

Homework #3

Due: May 19, 2017

Points: 100

Questions

1. (30 points) Devise an algorithm that generates an access control matrix A for any given history matrix H of the Chinese Wall model.
2. (20 points) Let $L = (S_L, \leq_L)$ be a lattice. Define:
 - (a) $S_{IL} = \{[a, b] \mid a, b \in S_L \wedge a \leq_L b\}$
 - (b) $\leq_{IL} = ([a_1, b_1], [a_2, b_2]) \mid a_1 \leq_L a_2 \wedge b_1 \leq_L b_2$
 - (c) $\text{lub}_{IL}([a_1, b_1], [a_2, b_2]) = (\text{lub}_L(a_1, a_2), \text{lub}_L(b_1, b_2))$
 - (d) $\text{glb}_{IL}([a_1, b_1], [a_2, b_2]) = (\text{glb}_L(a_1, a_2), \text{glb}_L(b_1, b_2))$Prove that the structure $IL = (S_{IL}, \leq_{IL})$ is a lattice.
3. (15 points) Extend the semantics of the information flow security mechanism in Section 17.3.1 for records (structures).
4. (15 points) In the flow certification requirement for the goto statement in Section 17.3.2.5, the set of blocks along an execution path from b_i to $IFD(b_i)$ excludes these endpoints. Why are they excluded?
5. (20 points) Section 17.6.1 says that enabling advertising libraries and the apps that invoke them execute in the same environment, with the same privileges, violates the Principle of Least Privilege (see Definition 14.2.1).
 - (a) Explain why. How might the principle be enforced?
 - (b) On the web, the protocol, host, and port in a URL define an “origin”. The *same origin policy* allows scripts in a web page to access data in a second web page only if they have the same origin. Older versions of the Android’s WebView component treated every object with the protocol `file://` (that is, the URL begins with that string) as though it had the same origin, violating the same origin policy. So any JavaScript embedded in HTML in a local file can, if loaded into WebView, access resources with the same permissions as the app. Why is this dangerous?