Name: _____

CSci 530 Midterm Exam
Fall 2022

This exam is open book and open note. You may use electronic devices to consult materials stored on the devices, but you may not use them to access material through the net, or for communication during the 100 minutes in which you are completing the exam. You have **100 minutes** to complete the exam. You must submit the completed exam through the DEN drop box for CSci530 before 115 minutes from the start of the exam. (the extra 15 minutes is to provide time to logistically upload the exam and you may not use additional time to complete the answers).

Type your answers in the exam itself using word, or if you prefer a different editor using the text version of the exam that is provided. The filled out exam document will be what you will return to me as described above. In answering the questions, please TYPE your answers rather than importing large quantities of text using cut and paste in hopes that the cut an pasted text might include an answer**. Pasted text in your responses will be ignored and you will not receive credit for words included in the pasted text.**

Be sure to include your **name in the exam document. Ideally, please rename the document to a file name that includes your name (e.g. csci530-f22-mt-FIRSTNAME-LASTNAME).**

To judge the amount of time you can spend on each question, consider that you have 100 minutes and there are 100 points across the 3 questions.

There are **100 points** in all and **3 questions.**

	Q1	Q2	Q3		Total Score
Score					

Complete the following statement:

I, **(replace with your first and last name)** attest to the fact that I completed this exam within the designated time allocated (e.g. in less than 100 minutes), that I did not have knowledge of the exam or answers in advance of its start, that I did not access external material (e.g. web sites) or use the internet during completion of the exam, and that I completed the exam on my own without accepting or providing assistance to anyone else.

Signed: (type you name here). Date: 10/7/2022.

Name: _____

1. **(30 points) Policy Management** - For each of the following methods of representing policy or implementing authorization, match the method with the **major** characteristics or relevant terms discussed in class. This is **not** a one-to-one mapping. So more than one approach may match a characteristic or term, and a single characteristic or term may also match more than one approach. We are looking for specific characteristics and terms, for which you will receive credit. If you list what is a minor characteristic, while you will not lose credit, you will not get credit either. You will lose a point if you associated a term with a characteristic that does not apply to the method. There are more blanks in the page below than actual correct answers, so you do not need to fill in all the blanks.

   You may include a comment after any of your answers to clarify your thought process. This is not required, but a reasonable justification could prevent points from being taken off if you answer incorrectly.

   1. Bell - La Padula Model
   2. Clark-Wilson Model
   3. A Restricted Proxy
   4. File permissions in Unix or Linux
   5. Generic Authorization and Access Control API (GAA-API)
   6. Passwords for Password Protected Files (we did not discuss this in class)

   a) Associated with object (this means stored and managed with the object)
      ____ ____ ____ ____ ____ ____ Comment: _____

   b) Implements a reference Monitor
      ____ ____ ____ ____ ____ ____ Comment: _____

   c) Star Property
      ____ ____ ____ ____ ____ ____ Comment: _____

   d) Integrity policy
      ____ ____ ____ ____ ____ ____ Comment: _____

   e) Mandatory Access Control
      ____ ____ ____ ____ ____ ____ Comment: _____

   f) Associated with user (or stored and managed by the user)
      ____ ____ ____ ____ ____ ____ Comment: _____

   g) Policy Decision Point
      ____ ____ ____ ____ ____ ____ Comment: _____

Name: _____

2. (35 points) Short and medium length answers

a. (10 points) Why do we include an expiration date in a public key certificate and also in a Kerberos ticket? What is the benefit of a longer lifetime (later expiration) to these credentials, and what is the benefit of a shorter lifetime? Why do we use a separate certificate status server (OCSP) with public key certificates when we do not use such a server with Kerberos?
(answer here)

b. (5 points) Explain the reason that we include a nonce or a timestamp in the message layout of cryptographic protocols. Briefly, what are the advantages and or disadvantages of each of the two approaches (timestamps or nonces).
(answer here)

c. (5 points) While a magnetic stripe credit card is technically a physical object, thus might be considered "something" you have, when used for authentication, it exhibits the same problems and operates in a manner similar to "something you know". Discuss in a couple of sentences why it is closer to something you know. Be sure to include in your discussion why attacks on such a method by an adversary is the same as an attack on "something you know".
(answer here)

d. (5 points) When connecting to a website using SSL or TLS, where do we obtain the public key belonging to the certification authority (CA) that issued a server's certificate? What would happen if we had an incorrect public key for the CA, or if we accepted the public key of a CA that is not worthy of our trust?
(answer here)

e. (10 points) End to End Encryption – End-to-end encryption depends on our trust that we are using the correct public key for the intended recipient of our message. What is the implication of relying on the intermediate transmission infrastructure (such as the What's App message service) to provide us with this public key? What kinds of attacks are enabled by such reliance?
(answer here)

Name: _____

3. (35 points) Los Angeles Unified School District

You have been hired by the Los Angeles Unified School district to advise them on changes needed in their system to prevent recurrence of the major system breach that occurred at the end of August. The greatest consequence of the August attack was the result of Ransomware, an example of malicious code that we will discuss after the mid-term exam.

I will explain here some of the background information regarding ransomware that will help you to better understand this question. Ransomware is a form of subversion, and the installation of ransomware requires the ability to make changes to programs and software already running on a system. Therefore, ransomware can only be installed within a system, if the adversary is able to gain access to modify such programs. The ransomware itself may modify files (often by encrypting them) or otherwise disable a computer system. A ransom is then demanded to provide the encryption key needed to recover the files or the system. In an alternate form of ransomware, data is read and exported from the system (called exfiltration), and the criminals demand a ransom in order to keep them from publishing the stolen data.

This question is NOT about the functioning of ransomware. Rather it is focused on technologies that we discussed in the first half of the semester that could make it more difficult for a criminal to install ransomware on LAUSD's systems, or technology that would make it more difficult for ransomware, once installed, to cause significant damage to LAUSD's operations.

a. (15 points) General Approach of the attack – Briefly describe (at least three sentences each) three different approaches by which an adversary might compromise or get into the LAUSD system. By three different approaches, please cover at least one approach that compromises or exploits lack of strong capabilities in each of the following areas a) Authentication, b) Cryptography, c) Policy or authorization.

   In the at least three sentences each (at least 9 sentences total), describe the capability that is missing or weak, the action taken by the adversary, and the impact of the action on the system.

   Note that I realize this is intentionally vague. What you should do is think about the techniques we covered in the Cryptography lecture, in the Authorization lecture, and the identity management lectures and explain how an adversary might get into the system or make changes to the system if appropriate measures were not taken.

b. (10 points) Policy and access control – Make some suggestions to LAUSD regarding the policies that should be applied for access (read, write, ability to login, etc) to systems and data maintained in the LAUSD systems. Please suggest which policy model(s) should be used to manage access to different kinds of data. (You may want to implement more than one model that applies to certain data). For each model that you recommend, explain the reason for applying the model.

c. (10 points) Authentication – A system such as that used by LAUSD has many types of users, including students, parents, teachers, district and school administrators, and system administration staff. These different classes of users may have different resources available for their use, and certainly the degree of risk associated with different classes of users may vary. For this part of the question, you are asked to discuss the various forms and technologies available for authentication as we discussed in lecture 4 and 5 and advise the district on which technologies they should deploy. Be sure to consider whether the same technologies are required for all users, or varying approaches may be applied depending on the user Explain the reasons for your recommendation. You may refer back to your discussion from parts (a) and (b) when explain your recommendations here in part (c).