CSci 530 Final 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 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-f22-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**.

<table>
<thead>
<tr>
<th>Q1</th>
<th>Q2</th>
<th>Q3</th>
<th>Total Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Score</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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: 12/12/2022.**
1. (25 points) Fill in the Blanks

a. ____________ enables the use of separate memory addresses for different ____________ running on a computer, preventing reads or writes across protection domains.

b. A Trusted Platform Module manages at least two encryption keys, the ____________ Key used to sign platform measurements, and the ____________ used to encrypt other keys which are themselves used to protect data.

c. ____________ attacks are a class of attacks that rely on manipulation of human behavior.

d. For IPSec, data confidentiality is provided by the ______ packet header, data integrity is provided by the ______ and ______ packet headers, and Key management is provided by ________________.

e. Traditional firewalls perform ________________ where individual messages are screened and forwarded from subnet to another only if they match the firewall’s policy rules. In a variant of this technique called ________________, the rules are modified dynamically when outbound connections are established.

f. IPSec's ________________ (two words) provides service similar to that of a Virtual Private Network, while ________________ (two words) supports the secure transport of packets between the actual communicating endpoints (computers).

g. The three main classes of malicious code are ____________, ____________, and ____________.

h. In the traditional domain name system, ________________ involves sending incorrect data to an intermediate name server expecting that name server to provide the incorrect data in response to subsequent queries.

i. The ________________ (3 words) is the combination of all the parts of a system that if compromised would result in a system that does not correctly enforce a security policy.

j. ________________ is the use of knowledge about the existence of communication to draw conclusions, without knowledge of the specific content of the communication.
k. A ______________ exists when tools are created or an adversary learns how to exploit a weakness in a program to allow the violation of the policies of a system.

l. In an intrusion detection system, the main approaches to detecting attacks are ___________, ____________, and ____________. (note that there may be more than one name for a particular approach, in which case you will get credit for either name, but to get 3 points, you must list the names of three different approaches).

m. When protecting critical infrastructure (cyber-physical systems), __________ and __________ are often more important than confidentiality.

2. (50 points) Short and medium length answers

a. **Trusted Platform Module (TPM)** – When using a trusted platform module, what does it mean to "extend the PCR", and in what situations do we extend it (the PCR). Explain how this allows us to attest to the identity of the entire software stack from firmware through an application. Specifically, explain why the subversion of any layer of software does not allow the subverted software to spoof (impersonate) the checksum of the software it loads in the next layer. (15 points)

(type your answer here)

b. **DNS Security** – In DNSSec, which two resource record types (together in combination) create the equivalent of a public key certificate that binds the name of a subdomain (zone) to the public zone signing key (which is then used to verify signatures on the resource records from the subdomain’s zone). (10 points) and how is this different from the validation of traditional SSL/TLS certificates that are validated using the public key of any CA whose certificate has been accepted/downloaded into a web browser. (5 points)

[that is 15 points total for this question]

(type your answer here)

c. **Isolation and Containment** – Describe (and name) at least four different techniques that provide isolation and/or containment within a computer system or network. For each of the techniques that you listed, state the two entities or protection domains that are separated or protected from one another. If the protection is one-way only (i.e. not one another), that is acceptable, but tell me the two entities or domains and which entity is protected. (20 points)

(type your answer here)

3. (25 points) Crypto-Currency Exchanges

There have been many recent attacks on cryptocurrency exchanges. As a cryptocurrency “investor” you want to be certain that the owners of an exchange are not able to walk off with your cryptocurrency, and also make sure that hackers breaking into the exchange, or your laptop or cellphone are also unable to steal funds from your accounts.
To get you started with your analysis, I provide some basic information about how cryptocurrencies work. With cryptocurrencies (whether bitcoin, etherium, dogecoin, or FTT (the FTX Tokens), or others), the balance of your account (in coins or fractional coins) is stored on a distributed ledger called the BlockChain. To use your cryptocurrency, you essentially write a check that transfers funds from your account to a destination account, except that this check is really a message directing the transfer that has been signed by your private encryption key that is associated with your account. Your account name, and the name of the destination account of a transfer is a public key, and it is the corresponding private key that is used to sign the message for a transfer from that account.

There are several ways that you are able to sign messages to transfer cryptocurrencies, and I am labeling them with numbers in this description. In one (1) approach, the private key for your account is encrypted using a passphrase and stored on your laptop, desktop, or mobile phone (much the same way that your private key was stored when using PGP in the second lab). In a second approach, (2) this file (with your encrypted private key) could also be stored in removable media (like a thumbdrive), or in a third approach (3) the private key can be stored in a special device (called a cold wallet) similar to a smartcard. In a fourth method (4) your private key is stored by the cryptocurrency exchange and you log in to the exchange and direct the exchange to sign messages transferring your funds. In yet other (5th) methods, you don’t actually have your own private key but simply have the exchange keep track of your balances, and the exchange sends cryptocurrency for your transactions from it’s own account, using its own key.

a. Discuss several attacks that an adversary (thief) might use to steal cryptocurrency that you have stored/saved using methods 1, 2, 4, and 5. Note that for each of the methods of key storage there might be multiple methods that may be used by the thief. I am asking this question to judge how well you understand the vulnerabilities present in these kinds of systems. Note also that full credit requires including at least one threat that might not be completely obvious, but which is fundamental. (10 points)
(type your answer here)

b. Discuss the tools/techniques/policies/approaches that may be used to defend against or mitigate the impact of the attacks that you listed in part a of this question. (15 points)
(type your answer here)