Assignment #3

Formal Methods for Information Security
Morteza Amini

Deadline: 10 Tir 1393

1. Study and shortly describe one of the two probabilistic models named AFM (Applied Flow Model) and PNI (Probabilistic Noninterference) for noninterference in nondeterministic systems.

2. Consider a time-sensitive RBAC model where there are some time constraints for each role in the system. A user can activate a role whenever the time constraints (defined over the role) are satisfied. Define a new RBAC model (e.g., name it RBAC₄) based on RBAC₁ model (RBAC with role hierarchies) with the above capability and also specify the login (or create session) procedure in this model.
   [Note: DO NOT copy the ideas mentioned by other researchers in their publications. Try to propose it yourself.]

3. Propose appropriate predicates formalizing “private roles” and “mutually disjoint roles” in RBAC₂.
   [Note: You can find the definitions of these concepts by a simple search]

4. In Abadi’s calculus of access control, it is mentioned that idempotency enforces complexity in the access control procedure. Hence, by receiving a request from $A \land B$ on $s$, we need to check the existing of both $A|B$ and $B|A$ in the ACL of $s$. Why?
   [Note: consider the property of idempotency on $A \land B$ principal and also the fact that $A \Rightarrow B$ iff $A = A \land B$.]

5. Disjunction operator for composing the principals ($A \lor B$) is replaced in Abadi’s calculus with implication (or group membership).
   (I) Add this operator to the the proposed logic by defining its semantics and providing the related axioms (which should be added to the proof theory of the logic).
   (II) Prove the soundness of the most important axiom.