Objectives

- Introduce the Bell LaPadula framework for confidentiality policy
- Discuss realizations of Bell LaPadula
References:

- Bell retrospective
- Bishop Chapter 5
- Anderson

Background

- Clearance levels
  - Top Secret
    - In-depth background check; highly trusted individual
  - Secret
    - Routine background check; trusted individual
  - For Official Use Only/Sensitive
    - No background check, but limited distribution; minimally trusted individuals
    - May be exempt from disclosure
  - Unclassified
    - Unlimited distribution
    - Untrusted individuals
Background

- Clearance levels are only half the story
  - They give a level of trust of the subject
- The “need to know” policy provides an orthogonal structure called compartmentalization
- A category (or compartment) is a designation related to the “need to know” policy
- Examples:
  - NUC: Nuclear
  - EUR: Europe
  - ASI: Asia

Categories and Coalitions

- Categories can be critical in complex coalitions
- The US may have two allies that do not wish to share information (perhaps Israel and Saudi Arabia)
- Policy must support:
  - Top Secret, Israel
  - Top Secret, Saudi Arabia
  - Top Secret, Israel and Saudi Arabia
  - (probably very few people in this set)
Classification Systems

• Both notions of classification induce a partial order
  – TS is more trusted than S
  – You can only see information if you are cleared to access all categories that label it
• Mathematicians Bell and LaPadula picked a lattice structure as a natural model for security levels

Partially Ordered Set

• A Set $S$ with relation $\leq$ (written $(S, \leq)$) is called a partially ordered set if $\leq$ is
  – Anti-symmetric
    • If $a \leq b$ and $b \leq a$ then $a = b$
  – Reflexive
    • For all $a$ in $S$, $a \leq a$
  – Transitive
    • For all $a$, $b$, $c$. $a \leq b$ and $b \leq c$ implies $a \leq c$
Poset examples

• Natural numbers with less than (total order)
• Sets under the subset relation (not a total order)
• Natural numbers ordered by divisibility

Lattice

• Partially ordered set \((S, \leq)\) and two operations:
  – greatest lower bound (\(\text{glb } X\))
    • Greatest element less than all elements of set \(X\)
  – least upper bound (\(\text{lub } X\))
    • Least element greater than all elements of set \(X\)
• Every lattice has
  – bottom (\(\text{glb } L\)) a least element
  – top (\(\text{lub } L\)) a greatest element
Lattice examples

- Natural numbers in an interval (0 .. n) with less than
  - Also the linear order of clearances (U ≤ FOUO ≤ S ≤ TS)
- The powerset of a set of generators under inclusion
  - E.g. Powerset of security categories {NUC, Crypto, ASI, EUR}
- The divisors of a natural number under divisibility

New lattices from old

- The opposite of a lattice is a lattice
- The product of two lattices is a lattice
- The lattice of security classifications used by Bishop is the product of the lattice of clearances and the lattice of sets generated from the categories (compartments)
Mandatory Access Control

- In a MAC system all documents are assigned labels by a set of rules
- Documents can only be relabeled under defined special circumstances
- Violations of the policy are considered very serious offenses (criminal or treasonous acts)

Bell LaPadula Context

- Pre-Anderson report policy was not to mix data of different classifications on a single system
- Still a good idea if it meets your needs
- Anderson report identified “on-line multi-level secure operation” as a goal of computer security
From Paper to Computers

- How to apply MAC to computers?
- Documents are analogous to objects in Lampson’s Access Control model
  - Every object can be labeled with a classification
- Cleared personnel are analogous to subjects
  - Every subject can be labeled with a clearance
- What about processes?

Note on subject labels

- A person is generally cleared “up to” a level
- Cross level communication requires that a person be able to interact below their level of clearance
- Subjects are given two labels:
  - The maximum level
  - The current level
- Current never exceeds maximum
- We will focus on static labelings
  - A subject will not dynamically change their current level
Bell LaPadula

- Task was to propose a theory of multi-level security
  - supported by a mechanism implemented in an Anderson-style reference monitor
  - prevents unwanted information flow

BLP model

- Adapt Lampson ACM
- Characterize system as state machine
- Characterize key actions, such as file system interaction, as transitions
  - Classify actions as
    - observation (reads)
    - alteration (writes)
    - [Aside: How to classify execute?]
- Show that only “safe states” are reachable
Simple Security

