Book Questions
Chapters 13
Devayan Mandal

13.1 Explain the important differences between application security engineering and infrastructure security engineering.

Ans: The important difference between application security and infrastructure security engineering is that the former focuses more on meeting external security requirements and the later focuses more on meeting internal security requirements. Application security has to do with security requirements specified by the customer's needs. Infrastructure security specifies internal security measures of the software system, team or organization.

13.6 Explain why it is important to use diverse technologies in the development of secure systems.

Ans: It is crucial to use diversified technologies while using distributed systems to prevent complete breakdown of the system by a malicious virus or attack. When diversified technologies are implemented, an external virus may be able to attack one or only a few system components as diversity in platform technology would not have common vulnerable entry points.

13.9 Suggest how you would go about validating a password protection system for an application that you have developed. Explain the function of any tools that you think may be useful.

Ans: System password validation can be carried out by using white-hat hacking strategies. This may include methods used by a hacker for defensive security purposes such as:

1. Testing a keygen or password generation tool to observe if the keygen can crack the password. If the keygen cracks the password, then it is essential to write code for the system which prevents the unauthorized entry.

2. Gaining access into the system by bypassing the password authentication step. If this is possible, it should be ensured that no other method exists which allows an external threat to enter.

3. Gaining access to the system password by the use of system independent hacking strategies such as physically stealing or stealing passwords from other stored databases.

If this is the case, it should be ensured that the system passwords are not stored in any other database and if physical stealing is a possibility then combining finger printing and eye scanning security protection should also be included.

4. Testing if the encryption method used to protect password cannot be easily reversed.