Name:Anne Sai Venkata Naga Saketh

CSci 530 Midterm 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 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**. 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-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.**

Complete the following statement:

I, **Anne Sai Venkata Naga Saketh** attest to the fact that I completed this exam within the designated time allocated (e.g. 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 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: 10/18/2024.

Name:Anne Sai Venkata Naga Saketh

1. (30 points) Identity / Key Management - For each of the following methods of authentication, identity management, or key management, list or describe the secret, private, or public data held by the two parties involved with the transaction at the conclusion of the exchange. For authentication or identity management the first party would be the prover (the one that is proving their identity), and the second party would be the verifier. For key management, the first party would be the initiator, and the second party might be referred to as the responder). Note that there are likely to be multiple items in each of the boxes below.

Method	Prover or initiator	Verifier or responder
Password Based Authentication	The Person holding the password to a server/website	(note: there are several approaches to verifying a password, you may list items from more than one approach) 1. Server with access to stored and hashed/encrypted passwords 2. Multi-Factor Verification
Encryption-based authentication such as the final exchange between the client and end-server in Kerberos.	Holds session key generated during Authentication and the Nonce/Timestamp received from KDC	Has a matching session key held by the prover and uses the Nonce and session key to validate the identity of the prover
Diffie-Hellman Key Exchange	Initially person who computes his public value(X) from his secret (x) and after exchange receives other party's Public value (Y)	With access to other party's public key and the ability to compute the shared secret involving his secret value (y)
Certificate-Based authentication (e.g. authentication of the server using SSL or TLS)	Holding its (clients) private key and public key of the CA	Holding private key to the certificate issued by CA like "Verisign" and verifies client certificate using the public key assigned by the CA

2. (40 points) Short and medium length answers

   a. (15 points) Mandatory Access Control Policies – The non-discretionary nature of mandatory access control models such as Bell-LaPadula is sometimes considered impractical for general

computer use because it makes it more difficult (by design) to share information with collaborators and get work done. Why might this non-discretionary aspect be less of an issue when using the Biba model (also non-discretionary, but focused on integrity) to protect a system from subversion (e.g. infection by a virus or worm). [note: you will not find this answer in the slides or the readings – rather you should focus on the likely assignment of labels to files when applying Biba for this purpose – we did mention this in passing in our class discussion].

Answer

The major reasons are as follows,

1. Unlike Bell-La Padula, where the concern is about the data confidentiality, The Biba model enforces that integrity is maintained over confidentiality, and it makes sure that the Lower Integrity process cannot influence the higher integrity process (modify data with a higher clearance). Due to this critical system data can be protected from being modified by less-trusted process like malicious code/software.
2. In the Biba model also differs in the labelling processes, the files are labelled based on their integrity level rather than the data sensitivity level. This is effective in stopping the worms/malicious code to make changes to system critical files. And since Biba is more concerned with integrity it allows better file sharing and collaboration

b. (10 points) **Brute Force Attacks** – List at least three factors that impact the time needed to mount a brute-force attacks on an encryption system, or on passwords. How does each factor impact the time that is required for such an attack.

Answer

Some factors that might affect are

1. Password length – The longer the password is the more time it takes to try out all the different combinations, if the password length is smaller, the number of combinations it takes to break the password using Brute Force is less
2. Password Character Combination – If the password contains only alphabetical characters the number of combinations that are needed by brute force may be reduced compared to a password that uses a combination of alphabets, numbers and special characters symbols.
3. Compute Capacity – The faster the compute the quicker it takes for the password to be cracked. We have also seen this during our lab assignment where using 1 machine takes 10 years, using 100 machines simultaneously can drastically reduce the time required.

c. (15 points) **Authorization** – In class I sated that authorization is the ultimate goal of computer security; that what we ultimately care about is a yes or no answer to the question of whether a particular operation is allowed. When authorization policies are implemented using an access control list, what are the inputs to this decision? To answer this, tell me all of the data that is consulted by the authorization mechanism to validate that an operation is permitted, to yield that yes or no decision. Where does each of piece of data (used as inputs) come from?

Answer

The data that is consulted during the authorization process is:

1. Identity of the subject – The person who is requesting access to a particular resource, this can be verified by authentication ideally to confirm the subject's identity
2. Access Control matrix/Access control list – To confirm if the subject has the access allowed to a particular resource/object that he is requesting access to including the specific operation on the requested object (read/Write/append/delete….)
3. The object that the subjects want to interact with and its allowed actions

Name:Anne Sai Venkata Naga Saketh

3. **Passkey (30 points)**

   Consider the following article from The Hacker News:

FIDO Alliance Drafts New Protocol to Simplify Passkey Transfers Across Different Platforms

Name:Anne Sai Venkata Naga Saketh

Oct 16, 2024Ravie LakshmananData Privacy / Passwordless

The FIDO Alliance said it's working to make passkeys and other credentials easier to export across different providers and improve credential provider interoperability, as more than 12 billion online accounts become accessible with the passwordless sign-in method.

