Name: _____

CSci 530 Midterm Exam
Fall 2021

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-f21-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: 10/8/2021.

Name: _____

1. **(30 points) Identity and Key Management** - In the systems and mechanisms in the table below indicate which entities are authenticated (Yes/No), one or two words describing the information held by the entity which is the basis for authentication, what third party (if any) is involved, and the keys held by the entities at the end of the exchange that can be used to protect subsequent communication (i.e. the session). I have completed the first entry for you as an example of what I am looking for.

Mechanism	Client Auth	Server Auth	Information Held Client	Information Held Server	Third Party	Keys held at end	
Needham and Schroeder	Yes	Yes	Kc	Ks	KDC	Session Key	
Kerberos							
Diffie Hellman							
SSL or TLS (server cert only)							
SSH							
PGP or GPG							

Name: _____

2. (35 points) Short and medium length answers

a. (5 points) When considering common mandatory access control policies, what is the main difference between the rules applies in confidentiality policies like Bell-Lapadula, as compared with integrity policies like Biba?

(answer here)

b. (5 points) Explain the advantages of using Cipher Block Chaining instead of Block Cipher mode (ECB) when encrypting communication streams. Specifically, give one example of an attack that would be easy to accomplish when using ECB that is made more difficult through Cipher Block Chaining.

(answer here)

c. (5 points) Why is it more secure to use a dedicated device such as a smart card or USB Key like UbiKey for Key Management in contrast to storing keys on your hard disk or Thumbdrive, and performing encryption operations on your computer, smartphone, or other general-purpose processor?

(answer here)

d. (10 points) Explain how authorization occurs for file access in Linux. Be sure to distinguish the authorization that occurs for read and write calls from the authorization that occurs on file open? In what ways is this file access capability based and in what ways is it based on access control lists.

(answer here)

e. (5 points) Why is it important that we use Cryptographic Hash functions that are resistant to collisions? Specifically, provide an example of an attack that could be performed if an adversary were able to find two pieces of plaintext that yield that same hash value?

(answer here)

f. (5 points) In a couple of sentences explain how a brute force attack on a cryptographic system works, and tell me why the size of the keyspace for the system might be a useful indicator of the difficulty of such an attack.

(answer here)

Name: _____

3. (35 points) Trojan Check

This question assumes some basic knowledge of the use of TrojanCheck to enter campus. If you have not been required to use TrojanCheck (perhaps because you are a remote student), such basic information can be found in the Daily Trojan Article quoted below. Some other general information is that upon completing the Trojan Check questionnaire on their cellphone or from a PC connecting to a website, user obtain a QR code that may be printed or displayed on their phone to gain access to campus for the current day. To obtain this QR code, students first log in to the Trojan Check application or website where their vaccine, testing, and training status is checked, and they then answer the daily health questions, before the QR code is displayed or denied.

Trojan Check Bypassed - By JENNA PETERSON – Daily Trojan September 10, 2021

Every morning at campus intersections, like McClintock and Jefferson, students bustle across the street with their heads down, rapidly typing their myUSC credentials on their phone or pulling up a screenshot to display the uniquely colored QR code to USC Care Crew workers. Since returning to campus, students have been required to complete Trojan Check, the daily coronavirus compliance survey, to enter campus.

Starting with the header of the survey, "Do you currently have any of the following symptoms," students answer yes or no to a series of symptoms, such as a fever of 100 degrees or higher and loss of taste or smell. Students and on-site employees are also required to comply with a weekly coronavirus test — twice weekly for unvaccinated individuals with medical or religious vaccination exemptions — and to complete the health and safety course, "Hygiene, Health and Safety," on TrojanLearn.

But some USC students have found ways to get around the University's Trojan Check system. When opening the Trojan Check app, users are presented with two options: log in with their USC NetID or fill out a guest pass, the latter which does not require a completed coronavirus test, either of the courses, or a full vaccination dosage. While guest passes are intended for non-USC visitors, some students have used the pass when non-compliant with Trojan Check and have gained access to campus.

