

Homework #2

Due: February 4, 2022

Points: 100

Questions

1. (20 points) Consider the construction of the three-parent joint creation operation from the two-parent joint creation operation shown in Section 3.5.2. One paper had $cr_C(s, c) = c/R_3$ and $link_2(\mathbf{S}, \mathbf{A}_3) = \mathbf{A}_3/t \in dom(\mathbf{S})$. Why is this not sufficient to derive the three-parent joint creation operation from the two-parent joint creation operation?
2. (18 points) Given the security levels L_4, L_3, L_2, L_1 , and L_0 (ordered from highest to lowest), and the categories C_1, C_2 , and C_3 , specify what type of access (read, write, both, or neither) is allowed in each of the following situations. Assume that discretionary access controls allow anyone access unless otherwise specified.
 - (a) Tom, cleared for $(L_4, \{C_2, C_3\})$, wants to access a document classified $(L_3, \{C_2\})$.
 - (b) Annie, cleared for $(L_2, \{C_1\})$, wants to access a document classified $(L_2, \{C_2\})$.
 - (c) Katie, cleared for $(L_0, \{C_3\})$, wants to access a document classified $(L_4, \{C_1, C_3\})$.
 - (d) Paul, cleared for $(L_3, \{C_1, C_2\})$, wants to access a document classified $(L_3, \{C_1, C_2\})$.
 - (e) Judy, cleared for $(L_4, \{C_1, C_2, C_3\})$, wants to access a document classified $(L_3, \{C_1, C_2\})$.
 - (f) Sylvester, cleared for (L_0, \emptyset) , wants to access a document classified $(L_4, \{C_1\})$.
3. (25 points) Prove that the two properties of the hierarchy function (see Section 5.2.3) allow only trees and single nodes as organizations of objects.
4. (17 points) Requirements are often difficult to derive, especially when the environment in which the system will function, and the specific tasks it will perform, are unknown. Explain the problems that this causes during development of assurance.
5. (20 points) Prove Theorem 6.1 for the strict integrity policy of Biba's model.