Name: Anne Sai Venkata Naga Saketh

CSci 530 Final Exam
Fall 2024

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**. If you do copy text from other documents (including transcripts or slides from our lectures), that text that is used MUST be cited in your answer. Note also that you will not receive credit for pasted text in your responses, only credit for your original commentary surrounding such quotes.**

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-f24-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.**

Complete the following statement:

> I, **(replace with your name)** attest to the fact that I completed this exam within the designated time allocated (e.g. 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 except in ways specifically permitted by the instructor, that I completed the exam on my own without accepting or providing assistance to anyone else, and that I did not use Generative AI tools (such as Chat-GPT and similar) in answering questions on this exam.

Signed: Anne Sai Venkata Naga Saketh. Date: 12/16/2024.

Name: Anne Sai Venkata Naga Saketh

1. (20 points) Matching threats to countermeasures

   For each of the following security technologies / methods / or countermeasures (the lettered items below) list those threats or attacks (the numbered items) that they are capable of preventing or in any way contribute to their mitigation.

   This is not a one-to-one mapping; more than one technology may mitigate a threat and technologies may mitigate multiple threats. 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 threat with an incorrect mitigation. There are more blanks in the page below than actual correct answers, so you do not need to fill in all the blanks.

   1) Eavesdropping
   2) Data Exfiltration
   3) Subversion
   4) Worms
   5) Viruses
   6) Denial of service
   7) Impersonation
   8) Modification of data
   9) Social Engineering attacks (e.g but not limited to phishing)

   a) Intrusion detection **Answer**: _Data Exfiltration_ _Subversion_ _Worms_ _Viruses_ _Denial of service_ _Modification of data_

   b) Firewalls **Answer**:_Eavesdropping_ _Data Exfiltration_ _Worms_ _Denial of Service_ _Viruses_ ___ ___ ___ ___

   c) Encryption **Answer**: _Eavesdropping_ _Data Exfiltration_ _Modification of data_ ___ ___ ___ ___ ___ ___

   d) Hash Functions **Answer**:_Subversion_ _Modification of Data_ ___ ___ ___ ___ ___ ___ ___

   e) Least Privilege **Answer**:_Subversion_ _Worms_ _Viruses_ _Modification of data_ ___ ___ ___ ___ ___

   f) Digital Signatures **Answer**:_Impersonation_ _Modification of Data_ ___ ___ ___ ___ ___ ___ ___

   g) Trusted Computing (e.g. TPM's or Secure Elements) **Answer**:_Subversion_ _Impersonation_ _Modification of Data_ ___ ___ ___ ___ ___ ___

   h) DNSSec **Answer:** _Modification of Data_ _Impersonation_ ___ ___ ___ ___ ___ ___

Name: Anne Sai Venkata Naga Saketh

2. **(20 points) Trusted Computing**

   How do the Endorsement Key (EK) and the Storage Root Key (SRK) within a Trusted Platform Module (TPM) contribute to the overall security and trustworthiness of a computing system?

   What specific roles do they play in protecting sensitive data, ensuring the integrity of cryptographic operations, and facilitating attestation processes to verify the system's integrity?
   (type your answer here)

   Answer:
   The Storage Root key and the Endorsement Key are very important keys in establishing trustworthiness and security in terms on trusted computing module
   Lets discuss both the Storage key and the Endorsement key and their functionality in detail below:

   Storage Root Key (SRK):
   Objective: Another asymmetric key pair produced within the TPM is the SRK. It serves as the base of the key hierarchy and is employed to safely encrypt and safeguard sensitive information kept in the TPM as well as other keys.
   How does it help in Trusted Computing: The SRK makes sure that sensitive data may only be accessible on the particular TPM where it is stored by encrypting user and application keys. The data becomes inaccessible if it is transferred to a different system.
   Integrity: Even in the event that the system is compromised, it protects cryptographic operations and guarantees that private keys stay safe.

   Endorsement Key (EK):
   Objective: A distinct, asymmetric key pair called the EK is incorporated into the TPM during the manufacturing process. Because the secret portion never leaves the TPM, it is impenetrable.
   How does it help in the Trusted Computing: It facilitates device identification verification by acting as the TPM's foundation of trust. The system demonstrates to outside parties that it has a legitimate TPM and is in a trusted state via the EK during remote attestation.
   Confidentiality: EK enables secure communication, such as building trust in platform settings, but it is not directly utilized for encryption or user data signing.