To that end, the alliance said it has published a draft for a new set of specifications for secure credential exchange, following commitments among members of its Credential Provider Special Interest Group (SIG).

This includes 1Password, Apple, Bitwarden, Dashlane, Enpass, Google, Microsoft, NordPass, Okta, Samsung, and SK Telecom.

"Secure credential exchange is a focus for the FIDO Alliance because it can help further accelerate passkey adoption and enhance user experience," the FIDO Alliance said in a statement.

"Sign-ins with passkeys reduce phishing and eliminate credential reuse while making sign-ins up to 75% faster, and 20% more successful than passwords or passwords plus a second factor like SMS OTP."

While passkeys have the advantage of being secure and phishing-resistant, they are essentially locked in to the operating system or the password manager service, making it impossible to transfer them when switching platforms and, therefore, requiring users to create new passkeys per device.

The new specification proposed by the FIDO Alliance aims to address this gap with the Credential Exchange Protocol (CXP) and Credential Exchange Format (CXF).

They "define a standard format for transferring credentials in a credential manager including passwords, passkeys, and more to another provider in a manner that ensures transfer are not made in the clear and are secure by default," it said.

The development comes as Amazon revealed that more than 175 million customers have enabled passkeys on their accounts, nearly one year after the initial rollout.

"Passkeys fundamentally shift the way we sign in to our online accounts for the better — and seeing Amazon roll out passkeys is evidence of its commitment to its customers' time, experiences, and security across Amazon web and mobile shopping experiences," said Andrew Shikiar, chief executive officer of FIDO Alliance.

Based on the discussion above, and our discussion during lecture regarding passkeys, answer the following questions.

How would you best describe passkey (with the extensions described in the article)?

a. (5 points) On what basis is a user initially authenticated (enrolled). More specifically tell me how the system (the website they log in to) initially learns their identity?

Answer

The initial Enrollment process is after a successful login using the current authentication mechanism when the system asks the user to confirm his identity using a trusted source (Biometric authentication or PIN or FaceID), then based on this a cryptographic key pair is generated and shared with server which is used for later authentications.

b. (5 points) Is a passkey a certificate-based system? If so, what constitutes the certificate, and who or what is the certificate authority (trusted third party). If not, then why not.

Answer

A passkey authentication is not a certificate-based authentication system, though it uses the public and private key cryptography, is does not use any digitally signed certificates. Since the passkey authentication happens directly between the server and the device the login is requested from, there is no need for use of any certificate-based system, and it also reduces the complexity

c. (10 points) In what way do passkeys support secure single-sign-on, and in what ways do they not support secure single-sign-on. (in answering this question, I would suggest drawing analogies and or contrasts to other kinds of SSO mechanisms).

Answer

Supporting secure single sign on:

1. Since they leverage public key cryptographic systems, the device can be authenticated using a passkey and once authenticated, can login to multiple services that are offered
2. As mentioned in the article, they are proven against password phishing, as they are directly authenticated using biometrics/device pin, like traditional SSO using multifactor authentications

Where it does not support secure SSO:

1. As of today, they are locked to specific devices, so on every device, the users are required to create a new passkey, which is not like traditional systems, where the same password can be used
2. Most of the SSO's today use central identity providers to help them authenticate, which is not the case with passkeys

d. (5 points) In what ways does the ability to share passkeys as described in the article make them less secure, or more vulnerable to compromise?

Answer

The sharing of passkeys across different services makes it more vulnerable as it increases the attack surface, and it also needs a very secure channel for transfer to happen, also the device security matters as a passkey transferred to a less secure device might expose it to others. Also, different security and encryption mechanisms on different platforms can make it vulnerable.

e. (5 points) While the ability to share passkeys probably does not make them more secure, what are some of the reasons that using the mechanism describe in the article might NOT make them significantly less secure? (yes, I realize that d and e seem to be opposite, what I really want to hear is a discussion of both sides of the question).

Answer

The security of the passkeys might not significantly reduce as they should be encrypted during transfer using the CXP and CXF protocols as mentioned in the article. Sharing passkeys mostly occurs between trusted systems for example Apple and Google, which will enforce strict security measures.