Lattices

Appendix A
Outline

• Overview
• Definitions
• Lattices
• Examples
Overview

• Lattices used to analyze several models
  • Bell-LaPadula confidentiality model
  • Biba integrity model

• A lattice consists of a set and a relation

• Relation must partially order set
  • Relation orders some, but not all, elements of set
Sets and Relations

• $S$ set, $R$: $S \times S$ relation
  • If $a, b \in S$, and $(a, b) \in R$, write $aRb$

• Example
  • $I = \{ 1, 2, 3 \}$; $R$ is $\leq$
  • $R = \{ (1, 1), (1, 2), (1, 3), (2, 2), (2, 3), (3, 3) \}$
  • So we write $1 \leq 2$ and $3 \leq 3$ but not $3 \leq 2$
Relation Properties

• Reflexive
  • For all $a \in S$, $aRa$
  • On $I$, $\leq$ is reflexive as $1 \leq 1$, $2 \leq 2$, $3 \leq 3$

• Antisymmetric
  • For all $a, b \in S$, $aRb \land bRa \Rightarrow a = b$
  • On $I$, $\leq$ is antisymmetric as $1 \leq x$ and $x \leq 1$ means $x = 1$

• Transitive
  • For all $a, b, c \in S$, $aRb \land b Rc \Rightarrow a Rc$
  • On $I$, $\leq$ is transitive as $1 \leq 2$ and $2 \leq 3$ means $1 \leq 3$
Example

• \( \mathbb{C} \) set of complex numbers
• \( a \in \mathbb{C} \Rightarrow a = a_R + a_I i \), where \( a_R, a_I \) integers
• \( a \leq_C b \) if, and only if, \( a_R \leq b_R \) and \( a_I \leq b_I \)
• \( a \leq_C b \) is reflexive, antisymmetric, transitive
  • As \( \leq \) is over integers, and \( a_R, a_I \) are integers
Partial Ordering

• Relation $R$ orders some members of set $S$
  • If all ordered, it’s a total ordering

• Example
  • $\leq$ on integers is total ordering
  • $\leq_{\mathbb{C}}$ is partial ordering on $\mathbb{C}$
    • Neither $3+5i \leq_{\mathbb{C}} 4+2i$ nor $4+2i \leq_{\mathbb{C}} 3+5i$ holds
Upper Bounds

• For $a, b \in S$, if $u$ in $S$ with $aRu, bRu$ exists, then $u$ is an upper bound
  • A least upper bound if there is no $t \in S$ such that $aRt, bRt$, and $tRu$
• Example
  • For $1 + 5i, 2 + 4i \in \mathbb{C}$
    • Some upper bounds are $2 + 5i, 3 + 8i$, and $9 + 100i$
    • Least upper bound is $2 + 5i$
Lower Bounds

• For $a, b \in S$, if $l$ in $S$ with $lRa$, $lRb$ exists, then $l$ is a lower bound
  • A greatest lower bound if there is no $t \in S$ such that $tRa$, $tRb$, and $lRt$

• Example
  • For $1 + 5i, 2 + 4i \in \mathbb{C}$
    • Some lower bounds are $0, -1 + 2i, 1 + 1i$, and $1+4i$
    • Greatest lower bound is $1 + 4i$
Lattices

• Set $S$, relation $R$
  • $R$ is reflexive, antisymmetric, transitive on elements of $S$
  • For every $s, t \in S$, there exists a greatest lower bound under $R$
  • For every $s, t \in S$, there exists a least upper bound under $R$
Example

- $S = \{ 0, 1, 2 \}$; $R = \leq$ is a lattice
  - $R$ is clearly reflexive, antisymmetric, transitive on elements of $S$
  - Least upper bound of any two elements of $S$ is the greater of the elements
  - Greatest lower bound of any two elements of $S$ is the lesser of the elements
Arrows represent ≤; this forms a total ordering
Example

• ℂ, ≤ℂ form a lattice
  • ≤ℂ is reflexive, antisymmetric, and transitive
    • Shown earlier
  • Least upper bound for a and b:
    • c_R = max(a_R, b_R), c_I = max(a_I, b_I); then c = c_R + c_I
  • Greatest lower bound for a and b:
    • c_R = min(a_R, b_R), c_I = min(a_I, b_I); then c = c_R + c_I
Arrows represent \( \leq \mathbb{C} \)