Risk

- *From the Aqua Book*:

  The probability that a particular threat will exploit a particular vulnerability of the system.

Controls

- Mitigate risk.
- Reduce potential for loss.
- Provide individual accountability.
- Control implementations can be:
  - Administrative
  - Logical/technical
  - Physical

Administrative Controls

- Administrative controls include:
  - Policies and procedures
  - Security awareness training
  - Background checks and work habit checks
  - Vacation history review.

Logical and Physical Controls

- Involve the restriction of access to systems.
  - Encryption, smart cards, anti-virus software, audit trails and ACLs.
- Physical controls incorporate, file backup, guards, gates, and building security.

Control Types

- Preventative
  - Prevents harmful occurrences.
- Detective
  - Detects after harmful occurrences.
- Corrective (Recovery)
  - Restores after harmful occurrences.

Assurance Procedures

- Assure that control mechanisms correctly implement the security policy for the entire information system life cycle.
- Assurance is trust based upon evidence.

Access Control Model

- A framework that defines how subjects access objects.
- Controlling access by a subject to an object involves establishing access rules. Three common frameworks:
  - Mandatory Access Controls (MAC)
  - Discretionary Access Control (DAC)
  - Non-Discretionary Access Control aka role based (NDAC)

MAC

- Military standard.
- Subject's access to an object depends upon labels.
  - A label indicate subject's clearance and classification or sensitivity of the object.
- Requires label for every subject and object.
- Based upon rules, system makes access decisions.
- Administrator makes access rules.

DAC

- Commercial standard.
- May be user directed or identity based.
- System makes access decisions.
- Enables a resource owner to specify what subjects can access what objects.
- Often implemented as a matrix utilizing Access Control Lists (ACLs).
- Role based access control is a form of DAC.

Non-Discretionary Access Control aka Role Based Control

- Useful in high turnover areas.
- Based on the organizational security policy, a central authority determines what subjects can have access to what objects.
- Lattice based access control models are considered Non-Discretionary.
- Lattice based models utilize pairs of elements that have the least upper bound of values and the greatest lower bound.
  - Subject's role, or task, determines access.

MAC, DAC, and NDAC Summary

- Discretionary Access Control
  - User decides what objects are shared with what subjects.
- Mandatory Access Control
  - Centralized framework decides what objects are shared with what subjects.
- Non Discretionary Access Control
  - Centralized with predefined roles determining access based upon users role or task.

Access Control Types

Preventive

- Administrative
- Technical
- Physical

Detective

- Administrative
- Technical
- Physical

Preventive/Administrative

- Policies and procedures
- Pre-employment checks
- Strict hiring practices
- Employment agreements
- Friendly and unfriendly employee termination procedures
- Vacation scheduling
- Labeling of sensitive materials
- Increased supervision
- Security awareness training
- Behavior awareness
- Sign up procedures to obtain access to information systems and networks.

Preventive/Technical

- Technology enforces access control policies
- Hardware or software based.
- Biometrics, protocols, encryption, database views, and smart cards.
- Aka logical controls.

Preventive/physical

- Measures restricting physical access to sensitive resources.
  - Biometrics
  - Swipe cards
  - Security perimeter.
  - AKA guards, guns, and gates.

Detective/Administrative

- Can be applied for prevention of future security policy violations or to detect existing violations.
- Examples include:
  - Job rotation
  - Sharing of responsibilities
  - Audit reviews.

Detective/Technical

- Uses technical means to reveal security policy violations.
- Include:
  - Intrusion detection systems
  - Alarms generated from audit information

Detective/Physical

- Usually require a human to evaluate the input from sensors or cameras to determine if a real threat exists.

Identification and Authentication

- Professing an identity to a system.
  - Logon ID
  - Facilitates user accountability.
- Authentication
  - Verification that the user's claimed identity is valid.
    - User password.
- Note authentication establishes a subject's identity, does not grant access to a specific resource.

