

Answer to the Question-1

Compartmentments are designed to enforce the need to know principle which means regardless of clearance, we have only access to info that we only need to know for our job. It basically creates a restriction access in a single level. This is usually needed in MLS applications. If there are two top secret activity and if we only want one of them for our work, in this case compartments help us to retrieve the only one we want instead of fetching all the top secret activities. The compartments 'basically help to identify the objects only the ones we need to know which is why it is called 'need to know' principle.

Answer to the Question-2

a) Advantages of signature based intrusion detection ~~detection~~ as compared to anomaly based intrusion detection:

1) It has low alarm rate. All it has to do is to look up the list of known signatures of attacks and if it finds a match reports it.

2) It is very accurate.

3) The systems are faster since they are only doing a comparison between what they are seeing and a predetermined rule.

b) Advantages of Anomaly based intrusion detection
in contrast to signature based intrusion is given below:-

1) It can track unknown unlike behaviour pattern of detrimental activity.

2) It helps to reduce the limitation problem of signature based IDS.

3) It always conducts through screening of what comes through.

4) It can be more efficient as it has no signatures in some cases.

c) Effective anomaly-based IDS inherently are more challenging than signature-based detection as ~~a~~ for the following reasons:

1) It uses statistical discrimination technique to measure abnormality which is quite complex.

2) In Anomaly based IDS it always has to

depend on known statistical discrimination techniques or fancy modeling technique which might always not be time efficient.

3) AI is really hard, since this technique uses AI in some cases it becomes often complex and challenging to solve a problem.

From the above discussion we can say that anomaly based detection FDs are more challenging because there we need to detect unknown type of pattern everytime we look into a case. So, everytime we need to compute all the factors before we come to a conclusion.

Answer to the Question-3

An example of real-world visual CAPTCHA which is not discussed in the lecture is confident ~~confident~~ CAPTCHA. Confident CAPTCHA is an image based CAPTCHA that can be easily solved by people. In this type of CAPTCHA one has to click images of certain objects that is mentioned above in the top of the CAPTCHA to prove that he is not a bot but a real person. It is actually very time efficient to solve the confidence. For example, if cat is written on the CAPTCHA title, we have to select all the pictures below that has cats in it to prove our confidence.

Answer to the Question - 4

Two advantages of ACLs over capabilities :-

- 1) The protection is data-oriented.
- ~~2) It is better when user is~~
- 2) It is easier comparatively to change rights to a resource.

two advantages of Capabilities over ACLs :

- 1) It is easy to avoid the confused deputy
- 2) It is easier to delete or add users.