

Class Eight

Topics:

- **Security Model Definition**
- **Bell-LaPadula Model**
- **Biba Integrity Model**
- **Clark-Wilson Transactional Integrity Model**
- **Overview of Network Security**

8/24/2007

Class 8

1

Formal Security Models

- Attempt to prove that a system built in a certain way cannot have its security policy violated
- Precise mathematical expression of security requirements
- A "calculus of security"
- Types of model:
 - State Machine – if you start in a secure state, you can never enter an insecure state
 - Non-interference – information cannot flow from a secure location to an insecure location

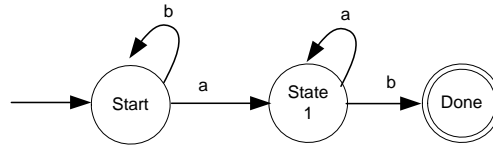
8/24/2007

Class 8

2

What's a State Machine

- An object is characterized by a state
- When something happens, state changes in a predicable way
- There is an initial state and a final accepting state
- Example:



First do "a", then do "b", then you are done

8/24/2007

Class 8

3

The Bell LaPadula Model

- Early effort at formal security model
- Focus on sensitivity of data, according to classification levels
- Influence on the Orange Book
- ***A State Machine Model***
- Properties:
 - Subjects and object have levels
 - Subjects and object interact through the dominates relationship
 - "No Write Down" (star property – object must dominate subject)
 - "No Read Up" (simple sensitivity rule – subject must dominate object)
 - Tranquillity property (labels don't change during an operation)
 - Strong Tranquillity: Labels NEVER change during an operation
 - Weak Tranquillity: Labels may change, as long as the change does not violate the security policy

8/24/2007

Class 8

4

This Policy can be expressed mathematically

- A type of set theory fits this well
- A mathematical object called a "Lattice"
- Partial ordering (better than, not better than, can't compare)
- Dominates relationship
- Requires high and low point
- Why bother?
 - Can manipulate very complex classification schemes
 - Can make mathematically provable statements about whether certain properties are true or not

8/24/2007

Class 8

5

The "Dominates" Relationship

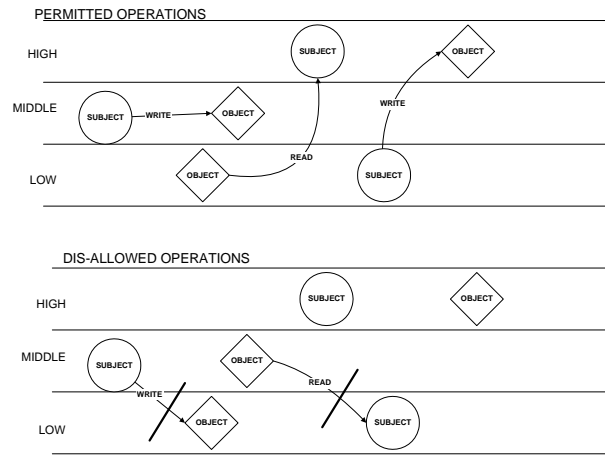
- How a lattice is ordered
- Mathematically precise way to describe relationships between user's clearance level and data's classification level
- Label "a" dominates label "b" when "b" is not more important than "a"
- Dominates may be taken to mean:
 - The security level of "a" is greater than or equal to the security level of "b"
 - The security categories of "a" are a superset of the security categories of "b"
- Examples:
 - {top secret, NATO} dominates {top secret}
 - {secret, NATO, Crypto} dominates {unclassified, NATO}
 - {unclassified, Nuclear} dominates {unclassified, Nuclear}

8/24/2007

Class 8

6

The Bell LaPadula Model



8/24/2007

Class 8

7

The Bell LaPadula Model

- Problems with Bell-LaPadula:
 - Blind write
 - Remote read (or any other sort of distributed system)
 - Trusted Subjects (system administrators)
 - "System Z" - hypothetical system which violates model by declassifying data before a read

