Fundamental Concepts of Data Security
ISEC2001

Security Systems III

Question 1

With the help of an example, explain the fundamental difference between incremental backup and differential backup.

Question 2

It has been suggested that an old hard drive can be securely erased by encrypting the whole drive with a sophisticated algorithm and key, and then destroy the key. Discuss whether this software approach to data erasure is sufficient.

Question 3

Research and find out why wiping data off an SSD drive needs more consideration than regular SATA/PATA hard drives.

Question 4

Compare the two archiving choices: tape vs disk: Discuss the pros and cons of each approach, and explain where you would consider one but not the other.

Question 5

Describe two (2) situations where data masking is particularly important and give three (3) reasons to explain why.

Question 6

Data involved in any data masking must remain meaningful at several levels. Explain what it means by ‘‘meaningful”.

Question 7

One important requirement of data masking is that it must prevent reverse engineering which can compromise the confidentiality of the data. Describe one example of a poor data masking practice that can be reverse engineered by a competent hacker.

Question 8

Explain the fundamental difference between two data masking techniques: substitution and shuffling.

Question 9

Explain the pros and cons of static data masking.

Question 10

Specify at least four major security problems associated with the Cloud Infrastructure-as-a-Service.

Question 11

Explain why it is often a poor practice to follow a vendor's approach to secure a system.

Question 12

SQL injection is a common type of attacks to database servers. In 2014, a university in the United States became a victim of such an SQL injection attack against one of its servers which stored personal information about students and staff. The attack exploited a vulnerability in the outdated database server software to steal personal details of about 900 students and staff. The attacker then contacted the university officials, detailing the breach and making extortion threat. As the university refused to hand over the credentials, the attacker posted the stolen information on a public website.

- Which security goal (Availability/Integrity/Confidentiality) was compromised by this SQL injection attack? Explain your reasoning.
- Suggest three (3) necessary actions that should have been taken by the affected organisation to prevent such an attack from happening and causing damage. For each action, *briefly* explain how it helps.

Question 13

Ransomware attacks are a major data security concern nowadays. In 2016, a ransomware attack known as Petya targeted at computers running certain vulnerable Windows operating systems. In this attack, the victim received an email purporting a job application. It directed the victim to a zip file containing a malicious program which appeared to the victim as a PDF document. Once the victim allowed this malicious program to be executed at the administrator privilege, the ransomware encrypted the master file table and this effectively removed all mappings to actual files on the hard disk. The ransomware then demanded payment from the victim.

- Which security goal (Availability/Integrity/Confidentiality) was compromised in this case? Explain your reasoning.
- Suggest three (3) necessary actions that should have been taken by the affected organisations to address this security threat. For each action, *briefly* explain how it helps.