Topics/Content/Outline:
Topics include: critical analysis of computer security from LAN and WAN perspective; evaluating operating system and application security; analysing a given case study to determine and evaluate security solutions.

Expanded Outcomes
Outcome 1 Critically analyse and describe elements of Computer System Security. (Range: Risk Analysis, types of Attacks, hacker techniques, security services, legal and policy issues etc).
Outcome 2 Critically analyse and describe a selection of hardware and physical layer security solutions. (Range: media deployment, encryption/decryption devices, smart cards, chip level and biometric technologies etc).
Outcome 3: Research and analyse network security issues and solutions from the LAN and WAN (Internet) perspectives (Students will submit and present a minor assignment based on a hypothetical or real life network system design) (Range: analysis of requirements, literature survey, appraisal of various approaches and the suggested design solution, includes firewalls, IPS, IDS, VPNs, encryption, trusts, PKE etc).
Outcome 4: Critically evaluate platform specific operating systems and application security issues and solutions. (Range: security issues of popular (e.g. Linux, Windows and significant Proprietary OSs) including multi tier client server architectured systems, networking devices etc.)
Outcome 5: Analyse a given case study with a view to determining and evaluating possible security solutions. (Range: Problem situations and small cases from the required text considered).

Assessment:

Weighting	Nature of assessment	Learning outcomes
60%	Final Exam	1, 2, 3, 4, 5
40%	Assignment on research and analysis of various aspects of security issues	3, 4, 5

Learning and teaching approaches: Lectures, Discussion, Practical – Labs and Research

Learning resources required:
Required Texts: refer to the current programme booklist.

Access to Hardware and Software as per the required text above.

Learning resources recommended: