Name: Rishit Saiya

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.**

	Q1	**Q2**	**Q3**		**Total Score**
Score					

Complete the following statement:

I, **Rishit Saiya** 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: Rishit Saiya Date: 12/12/2022.

1. **(25 points) Fill in the Blanks**

Name: Rishit Saiya

a. Virtual Memory (part of Operating System) enables the use of separate memory addresses for different processes running on a computer, preventing reads or writes across protection domains.

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

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

d. For IPSec, data confidentiality is provided by the ESP (Encapsulating Secure Payload) packet header, data integrity is provided by the AH (Authentication Header) and ESP (Encapsulating Secure Payload) packet headers, and Key management is provided by IKE (Internet Key Exchange).

e. Traditional firewalls perform packet filtering 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 stateful packet inspection, the rules are modified dynamically when outbound connections are established.

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

g. The three main classes of malicious code are Trojans, Virus, and Worms.

h. In the traditional domain name system, cache poisoning 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 Trusted Base Computing (TCB) (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. Traffic Analysis is the use of knowledge about the existence of communication to draw conclusions, without knowledge of the specific content of the communication.

Name: Rishit Saiya

k. A threat 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 anomaly-based detection, signature-based detection, and behavioral-based detection. (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), integrity and availability 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)

- Hardware known as a trusted platform module (TPM) offers secure storage for sensitive data, including cryptographic keys.
- An element of the TPM called PCR (Platform Configuration Register) is made up of a collection of registers that can be augmented with the hashes of certain software components.
- As a result, the TPM can use the generated cryptographic proof to confirm the legitimacy of the platform-loaded software.
- When we extend the PCR, the hash (20-bytes) of a particular piece of software is added. We are able to produce a cryptographic proof that validates the validity of that software as a result.
- The firmware hashes, operating system hashes, and any other important software installed on the platform might be added to the PCR, for example.
- The gauging of the OS will be done in the PCR once it has been loaded.
- The ability to establish the identification of the entire software stack, from the firmware all the way up to the application, is one of the major advantages of expanding the PCR in this way.
- This is so that the hash that is saved in the PCR, which attests to each layer of software, may be used. The PCR would still have the original hash of that program, which would not match the checksum that the attacker is attempting to spoof, therefore if any layer of software is subverted, the attacker would not be able to spoof the checksum of the software that it loads in the next layer.
- As a result, it is difficult for the attacker to pretend to be the platform's software.

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]

- The DNSKEY and RRSIG resource record types are used in DNSSec to build a public key certificate that links the name of a subdomain (zone) to the public zone signing key. The DNSKEY RR contains the public key of ZSK (Zone Signing Key) that is used for authentication whereas the RRSIG is the digital signature record that is created using the private key of Zone Signing Key.
- The RRSIG resource record provides a digital signature that was created using the private key that corresponds to the DNSKEY, whereas the DNSKEY resource record contains the public key that is used to validate signatures on resource records from the subdomain's zone.
- A public key certificate, which is used to confirm the legitimacy and integrity of the resource records from the subdomain's zone, is what these two resource record kinds give when combined.
- In contrast, the public key of a reputable certificate authority (CA) whose certificate has been accepted by/downloaded into a web browser is used to validate conventional SSL/TLS certificates.
- In this instance, the public key and digital signature on the certificate are both present, and the certificate is validated by using the public key of the CA to confirm the signature on the certificate.
- In the case of DNSSec, the Public Key Infrastructure is stringent and more authoritative since there aren't multiple CAs that can digitally sign the DNS records. There is a singular ZSK assigned for a particular part of the zone and therefore the records including all types have to be signed using only this particular ZSK.
- This is commonly accomplished by creating a chain of trust from the issuing CA's certificate to the certificate being verified, each certificate in the chain being validated using the issuing CA's public key. The name servers have to use the Public Key of this ZSK to authenticate the records.