   Overall Contribution and how they work:
   In combination, the Endorsement Key and the Storage Root key help the TPM module to support confidentiality, integrity and trust.

   a. The Endorsement Key helps in platform or server authentication and gives secure verification of the platform
   b. The Storage Root Key helps in securing the storage by using the right set of cryptographic functions, protecting sensitive data and maintaining system integrity across the platform

   Together, they improve a system's security state and guarantee that the TPM is an effective foundation of trusted computing.

3. **(20 points) Intrusion Detection**
   What are the primary distinctions between Host-Based Intrusion Detection Systems (HIDS), Network-Based Intrusion Detection Systems (NIDS), and Specification-Based Intrusion Detection Systems regarding their deployment, functionality, and the types of attacks they are designed to detect?

Name: Anne Sai Venkata Naga Saketh

Additionally, evaluate the pros and cons of each system in the context of a deployment for monitoring and detecting issues in a network of Internet of Things (IoT) devices. Please suggest an optimal deployment.

(type your answer here)

Answer:

1. **Differences Among Specification-Based IDS, HIDS, and NIDS:**
   a. **Intrusion Detection Systems (HIDS) that are host-based:** Installed on separate devices to keep an eye on internal operations such as running processes, file integrity, and system logs. It identifies dangers unique to a certain device, including malware, rootkits, and unauthorized modifications.
   b. **Intrusion Detection Systems (NIDS) that operate on networks:** installed at switches, routers, or network gateways to track and examine network traffic. Network-wide attacks like DoS and DDoS, virus propagation, and anomalies are all expertly detected by NIDS.
   c. **IDS Based on Specifications:** This system ensures that processes follow stringent policies by identifying deviations from established behaviors. It is especially good in spotting policy infractions, zero-day vulnerabilities, and unusual activity in restricted areas like the Internet of Things.

2. **Pros and Cons of each of the above systems are mentioned below:**
   a. HIDS:
      Pros: Offers detailed identification of host-level dangers like malware or illegal access.
      Cons: Incapable of detecting network-wide anomalies; resource-intensive for IoT devices with limited power.
   b. NIDS:
      Pros: It efficiently detects network-based threats including malware propagation and traffic irregularities by monitoring traffic across all devices.
      Cons: Limited ability to see encrypted traffic; inability to identify host-specific modifications.
   c. Specification Based IDS:
      Pros: Identifies zero-day attacks and behavioral anomalies; lightweight and effective for limited IoT devices.
      Cons: prone to false positives; requires precise behavioral models, which can be difficult to create.

3. **Optimal Deployment for IoT:**
   a. Set up NIDS at the network gateway to keep monitor on and examine all IoT device traffic for potential risks to the entire network.
   b. Use HIDS on important or valuable IoT devices that have enough power to keep monitor on internal operations and identify incursions unique to the device.
   c. Use specification-based intrusion detection systems (IDS) on limited devices, such as sensors and actuators, to track conformance and identify deviations

4. **(15 points) IPSec vs other security protocols**

What are the key differences in the protections provided by IPsec (Internet Protocol Security), TLS (Transport Layer Security), and PGP (Pretty Good Privacy)?

Be sure to mention in your answer the primary use cases of each approach, mechanisms for key exchange and management, and the layer of the OSI model or protocol stack at which they operate?

(type your answer here)

Answer:

Feature	IPSec	TLS	PGP
Primary Use Cases	IPSec is used for secure communications between networks (VPN). Also used in host-to-host or host-to-network encryption and authentication	TLS is used for communication between Web browsers and web servers (User applications like emails, messaging etc)	Secure Email communication and authenticity of individual messages
Key Exchange and Key Management	Uses Internet Key Exchange protocal for management of Security associations (SA's). It also supports Deffie Hellman Key exchange for secure communication	SSL/TLS handles key exchange during the handshake process. It usually uses RSA or Diffie-Hellma for public key exchange. SSL/TLS is all about quickly setting up a secure session over HTTPS	It uses a trust network instead of relying on certificate authorities. It combines public-key cryptography and symmetric encryption for key management and exchange.
OSI Layer	Operates at the Network Layer (layer 3)	Operates at Transport Layer (Layer 4)	Operates at Application Layer (Layer 7)
Protections	Provides Confidentiality, Integrity and Authentication of IP Packets, Works in Transport or Tunnel mode.	Ensures confidentiality, integrity, and authentication for application data. Protects against eavesdropping and data tampering during transmission.	Provides End-to-End encryption, digital signatures and and message integrity and also prevents unauthorized access of emails.

