

Name: _____

CIS/CSE 774 — Principles of Distributed Access Control
Exam 1
October 13, 2009

Question	Points Possible	Points Received
1	24	
2	12	
3	12	
4	12	
Total	60	

Instructions:

1. This exam is an open-book, open-notes exam.
2. **Legibility counts!** Make sure I can read (and find!) your answers.
If you need more room for an answer than that given, use the back side of the pages.
Be sure to leave a note indicating where the answer is.
3. This test should have 6 pages (including this cover sheet). Let me know **now** if your copy does not have the correct number of pages.

1. (24 points) Consider the Kripke structure $\mathcal{M} = \langle W, I, J \rangle$, where:

$$\begin{aligned} W &= \{x, y, t, w\} \\ I(q) &= \{y, t\} \\ I(r) &= \{x, t\} \\ I(s) &= \{x, w, y\} \\ J(\text{Fay}) &= \{(x, x), (y, x), (t, t), (t, w), (w, w)\} \\ J(\text{Lem}) &= \{(x, y), (x, w), (t, t), (w, x)\} \end{aligned}$$

- (a) (2 points) What is the value of $J(\text{Lem} \mid \text{Fay})$?
- (b) (2 points) What is the value of $J(\text{Fay} \mid \text{Lem})$?
- (c) (20 points) For each formula that follows, give the set of worlds in W in which it is true. You do not need to show your work.
- i. $r \supset q$
 - ii. $\neg(r \supset q)$
 - iii. *Fay* says $(r \supset q)$
 - iv. *Lem* says $(r \supset q)$

v. *Lem* says $\neg(r \supset q)$

vi. *Fay* & *Lem* says $(r \supset q)$

vii. *Fay* controls s

viii. $Lem \mid Fay \Rightarrow Fay$

ix. *Lem* says $(Lem \mid Fay \Rightarrow Fay)$

x. *Lem* controls $(Lem \mid Fay \Rightarrow Fay)$

2. (12 points) Give a formal proof of the following derivable rule:

$$\frac{Q \text{ controls } \varphi \quad P \text{ controls } (Q \text{ says } \varphi) \quad P \mid Q \text{ says } \varphi}{\varphi}$$

In addition to the inference rules and definitions of Figure 3.1, you may use *without proof* any derived rule that appears in Chapter 3 of the text, including those listed in exercises.

3. (12 points) Prove that the following proposed inference rule is *sound*:

$$\frac{P \text{ says } (R \Rightarrow Q) \quad \neg(R \Rightarrow Q)}{P \text{ says } \varphi}$$

That is, show that—for all Kripke structures \mathcal{M} , principals P, Q, R , and formulas φ —the following statement is true:

If $\mathcal{M} \models P \text{ says } (R \Rightarrow Q)$ and $\mathcal{M} \models \neg(R \Rightarrow Q)$, then $\mathcal{M} \models P \text{ says } \varphi$ as well.

4. (12 points) Show that the following proposed inference rule is *not sound*, and therefore should not be added to the logic:

$$\frac{P \text{ says } (\varphi_1 \vee \varphi_2)}{(P \text{ says } \varphi_1) \vee (P \text{ says } \varphi_2)}$$

That is, give a particular Kripke structure \mathcal{M} , formulas φ_1 and φ_2 , and principal P such that:

$$\mathcal{M} \models P \text{ says } (\varphi_1 \vee \varphi_2), \text{ but } \mathcal{M} \not\models (P \text{ says } \varphi_1) \vee (P \text{ says } \varphi_2).$$

For maximal credit, be sure to provide calculations to support your answer.