ECS 235B Module 19
Applying the Bell-LaPadula Model
Rule

• $\rho: R \times V \rightarrow D \times V$

• Takes a state and a request, returns a decision and a (possibly new) state

• Rule $\rho$ \textit{ssc-preserving} if for all $(r, v) \in R \times V$ and $v$ satisfying $ssc\ rel\ f$, $\rho(r, v) = (d, v')$ means that $v'$ satisfies $ssc\ rel\ f'$.
  • Similar definitions for *-property, ds-property
  • If rule meets all 3 conditions, it is \textit{security-preserving}
Unambiguous Rule Selection

• Problem: multiple rules may apply to a request in a state
  • if two rules act on a read request in state $v$ ...

• Solution: define relation $W(\omega)$ for a set of rules $\omega = \{ \rho_1, \ldots, \rho_m \}$ such that a state $(r, d, v, v') \in W(\omega)$ iff either
  • $d = i$; or
  • for exactly one integer $j$, $\rho_j(r, v) = (d, v')$

• Either request is illegal, or only one rule applies
Rules Preserving SSC

• Let $\omega$ be set of ssc-preserving rules. Let state $z_0$ satisfy simple security condition. Then $\Sigma(R, D, W(\omega), z_0)$ satisfies simple security condition.

Proof: by contradiction.

• Choose $(x, y, z) \in \Sigma(R, D, W(\omega), z_0)$ as state not satisfying simple security condition; then choose $t \in N$ such that $(x_t, y_t, z_t)$ is first appearance not meeting simple security condition.

• As $(x_t, y_t, z_t, z_{t-1}) \in W(\omega)$, there is unique rule $\rho \in \omega$ such that $\rho(x_t, z_{t-1}) = (y_t, z_t)$ and $y_t \neq i$.

• As $\rho$ ssc-preserving, and $z_{t-1}$ satisfies simple security condition, then $z_t$ meets simple security condition, contradiction.
Adding States Preserving SSC

• Let \( v = (b, m, f, h) \) satisfy simple security condition. Let \( (s, o, p) \notin b, b' = b \cup \{(s, o, p)\} \), and \( v' = (b', m, f, h) \). Then \( v' \) satisfies simple security condition iff:
  1. Either \( p = e \) or \( p = a \); or
  2. Either \( p = r \) or \( p = w \), and \( f_c(s) \text{ dom } f_o(o) \)

Proof:
  1. Immediate from definition of simple security condition and \( v' \) satisfying \( ssc_{rel f} \)
  2. \( v' \) satisfies simple security condition means \( f_s(s) \text{ dom } f_o(o) \), and for converse, \( (s, o, p) \in b' \) satisfies \( ssc_{rel f} \), so \( v' \) satisfies simple security condition
Rules, States Preserving *-Property

• Let $\omega$ be set of *-property-preserving rules and initial state $z_0$ satisfies the *-property. Then $\Sigma(R, D, W(\omega), z_0)$ satisfies *-property.

• Let $v = (b, m, f, h)$ satisfy *-property. Let $(s, o, p) \not\in b, b' = b \cup \{ (s, o, p) \}$, and $v' = (b', m, f, h)$. Then $v'$ satisfies *-property iff one of the following holds:
  1. $p = a$ and $f_o(o) \text{ dom } f_c(s)$
  2. $p = w$ and $f_c(s) = f_o(o)$
  3. $p = r$ and $f_c(s) \text{ dom } f_o(o)$
Rules, States Preserving ds-Property

• Let $\omega$ be set of ds-property-preserving rules, state $z_0$ satisfies ds-property. Then $\Sigma(R, D, W(\omega), z_0)$ satisfies ds-property

• Let $v = (b, m, f, h)$ satisfy ds-property. Let $(s, o, p) \not\in b$, $b' = b \cup \{(s, o, p)\}$, and $v' = (b', m, f, h)$. Then $v'$ satisfies ds-property iff $p \in m[s, o]$. 
Combining

• Let $\rho$ be a rule and $\rho(r, v) = (d, v')$,
  where $v = (b, m, f, h)$ and $v' = (b', m', f', h')$.

Then:

1. If $b' \subseteq b$, $f' = f$, and $v$ satisfies the simple security condition, then $v'$ satisfies the simple security condition
2. If $b' \subseteq b$, $f' = f$, and $v$ satisfies the *-property, then $v'$ satisfies the *-property
3. If $b' \subseteq b$, $m[s, o] \subseteq m'[s, o]$ for all $s \in S$ and $o \in O$, and $v$ satisfies the ds-property, then $v'$ satisfies the ds-property
Proof

1. Suppose \( v \) satisfies simple security property.
   a) \( b' \subseteq b \) and \( (s, o, r) \in b' \) implies \( (s, o, r) \in b \)
   b) \( b' \subseteq b \) and \( (s, o, w) \in b' \) implies \( (s, o, w) \in b \)
   c) So \( f'(s) \text{ dom } f_o(o) \)
   d) But \( f' = f \)
   e) Hence \( f'(s) \text{ dom } f'_o(o) \)
   f) So \( v' \) satisfies simple security condition