Three Authentication Criteria

- Something you know.
  - Username, password
- Something you have.
  - Token, key
- Something you are.
  - Biometrics

Two-factor Authentication

- Requires two of the three authentication factors.
  - ATM card & PIN
  - Credit Card & Signature
  - Username & password

Password Problems

- Vulnerable
- Password files must be protected.
- Inconvenient – Users forget them.
- Reputable – Users tell them to other people.

- Expensive – When users forget, enterprise has to pay people to reset password, staff help desk, investigate password compromises …

Password Issues

- Composition
- Length
- Lifetime
- Source
- Ownership
- Distribution
- Storage
- Entry
- Transmission
- Authentication period.

Password Attacks

- Brute force – Try every possible combination.
- Dictionary – Run a dictionary.
  - Brute Force and Dictionary attacks are also available in a “smart” form for quicker compromise
- Trojan horse – Capture password on system.
- Key logger – Capture all keystrokes on system.
- If password passes over a network, then protocol call analyzers will also capture them.

Password Countermeasures

- Time restrictions.
- Length restrictions.
- Limit unsuccessful logons.
- Limit concurrent connections.
- Enable auditing.
- Put last login date into banner.

Password Terms

- One time password provides maximum security.
  - Tokens can be used to facilitate one time passwords.
  - May be credit card size memory cards or smart cards.
- Static password is the same for each log-on.
- Passphrase
  - Sequence of characters that is usually longer than the allotted number for a password.
    - Converted into a virtual password.

Tokens

- Static or dynamic
- Synchronous dynamic password tokens
  - Time based e.g. secret key encryption of the system time.
- Asynchronous Dynamic password tokens
  - No time dependency
- Challenge-response tokens.
  - System generates a random challenge string and the owner enters the string into the token along with the proper PIN.

Biometrics

- Automated means of identifying and/or authenticating the identity of a person based on physiological or behavioral characteristics.
- Three performance measures
  - False Rejection Rate (FRR) -- Type I error
  - False Acceptance Rate (FAR) -- Type II error
  - Crossover Error Rate (CER) – Expressed as a percentage, false acceptance rate equals the false acceptance rate. (lower is better)

Biometric Issues

- Enrollment Time
  - Acceptable rate is 2 minutes per person
- Throughput Time
  - Acceptable rate is 10 people per minute
- Acceptability Issues
  - Privacy
  - Physical
  - Psychological

Biometric Criteria

- Fingerprints
- Retina scans
- Iris scans
- Facial scans
- Palm scans
- Hand geometry
- Voice
- Handwritten signature dynamics

41

Biometrics Summary

Advantages

- Can not be forgotten
- Lasts forever
- Makes login & authentication easier
- Possible cost advantages when compared to passwords

Disadvantages

- Relatively expensive
- Not mature
- Problematic user acceptance

Access Control Methodologies

- Centralized
  - For dial up users, Radius, CHAP, TACUS, and TACUS +
    - TACUS+ can use 2 part authentication
    - Open Radius
- Decentralized
  - Utilizes Database
- Hybrid

