EECE 412, Fall 2007

Final Examination

Your Family name: _____

Your Given name: _____

Your student ID: _____

Name of your left neighbor: _____

Name of your right neighbor: _____

#	Points	Out of
1		10
2		7
3		10
4		15
5		16
6		9
7		8
8		9
9 (bonus)		8
TOTAL		84

Attention: If to answer any of the following questions, you need to make additional assumptions, do so but specify these assumptions explicitly writing "Additional assumptions: …"

1. **For the RBAC system defined through the following permission-to-role assignment, user-to-role assignment, and role hierarchy, fill out the pseudo access matrix on the next page.**

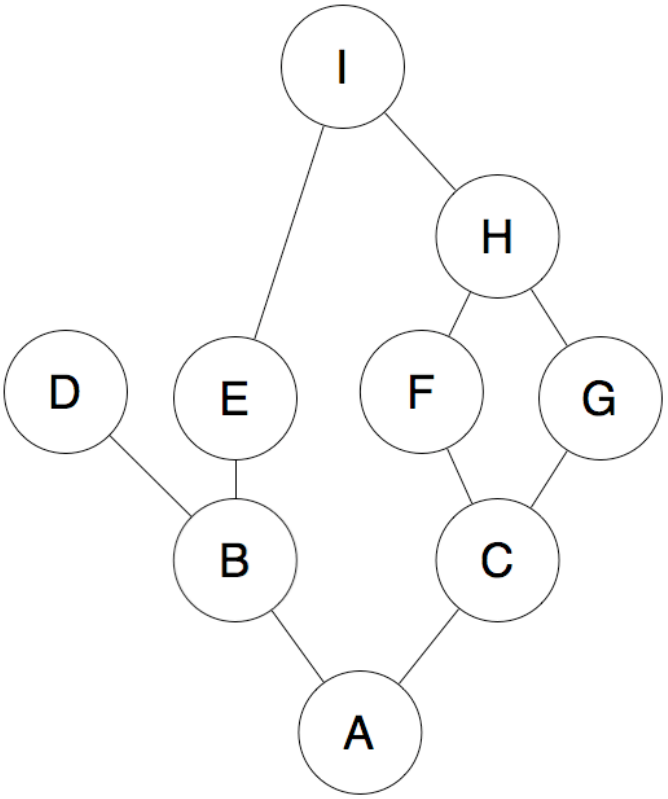
Permission to Role Assignment

		Permissions										
		P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11
Roles	A	√										
	B		√									
	C			√							√	
	D				√							√
	E					√						
	F						√					
	G							√				
	H								√		√	
	I									√		

User to Role Assignment

		Permissions									
		U1	U2	U3	U4	U5	U6	U7	U8	U9	U10
Roles	A	√									
	B		√								
	C		√	√							
	D				√						√
	E					√					
	F						√				
	G							√			
	H								√		
	I									√	

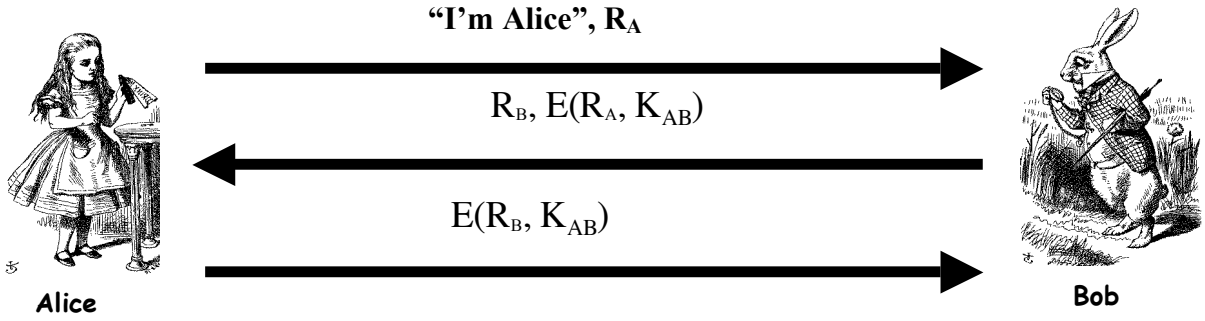
Role Hierarchy



Fill out the following pseudo-access matrix (follow the example for U1 x P1):

		Permissions										
		P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11
Users	U1	√										
	U2											
	U3											
	U4											
	U5											
	U6											
	U7											
	U8											
	U9											
	U10											

2. (7 points) Consider the following mutual authentication protocol, where K_{AB} is a shared symmetric key.



Show that Trudy can attack the protocol to convince Bob that she is Alice, where we assume that the cryptography is secure.

3. (10 points) Modify the protocol from the previous problem to prevent the attack you identified.

4. (15 points) The handout with supplementary material given to you includes

a. a short article by Bruce Schneier in Wired Magazine and
b. an abridged (by Kosta) version of the analysis of Storm Worm, which is estimated to be currently in the wild and to control a botnet of size between 1 and 5 million computers. This analysis has been published by SRI International.

You are expected to be able to scan through the handout and identify those parts of it that can help you to answer this and other questions in this exam.

Explain how the worm does the following standard functions: Reconnaissance, Attack, Communication, Command, Intelligence.

5. (16 points) Explain

1) (8 points) Which principles of designing secure systems have been violated by the owners of those computers that have been compromised by Storm Worm.

2) (8 points) How should the above mistakes have been corrected in a practical way by either owners or OS and/or application developers.

6. **(9 ppoints) Imagine that you are in charge of IT security in a small marketing company that employs 10 marketing consultants, an accountant, and a 2-person "IT department" (you are one of the two). Based on what the supplementary material describes about Storm Worm, analyze 1) the value of the assets at risk, 2) threats to these assets, and 3) threat agents associated with Storm Worm.**

   Value of the assets at risk

   Threats to these assets

   Threat agents

7. **(8 points) For each of the four types of approaches to risk management, suggest specific ways to manage the risk of Storm Worm for an organization such as UBC. Clearly identify the type of the risk management approach.**

8. **(9 points) Now, you are a network administrator at an oil company. As such, you can only make changes to network routers, switches, and firewalls. Which countermeasures would you employ in order to mitigate the threat of Storm Worm? Explain your answer.**

9. **(Bonus question) In class we identified some factors that make it especially challenging to implement "usable security". Discuss phishing in light of these two factors.**