8/24/2007

Class 8

8

The Biba Integrity Model

- "Looks like" Bell-LaPadula "upside down"
- Focus on integrity labels, rather than sensitivity
- Properties:
 - No Write Up
 - No Read Down
 - Low Water Mark - subject falls to the lowest level of information accessed
 - Possible collision if you use Biba and Bell-LaPadula
- Issues:
 - Distributed systems difficult to model
 - No provision for increasing the integrity of objects, hence over time the integrity of a system will degrade to the lowest level
 - Trusted process/Trusted subjects

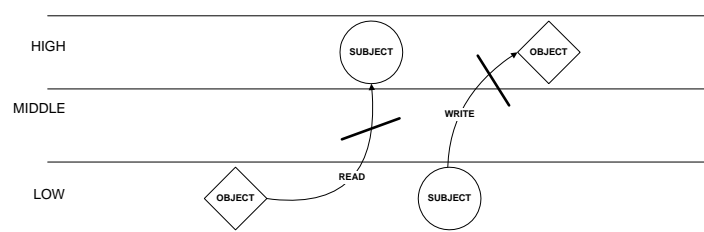
8/24/2007

Class 8

9

The Biba Model

Integrity Classification

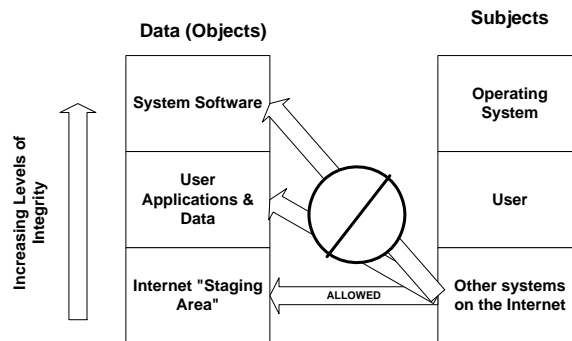


8/24/2007

Class 8

10

The Biba Model - an example



8/24/2007

Class 8

11

The Clark Wilson Model

- Attempt to define a security model based on accepted business practices for transaction processing
- Clark Wilson Model's Objects:
 - *Data items* may be either constrained (CDI) or unconstrained (UDI)
 - *Subjects, objects, and transformational procedures (TP)* included - a 3-way relationship, rather than the 2-way subject-object
 - Subjects - initiate transformational procedures
 - Transformational procedures are:
 - A sequence of atomic actions, which must be executed as a whole
 - Associate a subject with an old data item and a new one
 - The ONLY way a CDI can be changed
 - Integrity Validation Procedure (IVP) - A type of TP, which validates that a CDI possesses the proper integrity
 - Audit CDI - a special sort of CDI. Append-only, can reconstruct the sequence of TPs applied to a CDI

8/24/2007

Class 8

12

The Clark Wilson Transformational rules

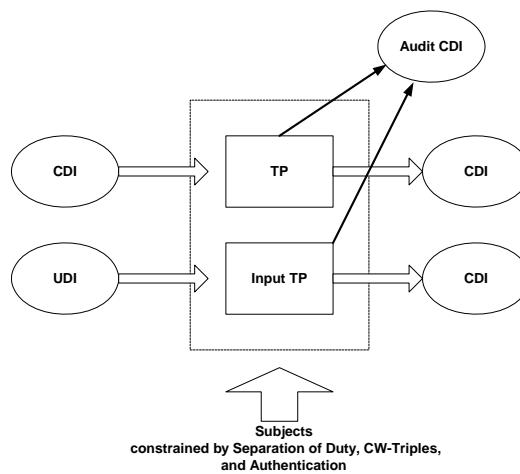
- Separation of duties when executing a TP
- Authentication of subjects by a TP
- Access Control:
 - Only certain subject can execute specified TPs
 - Only special subjects (i.e. security officers) can change the authorization to execute TPs
- Integrity Upgrade:
- Certain special TPs can convert UDIs to CDIs, through integrity enhancement

8/24/2007

Class 8

13

Clark Wilson Model Summarized



8/24/2007

Class 8

14

More Models

- Chinese Wall
 - Models conflict of interest restrictions
 - Ability to access information prohibited if prior access to a different company in same conflict of interest class
 - Information may be “sanitized” to avoid conflict
- Harrison Ruzzo Ullman (HRU)
 - How to model state changes in an access matrix
 - Models changing access rights, creating/deleting subjects and object
- Take-Grant
 - When can subjects take or grant rights to other subjects