2, 3 proved similarly
Example Instantiation: Multics

• 11 rules affect rights:
  • set to request, release access
  • set to give, remove access to different subject
  • set to create, reclassify objects
  • set to remove objects
  • set to change subject security level

• Set of “trusted” subjects $S_T \subseteq S$
  • *-property not enforced; subjects trusted not to violate it

• $\Delta(\rho)$ domain
  • determines if components of request are valid
get-read Rule

• Request \( r = (\text{get}, s, o, r) \)
  • \( s \) gets (requests) the right to read \( o \)

• Rule is \( \rho_1(r, v) \):
  \[
  \text{if } (r \neq \Delta(\rho_1)) \text{ then } \rho_1(r, v) = (i, v); \\
  \text{else if } (f_s(s) \text{ dom } f_o(o) \text{ and } [s \in S_T \text{ or } f_c(s) \text{ dom } f_o(o)]) \text{ and } r \in m[s, o]) \text{ then } \rho_1(r, v) = (y, (b \cup \{ (s, o, r) \}, m, f, h)); \\
  \text{else } \rho_1(r, v) = (n, v);
  \]
Security of Rule

• The get-read rule preserves the simple security condition, the *-property, and the ds-property

Proof:
  • Let v satisfy all conditions. Let $\rho_1(r, v) = (d, v')$. If $v' = v$, result is trivial. So let $v' = (b \cup \{ (s_2, o, r) \}, m, f, h)$. 
Proof

• Consider the simple security condition.
  • From the choice of \( v' \), either \( b' - b = \emptyset \) or \( \{ (s_2, o, r) \} \)
  • If \( b' - b = \emptyset \), then \( \{ (s_2, o, r) \} \in b \), so \( v = v' \), proving that \( v' \) satisfies the simple security condition.
  • If \( b' - b = \{ (s_2, o, r) \} \), because the get-read rule requires that \( f_s(s) \text{ dom } f_o(o) \), an earlier result says that \( v' \) satisfies the simple security condition.
Proof

• Consider the *-property.
  • Either $s_2 \in S_T$ or $f_c(s) \text{ dom } f_o(o)$ from the definition of get-read
  • If $s_2 \in S_T$, then $s_2$ is trusted, so *-property holds by definition of trusted and $S_T$.
  • If $f_c(s) \text{ dom } f_o(o)$, an earlier result says that $v'$ satisfies the *-property.
Proof

• Consider the discretionary security property.
  • Conditions in the *get-read* rule require \( r \in m[s, o] \) and either \( b' - b = \emptyset \) or \{ (s_2, o, r) \}
  • If \( b' - b = \emptyset \), then \{ (s_2, o, r) \} \in b \), so \( v = v' \), proving that \( v' \) satisfies the simple security condition.
  • If \( b' - b = \{ (s_2, o, r) \} \), then \{ (s_2, o, r) \} \notin b \), an earlier result says that \( v' \) satisfies the ds-property.
give-read Rule

• Request \( r = (s_1, \text{give}, s_2, o, r) \)
  • \( s_1 \) gives (request to give) \( s_2 \) the (discretionary) right to read \( o \)
  • Rule: can be done if giver can alter parent of object
    • If object or parent is root of hierarchy, special authorization required

• Useful definitions
  • \( \text{root}(o) \): root object of hierarchy \( h \) containing \( o \)
  • \( \text{parent}(o) \): parent of \( o \) in \( h \) (so \( o \in h(\text{parent}(o)) \))
  • \( \text{canallow}(s, o, v) \): \( s \) specially authorized to grant access when object or parent of object is root of hierarchy
  • \( m \land m[s, o] \leftarrow r \): access control matrix \( m \) with \( r \) added to \( m[s, o] \)
give-read Rule

• Rule is \( \rho_6(r, v) \):
  
  \[
  \begin{align*}
  &\text{if } (r \neq \Delta(\rho_6)) \text{ then } \rho_6(r, v) = (i, v); \\
  &\text{else if } ([o \neq \text{root}(o) \text{ and parent}(o) \neq \text{root}(o) \text{ and parent}(o) \in b(s_1:w)] \text{ or } \\
  &\quad \text{[parent}(o) = \text{root}(o) \text{ and canallow}(s_1, o, v) ] \text{ or } \\
  &\quad \text{[o = root}(o) \text{ and canallow}(s_1, o, v) ])} \\
  &\quad \text{then } \rho_6(r, v) = (y, (b, m \land m[s_2, o] \leftarrow r, f, h)); \\
  &\text{else } \rho_1(r, v) = (n, v);
  \end{align*}
  \]
Security of Rule

• The \textit{give-read} rule preserves the simple security condition, the \textit{*}-property, and the \textit{ds}-property

\textbf{Proof:}

• Let $v$ satisfy all conditions. Let $\rho_1(r, v) = (d, v')$.
• If $v' = v$, result is trivial.
• So let $v' = (b, m[s_2, o] \leftarrow r, f, h)$.
• Then $b' = b, f' = f, m[x, y] = m'[x, y]$ for all $x \in S$ and $y \in O$ such that $x \neq s$ and $y \neq o$, and $m[s, o] \subseteq m'[s, o]$.
• And by earlier result, $v'$ satisfies the simple security condition, the \textit{*}-property, and the \textit{ds}-property.