CS 5323 SPRING 2017 EXAMINATION 2
PROF. RAVI SANDHU
DUE WEDNESDAY MAR 29, 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 2. Please name the file, starting with lastname_firstname.
- 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. Redo Q1 OR Q2 of exam1, to give an improved answer, to the extent possible.

2. Redo Q3 of exam1, to give an improved answer, to the extent possible.

For Q3 and Q4, consider the following statement on page 73 of the paper assigned for Q2 of Exam 1:

"Hardware security modules (HSMs). A properly used HSM eliminates the risk of a hash file leaking or, equivalently, eliminates the risk of a decryption key (or backup thereof) leaking in the case that the means used to protect the information stored system side to verify passwords is reversible encryption. In such a proper HSM architecture, rather than a file of the one-way hashes of salted passwords, what is stored in each file entry is a message authentication code (MAC) computed over the corresponding password using a secret key. When a password candidate is presented for verification, the candidate plus the corresponding MAC from the system file are provided as HSM inputs. The HSM holds the system secret key used to compute the MAC; importantly, this secret key is by design never available outside the HSM. Upon receiving the (MAC, candidate password) input pair, the HSM

independently computes a MAC over the input candidate, compares it to the input MAC, and answers yes (if they agree) or no if they do not. Stealing the password hash file---inthis case a password MAC filee---is now useless to the offline attacker, because the HSM is needed to verify guesses; that is, offline attacks are no longer possible."

3. Explain what you understand from this statement.

4. Identify any one attack that this system would be vulnerable to.