

CS 6V81-002: Quiz 16 Solutions

March 31, 2008

1. Which of the following are security policies that an EM could enforce exactly? (circle all that apply)

- (a) programs must never terminate
- (b) programs must never attempt to access a memory address outside the process's address space**
- (c) programs must not print a user's password to the screen**
- (d) each program must either halt on all inputs or not halt on any inputs

Answer (a) is a liveness policy, so is not EM-enforceable. Answer (b) is a classic example of a safety policy, so it is EM-enforceable. Answer (c) is also safety because an EM could just check each output before committing it to see if it contains the password. Answer (d) is not enforceable because it requires knowledge of all possible runs, not just inspection of each given run in isolation.

2. Schneider recommends using which formalism to simplify the specification of a security automaton? (circle one)

- (a) Dijkstra guarded commands**
- (b) Hoare logic triples
- (c) Kripke structures
- (d) Büchi automata

3. The set Ψ of all EM-enforceable policies is closed under which operations? (circle all that apply)

- (a) conjunction (i.e., if $\mathcal{A}, \mathcal{B} \in \Psi$ then $\mathcal{A} \wedge \mathcal{B} \in \Psi$)**
- (b) disjunction (i.e., if $\mathcal{A}, \mathcal{B} \in \Psi$ then $\mathcal{A} \vee \mathcal{B} \in \Psi$)**
- (c) negation (i.e., if $\mathcal{A} \in \Psi$ then $\neg \mathcal{A} \in \Psi$)
- (d) implication (i.e., if $\mathcal{A}, \mathcal{B} \in \Psi$ then $(\mathcal{A} \Rightarrow \mathcal{B}) \in \Psi$)

The negation of a safety policy is typically a liveness policy, so the class of EM-enforceable policies is not closed under negation. Implication is defined in terms of negation ($p \Rightarrow q \equiv \neg p \vee q$), so Ψ is not closed under implication either.

4. EM's cannot enforce Real-Time Availability policies because... (circle one)

- (a) EM's can't effectively terminate automata whose input symbols model real time**
- (b) EM's can't look into the future to see if an execution will eventually satisfy the policy
- (c) violations of such policies cannot be detected until after they occur

(d) the EM would need infinite storage space to model the security state

In a real-time availability policy the security-relevant events encode the passage of real time. An EM cannot halt the passage of real time, so it cannot terminate such an automaton.

5. Schneider defines EM-enforceable predicates \mathcal{P} as those having a definition of the form $\mathcal{P}(\Pi) : (\forall \sigma \in \Pi : \hat{\mathcal{P}}(\sigma))$. If \mathcal{P} is the policy that rejects programs that write to file f , what is $\hat{\mathcal{P}}$?

$\hat{\mathcal{P}}$ is the predicate that rejects each individual execution that contains an operation that writes to file f .