**CSci 530 Midterm 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 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 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-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, **Rishit Saiya** 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: Rishit Saiya . Date: 10/7/2022.**

1. **(30 points) Policy Management -** For each of the following methods of representing policy or implementing authorization, match the method with the **major** characteristics or relevant terms discussed in class. This is **not** a one-to-one mapping. So more than one approach may match a characteristic or term, and a single characteristic or term may also match more than one approach. We are looking for specific characteristics and terms, for which you will receive credit. If you list what is a minor characteristic, while you will not lose credit, you will not get credit either. You will lose a point if you associate a term with a characteristic that does not apply to the method. There are more blanks in the page below than actual correct answers, so you do not need to fill in all the blanks.

**You may include a comment after any of your answers to clarify your thought process. This is not required, but a reasonable justification could prevent points from being taken off if you answer incorrectly.**

1. Bell – LaPadula Model
2. Clark-Wilson Model
3. A Restricted Proxy
4. File permissions in Unix or Linux
5. Generic Authorization and Access Control API (GAA-API)
6. Passwords for Password Protected Files (we did not discuss this in class)
7. Associated with object (this means stored and managed with the object)  
   \_\_4\_\_5 \_\_\_\_ \_\_\_\_ \_\_\_\_ \_\_\_\_ \_\_\_\_ Comment: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
8. Implements a reference Monitor  
   \_1\_2\_5\_ \_\_\_\_ \_\_\_\_ \_\_\_\_ \_\_\_\_ \_\_\_\_ Comment: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
9. Star Property   
   \_1\_\_\_ \_\_\_\_ \_\_\_\_ \_\_\_\_ \_\_\_\_ \_\_\_\_ Comment: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
10. Integrity policy  
    \_\_2\_\_ \_5\_\_\_ \_\_\_\_ \_\_\_\_ \_\_\_\_ \_\_\_\_ Comment: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
11. Mandatory Access Control  
    \_\_1\_2\_ \_\_\_\_ \_\_\_\_ \_\_\_\_ \_\_\_\_ \_\_\_\_ Comment: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
12. Associated with user (or stored and managed by the user)  
    \_\_1 3\_4\_ 6\_\_\_\_ \_\_\_\_ \_\_\_\_ \_\_\_\_ \_\_\_\_ Comment: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
13. Policy Decision Point  
    \_\_5\_\_ \_\_\_\_ \_\_\_\_ \_\_\_\_ \_\_\_\_ \_\_\_\_ Comment: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
14. **(35 points) Short and medium length answers**
15. (10 points) Why do we include an expiration date in a public key certificate and also in a Kerberos ticket? What is the benefit of a longer lifetime (later expiration) to these credentials, and what is the benefit of a shorter lifetime? Why do we use a separate certificate status server (OCSP) with public key certificates when we do not use such a server with Kerberos?

The long lifetime of the credential drastically reduces the risk of spreading of new credentials to the related transactional parties. With the massive increase in computational powers in state-of-the-art tech, it is easier to crack key pairs nowadays. In such scenarios, the public key

certificates with expiry dates avoid them being exploited so that adversaries can’t do anything even with private key possession. A short life of a certificate might help wherein the credential expires by passing time, a hacker might get privilege to access the keys which might be private.

In any event, if the private key gets in public, then the corresponding public key certificates might be needed to get into CRL (Revocation Lists). This can be done using protocols like OSCP. The CRLs can be maintained to avoid propagation of revocation updates and get a common ground to notify all systems.

In any event, where in the Kerberos is used, as one key is linked with one pair of Client and Server is shared between client and TGS. In such a case, when the key needs to be revoked, the update doesn’t need to notify all parties as the KDC/TGS takes care of it.. Hence in that case, OCSP is not required.

1. (5 points) Explain the reason that we include a nonce or a timestamp in the message layout of cryptographic protocols. Briefly, what are the advantages and or disadvantages of each of the two approaches (timestamps or nonces).