8/24/2007

Class 8

15

An Overview of Networking

- Types of Network:
 - Local Area Network
 - Metropolitan Area Network
 - Wide Area Network
 - Common Carrier Network
- Physical Network Media
 - Wire (Twisted pair, coaxial cable, etc.)
 - Radio (point-to-point terrestrial, satellite, broadcast, etc.)
 - Fiber optic
- Types of Network Protocols:
 - Circuit Switching
 - Packet Switching
 - Broadcast/Collision-based (Ethernet, shared RF communication)

8/24/2007

Class 8

16

Network Components

- Physical/Lower Data Link Layer:
 - Modem - for dial-up (switched) phone lines
 - CSU/DSU - For dedicated lines
 - Adapter/Transceiver - For LAN connectivity
 - Media converter (fiber to copper, etc.)
 - Wireless access point (also functions at higher layers)
- "Upper" Data Link Layer
 - Switch - To connect different devices to the same LAN segment via unshared media
 - Hub - To connect different devices to the same LAN segment via shared media
 - Bridge - To link two LAN segments, optionally with different data link protocols (ethernet and token ring) but the same network layer protocol (IP)
- Network Layer:
 - Router
 - PBX, telco central office switch
- Transport/Session Layer
 - "Layer 4 Switch"
- Application Layer
 - Server (mail, Web, etc.)
 - Gateway
 - "Layer 7" switch
 - Content Engine

8/24/2007

Class 8

17

Attacks on Networks

- Passive Attacks
 - Eavesdropping
 - Traffic Analysis
- Active attacks
 - Data alteration (insertion, deletion, re-playing, etc.)
 - Impersonation
 - Spoofing
 - Repudiation
- Denial of Service Attacks
 - Malicious software
 - Protocol-based attacks (SYN attacks, etc.)
 - Malicious EMF (jamming, so-called HERF guns)
- Routing Attacks
 - Send traffic through a compromised system
 - Send traffic to "nowhere"

8/24/2007

Class 8

18

The OSI 7-layer Model and Security

Application	Applications that use network services – email, file transfer, streaming audio, etc.
Presentation	Data formatting – ASCII vs. EBCDIC, fixed vs. floating point numbers, etc.
Session	Session – Maintains end-to-end state between two end points
Transport	Establishes reliable end-to-end communication by buffering packets, ensuring they are properly sequenced, etc.
Network	Determines how to send a packet across the network, so it arrives at the proper destination
Data Link	Delivers information frames from one point to the next
Physical	Defines transmission media, modulation, signal characteristics, etc.

8/24/2007

Class 8

19

The OSI 7-layer Model and Security: Security Implications:

Application	Security issues involving application functioning. Email, secure sign on, etc.
Presentation	Session encryption (conventionally)
Session	Authenticating session end points. Preventing an intruder from inserting themselves into the session.
Transport	Ensure integrity of packet sequencing, end-to-end buffering, and flow control
Network	Ensure traffic routing is correct. Secure traffic protected from insecure or compromised links. Integrity of routing updates
Data Link	Ensure integrity of link-to-link data. Link encryption to protect data (e.g. over radio links)
Physical	Protect against wire tapping, eavesdropping, vandalism, and theft of service

8/24/2007

Class 8

20

The OSI 7-layer Model and Security: Products and Services

Application	Application proxy firewalls Secure Email Virus scanning
Presentation	SSL for session level confidentiality via encryption
Session	SSL for session level authentication and session integrity Circuit Relay Firewalls (SOCKS)
Transport	(usually included in other layers)
Network	Packet filter firewalls Secure routing protocols IPSec VPN
Data Link	Encrypting modems Encrypting wireless data transmission (WEP, WPA, etc) Most non-IPSec VPNs
Physical	Physical protection RF emission control via TEMPEST or ZONE certified equipment Spread Spectrum modulation for security purposes

8/24/2007

Class 8

21