### **3413ICT Network Security**

### **Workshop – 10A**

**Review Questions:**

1. Compare ‘information assurance’ and ‘security assurance’.
2. What is Service Level Agreement? Discuss a case study SLA draft (no more   
   than 5 points) between an ISP and the small-scale entrepreneur where quantifiable security measures should be part of the SLA. (Hint: time taken by the process of detection of intrusions, time taken by the response to intrusions, defined user roles, etc.).
3. Briefly explain following threat types and identify how each of them confidentiality, availability, integrity and non-repudiation:

* Spoofing
* Tampering
* Denial of service
* SQL Injection
* Cross Side Scripting
* Session Hijacking

1. What is threat modelling? Why appropriate threat model is important to design a security framework? Discuss with the help of examples.
2. Briefly explain relative path traversal and SQL injection threats.
3. Explain, with an example (include pseudo code) how ‘sanitise and declassify’ can assist security assurance.
4. How does ‘Attack Surface Analyser’ help in analysing threats to the Microsoft Windows?
5. Briefly explain how ‘Veracode’ service helps to identify security flaws.
6. Discuss potential security vulnerabilities in an e-voting machine (Hint: Compuware report).
7. Explain how ‘Build Security In’ aims to enhance security and software assurance?
8. Give a critical review (200 words) of the paper “Comprehensive experimental analyses of automotive attack surfaces” by Checkoway etal.

**Hands-on Exercises:**

This week you need to complete the lab 4 (available on the course website). Please ensure that you have already completed the previous labs.