A student who wished to remain anonymous out of fear of disciplinary action said he found difficulty arranging time to get a coronavirus test because of long queues."I used the guest pass method," he said. "I know a lot of people use it that way because they have interviews and things like that and waiting in line for like two or three hours is a huge commitment."

In light of the student workarounds of campus coronavirus guidelines, the University looks to increase Trojan Check enforcement at campus entrance stations but are concerned about creating holdups, Chief Health Officer Dr. Sarah Van Orman said during a media briefing Sept. 2. "It's always a balance with the Trojan Check. The people at the gates don't want to create long lines and backups," Van Orman said. "They want to try to trust people so we can have a better experience, but we also know it's important that it's enforced."

A sophomore majoring in law, history and culture, who wished to remain anonymous because of concerns of disciplinary action for disregarding coronavirus protocols, used another student's pass to get onto campus the week before classes began. When trying to complete Trojan Check at the crosswalk before the entrance, she found out she was unable to get a pass. "I didn't know you needed the [health and safety module] requirement," they said. "I asked [another student that was crossing] if I could just use a screenshot of theirs because [the staff] weren't scanning. They were just kind of looking at the color."

Her plan worked and she got onto campus. However, the sophomore said USC could take further measures to prevent students from entering campus without a valid pass, such as looking at students' Trojan Check before they enter classrooms. According to school updates acquired by the Daily Trojan, the Gould School of Law and Herman Ostrow School of Dentistry implemented policies to screen each student as they enter the building, but the majority of schools rely on accurate screenings at the campus entrances. "I think [checking at classroom doors] would be easier to see whether or not the students in the class actually have a real Trojan Check, than to just check at the entrance where you could swim around everyone to not scan or just use somebody else's [pass], or the guest pass," the student said. "You have class, you have recruiting season, you have a bunch of things going on in the students' lives and having [the majority of testing] during the week during shop hours is really inconvenient," he said. "I know a lot of people who just have been skipping their weekly test just to avoid that clash."

Students with fraudulent Trojan Checks are in violation of the student conduct code regarding coronavirus public health measures and are subject to disciplinary action, Van Orman said."I'd like to think that we don't have to enforce this with any students — that if you're a Trojan, and you are a part of our community — you understand why we're doing this," Van Orman said during another media briefing Thursday. "It's really not about finding ways to subvert the system, it's finding ways to understand why those systems are in place."

Name: _____

Now, On to the exam questions:

The steps required to obtain your daily pass and to get on to campus involve processes that we have discussed in the first half of the semester: Authentication, authorization, and verification of data. I will ask you some questions about different parts of this process.

3a) Authorization Models (10 points)

When we discussed the access matrix as one way to represent policy for computer systems, I presented the use of physical keys or access cards to gain to a building as an analogy to capabilities or access control lists. Please explain which of these approaches (capabilities or access control lists) is the better description for the authorization method implemented by Trojan Check.

3b) Attack Methods (10 points)

In our discussion of authentication protocols, we discussed certain steps an adversary might use to impersonate the sender of a message if they do not have access to an encryption key. We also discussed the additions to such protocols to prevent an adversary from using this technique.

While Trojan Check is more of an authorization method, rather than authentication, it is still vulnerable to this kind of attack. Specifically, this attack is one of the methods used to bypass Trojan Check as described in the article: taking a photo or screenshot of someone else daily pass and using it to enter through the gate.

Name the type of attack as we described it in class (in the context of network protocols). What are the steps or additions that would be needed to the TrojanCheck Day Pass QR code to prevent this type of attack?

3c) Authentication (15 points)

Where does “authentication” occur or enter into the Trojan check system. Keep in mind that authentication can be performed in the context of identity management, but it can also occur in the context of “data origin” authentication. The latter component is similar to a digital signature. Hint: So, in this question I am really asking where authentication SHOULD occur within the system, and there are probably several places where it should occur.