5. (25 points) Ransomware Prevention, Detection, and Recovery – PIH Health Attack

Recently, PIH Health hospitals in Southern California were targeted in a **ransomware attack**. Hackers claimed to have stolen **17 million patient records**, including personal and medical information. The attack disrupted operations at three hospitals and several other facilities, causing significant issues with accessing health records, laboratory systems, and phone systems1. The hospitals are working with cyber forensic specialists and the FBI to investigate the incident.

In this question we will consider the causes of such breaches and the steps and mechanisms that can be deployed to prevent and or mitigate the impact of such a breach.

a) (5 points) Often, such breaches occur when an adversary is able to perform actions on the system with privileges that of a user that has access to patient records, or access to update software within the system.

Name: Anne Sai Venkata Naga Saketh

Discuss some of the ways that an adversary is able to obtain such access (note that there are at least two important ways, and you must mention those two).

(type your answer here)

Answer:

There are multiple ways in which an adversary can obtain such access, some of them are mentioned below:

1. **Phishing and Social Engineering attacks:**
   a. Users/employees receive a legit disguised email from a trusted sender with some links or from their IT team asking for their credentials, and once the credentials are stolen, they are used to login/access the systems that the user has access to and install ransomware, lock access, change passwords and many other things that the actual employee has access to
2. **Software Vulnerabilities:**
   a. The Adversary exploits any unpatched/zero-day vulnerabilities to access some parts of the code and then escalate the privileges within the system
   b. These vulnerabilities can help in remote code execution and injection of malware(ransomware). They can also modify a small piece of the code to form subversions
3. **Insider Threats:**
   a. Legit employees with access who might want to defame the system, or under the influence of external factors can compromise security and install ransomware and provide access to the adversaries
4. **Websites or Marcos:**
   a. Users un-knowingly execute/click on links that help the adversary to plant code that can access system, track keystrokes and install ransomware.

b) (10 points) What are some of the specific techniques/mechanisms that can be used for early detection of ransomware attacks? What does each of these techniques look for as indicators of an attack?

(type your answer here)

Answer:

Some of the techniques for detection of ransomware attacks are as follows:

1. **Behavior Based Anomaly Detection:**
   a. Uses statistical modules to identify a sudden unusual change in the behavioral patterns of a system access, we can look for indicators like file permission modifications, file transfers, increased I/O activity.
2. **Network Traffic Analysis:**
   a. We can monitor the network to see unusual activity in terms of data transfers or communication with other command servers. We can look for indicators like High outbound traffic to suspicious IP addresses.
3. **Honeypots:**
   a. Honeypots are decoy systems, that mimic the real systems, these can help to attract the attackers without impacting the actual data.
   b. We can look for indicators like any interaction with honeypot is a malicious activity and can be terminated and blocked from any further communication.
4. **File Integrity monitoring:**

   a. Monitor file permissions and changes and any unusual activity on them, we can look for indicators like sudden changes to many files or system files and changes of file extensions. Tools like Tripwire can be used

5. **Realtime monitoring of System Logs:**
   a. Continuously analyze system logs for any activity of ransomware or file modifications or user access modifications

c) (10 points) What are some of the specific techniques/mechanisms that can be used to contain such attacks and/or mitigate the impact of these attacks? Explain how each technique/mechanisms improves containment or mitigates impact.
(type your answer here)

Answer:

Some of the techniques are as follows:

1. **Network Segmentation:**
   a. Diving the network into smaller subnets to contain the ransomware attack, as we can limit the attack to only one segment. Critical systems can be places in more secure zones.
2. **Least Privilege:**
   a. We can restrict user and system access controls to the bare minimum level to the necessary parts to contain the spread of the attack, this can help because it limits the user access to access any secure data and files.
3. **Containment Techniques:**
   a. Immediately disconnecting compromised systems from the network to stop the spread, this can help as it prevents any further encryption of files and systems by the adversary.
4. **Backup and recovery:**
   a. It is always better to take a periodical backup of the data and the applications, and they be stored on a separate server and network, so that it can be used to recover the systems from the latest backup in case of a ransomware attack.
5. **Endpoint Detection and Response:**
   a. We can deploy endpoint detection and response systems as they can constantly monitor files across and immediately quarantine files that seem to be from an unknown source or an adversary
6. **Firewalls:**
   a. Firewalls help in allowing the right network traffic to and from the system/server that can majorly help. As soon as an IP is classified as a suspicious, we can block it at the firewall level to prevent any further interaction.
7. **Sandboxing:**
   a. We can execute risky applications in controlled environments so that they cannot affect the host system or network, in this manner combined with honeypots we can easily identify an attack and immediately contain it.