This file contains the frequent questions from previous students. The answers are from the previous students plus from the slides. Yellow highlight means a question to ease navigating thru them.

Prepared by: Mosheer

-------------------------------------------------------------------------------------------------------------------------  
**Policy:**

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:

Threat: potential violation of a security policy

Attack: An action that could cause a threat to be realized

Attacker: The perpetrator of an attack

Vulnerabilities: allow an attacker to carry out a threat.

Risk = Assets \* Threats \* Vulnerabilities

Four Classes of Threats

• disclosure - unauthorized access to information (confidentiality)

• deception - acceptance of false data (integrity)

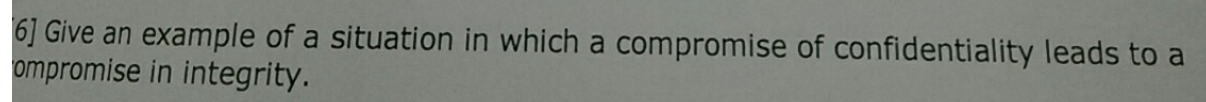
• disruption - interruption or prevention of correct operation (availability)

• usurpation - unauthorized control of some part of a system (confidentiality, integrity, availability)

Policy vs Mechanism:

A security policy is a statement of what is, and what is not allowed. OR A security policy is a statement that partitions the states of the system into a set of authorized, or secure, states and a set of unauthorized, or non-secure, states  
A security mechanism is a method, tool, or procedure for enforcing a security policy.   
a policy you can think of it as a word document. The mechanism is the actual implementation.

A scenario need an answer



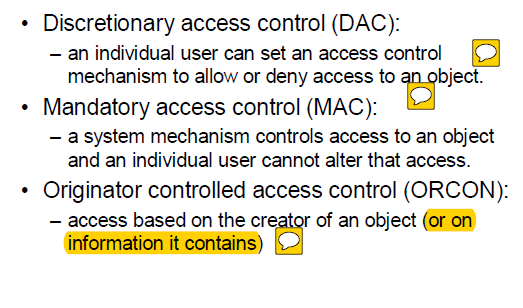
-------------------------------------------------------------------------------------------------------------------------

**ACM questions and access types** Lec#2

Meaning of ACM: a way of specifying policy, – namely, what are the access permissions of the subjects of the system

Prove that ACM is a policy: mention that the mechanisms for ACM would be ACL, CL, PACL etc.  
The main difference between ACL and CL is with reference to revoking access to an object.

Access Types:



-------------------------------------------------------------------------------------------------------------------------

**Confidentiality vs Integrity policy** Lec#3 and #4

A confidentiality policy, also called an information flow policy, prevents the unauthorized disclosure of information. It is not concerned with the integrity or availability of the information.

Integrity security policies deal with things like separation of duty, separation of function, and auditing. – These are meant to minimize errors that would violate the integrity of the system, not its confidentiality.

-------------------------------------------------------------------------------------------------------------------------

**Bell-LaPadula** Lec#3

You needed to remember that for a subject not to have r/w access to an object, following 2 conditions should be in effect.

Clearance of S < Classification of O       ANDCategory of O is not a subset of Category of S

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}).

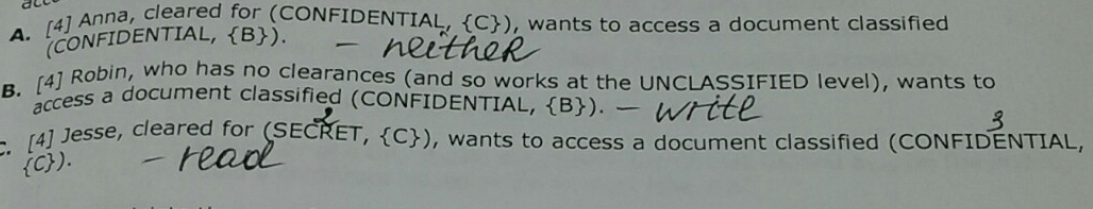
No Read (Top Secret > secret but {B,C} ⊄ {A,C})

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)



Briefly explain how clark-wilson integrity model support the separation of duty.

The system must associate a user with each TP and set of CDIs. The TP may access those CDIs on behalf of the associated user. The TP cannot access that CDI on behalf of a user if she/he is not associated with that TP and CDI.

-------------------------------------------------------------------------------------------------------------------------  
  
**Attacks types**: Lecture 6

Three Types of Attacks

Ciphertext only (adversary only has ciphertext, wants to find plaintext or key)

Known plaintext (adversary has the ciphertext for a known plaintext, wants to find the key)

Chosen plaintext (adversary can generate ciphertext for any plaintext, wants to find the key)

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.

-------------------------------------------------------------------------------------------------------------------------

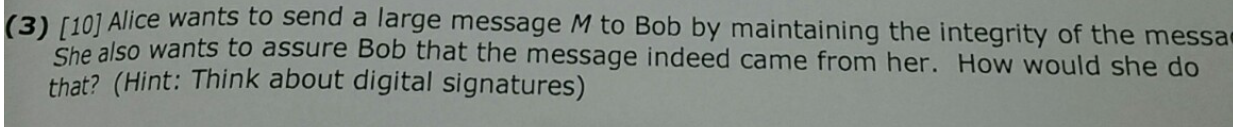
**Digital Signature:** lect7

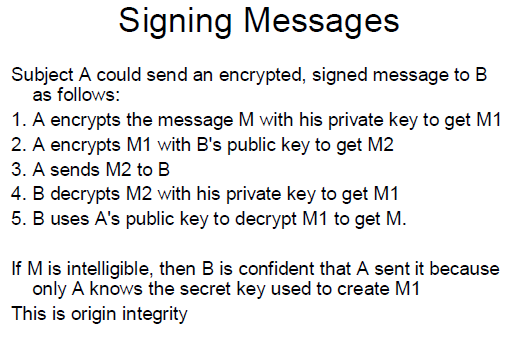
What is digital signature?

