RCETCSAC03 - Information Security

Course outcomes:

- Appreciate the value of information to the modern organization
- Understand the CIA triad of Confidentiality, Integrity and Availability
- Appreciate the difficulties that arise when valuable information needs to be shared
- Identify the five leading-edge resources that have up-to-date information on information security.

Syllabus:

UNIT I

Introduction - Security Attacks and Mechanisms

Security Attacks - Security Attacks (Interruption, Interception, Modification and Fabrication), Security Services (Confidentiality, Authentication, Integrity, Non- repudiation, access Control and Availability)-Security Mechanisms - A model for Internetwork security, Internet Standards and RFCs, Buffer overflow & format string vulnerabilities, TCP session hijacking, ARP attacks, route table modification, UDP hijacking and man-in-the-middle attacks.

UNIT II

Encryption

Conventional Encryption Principles - Conventional Encryption Principles, Conventional encryption algorithms, cipher block modes of operation, location of encryption devices.Key Distribution - key distribution Approaches of Message Authentication, Secure Hash Functions and HMAC.

Reference Text Books:

1. ICT-EurAsia (Conference), & Mustofa, K. (2013). Information and communication technology: International Conference, ICT-EurAsia 2013, Yogyakarta, Indonesia, March 25-29, 2013. Proceedings. Berlin: Springer.

2. Kizza, J. M. (2013). Guide to computer network security. London: Springer.