

Name: \_\_\_\_\_

CIS/CSE 774 — Principles of Distributed Access Control  
Exam 1  
October 6, 2011

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:

$$\begin{aligned} W &= \{a, b, c, g\} \\ I(r) &= \{c, g\} \\ I(s) &= \{a, b, c\} \\ I(t) &= \{b, c, g\} \\ J(\text{Sid}) &= \{(a, a), (a, b), (b, c), (g, g)\} \\ J(\text{Al}) &= \{(a, b), (b, b), (c, b), (g, a)\} \\ J(\text{Cam}) &= \{(a, a), (a, b), (b, g), (b, c), (c, g), (g, g)\} \end{aligned}$$

(a) (2 points) What is the value of  $J(\text{Sid} | \text{Al})$ ?

(b) (2 points) What is the value of  $J(\text{Al} | \text{Cam})$ ?

(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.  $r \supset (s \wedge t)$

ii.  $\neg(r \supset (s \wedge t))$

iii. *Sid* says  $r$

iv. *Sid* controls  $r$

v. *Al* says *r*

vi. *Al* controls *r*

vii. *Sid*  $\Rightarrow$  *Cam*

viii. *Al* | *Cam* says *r*

ix. *Sid* says *Al* says *r*

x. *Cam* & *Al*  $\Rightarrow$  *Sid* | *Al*

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

$$\frac{P \mid Q \text{ controls } (S \Rightarrow T) \quad R \Rightarrow Q \quad R \text{ says } (S \Rightarrow T)}{S \mid Q \Rightarrow T \mid Q}$$

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.

*Note:* Do not use more than one logical rule on a single line of the proof.

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

$$\frac{P \Rightarrow Q \& R \quad Q \text{ controls } \varphi}{P \text{ controls } \varphi}$$

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

If  $\mathcal{M} \models P \Rightarrow Q \& R$  and  $\mathcal{M} \models Q \text{ controls } \varphi$ , then  $\mathcal{M} \models P \text{ controls } \varphi$  as well.

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

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

That is, give a particular Kripke structure  $\mathcal{M}$ , formulas  $\varphi_1$  and  $\varphi_2$ , and principal  $P$  such that:

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

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