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

A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document. Digital signatures are based on public key cryptography, also known as asymmetric cryptography. Using a public key algorithm such as RSA, one can generate two keys that are mathematically linked: one private and one public. To create a digital signature, signing software (such as an email program) creates a one-way hash of the electronic data to be signed. The private key is then used to encrypt the hash.

Kathy wanted to send a secret message to Jack and also assure Jack that the message came from Kathy only. Here you needed to use digital signature with encryption of the message. Most of you did well on this one.





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.

In this PGP question, you need to mention that if the compression is done after the plaintext is encrypted, it won’t find any pattern in the encrypted text and so the size of the encrypted plaintext won’t decrease

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)

Need an answer

This is scenario is wrong because this is not how digital signature works. in order to sign it, that what should happen:

* digitally sign start and stop by my key to get M1
* encrypt M1 with the server's public key to get M2
* then send M2 to the server
* server decrypts M2 with his private key to get M1
* server my public key to decrypt M1 to get M

In the scenario, "start" and "stop" are not encrypted with the server's public key after they signed by my private key, and the server does not use his private key to decrypt the message before using my public key

-------------------------------------------------------------------------------------------------------------------------  
  
**Kereberos**: lect#8

Used for cryptographic key exchange in classical cryptography along with authentication.

Describe briefly the roles of the 3 different servers used in Kereberos.

* The authentication server that authenticates a user and issues him a ticket that allows him to use the authorization server
* The authorization (ticket-granting) server checks whether the user is authorized to use the requested server and if so issues him a ticket to use the server.
* Requested/Target Server: The server checks to make sure the authorization server's ticket is valid and if so grants the user access to the server. For example, the server that serves user request e.g. print server

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

* Kerberos relies on clock synchronization and also dictionary attack is possible which can break this protocol.
* Has to be online
* Single point of failure. If Kerebero server fail, we cannot communicate
* Compromised Kereberos can decipher the message

A ticket will look like this: TX,Y = Y || {X || X address || valid time || kX, Y}kY

-------------------------------------------------------------------------------------------------------------------------

**CAs and KDCs**: lect9

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

* 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 (as described in lecture 8) to get a session key.

• Since a CA is not online, it can be simpler (economy of mechanism)

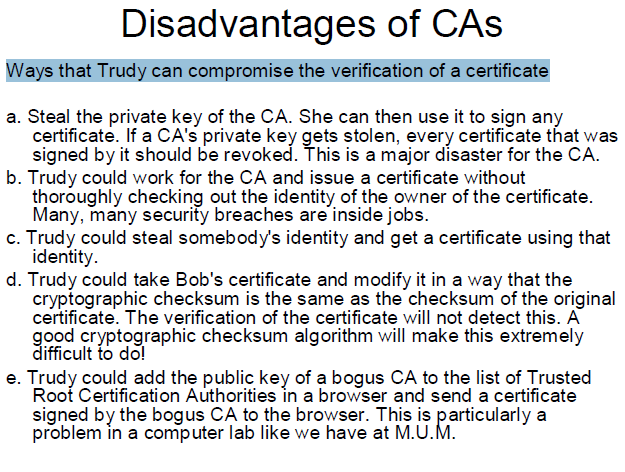
• There is no single point of failure for a CA. But if the KDC (Cathy) goes down, Alice and Bob cannot create a session key.

• 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.

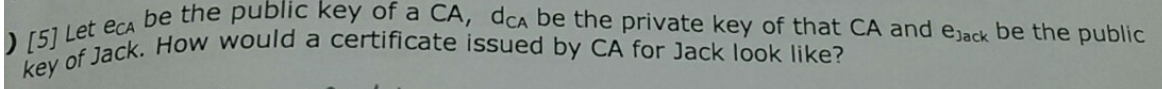
• Since a compromised CA doesn't have a private key, it can't decipher conversations but a compromised KDC can (it has the keys that it shares with the users that trust it). That is, you have to trust a KDC more than a CA. All you give the CA is your public key.

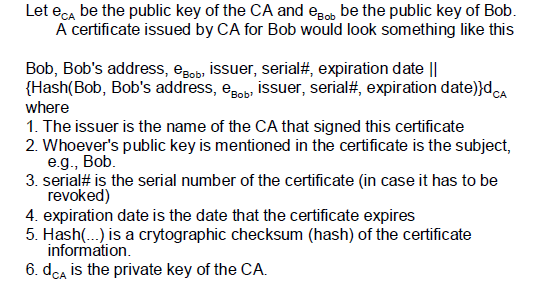
The major disadvantage of a CA is the certificate revocation problem (point number#1 in disadvantage picture)

How a trudy could compromise the verification of a certificate – straight from the lecture notes.



How the certificte issued by CA will look like:





-------------------------------------------------------------------------------------------------------------------------

**Miscellaneous**:

Fill in the blank:

*Vulnerabilities* are weaknesses in the systems that allow an attacker to carry out a threat.

b)        *Chinese Wall Model* is a model of a security policy that refers equally to confidentiality and integrity, and deals with conflict of interest.

c)        Maharishi’s Vedic Science is based on *knower (Rishi)*, process of knowing (Devata) and the known (Chandas) and the wholeness from which they arise.

d)        In an ACM, only allowed permissions are shown. A blank square in the ACM means that the associated process has no permissions on the associated object. This follows the principle of *fail-safe defaults*.

-------------------------------------------------------------------------------------------------------------------------  
  
**SCI**:

Relate 2 security principles 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)