COMP_SEC
Homework 3
Due on April 12, 2023, at 11:59pm
Total: 60 points

You need to submit a pdf. If you do not have a local LaTeXsetup, I suggest https://www.overleaf.com. Write the math formulas correctly using LaTeX. This homework should be fun, but violations are taken seriously.

1. This question explores different text-based password options. We constrain our discussion to 8-character passwords. Calculate the number of possible passwords in each category below:

(i) Passwords composed of any of the 96 printable ASCII characters. (ii) Passwords composed of lowercase letters or digits.

(iii) [10 points] Passwords composed of lowercase or uppercase characters, where at least one character has to be a lowercase letter and at least one character has to be an upper case letter.

2. [10 points] This question is about RBAC. Suppose there is a medical office with two divisions: surgery and radiology that treat separate sets of patients. Everyone who works at the office is entitled to have access to some basic resources. There are also nurses who are given privileges specific to their jobs, doctors (a doctor is either a surgeon or a radiologist, but not both), and there are administrators with access to financial and other information which is not necessarily accessible to medical personnel.

Design an RBAC system for the office. Your specification needs to include (i) the set of roles in the system and the role hierarchy if a hierarchy is used, (ii) what privileges are associated with each role (provide text description, it doesn't need to be specific), (iii) if an individual can be assigned more than a single role, specify when this is the case and what roles are assigned (otherwise, we assume each employee is assigned a single role according to their job description), (iv) optionally, any other constraints you think are relevant to the RBAC design (e.g., specifying constraints). Note that the medical office specification above may not be complete with respect to the exact privileges and roles and as a system designer you have a flexibility to specify it the way you think it should be set up. Explain your design choices and explicitly state any assumptions you make.

3. [10 points] A cryptographer once claimed that security mechanisms other than cryptography were unnecessary because cryptography could provide any desired level of confidentiality and integrity. Ignoring availability, either justify of refute the cryptographer's claim. Think of significant security concepts that we covered so far (e.g., access control) and perhaps your own encounters with security and use that to reason about the claim.

4. [10 points] Read the article "Messin' with Texas Deriving Mother's Maiden Names Using Public Records" by Griffith and Jakobsson from 2005 (which can be retrieved, e.g., from https://link.springer.com/content/pdf/10.1007%2F11496137_7.pdf) and answer the following questions in your own words: (a) List the different types of records and sources of information helpful in determining one's mother's maiden name that the article mentions. Explain how each of them might be useful for this task. (b) The article uses entropy as a security-related metric. Describe what entropy is (this may require additional reading if you are not familiar with the concept) and why the authors found it to be a suitable metric for their analysis. (c) State what the main conclusion of the paper was.

5. [10 points] Consider the following authentication protocol that uses conventional encryption. Alice authenticates to a server, using a shared key k_A that both of them store. When Alice wants to authenticate, she sends an authentication request to the server with her ID. The server retrieves the key k_A associated with that ID, generates a random value r, encrypts it with k_A, and sends the encrypted message $E_{k_A}(r)$ to Alice. The server decrypts it, adds 1 to r, and sends $E_{k_A}(r+1)$ back to the server. Alice decrypts the value and compares it to r. If the difference is 1, the server concludes that the person authenticating knows k_A and is therefore Alice. Otherwise, authentication fails.

Now suppose Mallory would like to violate security with the ultimate goal of being able to authenticate as Alice. Discuss whether violations of security are possible when (i) [5 points] Mallory is passive, i.e., listens to the

communication, but does not interfere with Alice's sessions or interacts with her, and (ii) [5 points] Mallory is active, i.e., can actively interfere with sessions, send messages to different parties, etc.