

Complete the following three exercises as described.

1. Access Control Scenario

Consider the situation in which your team has been tasked with designing an access control system that includes proxiable tickets. Users of the system should be able to use a *single signon* whereby the user authenticates himself/herself once and receives an unforgeable token referred to as a “ticket-granting ticket” that can be used to authenticate the user in subsequent operations. Refer to appropriate sections in your textbooks for additional steps taken when users access and authenticate themselves on the system.

Because you work for a very large multi-national financial corporation, the task your team has been assigned also includes a variety of requirements as follows:

- A. Initial design of a very large distributed network that includes authentication and access to non-local file systems. To demonstrate the functionality of your design you must provide the steps and items required illustrating the system’s operation when a user requests that a file be printed. The steps you include should describe artifacts such as tickets and session keys that are generated including their permanency if any. These steps and items should include the final derived inference rule required for the system to complete the request.
- B. In addition, the design of the system must include support for proxiable tickets. To demonstrate this feature you must provide the steps and items the system is required to perform and needs in its operations when a request is made requiring a proxiable ticket, including the final derived inference rule. That is, the steps you include should describe artifacts such as tickets and session keys that are generated.

For this exam complete one of the two requirements described above including a formal proof of your derived inference rule using HOL.

2. State Machines Scenario

Having completed Project 8, follow the same steps to define a garage door opener. A table of the garage door opener’s behavior is given below. To complete this you should: define the datatypes for inputs, states, and outputs proving the corresponding theorems about datatypes; define the next state and next output functions; and, prove the appropriate theorems. To keep it simple, the garage door opener can be started or stopped.

Command	Present State	Input	Output	Next State
Start	S0 (stopped)	i1	o1	Running
Stop	S1 (running)	i0	o0	Stopped

To complete this exercise define a state machine representing this simple garage door opener by developing a theory, `simpleOpenerTheory`, and following the process outlined in your textbook, *Certified Security By Design*.

3. Healthcare is an area that is fraught with challenges for information system designers, particularly with respect to access control. In general, many methods of access control exist, e.g. discretionary access control (DAC) and role-based access control (RBAC). In the paper, “Access Control for Smarter Healthcare Using Policy Spaces” the authors describe a different, exception-based access control system built on the definition of “policy spaces”. Based on the knowledge and skills you have learned in CIS634, do you believe this approach has merit? To complete your response to this question include an approximately 1-page summary in your Exam 4 report that expresses your thinking about this approach including a sentence that summarizes your conclusion.

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!