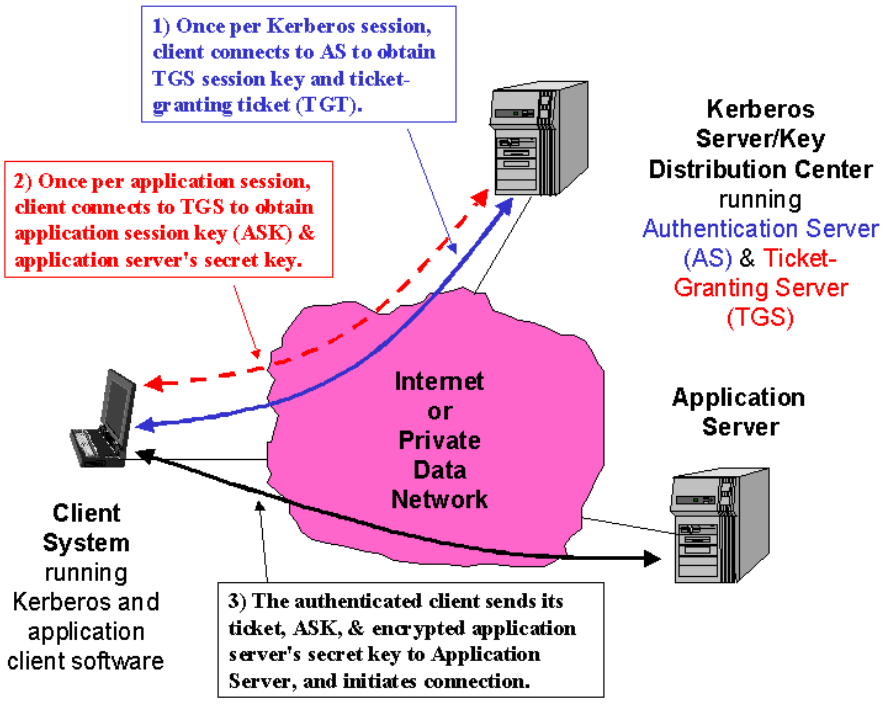
Single Sign On (SSO)

- Addresses logging on multiple times to access different resources.
- User has one password for all enterprise resources.
- Difficult to implement.
- Kerberos, SESAME, and KryptoKnight

Kerberos

- Defacto SSO standard for heterogeneous networks.
- Centralized access control methodology.
  - Utilizes symmetric key cryptography.
- Kerberos authenticates clients to other entities on a network from which a client requires services.
- Assumes that messages are not secure.
- Specifically designed to eliminate the need to transmit passwords over the network.

Kerberos Overview



Kerberos Components

- Key Distribution Center (KDC)
  - Hold all secret keys
  - Initially exchanges information with the client and server by using the secret keys
- Authentication Service (AS)
  - Authenticates network entities
- Ticket granting Service (TGS)
  - Generates temporary session keys

Kerberos Fundamentals

- KDC initially uses secret keys to exchange information with the client and server.
- KDC provides security services to principles.
  - Principles may be users or processes
- Security unit called a realm.
  - Realm is a logical grouping of resources.

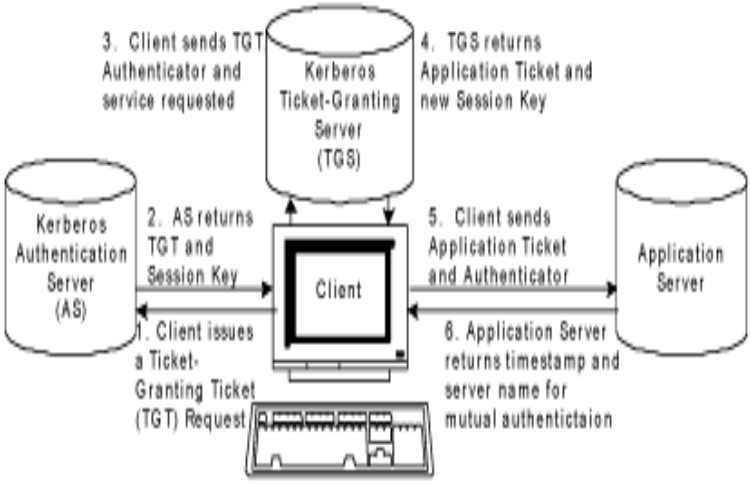
Kerberos Fundamentals

- Kerberos authenticates a client to a requested service on a server through Ticket Granting Service (TGS).
  - Issues temporary symmetric session keys for communications between:
    - Client and KDC (share a secret key)
    - Server and the KDC (share a different key)
    - Client and server.
- Communication then takes place between client and server using those temporary session keys.

Kerberos Operation

- Client-TGS Server:Initial Exchange
- Client to TGS Server:Request for Service
- TGS Server to Client: Issuing of Ticket for Service
- Client to Server Authentication: Exchange and Providing of Service

Kerberos Operation



Client-TGS Server:Initial Exchange

- On client, user enters ID and password.
- Using a one way hash, client temporarily generates the client's secret key from the password.
- Client sends a request for authentication to the TGS server using the client's ID in the clear. (Note, no password or key.)

