

CS 5323 SPRING 2017 EXAMINATION 1
PROF. RAVI SANDHU
DUE MONDAY FEB 27, 2017 BY 5:00pm

- **Each solution must be accompanied by the following honor code statement: I have not taken any help on this examination from anybody and have not given any help to anybody. Put this statement in a cover page to your solution. Sign it electronically by putting your name under it.**
- Each examination is to be solved by students individually. Students can access whatever material they choose but cannot discuss with **anyone**.
- It is highly unlikely that web browsing will effectively help with the solution. Anything you find on the web may well be wrong and too complicated. Spend more time and effort thinking. Don't waste all your time browsing. Some browsing is appropriate and should help craft a good answer.
- If your answer is based on material you found elsewhere, you must cite the source. No penalty for using an external source. Failure to cite a source is an act of academic misconduct.
- I am not looking for a specific or "correct" answer. I am looking for demonstration that you can think through the question and answer it coherently based on my lectures and supporting material.
- Each solution must be within the length limits provided.
- Solutions are to be submitted by email in pdf to ravi.utsa@gmail.com with subject title Exam 1.
- Text must be typed. Hand drawn figures are acceptable if appropriate but must be scanned and incorporated in submitted pdf. Figures must fit within the specified size limit for the entire answer.
- If you have doubts about the meaning of any of the questions, note that in your answer and explain how you understood the question.
- Discussion and mention of irrelevant issues will be penalized.
- Use of incorrect and sloppy English will be penalized.
- I have not thought through what my own answer to these questions might be. I am really interested in seeing what answers the class can come up with.

Answer all questions. All questions have equal weight.
Each question has maximum 1/2 page allowance for answer in 11 point font single space.
You are not required to use the full space.
A significantly shorter answer is likely to be inadequate.

1. Covert channels and side channels are definitely a concern for confidentiality. Consider a BLP lattice with low integrity (LI) at the top and high integrity (HI) at the bottom. Discuss whether or not covert channels and side channels are a concern for integrity in this context.
2. On page 71 of the Florincio et al paper authors state: "Focusing as our model does on a single site, we remind readers that the additional benefit of withstanding guessing to users who have reused their password at other sites is not captured in this model." (a) Briefly explain what this statement means, and (b) Discuss how the model can be extended to multiple sites.
3. Consider the role hierarchy in slide 15 of L4. You are told that the aggregation of read permissions in the DIR role is acceptable but the aggregation of write permissions is too risky. Outline a model that modifies RBAC to address this concern. You can bring in concepts such as MAC, DAC, ABAC, UCON, that have been covered in the lectures but only as relevant to your solution. You may go beyond techniques discussed in class.
4. Give an alternate solution to problem 3.