Mid Term Old Questions Answers:

1. What is digital signature?(5)

* Message is hashed( providing integrity)
* Hash encrypted with sender’s private key
* Public key can decrypt (providing authentication and  non-repudiation)

1. Let m be a message. Suppose Alice and Bob share a secret key k. Alice sends bob m | | {m}k (i.e. the message and it‘s encipherment under k). Is this a digital signature? Why or why not?  Explain your answer.(7)

* This implements symmetric cryptography mechanism( sharing the same secret key k) whereas digital signature should implement with Asymmetric cryptography mechanism i.e. public key cryptography. Message should be encrypted  by .owners i.e Alice private key so that Bob can decipher the message with Alice (non secret) public key to be Alice digital signature which provides integrity , authentication and non-repudiation. Here, Alice and Bob share same secret key so that Bob is able to repudiate same signature and can use as Alice digital signature which is not the purpose of digital signature, it should be non -repudiation.

1. Describe briefly the roles of the 3 different servers used in Kereberos.(6)

* Authentication Server (AS): Authenticate the user and give ticket to use Ticket Generating Server
* Ticket Granting Server (TGS): Validate the user ticket (ie. user is allowed to use the server/service requested eg. print server)
* Requested/Target Server: The server that serves user request eg. print server

1. What is a potential problem of the Kereberos protocol?(5)

* Has to be online
* Single point of failure.. If Kerebero server fail, we cannot communicate
* Compromised Kereberos can decipher the messsage

1. Policy restricts the use of e-mail on a particular system to faculty and staff. Students cannot send or receive e-mail on that host. Classify the following mechanisms as secure, precise, or broad and briefly justify your answer. (9)
   1. The e-mail sending and receiving programs are  disabled.(3)

Broad:

* 1. As each letter is sent or received, the system looks up the sender (or recipient) in a database. If that party is listed as faculty or staff, the mail is processed. Otherwise, it is rejected. (Assume that the database entries are  correct.) (3)

Secure:

* 1. The e-mail sending programs ask the user if he or she is a student. If so, the mail is refused. The e-mail receiving programs are disabled.(3)

Precise:

1. In Bell-LaPadula model, the security levels are TOP SECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED (ordered from highest to lowest), and the categories are A, B, and C.  Specify what type of“access (read, write, both, or neither) is allowed in each of the following situations.Also briefly explain your answer. Assume that discretionary access controls allow anyone access unless otherwise specified. (9)

<security level: set of categories>

* 1. [3] Robin, who has no clearances (and so works at the UNCLASSIFIED level), wants to access a document classified (CONFIDENTIAL, {B}).

No read (Unclassified< Confidential )

can write (empty set  ⊆ {B})

* 1. [3] Paul, cleared for (TOP SECRET, {A, C}), wants to access a document classified (SECRET, {B, C}).

No Read (Top Secret > secret but {B,C} ⊄ {A,C})

No write  ( {B,C} ⊄ {A,C})

* 1. [3] Sammi, cleared for (TOP SECRET, {A, C}), wants to access a document classified (CONFIDENTIAL, {A}).

Can Read(confidential < top secret and {A}⊆ {A,C})

No Write (confidential < top secret)

1. Briefly explain  how  Clark-Wilson integrity model supports the principle of separation of duty. (6)
2. Difference between a known plaintext attack and a chosen plaintext attack. (6)

ANS: Known plaintext attack have the ciphertext for a known plaintext but Chosen plaintext attack can generate ciphertext for any plaintext.

1. We’ve learnt 12 design principles in this course till now. Please relate 2 of them to the SCI principles that we’ve studied. [Hint:  Principle of complete meditation - infinity at a point] (6)

1. Principle of Least Privilege: A subject should only be given those privileges needed to do its task

(SCI: disallow the birth of an enemy)

Example: Faculty don't get administrator

Principle of Fail-Safe Defaults: Unless a subject is

given explicit access to an object, access should be denied

(SCI: spontaneous right action)

1. What is the cipher text for word “SECURITY” using rail-fence cipher with a key of 3? (4)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| S |  |  |  | R |  |  |  |
|  | E |  | U |  | I |  | Y |
|  |  | C |  |  |  | T |  |

SREUIYCT

1. Briefly explain any 3 advantages of CAs (Certificate Authorities) over KDCs (Key Distribution Center) (9)

**ANS:**

* **\***There is no single point of failure for a CA. But if the KDC (Cathy) goes down, Alice and Bob cannot create a session key.
* **\***Certificates are not security sensitive. All an attacker can do is delete certificates, he can't create bogus certificates because he doesn't have the private key of the CA.
* **\***Since a compromised CA doesn't have a private key, it can't decipher conversations but a compromised KDC can (it has the keys that it shares with the users that trust it). That is, you have to trust a KDC more than a CA. All you give the CA is your public key.
* The CA doesn't have to be online. It can be in a locked room, create a certificate and put it on a floppy disk. A user has to communicate with a KDC online to get a session key.
* Since a CA is not online, it can be simpler (economy of mechanism)

1. Please give an example of a trade-off between the principle of psychological acceptability and the principle of least privilege (6)
2. Consider a computer system with the three users: Alice, Bob and Cyndy. Alice owns the file Alicerc, and Bob and Cyndy can read it. Cyndy can read and write the file Bobrc, which Bob owns, but Alice  can only read it. Only Cyndy can read and write the file Cyndyrc, which she owns. Assume the owner of each  of these file can execute it. Create the corresponding access control matrix. (6)

|  |  |  |  |
| --- | --- | --- | --- |
|  | Alicerc | Bobrc | Cyndyrc |
| Alice | execute,own | read |  |
| Bob | read | execute,own |  |
| Cyndy | read | Read, write | read,write,execute,own |

1. Considering  role of trust, sometimes a “back-door” is purposefully used through which the security mechanism can be bypassed. The trust resides in the belief that this back door will not be used except as specified by the policy.Based on your experience as an IT professional, briefly describe a situation in which planting a back door would be needed and explain how it could be used and misused. (8)
2. Let’s say that I can control some process by sending  a “stop” and “start” message to a  server. The fact that I am starting and stopping the process is not  a secret, so I don’t have to encrypt the start and stop message. But it is important that I am the only person who can  stop and start  the process. Therefore. I digitally sign the “stop” or “start” message with my private key. The server then decrypts the hash with my public key to make sure that I was  the  one who sent the message. Briefly describe what is wrong with this protocol. (8)
3. Bob’s password is “flower”, but one day by accident he discovers that the password “blowfish” also works. This is a complete mystery to him because he has never used “blowfish” as a password. Please give an explanation for this behavior. The following answers are not acceptable.
   1. “There is a bug in the program”
   2. “Blowfish” was a back door planted by the vendor
   3. Bob added “blowfish” and forget about it.