As we've discussed, CIS634 is concerned with making sure that decisions made by a reference monitor is mathematically derived given the request policy, certifications, jurisdictions of authorities, and trust assumptions. We have talked about each of these aspects of access control individually as well as how we conduct the mathematical operations that are the backbone of an access control system. This exam asks you to put all these pieces together to form an access control system for a given scenario.

Access Control Scenario

Our old friends Alice, Bob and Eve are at work and collaborating on a new design for the Acme Corporation. Acme's primary customer, Wiley Coyote, is asking about Acme's security because he wants to ensure the new design is secure. Your job is to prove to Mr. Coyote that the system and therefore the design are indeed secure.

Alice is an engineer working for the Acme Corporation and has access to Acme's engineering files. She works on custom, new designs for Acme's customers. She has access to enter information about her work in the company's relational database. Alice also has access to accounting records in this database in order to enter her timekeeping.

Bob is the chief accounting officer for the Acme Corporation. His job is to ensure that information about all projects and all information required for accounting are entered into Acme's accounting systems in a timely and accurate manner. Therefore, Bob also has access to the all department's files in additional to accounting's files. He does not have access to the CEO's files.

Eve works for Acme as a customer representative. Eve's principal job is to interact with Acme's customers, e.g. describing Acme's products to them or getting them in touch with Technical Support, etc. In her capacity, Eve has been delegated access to information in the company's relational database that is about or for customers she represents. Of course she must also enter her time in the timekeeping system that goes into the accounting (payroll) records in the company's relational database. The company's relational database is managed by the Customer Relationship Department.

Mr. Knowsitall, Acme's CEO has complete access to the company's relational database. He has had his staff investigating Eve for a while now but has not been able to find anything concrete that would indicate she is acting nefariously, even though her current boyfriend is the Roadrunner. In any event, Acme's principal competition seems to know more than it should about Acme's business and its custom design work.

To answer Mr. Coyote's question and prove the system is secure you need to set-up an appropriate access control system as follows:

1. First, consistent with the Access Control Matrix shown on page 59 of our ***Access Control, Security, and Trust, A Logical Approach*** textbook, construct an access control matrix for Alice, Bob and Eve. There are other examples of access control matrices in our textbook, e.g. on page 92. Assume that the following relationships exist:
   - File 1 comprises the engineering files, including the engineering drawings Alice is working on for a new, custom, design which are considered proprietary.
   - File 2 are the accounting department's records including for Mr. Coyote's account with Acme, past billing, payments, project data (hours) for custom projects, etc., as well as various company data regarding assets, liabilities, revenue, etc.
   - File 3 is a relational database that stores all Acme's basic account information for its customers, e.g. Customer name, address, type of business, contacts with the customer (data, Acme rep contacting customer, product(s) discussed, type of contact e.g. phone call, letter, etc.), and past purchases including date of purchase, product(s) purchased, etc. This relational database is managed by Acme's Customer Relationship Department.
   - File 4 contains Acme's CEO, Mr. Knowsitall, personal files. For example, this include the correspondence with Acme's customers as is typically generated by accessing Acme's relational database to merge product data, accounting data used to create proposed product pricing, etc.

2. Previously, we have considered the security of discretionary access control and how delegation impacts it. Consider the access control matrix you generated and a concept of operations as discussed in our textbook ***Certified Security by Design Using Higher Order Logic*** in which Eve, as Mr. Coyote's customer rep, wants to create a new letter for Mr. Coyote. Eve wants this letter to describe the wonderful things Acme's new, custom design will do for him and how little it will cost him to get it. Derive the inference rule that controls this situation and prove it using the techniques we've learned in CIS634, e.g. HOL.

   I have given you a great deal of leeway here in setting this up. However you do set this up you need to describe it in the narrative of your report. (Hint: as usual there are a couple different ways you can approach this problem. For example, you can think of this in terms of Eve and delegation, etc. Or, you can use Kripke structures and the related mathematics, see my additional notes at the end of this exam handout.)

3. In an additional paragraph, discuss if the derived inference rule has been proven and if so is adequate to answer Mr, Coyote's concerns about security. If it is adequate to answer these concerns, you need to support that assertion. That is, you need to specifically say why it is adequate. In addition, briefly discuss if this access control system could result in Eve

providing information to Acme's competitors, which would enable them to work for or against Acme's customers.

4. (Extra Credit: Completing this question will replace 1 (one) missing project! If you completed all projects you will earn up to 50 points distributed across projects you did not earn 100% on.) In the above questions, we made no assumptions about the Acme's relational database. Now let's assume that the information in it is encrypted. Remember that Eve wants to generate what is essentially a marketing letter to Mr. Coyote. To make this simple you can also assume that, for this exam, the information in the database is encrypted text. Assume that Eve will get a key from each of the departments she needs to in order to generate the letter for Mr. Coyote, i.e. engineering and accounting. That is, for Eve to access the database, retrieve information, and to decrypt it for use in the letter to Mr Coyote, she needs to get the keys. When Eve generates these letters she acts as a rep for the departments whose information she includes in them.

   As you know from Project 7, chapter 6 in our ***Access Control, Security, and Trust, A Logical Approach*** textbook and chapter 15 in our ***Certified Security by Design Using Higher Order Logic*** textbook discuss cryptography in terms of access control. To answer this question add the required elements to the access control system you designed in questions 1 and 2 above that provide Eve with the public keys she needs. Derive and prove the associated inference rule.

Additional notes for Question 2:

Start by thinking about using your access control matrix and the set of worlds that includes $(Alice, Bob, Eve)$. Eve could generate the letter she is working on through her access to the company's relational database which includes engineering files, en, accounting records, ac, and the records of her own department, cr. That is, to generate her letter to Mr. Coyote the interpretation function is

$$I_0 : PropVar \rightarrow \mathcal{P}(W_1)$$

Using your initial access control matrix you should get something similar to,

$$I_1(Alice) = \{en, ac\}$$

$$I_1(Bob) = \{(ac, en), (ac, cr)\}$$

$$I_1(Eve) = \{cr, ac\}$$

You can move forward in the proof from here. You can also consider the video I uploaded about Kripke structures and some of the answers to Dr. Chin's Exam 1 we went over in class. You might also want to consider Example 3.4 on page 52 in our ***Access Control, Security, and Trust, A Logical Approach*** textbook. If you can follow the logic in this example it will help you think through the logic for your solution here.

As usual, your report should include a complete folder and subfolders with all sections included in a LaTex final report. You should have the following:

1. Title page
2. Abstract
3. Acknowledgements
4. Table of Contents
5. Executive Summary
6. Chapter 1: Your submission to answer Question 1 of this exam
7. Chapter 2: Your submission to answer Question 2 of this exam
8. Chapter 3: Your submission to answer Question 3 of this exam
9. Appendices of source code – as required

Good luck!