Access Control

* *The method by which systems determine whether and how to admit a users into a trusted area of the organization.*
* Discretionary Access Controls (DACs)
  + Provide the ability to share resources in a peer-to-peer configuration that allows users to control and possibly provide access to information or resources at their disposal.
  + The user can allow general, unrestricted access, or they can allow specific people or groups of people to access these resources.
* Non-discretionary Access Controls (NDACs)
  + *Managed by a central authority in the organization.*
  + Lattice-Based Access Control (LBAC)
    - Users are assigned a matrix of authorizations for particular areas of access.
    - Authorization may vary between levels, depending on the classification of authorizations that users possess for each group of information or resources.
      * Role-Based Access Controls (RBACs)
        + Associated with the duties a user performs in an organization.
      * Task-Based Access Controls (TBACs)
        + Tied to a particular chore or responsibility
    - Mandatory Access Controls (MACs)
      * Uses data classification schemes.
      * They give users and data owners limited control over access to information resources.
    - Attribute-Based Access Controls (ABACs)
      * Uses one of these attributes to regulate access to a particular set of data.

Identification

* A mechanism whereby unverified or unauthenticated entities who seek access to a resource provide a label by which they are known to the system.
  + Called an Identifier (ID) must be identified with only one entity within the security domain

Authentication

* The process of validating an unauthenticated entity’s purported identity.
  + Something you know
  + Something you have
  + Something you are.

Authorization

* *The matching of an authenticated entity to a list of information assets and corresponding access levels*
  + The list is called ACL Access Control List or Access Control Matrix
* 3 Methods
  + Authorization for each authenticated user
  + Authorization for members of a group.
  + Authorization across multiple systems.

Accountability.

* *Ensures that all actions on a system - authorized or unauthorized - can be attributed to an authenticated identity.*
* Systems logs record specific information, such as failed access attempts and systems modifications.

Biometrics

* Biometric Access Control - Relies on recognition.
* Fingerprint
* Palm Print
* Hand Geometry
* Facial Recognition using photo id
* Facial recognition using a digital camera
* Retinal print
* Iris pattern comparison.

Access Control Architecture Models

* Theoretical illustration of access control implementations
* TCSEC (Trusted Computer System Exaluation Criteria)
  + Older DoD system for assessing controls in a computer system
* ITSEC (Information Technology System Evaluation Criteria)
  + *An international set of criteria for exaluating computer systems, similar to TCSEC*
* Common Criteria (CC)
  + ISO/IEC 15408
  + Successor to TCSEC & ITSEC
  + Target of Evaluation (ToE)
  + Protection Profile
  + Security Target
  + Security Functional Requirements
  + Evaluation Assurance Levels
    - EAL1:
      * Functionally Tested
      * Confidence in operation against nonserious threats
    - EAL2
      * Structurally Tested
      * More confidence required but comparable with good business practices.
    - EAL3
      * Methodically tested and checked
      * Moderate level of security assurance.
    - EAL4
      * Methodically designed, tested and reviewed
      * Rigorous level of security assurance but still economically feasible without specialized development
    - EAL5
      * Semiformally Designed and tested
      * Certification requires specialized development above standard commercial products
    - EAL6:
      * Semiformally verified design and tested
      * Specifically designed security ToE
    - EAL7:
      * Formally verified design and tested
      * Developed for extremely high-risk situations or for high-value systems.
* Bella-LaPadula Confidentiality Model
  + State machine reference model
  + A model of an automated system that is able to manipulate its state or status over time.
* Biba Integrity Model
  + Based on the premise that higher levels of integrity are more worthy of trust than lower ones.
  + The intent is to provide access controls to ensure that objects or subjects cannot have less integrity as a result of read/write operations
* Clark-Wilson Integrity Model
  + Built upon principles of change control rather than integrity levels designed for commercial environment
  + Control Principles
    - No changes by unauthorized subjects
    - No unauthorized changes by authorized subjects
    - The maintenance of internal and external consistency
  + Elements:
    - Constrained data item CDI: Data item with protected integrity
    - Unconstrained data item: Data not controlled by Clark-Wilson; nonvalidated input or any output.
    - Integrity verification procedure IVP: Procedure that scans data and confirms its integrity.
    - Transformation procedure TP: Procedure that only allows changes to a constrained data item.
* Graham-Denning Access Control Model
  + Set of objects
  + Set of subjects
  + Set of rights.
  + 8 primitive Protection rights
    - 1. Create object
    - 2. Create Subject
    - 3. Delete object
    - 4. Delete subject
    - 5. Read access right
    - 6. Grant access right
    - 7. Delete access right
    - 8. Transfer access right
* Harrison-Ruzzo-Ullman Model (HRU)
  + *Defines a method to allow changes to access rights and the addition and removal of subjects and objects, a process that the Bell-LaPadula model does not allow.*
  + Commands
    - Create subject/create object
    - Enter right X into
    - Delete right X from
    - Destroy subject/destroy object.
* Brewer-Nash Model
  + Chinese Wall
  + Designed to prevent a conflict of interest between two parties.

