Jaypee Institute of Information Technology, Noida

T1 Examination, 2023
B.Tech CSE & IT, Integrated B.Tech-M.Tech Semester VII

Course Title : Secure Design of Software Systems **Maximum Time : 1 Hour**
Course Code : 21B12CS415 **Maximum Marks : 20**

C431-13.1	Contrast various methods of securing data and invading(breaching) security and privacy.	Understand (Level 2)
C431-13.2	Apply different secure coding practices for improving the security and robustness of software systems.	Apply (Level 3)
C431-13.3	Use various open source security testing tools to discover security problems in the software systems.	Apply (Level 3)
C431-13.4	Analyse and model security requirements during the secure development of the software system.	Analyze (Level 4)
C431-13.5	Evaluate risks and associated impact of various threats and attacks on different vulnerable points present in the software systems.	Evaluate (Level 5)

Question 1. Consider a file transfer service which is used in many organisations to securely transfer sensitive files. This service is attacked by an adversary and some of the victims of the attack includes the BBC, Bristish Airways, US states Oregon DMV (Department of Motor Vehicles). The attack used a zero-day vulnerability. This means the vulnerability is unknown to the developers of the service or anyone capable of mitigating it. The Oregon DMV uses the file transfer service to share files. The Oregon DMV recommend individual to take precautionary measures to protect themselves from the misuse of the information.

You are required to wear a black hat and play the role of the adversary who has attacked the file transfer service. Answer the following questions:

a) Describe four different ways in which the security can be breached in the above scenario? [C431-13.1- 4 marks]

b) Examine and list all possible assets, threats and vulnerabilities corresponding to the system functionalities. [C431-13.4- 6 marks]

c) Examine and list all possible use and abuse cases and model them in a Use Case-Abuse Case Diagram. [C431-13.4- 5 marks]

Question2: Consider a fictious company selling consumer products online. The company has a web server that interacts with customers and backend ERP system. Customer login to website, requests a catalogue which the Webserver displays it to customers, after retrieving the same from the ERP system. Once the customer selects items and quantities, the Webserver edits the customer inputs for accuracy of all fields filled in the order form and sends the list to ERP System. The ERP system send the final order which is displayed by the Web Server back to customer for final review. The Shipping and credit card information is provided by the customer after final verification of the order. The Web server verifies the accuracy of the data filled and send the credit card information and amount of the sale to the credit card company. The credit card company sends an OTP and customer makes final payment. The Webserver notifies the ERP system that sends the information to warehouse which generate the ticket and ship the product.

As a security analyst, you are required to make the context level and Level-1 DFD showing all the possible components of DFD and important trust boundaries. [C431-13.4- 5 marks]