1.

I am a little confused about the features of storing access control matrix by columns(ACL) and by rows(capabilities).

According to the reading material, I think the reason why ACL is suitable for data-oriented is that it stores the matrix by columns so the system can easy to find out whether a user has the access permission to a specific files/program. On the other hand, it is not suitable when the user population is large and constantly changing because the access permission of a user to different file/program is stored in different columns. Thus when the population is large, a column will be too long and when the data of a user changes, all columns need to be manipulated.

For capabilities, the passage says, 'The strengths and weaknesses of capabilities are more or less the opposite of ACLs '. I can understand the reason why it is suitable for user population changing constantly but I have no idea if it suits for the large population. In my opinion, when the user population is large, we need to create a large amount of rows to store this data. Could you tell me what I think is correct?

2.

According to the reading material, 'The Slammer worm in January 2003 propagated itself using a stack-overflow in Microsoft SQL Server 2000 and created large amounts of traffic and compromised machines sent large numbers of attack packets to random IP addresses'. I am curious about how this worm attacked database and why it can do that.

3.

Software sandbox: a restricted environment in which it has no access to the local hard disk (or at most only temporary access to a restricted directory), and is only allowed to communicate with the host it came from.

Visualization: Systems that enable a single machine to emulate a number of machines independently. A company that bought two mainframes could use one for its production environment and the other as a series of logically separate machines for development, testing, and minor applications.

Compared with above two methods, trusted computing seems a little more complicated. Could you explain this method to us precisely?

4.

CIA: Confidentiality: Cannot be read

Integrity: Cannot be altered

Availability: Cannot be interrupted

IAAA: Identity: Unique label for unique principle

Authentication: Validation of the principle's identity

Authorization: Permissions granted the principle

Accountability: Metering and auditing of principle