Firewalls

* Concrete or masonry walls that run from the basement through the roof to prevent a fire from spreading from one section of the building to another.

Firewall Processing Modes

* Packet-Filtering Firewalls
  + Examines the header information of data packets that come into a network.
  + Typically installed at the IP layer and determines whether to deny a packet or allow a packet. (allow/forward)
  + Static Packet Filtering
    - Requires that the filtering rules be developed and installed with the firewall.
    - Common in network routers and default gateway.
  + Dynamic Packet Filtering
    - Can react to an emergent event and update or create rules to deal with the event.
  + Stateful Packet Inspection
    - Keep track of each network connection between internal and external systems using a state table.
    - State table tracks the state and context of each packet in the conversation by recording which station sent what packet and when.
* Application Layer Proxy Firewalls
  + Proxy or reverse proxy.
  + DMX
* Media Access Control Layer Firewalls
  + Filters by MAC address.
* Hybrid Firewall
  + Unified Threat Management
    - SPI,
    - Network intrusion detection and prevention,
    - Content filter
    - Spam filter
    - Malware scanner and filter
  + Next Generation Firewall

Firewall Architectures.

* Single Bastion Hosts
* Screened Host Architecture
* Screened Subnet Architecture with DMZ

Configuring and Managing Firewalls

* Best Practices for Firewalls
  + All traffic from the trusted network is not allowed out.
  + The firewall device is never directly accessible from the public network for configuration or management purposes
  + SMTP data is allowed to enter through the firewall, but is routed to a well-configured SMTP gateway to filter and route messaging traffic securely.
  + All ICMP data should be denied
    - (ping is used for hacker reconnaissance)
  + Telnet (terminal emulation) access should be blocked to all internal servers from the public networks.
  + When web services are offered outside the firewall, HTTP traffic should be blocked from internal networks through the use of some form of proxy access or DMX architecture.
    - If web server is behind the firewall, allow HTTP or HTTPS traffic (SSL) so users on the internet at large can view it.
    - Best solution is to place the web servers that contain critical data inside the network and use proxy services from a DMZ, and to to restricp web traffic bound for internal addresses.
      * This restriction can be accomplished using NAT or other stateful inspection or proxy server firewalls.
    - All other HTTP traffic should be blocked.
* Firewall Rules
  + 1. Responses to internal requests are allowed. In most firewall implementations, it is desirable to allow a response to an internal request for information.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source address** | **Source port** | **Destination address** | **Destination port** | **Action** |
| Any | Any | 10.10.10.0 | >1023 | Allow |

* 2. Firewall device is never accessible directly from the public network.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source address** | **Source port** | **Destination address** | **Destination port** | **Action** |
| Any | Any | 10.10.10.1 | Any | Deny |
| Any | Any | 10.10.10.2 | Any | Deny |
| 10.10.10.1 | Any | Any | Any | Deny |
| 10.10.10.2 | Any | Any | Any | Deny |

* 3. All traffic from the trusted network is allowed out.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source address** | **Source port** | **Destination address** | **Destination port** | **Action** |
| 10.10.10.0 | Any | Any | Any | Allow |

* 4. SMTP rule set

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source address** | **Source port** | **Destination address** | **Destination port** | **Action** |
| Any | Any | 10.10.10.0 | 25 | Allow |

* 5. All ICMP data should be denied.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source address** | **Source port** | **Destination address** | **Destination port** | **Action** |
| 10.10.10.0 | Any | Any | 7 | Allow |
| Any | Any | 10.10.10.0 | 7 | Deny |

* 6. Telnet (Terminal emulation)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source address** | **Source port** | **Destination address** | **Destination port** | **Action** |
| 10.10.10.0 | Any | 10.10.10.0 | 23 | Allow |
| Any | Any | 10.10.10.0 | 23 | Deny |

