

Remember that these are *outline* answers only, a full answer may need more detail. If you have a specific question please contact me.

If you think one of my answers is wrong, please let me know. We all make mistakes.

QUESTION 1

Does Mandatory Access Control (MAC) provide a partial or complete solution to the confinement problem or no solution at all? Why/Why not?

Yes, a partial one. It does keep information confined to some extent, in that you can't write to or access some documents. For example, in a simple one dimensional hierarchy you can't write below your security level. However, this doesn't stop you copying information from a document that you can see into another document you can write to.

QUESTION 2

Consider an access control system based on the Chinese Wall principle. There are four conflict of interest classes, each with three members.

- i) Assume that a user has the label [2, null, null, 1]. Could the user view a document with the label [null, 2, null, 1]?
 - ii) Assume that a user has the label [null, 2, null, 1]. What is the user's label after attempting to view a document with the label [3, null, 2, 1]?
 - iii) Assume a user has a label which is the same as your answer to part ii). Give a document label for which that user could not view that document.
- i) Yes
 - ii) [3,2,2,1]
 - iii) For example [3,2,2,2]. Any label where they differ in at least one entry where both of them aren't null will do

QUESTION 3

What is a CRL? How is it used? What is a delta CRL? How is it used?

A Certificate Revocation List. It is used to inform certificate verifiers of issued certificates that should no longer be regarded as valid. When a certificate is checked the list of certificate serial numbers in the CRL is checked and, if the number of the certificate being checked appears in the list, the certificate is considered invalid.

A delta Certificate Revocation List is a small update to the main CRLs. Rather than issuing a complete, new, CRL, a delta CRL is issued, giving the serial

numbers only of certificates recently revoked. It is used in conjunction with CRL, in the same way.

QUESTION 4

Physicians prescribe medication. However, it is not a good idea to allow physicians to prescribe medication for themselves. Using RBAC, give the necessary definitions, including a role *Physicians*, that will allow users assigned to that role to prescribe medications, but not to themselves.

Roles: R1(Doctor), R2(Patients)

Permissions: P1 (Prescribe medication for Patients)

Assign P1 to R1

Doctors have both R1 and R2 as assigned roles

The tricky bit is how to stop doctors prescribing to themselves

Two possible ways

1. Use the difference between assigned (long term roles) and active (current session) roles. Remember that active roles are a subset of a user's assigned roles.

Put a condition on R1: Not active(R2)

Put a condition on R2: Not active(R1)

This means the roles can't be made active if the other one is

2 Put a condition on the permission

Not user = patient

That is the active user (the member of the doctor role) can't be the same user as is being prescribed to

QUESTION 5

In a system which uses a KDC, what is the minimum necessary information that a ticket should contain?

A key to be used for communication

The entity the key is to be used with

Expiry time and identification of issuing KDC would also be nice, but aren't absolutely necessary

QUESTION 6

Describe how Kerberos handles delegation.

Via forwardable and proxiable tickets – see the lecture notes for this one