We typically include nonce or a timestamp as a randomizing factor in our cryptographic protocol system. A nonce or a timestamp is generally a random number/present factor (similar to IV (Initialization Vector)) that might be used to differentiate the similar requests with similar data coming with some factor. This nonce or a timestamp will act as a differentiating factor here. These timestamps or nonces are implemented in order to make sure that our system doesn’t undergo replay attack wherein we can send similar requests and make the system interpret that our latest requests are from the past and bypass in this way. Some systems like Kerberos or Needham Schroder where in these timestamps or nonces are used, it is integrated into the ticket wherein our data or request is hashed in these cryptographic protocols.

Advantages: The requirements on the TGS/server side to authenticate the requests are stringent in that sense, so the TGS/server precisely looks for the nonce data and doesn’t authorize until it knows it's authentic.

Disadvantages: Delayed requests due to network traffic, packet losses, low significance in time testing can lead to replicating or guessing the timestamps.

1. (5 points) While a magnetic stripe credit card is technically a physical object, thus might be considered “something” you have, when used for authentication, it exhibits the same problems and operates in a manner similar to “something you know”. Discuss in a couple of sentences why it is closer to something you know. Be sure to include in your discussion why attacks on such a method by an adversary is the same as an attack on “something you know”.

I feel that it is closer to something you know because the magnetic stripe credit card has internal RFIDs which are authenticating the access/transaction. The key is checked internally and the key never leaves the card. It is similar to encryption key or password; we know that only we know and doesn’t leave us.

Attack Scenario: Let’s say that if the key stripe is used for transaction and the adversary by some means actually has the access to the key, then the stipe could be read by an adversary who can impersonate user into some reader that user isn’t authorized to in any event.

1. (5 points) When connecting to a website using SSL or TLS, where do we obtain the public key belonging to the certification authority (CA) that issued a server’s certificate? What would happen if we had an incorrect public key for the CA, or if we accepted the public key of a CA that is not worthy of our trust?

We receive the server's certificate, which contains the public key of the CA that certified the certificate, when we connect to a website using SSl or TLS. Verification cannot be done properly if there is an invalid public key present. If we use a key from an unreliable CA, it can lead us to a fake website that steals information since it seems real.

1. (10 points) End to End Encryption – End-to-end encryption depends on our trust that we are using the correct public key for the intended recipient of our message. What is the implication of relying on the intermediate transmission infrastructure (such as the What’s App message service) to provide us with this public key? What kinds of attacks are enabled by such reliance?

If the database is compromised, we are vulnerable to a Man-in-the-Middle attack. If we know the attacker's public key, we will believe that we are speaking with them while actually speaking with the attacker via a legal Whatsapp application.

1. **(35 points) Los Angeles Unified School District**

You have been hired by the Los Angeles Unified School district to advise them on changes needed in their system to prevent recurrence of the major system breach that occurred at the end of August. The greatest consequence of the August attack was the result of Ransomware, an example of malicious code that we will discuss after the mid-term exam.

I will explain here some of the background information regarding ransomware that will help you to better understand this question. Ransomware is a form of subversion, and the installation of ransomware requires the ability to make changes to programs and software already running on a system. Therefore, ransomware can only be installed within a system, if the adversary is able to gain access to modify such programs. The ransomware itself may modify files (often by encrypting them) or otherwise disable a computer system. A ransom is then demanded to provide the encryption key needed to recover the files or the system. In an alternate form of ransomware, data is read and exported from the system (called exfiltration), and the criminals demand a ransom in order to keep them from publishing the stolen data.

This question is NOT about the functioning of ransomware. Rather it is focused on technologies that we discussed in the first half of the semester that could make it more difficult for a criminal to install ransomware on LAUSD’s systems, or technology that would make it more difficult for ransomware, once installed, to cause significant damage to LAUSD’s operations.

* 1. (15 points) General Approach of the attack – Briefly describe (at least three sentences each) three different approaches by which an adversary might compromise or get into the LAUSD system. By three different approaches, please cover at least one approach that compromises or exploits lack of strong capabilities in each of the following areas a) Authentication, b) Cryptography, c) Policy or authorization.

