LATTICE-BASED ACCESS-CONTROL MODELS

Ravi Sandhu
LATTICE-BASED MODELS

- Denning's axioms
- Bell-LaPadula model (BLP)
- Biba model and its duality (or equivalence) to BLP
- Dynamic labels in BLP
DENNING'S AXIOMS

\[ \langle SC, \rightarrow, \oplus \rangle \]

- **SC**: set of security classes
- **\( \rightarrow \)**: \( \subseteq SC \times SC \) - flow relation (i.e., can-flow)
- **\( \oplus \)**: \( SC \times SC \rightarrow SC \) - class-combining operator
DENNING'S AXIOMS

\(< SC, \rightarrow, \oplus >\)

1. SC is finite
2. \(\rightarrow\) is a partial order on SC
3. SC has a lower bound L such that \(L \rightarrow A\) for all \(A \in SC\)
4. \(\oplus\) is a least upper bound (lub) operator on SC

Justification for 1 and 2 is stronger than for 3 and 4. In practice we may therefore end up with a partially ordered set (poset) rather than a lattice.
DENNING'S AXIOMS IMPLY

- SC is a universally bounded lattice
- there exists a Greatest Lower Bound (glb) operator $\otimes$ (also called meet)
- there exists a highest security class $H$
LATTICE STRUCTURES

Hierarchical Classes

reflexive and transitive edges are implied but not shown
LATTICE STRUCTURES

dominance \geq \text{can-flow}

Top Secret
Secret
Confidential
Unclassified
LATTICE STRUCTURES

\{\text{ARMY, CRYPTO}\}

Compartments and Categories

\{\text{ARMY}\}

\{\text{CRYPTO}\}

\{\}

\{\}
LATTICE STRUCTURES

{ARMY, NUCLEAR, CRYPTO}

{ARMY, NUCLEAR}  {ARMY, CRYPTO}  {NUCLEAR, CRYPTO}

{ARMY}  {NUCLEAR}  {CRYPTO}

{}
LATTICE STRUCTURES

Hierarchical Classes with Compartments

product of 2 lattices is a lattice
LATTICE STRUCTURES

Hierarchical Classes with Compartments
SMITH'S LATTICE

- With large lattices a vanishingly small fraction of the labels will actually be used
  - Smith's lattice: 4 hierarchical levels, 8 compartments, therefore
    number of possible labels = $4 \times 2^8 = 1024$
    Only 21 labels are actually used (2%)
  - Consider 16 hierarchical levels, 64 compartments which gives $10^{20}$ labels
EMBEDDING A POSET IN A LATTICE

• Smith's subset of 21 labels do form a lattice. In general, however, selecting a subset of labels from a given lattice
  • may not yield a lattice, but
  • is guaranteed to yield a partial ordering
• Given a partial ordering we can always add extra labels to make it a lattice
EMBEDDING A POSET IN A LATTICE

such embedding is always possible
BLP BASIC ASSUMPTIONS

- \( \text{SUB} = \{S_1, S_2, \ldots, S_m\} \), a fixed set of subjects
- \( \text{OBJ} = \{O_1, O_2, \ldots, O_n\} \), a fixed set of objects
- \( R \supseteq \{r, w\} \), a fixed set of rights
- \( D \), an \( m \times n \) discretionary access matrix with \( D[i,j] \subseteq R \)
- \( M \), an \( m \times n \) current access matrix with \( M[i,j] \subseteq \{r, w\} \)
BLP MODEL

• Lattice of confidentiality labels

\[ \Lambda = \{ \lambda_1, \lambda_2, \ldots, \lambda_p \} \]

• Static assignment of confidentiality labels

\[ \lambda: \text{SUB} \cup \text{OBJ} \to \Lambda \]

• \( M \), an \( m \times n \) current access matrix with

  • \( r \in M[i,j] \Rightarrow r \in D[i,j] \land \lambda(S_i) \geq \lambda(O_j) \)  
    simple security

