ECS 235B Module 49
Information Flow Policies
Information Flow Policies

Information flow policies are usually:

• reflexive
  • So information can flow freely among members of a single class

• transitive
  • So if information can flow from class 1 to class 2, and from class 2 to class 3, then information can flow from class 1 to class 3
Non-Transitive Policies

• Betty is a confident of Anne
• Cathy is a confident of Betty
  • With transitivity, information flows from Anne to Betty to Cathy
• Anne confides to Betty she is having an affair with Cathy’s spouse
  • Transitivity undesirable in this case, probably
Non-Lattice Transitive Policies

• 2 faculty members co-PIs on a grant
  • Equal authority; neither can overrule the other
• Grad students report to faculty members
• Undergrads report to grad students
• Information flow relation is:
  • Reflexive and transitive
• But some elements (people) have no “least upper bound” element
  • What is it for the faculty members?
Confidentiality Policy Model

• Lattice model fails in previous 2 cases

• Generalize: policy \( I = (SC_i, \leq_i, \text{join}_i) \):
  • \( SC_i \) set of security classes
  • \( \leq_i \) ordering relation on elements of \( SC_i \)
  • \( \text{join}_i \) function to combine two elements of \( SC_i \)

• Example: Bell-LaPadula Model
  • \( SC_i \) set of security compartments
  • \( \leq_i \) ordering relation \( \text{dom} \)
  • \( \text{join}_i \) function \( \text{lub} \)
Confinement Flow Model

• \((I, O, \text{confine}, \rightarrow)\)
  • \(I = (SC_I, \leq_I, \text{join}_I)\)
  • \(O\) set of entities
  • \(\rightarrow\): \(O \times O\) with \((a, b) \in \rightarrow\) (written \(a \rightarrow b\)) iff information can flow from \(a\) to \(b\)
  • for \(a \in O\), \(\text{confine}(a) = (a_L, a_U) \in SC_I \times SC_I\) with \(a_L \leq_I a_U\)
    • Interpretation: for \(a \in O\), if \(x \leq_I a_U\), information can flow from \(x\) to \(a\), and if \(a_L \leq_I x\), information can flow from \(a\) to \(x\)
    • So \(a_L\) lowest classification of information allowed to flow out of \(a\), and \(a_U\) highest classification of information allowed to flow into \(a\)
Assumptions, etc.

• Assumes: object can change security classes
  • So, variable can take on security class of its data
• Object $x$ has security class $x$ currently
• Note transitivity *not* required
• If information can flow from $a$ to $b$, then $b$ dominates $a$ under ordering of policy $I$:
  $$(\forall a, b \in O)[ a \rightarrow b \Rightarrow a_L \leq_I b_U ]$$
Example 1

- $SC_I = \{ U, C, S, TS \}$, with $U \leq_I C$, $C \leq_I S$, and $S \leq_I TS$
- $a, b, c \in O$
  - $\text{confine}(a) = [C, C]$
  - $\text{confine}(b) = [S, S]$
  - $\text{confine}(c) = [TS, TS]$
- Secure information flows: $a \rightarrow b$, $a \rightarrow c$, $b \rightarrow c$
  - As $a_L \leq_I b_U$, $a_L \leq_I c_U$, $b_L \leq_I c_U$
  - Transitivity holds
Example 2

• $SC_I, \leq_I$ as in Example 1

• $x, y, z \in O$
  • $\text{confine}(x) = [C, C]$
  • $\text{confine}(y) = [S, S]$
  • $\text{confine}(z) = [C, TS]$

• Secure information flows: $x \rightarrow y, x \rightarrow z, y \rightarrow z, z \rightarrow x, z \rightarrow y$
  • As $x_L \leq_I y_U, x_L \leq_I z_U, y_L \leq_I z_U, z_L \leq_I x_U, z_L \leq_I y_U$
  • Transitivity does not hold
    • $y \rightarrow z$ and $z \rightarrow x$, but $y \rightarrow x$ is false, because $y_L \leq_I x_U$ is false
Transitive Non-Lattice Policies

• $Q = (S_Q, \leq_Q)$ is a quasi-ordered set when $\leq_Q$ is transitive and reflexive over $S_Q$

• How to handle information flow?
  • Define a partially ordered set containing quasi-ordered set
  • Add least upper bound, greatest lower bound to partially ordered set
  • It’s a lattice, so apply lattice rules!
In Detail ...

• \( \forall x \in S_Q: \text{ let } f(x) = \{ y \mid y \in S_Q \land y \leq_Q x \} \)
  • Define \( S_{QP} = \{ f(x) \mid x \in S_Q \} \)
  • Define \( \leq_{QP} = \{ (x, y) \mid x, y \in S_{QP} \land x \subseteq y \} \)
    • \( S_{QP} \) partially ordered set under \( \leq_{QP} \)
    • \( f \) preserves order, so \( y \leq_Q x \) iff \( f(x) \leq_{QP} f(y) \)

• Add upper, lower bounds
  • \( S_{QP}' = S_{QP} \cup \{ S_Q, \emptyset \} \)
  • Upper bound \( ub(x, y) = \{ z \mid z \in S_{QP} \land x \subseteq z \land y \subseteq z \} \)
  • Least upper bound \( lub(x, y) = \cap ub(x, y) \)
    • Lower bound, greatest lower bound defined analogously
And the Policy Is ...