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)

There are different techniques which can potentially be used to provide isolation and/or containment within a computer system or network. Few of them are as follows:

- Virtualization: This method creates a virtual computer environment that is separate from the host system. The host system and the virtualized environment are the protected entities in this situation. It might be an OS running in a virtualized environment as a basic example (VM).
- Containerization: In this method, a container is made to isolate a certain application or process from the rest of the system along with the associated dependencies. The separated entities in this case are protected and independent containerized applications or processes.
- Access Control: In this technique, access to various resources and services within a system is restricted based on the identity and permissions of the user or process requesting access. This provides isolation by limiting the actions that a user or process can perform, protecting sensitive resources and services from unauthorized access. For example, a user with read-only access to a database would not be able to make any changes to the database, protecting it from unauthorized modifications.
- Separating Privilege: In this method, an untrusted or potentially harmful software is run in a supervised setting that is separate from the rest of the system, such as a virtual machine or container. As a result, the sandboxed software is isolated from the rest of the system, shielding it from any potential damage brought on by the untrusted program.

- Segmentation of Network: This method includes breaking up a network into smaller, separate portions, such as by using virtual private networks (VPNs) or local area networks (VLANs) (VPNs). By limiting communication between the segments and allowing only certain traffic to travel through, this creates isolation between them. The network segments and the restricted traffic are the discrete entities.
- Sandboxing: In this method, a process is actively running in a protected (limited) environment that is isolated from the rest of the system or network. The parties engaged could be potentially malicious software executing in a container or virtual machine that is separate from the rest of the system. Sandboxed processes and the rest of the system on which they are running are the entities that are protected.

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 its 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)

Some of the attacks that are possible when using the methods 1, 2, 4 and 5 are as follows:

- Attacks possible in Method-1. Dictionary attacks are a possibility, in which an attacker uses a list of frequent words to brute force their way to the passphrase. Since the passphrase is used to encrypt the private key, knowing the passphrase plus having access to the device media can result in the theft of the private key. The other attacks possible here are by means of brute-force attacks and also social engineering.

- Attacks possible in Method-2. By using a dictionary or guessing attack to break the drive's password encryption, the attacker can take the file and the key. An adversary might be able to physically steal access to my thumb drive and take the file out by doing so. If the key is stored in a removable media or copies the file using a subversion method, then my compromised device can be used to get access to the file. The access to the file will enable us to guess the passphrase and break the security of the encryption.

- Attacks possible in Method-4. The exchange can be compromised and the private key can be accessed easily from there. Moreover, social engineering attacks or phishing attacks where an adversary can elicit information can be extracted to get the login password. Also, assuming the exchange has been compromised, the keys can be compromised and the order of keys can be compromised.

- Attacks possible in Method-5. By pretending to be a customer of the exchange and asking access to withdraw money to a specific address, an attacker can launch an attack. Another strategy would involve using malware to attack the software flaws in the exchange.

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)

Some of the defense techniques for the above listed attack vectors would be as follows:

- Defense Techniques possible in Method-1: The password should be protected with a stronger password manager. The password should also be a complex compilation of characters, numbers, special characters.

- Defense Techniques possible in Method-2: The removable media should be encrypted with a stronger passphrase in practice. Some of the personal information such as retina scan, fingerprints sensors can add another form of authentication layer. Some of the firewall techniques which can be resilient against subversions can be installed.

- Defense Techniques possible in Method-4: The exchange cannot be completely trusted as this is a part of 3rd party service. Hence the architecture should be in place where the private key is not openly placed on the server. The authentication signature should always be through a chain of trusted root certificates and through trusted PKI. Unsolicited links/untrusted sources' links should not be opened as it can act as an entry point for an adversary to get into the system.

- Defense Techniques possible in Method-5: Since the exchange cannot be trusted with the private key, it should be designed in such a way that it remains as something which-you-have or which-you-know. Other methods such as Multi Factor Authentication can be used to add and buff the security layers to it.