- The simple security property
  - The current level of a subject dominates the level of every object that it observes

- This property strongly analogous to paper systems
- It is referred to by the slogan “no read up”

Problem

Figure from Bell 2005
Problem

• Simple Security does not account for alterations (writes)
• Another property is needed to characterize alterations

* - Property

Figure from Bell 2005
*- Property

- In any state, if a subject has simultaneous “observe” access to object-1 and “alter” access to object-2, then level (object-1) is dominated by level (object-2).
  - From BLP 1976, Unified Exposition
- Slogan: “No write down”

Discretionary

- In addition to the MAC mechanisms of the simple security and *-properties, the BLP model also has a discretionary component
  - All accesses must be allowed by both the MAC and discretionary rules
BLP Basic Security Theorem

• If all transitions (considered individually) satisfy
  – simple security property
  – *-property
  – discretionary security property
• Then system security is preserved inductively (that is, all states reached from a “secure” state are “secure”)

Bell Retrospective

• Note: This presentation and Bishop largely follow “unified exposition”
• How did the *-property evolve?
• Where did current security level come from?
Bell Discussion

- What was the motivating example of a “trusted subject”
  - Explain the concept
  - How must the BLP model be adapted?
- Bell’s paper changes mode in Section 5
  - transitions from description of BLP to reflections on impact
  - Will return to these topics periodically

Systems Built on BLP

- BLP was a simple model
- Intent was that it could be enforced by simple mechanisms
- File system access control was the obvious choice
- Multics implemented BLP
- Unix inherited its discretionary AC from Multics
BLP in action

- Bishop describes Data General B2 UNIX system in detail
  - Treatment addresses:
    - Explicit and implicit labeling (applied to removable media)
    - Multilevel directory management
      - Consider challenges of a multilevel /tmp with traditional UNIX compilation tools
    - MAC Regions (intervals of levels)

MAC Regions

<table>
<thead>
<tr>
<th>Hierarchy levels</th>
<th>A&amp;A database, audit</th>
<th>Administrative Region</th>
</tr>
</thead>
<tbody>
<tr>
<td>VP–1</td>
<td>Site executables</td>
<td>User data and applications</td>
</tr>
<tr>
<td>VP–2</td>
<td>Trusted data</td>
<td>User Region</td>
</tr>
<tr>
<td>VP–3</td>
<td>Executables not part of the TCB</td>
<td>Virus Prevention Region</td>
</tr>
<tr>
<td>VP–4</td>
<td>Executables part of the TCB</td>
<td></td>
</tr>
<tr>
<td>VP–5</td>
<td>Reserved for future use</td>
<td></td>
</tr>
</tbody>
</table>

IMPL_HI is “maximum” (least upper bound) of all levels
IMPL_LO is “minimum” (greatest lower bound) of all levels
Slide from Bishop “05.ppt”
Discussion

• When would you choose to apply a model this restrictive?

Further Reading

• Ross Anderson’s *Security Engineering*, Chapter 7: Multilevel security
  – Standard Criticisms
  – Alternative formulations
  – Several more examples
Criticisms of Bell LaPadula

• BLP is straightforward, supports formal analysis
• Is it enough?
• McLean wrote a critical paper asserting BLP rules were insufficient

McLean’s System Z

• Proposed System Z = BLP + (request for downgrade)
• User L gets file H by first requesting that H be downgraded to L and then doing a legal BLP read
• Proposed fix: tranquility
  – Strong: Labels never change during operation
  – Weak: Labels never change in a manner that would violate a defined policy
Alternatives

- Goguen & Meseguer, 1982: Noninterference
  - Model computation as event systems
  - Interleaved or concurrent computation can produce interleaved traces
  - High actions have no effect on low actions
    - The trace of a “low trace” of a system is the same for all “high processes” that are added to the mix
  - Problem: Needs deterministic traces; does not scale to distributed systems

Nondeducibility

- Sutherland, 1986.
  - Low can not deduce anything about high with 100% certainty
  - Historically important, hopelessly weak
  - Addressed issue of nondeterminism in distributed systems
Intranstitive non-interference

• Rushby, 1992
  – Updates Goguen & Meseguer to deal with the reality that some communication may be authorized (e.g. High can interfere with low if it is mediated by crypto)

Looking forward

• Chapter 6: Integrity Policies