- Now \((S_{QP'}, \leq_{QP})\) is lattice
- Information flow policy on quasi-ordered set emulates that of this lattice!
Nontransitive Flow Policies

• Government agency information flow policy (on next slide)
• Entities public relations officers PRO, analysts A, spymasters S
  • \textit{confine}(\text{PRO}) = [ public, analysis ]
  • \textit{confine}(\text{A}) = [ analysis, top-level ]
  • \textit{confine}(\text{S}) = [ covert, top-level ]
Information Flow

• By confinement flow model:
  • PRO ≤ A, A ≤ PRO
  • PRO ≤ S
  • A ≤ S, S ≤ A

• Data cannot flow to public relations officers; not transitive
  • S ≤ A, A ≤ PRO
  • S ≤ PRO is false
Transforming Into Lattice

- Rough idea: apply a special mapping to generate a subset of the power set of the set of classes
  - Done so this set is partially ordered
  - Means it can be transformed into a lattice

- Can show this mapping preserves ordering relation
  - So it preserves non-orderings and non-transitivity of elements corresponding to those of original set
Dual Mapping

• \( R = (SC_R, \leq_R, join_R) \) reflexive info flow policy
• \( P = (S_P, \leq_P) \) ordered set
  • Define dual mapping functions \( l_R, h_R: SC_R \rightarrow S_P \)
    • \( l_R(x) = \{ x \} \)
    • \( h_R(x) = \{ y \mid y \in SC_R \land y \leq_R x \} \)
• \( S_P \) contains subsets of \( SC_R; \leq_P \) subset relation
• Dual mapping function order preserving iff
  \[
  (\forall a, b \in SC_R)[ \ a \leq_R b \Leftrightarrow l_R(a) \leq_P h_R(b) ]
  \]
Theorem

Dual mapping from reflexive information flow policy $R$ to ordered set $P$ order-preserving

Proof sketch: all notation as before

$(\Rightarrow)$ Let $a \leq_R b$. Then $a \in l_R(a)$, $a \in h_R(b)$, so $l_R(a) \subseteq h_R(b)$, or $l_R(a) \leq_P h_R(b)$

$(\Leftarrow)$ Let $l_R(a) \leq_P h_R(b)$. Then $l_R(a) \subseteq h_R(b)$. But $l_R(a) = \{a\}$, so $a \in h_R(b)$, giving $a \leq_R b$
Information Flow Requirements

• Interpretation: let $confine(x) = [x_L, x_U]$, consider class $y$
  • Information can flow from $x$ to element of $y$ iff $x_L \leq_R y$, or $l_R(x_L) \subseteq h_R(y)$
  • Information can flow from element of $y$ to $x$ iff $y \leq_R x_U$, or $l_R(y) \subseteq h_R(x_U)$
Revisit Government Example

• Information flow policy is $R$

• Flow relationships among classes are:
  
  public $\leq_R$ public
  public $\leq_R$ analysis      analysis $\leq_R$ analysis
  public $\leq_R$ covert       covert $\leq_R$ covert
  public $\leq_R$ top-level    covert $\leq_R$ top-level
  analysis $\leq_R$ top-level  top-level $\leq_R$ top-level
Dual Mapping of $R$

- Elements $l_R$, $h_R$:
  
  $l_R$(public) = \{ public \}
  
  $h_R$(public) = \{ public \}
  
  $l_R$(analysis) = \{ analysis \}
  
  $h_R$(analysis) = \{ public, analysis \}
  
  $l_R$(covert) = \{ covert \}
  
  $h_R$(covert) = \{ public, covert \}
  
  $l_R$(top-level) = \{ top-level \}
  
  $h_R$(top-level) = \{ public, analysis, covert, top-level \}
confine

• Let $p$ be entity of type PRO, $a$ of type A, $s$ of type S
• In terms of $P$ (not $R$), we get:
  • $confine(p) = [ \{ \text{public} \}, \{ \text{public, analysis} \} ]$
  • $confine(a) = [ \{ \text{analysis} \}, \{ \text{public, analysis, covert, top-level} \} ]$
  • $confine(s) = [ \{ \text{covert} \}, \{ \text{public, analysis, covert, top-level} \} ]$
And the Flow Relations Are ...

- $p \rightarrow a$ as $l_R(p) \subseteq h_R(a)$
  - $l_R(p) = \{ \text{public} \}$
  - $h_R(a) = \{ \text{public, analysis, covert, top-level} \}$
- Similarly: $a \rightarrow p$, $p \rightarrow s$, $a \rightarrow s$, $s \rightarrow a$
- But $s \rightarrow p$ is false as $l_R(s) \not\subset h_R(p)$
  - $l_R(s) = \{ \text{covert} \}$
  - $h_R(p) = \{ \text{public, analysis} \}$
Analysis

• \((S_p, \leq_p)\) is a lattice, so it can be analyzed like a lattice policy
• Dual mapping preserves ordering, hence non-ordering and non-transitivity, of original policy
  • So results of analysis of \((S_p, \leq_p)\) can be mapped back into \((SC_R, \leq_R, \text{join}_R)\)