* 7a. Allows HTTP traffic to reach Web server and uses the cleanup rule (Rule 8) to prevent non-HTTP traffic from reaching the webserver. (Other than port 80)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source address** | **Source port** | **Destination address** | **Destination port** | **Action** |
| Any | Any | 10.10.10.4 | 80 | Allow |

* 7b. (Proxy)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source address** | **Source port** | **Destination address** | **Destination port** | **Action** |
| Any | Any | 10.10.10.5 | 80 | Allow |

* 7c.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source address** | **Source port** | **Destination address** | **Destination port** | **Action** |
| 10.10.10.5 | Any | 10.10.10.8 | 80 | Allow |

* 8. Cleanup rule.
  + Deny by default.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source address** | **Source port** | **Destination address** | **Destination port** | **Action** |
| Any | Any | Any | Any | Deny |

* External Filtering Firewall Inbound Interface Rule Set.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Rule #** | **Source address** | **Source port** | **Destination address** | **Destination port** | **Action** |
| 1 | 10.10.10.0 | Any | Any | Any | Deny |
| 2 | Any | Any | 10.10.10.1 | Any | Deny |
| 3 | Any | Any | 10.10.10.2 | Any | Deny |
| 4 | 10.10.10.1 | Any | Any | Any | Deny |
| 5 | 10.10.10.2 | Any | Any | Any | Deny |
| 6 | Any | Any | 10.10.10.0 | >1023 | Allow |
| 7 | Any | Any | 10.10.10.6 | 25 | Allow |
| 8 | Any | Any | 10.10.10.0 | 7 | Deny |
| 9 | Any | Any | 10.10.10.0 | 23 | Deny |
| 10 | Any | Any | 10.10.10.4 | 80 | Allow |
| 11 | Any | Any | Any | Any | Deny |

* External Filtering Firewall Outbound Interface Rule Set

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Rule #** | **Source address** | **Source port** | **Destination address** | **Destination port** | **Action** |
| 1 | 10.10.10.12 | Any | 10.10.10.0 | Any | Allow |
| 2 | Any | Any | 10.10.10.1 | Any | Deny |
| 3 | Any | Any | 10.10.10.2 | Any | Deny |
| 4 | 10.10.10.1 | Any | Any | Any | Deny |
| 5 | 10.10.10.2 | Any | Any | Any | Deny |
| 6 | 10.10.10.0 | Any | Any | Any | Allow |
| 7 | Any | Any | Any | Any | Deny |

* Internal Filtering Firewall Inbound Interface Rule Set

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Rule #** | **Source address** | **Source port** | **Destination address** | **Destination port** | **Action** |
| 1 | Any | Any | 10.10.10.3 | Any | Deny |
| 2 | Any | Any | 10.10.10.7 | Any | Deny |
| 3 | 10.10.10.3 | Any | Any | Any | Deny |
| 4 | 10.10.10.7 | Any | Any | Any | Deny |
| 5 | Any | Any | 10.10.10.0 | >1023 | Allow |
| 7 | 10.10.10.5 | Any | 10.10.10.8 | Any | Allow |
| 8 | Any | Any | Any | Any | Deny |

* Internal Filtering firewall Outbound Interface Rule Set

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Rule #** | **Source address** | **Source port** | **Destination address** | **Destination port** | **Action** |
| 1 | Any | Any | 10.10.10.3 | Any | Deny |
| 2 | Any | Any | 192.168.2.1 | Any | Deny |
| 3 | 10.10.10.3 | Any | Any | Any | Deny |
| 4 | 192.168.2.1 | Any | Any | Any | Deny |
| 5 | Any | Any | 192.168.2.0 | >1023 | Allow |
| 6 | 192.168.2.0 | Any | Any | Any | Allow |
| 7 | Any | Any | Any | Any | Deny |

Content Filtering

Remote Access

* RADIUS, Diameter, TACACS
* Kerberos
* SESAME
  + Secure European System for Applications in a Multivendor Environment.

Virtual Private Networks (VPNs)

* *A VPN is a private data network that uses the public telecommunications infrastructure to create a means for private communication via a tunneling protocol coupled with security procedures.*
* *Encapsulation of incoming and outgoing data.*
* *Encryption of incoming and outgoing data.*
* *Authentication of the remote computer and perhaps the remote user as well.*
* Transport Mode
  + The data within an IP packet is encrypted, but header info is not.
  + Eavesdroppers can still identify the destination system.
* Tunnel Mode
  + Establishes two perimeter tunnes servers to encrypt all traffic that will traverse an unsecured network.
  + Entire packet is encrypted.

Case Exercise.