  • \( w \in M[i,j] \Rightarrow w \in D[i,j] \land \lambda(S_i) \leq \lambda(O_j) \)  
    star-property
BLP MODEL

dominance ≥ can-flow

Top Secret
  Secret
  Confidential
  Unclassified
STAR-PROPERTY

- applies to subjects not to users
- users are trusted (must be trusted) not to disclose secret information outside of the computer system
- subjects are not trusted because they may have Trojan Horses embedded in the code they execute
- star-property prevents overt leakage of information and does not address the covert channel problem
BIBA MODEL

• Lattice of integrity labels

\[ \Omega = \{ \omega_1, \omega_2, ..., \omega_q \} \]

• Assignment of integrity labels

\[ \omega : \text{SUB} \cup \text{OBJ} \rightarrow \Omega \]

• \( M \), an \( m \times n \) current access matrix with

  • \( r \in M[i,j] \Rightarrow r \in D[i,j] \land \omega(S_i) \leq \omega(O_j) \) simple integrity
  • \( w \in M[i,j] \Rightarrow w \in D[i,j] \land \omega(S_i) \geq \omega(O_j) \) integrity confinement
EQUIVALENCE OF BLP AND BIBA

• Information flow in the Biba model is from top to bottom
• Information flow in the BLP model is from bottom to top
• Since top and bottom are relative terms, the two models are fundamentally equivalent
EQUIVALENCE OF BLP AND BIBA

HI (High Integrity) \[\Rightarrow\] Li (Low Integrity)

LI (Low Integrity) \[\Rightarrow\] HI (High Integrity)

BIBA LATTICE \[\Rightarrow\] EQUIVALENT BLP LATTICE
EQUIVALENCE OF BLP AND BIBA

\[ \text{HS (High Secrecy)} \quad \Rightarrow \quad \text{BLP LATTICE} \quad \text{EQUIVALENT BIBA LATTICE} \quad \text{LS (Low Secrecy)} \]

\[ \text{HS (High Secrecy)} \quad \Rightarrow \quad \text{LS (Low Secrecy)} \]
COMBINATION OF DISTINCT LATTICES

\[ \text{BLP} \quad \Rightarrow \quad \text{H}_S, \text{L}_I \quad \text{H}_I, \text{L}_I \quad \text{L}_S, \text{L}_I \quad \text{L}_S, \text{H}_I \]

EQUIVALENT BLP LATTICE
BLP AND BIBA

- BLP and Biba are fundamentally equivalent and interchangeable
- Lattice-based access control is a mechanism for enforcing one-way information flow, which can be applied to confidentiality or integrity goals
- We will use the BLP formulation with high confidentiality at the top of the lattice, and high integrity at the bottom
LIPNER'S LATTICE

S: System Managers
O: Audit Trail

S: System Control

S: System Programmers
O: System Code in Development

S: Application Programmers
O: Development Code and Data

S: Repair
S: Production Users
O: Production Data

O: Repair Code

O: Production Code

O: Production Code

O: System Programs

O: Tools

LEGEND
S: Subjects
O: Objects
LIPNER'S LATTICE

- Lipner's lattice uses 9 labels from a possible space of 192 labels (3 integrity levels, 2 integrity compartments, 2 confidentiality levels, and 3 confidentiality compartments)
- The single lattice shown here can be constructed directly from first principles
LIPNER'S LATTICE

- The position of the audit trail at lowest integrity demonstrates the limitation of an information flow approach to integrity.
- System control subjects are exempted from the star-property and allowed to:
  - write down (with respect to confidentiality)
  or equivalently
  - write up (with respect to integrity)
DYNAMIC LABELS IN BLP

- Tranquility (most common): $\lambda$ is static for subjects and objects
- BLP without tranquility may be secure or insecure depending upon the specific dynamics of labelling
- Noninterference can be used to prove the security of BLP with dynamic labels
DYNAMIC LABELS IN BLP

• High water mark on subjects:
  $\lambda$ is static for objects
  $\lambda$ may increase but not decrease for subjects

  Is secure and is useful

• High water mark on objects:
  $\lambda$ is static for subjects
  $\lambda$ may increase but not decrease for subjects

  Is insecure due to disappearing object signaling channel