In at least three sentences each (at least 9 sentences total), describe the capability that is missing or weak, the action taken by the adversary, and the impact of the action on the system.

Note that I realize this is intentionally vague. What you should do is think about the techniques we covered in the Cryptography lecture, in the Authorization lecture, and the identity management lectures and explain how an adversary might get into the system or make changes to the system if appropriate measures were not taken.

Some of the different approaches that compromises or exploits lack of strong capabilities would be something like:

**Authentication:**

- If there is a weak authentication system (which can be brute forced easily) or if the authentication system is using insecure versions protocols, then our system can be exploited.

- Using deprecated versions of protocols and not using upto authentication protocols can affect the exploitation levels of our system.

- Lack of awareness induces weak passwords, or putting passwords on notes on PCs, etc. can adversely affect us as well.

- If our randomizing factor generator (say TGS is compromised), then our requests might be altered and using the integrity-less requests our systems can be affected.

- If our private keys are stored in an insecure manner, they can be used to impersonate and infiltrate into the system and exploit and access all the data.

**Cryptography:**

- Usage of weak hash functions which have frequent collisions can be reverse engineered.

- If the key space is sparse, then the cryptanalysis is harder but if the key space is dense, then with the increasing computational technology, we can find the key by trial and error.

- Usage of old or weakness proven cryptographic algorithms like DES

**Policy or authorization:**

If access is not restricted to need to know basis (violation of BLP)

- If highly critical data’s access is with lower clearance users, then privilege is at stake.

- If the required compliance like HIPAA, not revealing student data in public records is violated, then there is a huge impact on the organization in terms of legalities.

- The access policies and corresponding mechanisms (like DAC, MAC) are not correctly implemented or have logic flaw, then the information flow can be misdirected.

* 1. (10 points) Policy and access control – Make some suggestions to LAUSD regarding the policies that should be applied for access (read, write, ability to login, etc) to systems and data maintained in the LAUSD systems. Please suggest which policy model(s) should be used to manage access to different kinds of data. (You may want to implement more than one model that applies to certain data). For each model that you recommend, explain the reason for applying the model.

In such complex organizations, it is safer to implement MAC policies as they allow higher assurance in general. Some of those would be as follows:

Biba: This might be used to maintain the integrity of the system. This can be done via a no write-up feature of this model wherein it will not grant the subjects with low clearance to spread exploits to high critical data Biba has no read-down i.e. it enforces read up since users with higher security clearance are more trusted.

Bell-LaPadula Model: Critical data’s confidentiality can be maintained by implementing the no-read up feature of BLP model. In this way, the people with lower assurance won’t be able to access highly critical data. The No write-down feature of BLP model will ensure that if an exploit affects a system then it cannot declassify critical data maintaining the confidentiality of the system.

DAC policies might be also used but on Non trivial data like class assignments, marks of students, etc. (requires confidentiality but not as much critical as students’ personal details, non public records)

* 1. (10 points) Authentication – A system such as that used by LAUSD has many types of users, including students, parents, teachers, district and school administrators, and system administration staff. These different classes of users may have different resources available for their use, and certainly the degree of risk associated with different classes of users may vary. For this part of the question, you are asked to discuss the various forms and technologies available for authentication as we discussed in lecture 4 and 5 and advise the district on which technologies they should deploy. Be sure to consider whether the same technologies are required for all users, or varying approaches may be applied depending on the user Explain the reasons for your recommendation. You may refer back to your discussion from parts (a) and (b) when explain your recommendations here in part (c).

Some of the authentication techniques here might be:

Something about you: Using face id, fingerprint, biometrics to authenticate subjects into the systems.

Something you have: Storage of private keys and using up to date encryption algorithms.

Something you know: Using systems immune to dictionary and brute force attacks.

Sys Admins should only use OTPs or encryption based authentication and not biometrics only. Since they have access to sensitive data. Moreover, they should be forced to use techniques like MFA.