# School of Information Technology
# IIT Kharagpur

**Course Id: IT60112 Information and System Security** **End-semester Examination**

**Date: April 27, 2007** **Total Time: 3 Hours**
**Max. Marks: 100**

*Instructions: Answer any five questions. You may answer the questions in any order. However, all parts of the same question must be answered together. Clearly state any reasonable assumption you make.*

1.

(a) What is the importance of review in security assurance? How is it carried out and how is it measured?

(b) How does configuration management help to ensure administrative and operational assurance?

(c) What are the main differences between TCSEC and ITSEC evaluation criteria?

**[8+8+4=20]**

2. In the S/KEY one time password based authentication system, assume that the initial secret number is termed as ‘x’. At some point of time, the password that was used is $h^{t-1}(x)$, where $h^{t-1}(x)$ denotes application of the hash function ‘t-1’ number of times on ‘x’.

(a) Explain stepwise how the challenge response will work for the next password, clearly identifying the challenge, the response, and the verification procedure.

(b) How are the passwords actually entered by a user against a challenge in such a system?

(c) If a user is on a trip where he might be using unsecure client machines like those provided at airports, how can he use the S/KEY scheme?

(d) Which secure system design principles are followed in S/KEY and how?

**[8+4+4+4=20]**

3. Consider a system in which the probability of occurrence of an intrusion is 0.001. While designing an anomaly detection system (ADS), it was found that due to algorithmic inter-dependence, the probability of false positives (raising an alarm when there is no intrusion) is 2% and the probability of true positives (raising an alarm when there is an intrusion) is 99% of the probability of true negatives.

The system administrator (SA) feels that if at least 60% of the alarms generated by the ADS are genuinely due to intrusion, then only he will pay heed to the ADS. Else, he will not use the ADS at all.

(a) Show whether the ADS is acceptable to the SA or not.

(b) If your answer to Question (a) is acceptable, determine what is the minimum rate of occurrence of intrusion up to which the ADS will remain acceptable. If your answer to Question (a) is “Not acceptable”, determine what should be the minimum rate of intrusion so that the system becomes acceptable to the SA? **[10+10=20]**

4.

(a) Briefly describe the different components of an auditing system.
(b) What are the different approaches to auditing?
(c) Describe an application/system software you have developed before and explain how the various approaches to auditing can be included to enhance the security of that system. You must highlight the information you would like to maintain in the log(s).

**[5+5+10=20]**

5.

(a) Briefly explain how an executable-infecting virus can append itself to another executable.
(b) A computer system provides protection using Biba's Low Water Mark Policy. How can a virus spread in this system if the virus was placed on the system at the lowest integrity level?
(c) A computer system provides protection using Bell-LaPadula model. How can a virus spread in this system if the virus was placed on the system at the highest confidentiality level? **[10+5+5=20]**

6.

(a) Briefly explain the different components of Role Based Access Control (RBAC) Model.
(b) What are the different types of constraints that can be used in RBAC?
(c) Describe an application software (for example, banking application, library management system, etc.) that you have developed before and explain how RBAC including various constraints can be applied to this application. **[10+5+5=20]**