Client-TGS Server:Initial Exchange

- If the client is in the Authentication Server database, the TGS server returns:
  - A client/TGS session key which is encrypted in the secret key of the client and
  - A ticket granting ticket (TGT) encrypted in the secret key of the TGS server.
- Because the session key is known only to the TGS server, neither the client nor any other entity can read the contents of the TGT.

Client-TGS Server:Initial Exchange

- The client decrypts the session key with its secret key and uses the session key to communicate with the TGS server.

Client to TGS Server:Request for Service

- When requesting access to a specific network service from the TGS server, the client sends two messages to the TGS server.
- One
  - The client submits the previously obtained TGT which is encrypted with the secret key of the TGS server.
- Two
  - An authenticator that is encrypted in the assigned session key.
    - The authenticator contains the client ID, a timestamp, and an optional additional session key.

TGS Server to Client: Issuing of Ticket for Service

- After receiving a valid TGT and an authenticator from the client requesting a service, the TGS server issues:
  - A ticket to the client that is encrypted in the server's secret key and
  - A client/server session key that is encrypted in the client/TGS session key.

Client to Server Authentication: Exchange and Providing of Service

- To receive service from the server the client sends the Ticket and an authenticator to the server.
- The server decrypts the message with its secret key and checks the contents.

Kerberos Problems

- All software must be kerberized.
- Time clocks must be synchronized.
- Uses UDP
- KDC is a single point of failure.

Kerberos Vulnerabilities

- Kerberos addresses confidentiality and integrity.
- Does not directly address availability.
- Kerberos servers are vulnerable to both physical attacks and attacks from malicious code.

Kerberos Vulnerabilities

- Password guessing can be used to impersonate a client.
- A client's secret key is stored temporarily on the client workstation and can be compromised as well as the session keys that are stored at the client's computer and at the servers.
- Network monitor could initiate a replay attack.

SESAME

- Secure European System for Applications in a Multivendor Environment.
- Uses public key cryptography for the distribution of secret keys.
- Provides additional access control support.
- Uses a ticket called a Privilege Attribute Certificate
- Scalable

KryptoKnight

- From IBM, KryptoKnight provides authentication, SSO, and key distribution services.

Security Domain

- Decentralized access control methodology.
- Realm of trust.
- Defines the objects a subject can access.
- Ensures that random activities do not damage system resources.

Monitoring

- IDS
- Logs
- Audit trails
- Network tools

Auditing

- Ensures that users are accountable for their actions.
- Verifies that security policies are enforced.
- Works as a deterrence to improper actions.
- Used as an investigative tool.

Intrusion Detection Systems

- Monitors system (host) or network
- Determines adherence to security policy.
- Network or host based.
- Utilizes behavior or signature based technologies.

Network based IDS

- Agents passively acquire data.
- Monitors in real time.
- Impacts network performance.

Host Based IDS

- Reviews host audit logs.
- Limited.
- Often combined with aspect of Network based IDS.

Intrusion Detection Methods

- Signature or statistical anomaly based.
- In a signature based ID, signatures or attributes which characterize an attack, are stored for reference. This data is compared with the attack signature database.
- A statistical anomaly based IDS acquires data and defines a normal usage profile.
- Relatively young technology, ID methods are expected to improve as they mature.

Access Control Issues

- The cost of access control must be commensurate with the value of the information being protected.
- Access control must offer protection from an unauthorized, unanticipated, or unintentional modification of systems or information.
- Compensating technologies include Backups, RAID, Fault Tolerance, BCP, and Insurance.

TEMPEST

- Study and control of electrical signals emitted by systems.
- If not controlled, these signals can function as covert channels.
- For PCs, normally implemented by placing system within a Faraday Cage.

Object Reuse

- Ensures that magnetic media must not have any remanence of previous data.
- Erased magnetic data can often be recovered.

Questions?