**Name:** _____

# CSci 530 Final Exam
# Fall 2020

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 120 minutes in which you are completing the exam. You have **120 minutes** to complete the exam. You must submit the completed exam through the DEN drop box for CSci530 before 130 minutes from the start of the exam. (the extra 10 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 and 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-f20-final-FIRSTNAME-LASTNAME).**

*To judge the amount of time you can spend on each question, consider that you have 120 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 120 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: 12/7/2020.**

**Name:** _____

1. **(25 points) Matching Systems with Vulnerabilities**

   For each of the following systems or approaches to security, note the vulnerabilities that remain unaddressed. Tell me what weaknesses remain and might be exploited by an adversary to render the security of the mechanism ineffective. To put this in other terms, if an adversary can perform the action in the lettered item, would it make the technique or security provided in the numbered item ineffective.

   This is not a one-to-one mapping; more than one system may suffer from a vulnerability or weakness We are looking for specific matches for which you will receive credit. If you list a match that we are not looking for, but which is still correct, while you will not lose credit, you will not get credit either. You will lose a point if you associated a system a vulnerability that does not exist. There are more blanks in the page below than actual correct answers, so you do not need to fill in all the blanks.

   1. Smartcards
   2. Digital Signatures
   3. Diffie Hellman Key Exchange
   4. The Domain Name System (traditional, NOT DNSSEC)
   5. Host Based Intrusion Detection
   6. Kerberos
   7. Host Based Firewalls
   8. Trusted Computing

[Type the corresponding numbers above, separated by commas following the lettered entries below]

a) Modification of returned data:

b) Man in the Middle attack:

c) System or end-point Subversion:

d) Worm:

e) Stolen Credentials:

f) Phishing or password guessing:

**Name:** _____

2. (40 points) Short and medium length answers

a. Attestation – What is the meaning of attestation in trusted computing? How is attestation implemented / accomplished by the Trusted Platform Module (TPM). In answering the second part of this question, please note that there are multiple steps that occur at different times. Do not just describe the final step. (10 points)
**(type your answer here)**

b. IPSec Authentication – Explain how authentication for IPSec in transport mode is fundamentally different from authentication of connections through HTTPS (SSL or TLS) and also how it is different from authentication performed by an application using a method like Kerberos. I am **not** concerned with the differences in the protocols used, but rather in the fundamental differences in what we know once the authentication steps are completed. (10 points)
**(type your answer here)**

c. How is Secure DNS (i.e. DNSSEC) similar to public key infrastructure used by SSL and TLS. What entities or components in DNSSEC corresponded to the Certification Authority (CA) and to certificates in SSL/TLS. (10 points)
**(type your answer here)**

d. List some of the advantages of a network-based intrusion detection system over a monolithic intrusion detection system located solely on the end-system that is being protected. (10 points)
**(type your answer here)**

**Name:** _____

3. (35 points) Impact of the pandemic on security

As a result of the pandemic, more and more employees (and students, and faculty) are working from home than ever before. This change in the location of our work creates significant changes to computer security technologies. Many of the assumptions we have made in the past no longer apply, and this changes the effectiveness of various security techniques and technologies. In this question you are asked to comment on some of these changes, and to suggest approaches to mitigate the impact these changes have on security.

a. Containment – In the second lecture following the mid-term exam we discussed the placement of data in systems, and I used the term containment architecture to describe the relationship of the different protection domains in a system, and the placement of different kinds of data in those domains relative to the locations from which different classes of users required access.

   Discuss how increased instances of work from home has changed the boundaries of the containment architecture for many organizations. Discuss also the technologies that are used to provide isolation / separation of protection domains both prior to the pandemic, and during the pandemic when more employees work from home.

   Are there any organizational steps and guidelines (company policies) that could be applied to ensure that the containment architecture for the organization when employees work from home is as close as possible to that when employees worked from the office? (10 points)
   **(type your answer here)**

b. Discuss some of the difficulties for corporate intrusion detection system when applied to systems running in the work-from-home configuration. (5 points)
   **(type your answer here)**

c. Discuss the potential use of trusted computing technologies (including use of a Trusted Platform Module (TPM) to ensure that corporate information is only accessed and processed in accordance with company policy even when applications are running in an employee's home environment. Explain how your approach would prevent an adversary from accessing such data even though subversion (virus, trojan horses) of applications on the employee's computer system. (20 points)
   **(type your answer here)**