George Mason University
Graduate Course Approval/Inventory Form

Please complete this form and attach a copy of the syllabus for new courses. Forward it as an email attachment to the Secretary of the Graduate Council. A printed copy of the form with signatures should be brought to the Graduate Council Meeting. Complete the Coordinator Form on page 2, if changes in this course will affect other units.

Please indicate:  ___X__ NEW  ____ MODIFY  ____ DELETE

Local Unit:  ECE/TCOM  Graduate Council Approval Date:

Course Abbreviation:  TCOM  Course Number:  557

Full Course Title:  Network Security Fundamentals

Abbreviated Course Title (24 characters max.):  Network Security Fund.

Credit hours:  3  Program of Record:  MS in Telecommunications

Repeateable for Credit?  ___ D=Yes, not within same term  ___ T=Yes, within the same term  ___ N=Cannot be repeated for credit

Up to hours

Activity Code (please indicate):  ___ Lecture (LEC)  ___ Lab (LAB)  ___ Recitation (RCT)

___ Studio (STU)  ___ Internship (INT)  ___ Independent Study (IND)

Catalog Credit Format  3 : 0 : 0  Course Level:  GF(500-600)  ___X__ GA(700+)

Maximum Enrollment:  45  For NEW courses, first term to be offered:  Fall 2004

Prerequisites or corequisites:

Catalog Description (35 words or less):  Please use catalog format and attach a copy of the syllabus for new courses.: Introduction to full spectrum of network security: Taxonomy, Cybersecurity, organizational structure for network defense, security threats, vulnerability, countermeasures, firewalls, intrusion detection, disaster recovery, law enforcement, and privacy issues. Course reviews actual case studies.

For MODIFIED or DELETED courses as appropriate:

Last term offered:  Previous Course Abbreviation:  Previous number:

Description of modification:

APPROVAL SIGNATURES:

Submitted by:  __Jeremy Allnutt__________________ email: jallnutt@gmu.edu

Department/Program:  __ECE/MS in Telecommunications____ Date:  __June 2003____

College Committee:  ________________________________ Date:  __________________

Graduate Council Representative:  ________________________________ Date:  __________________
1. CATALOG DESCRIPTION
   (a) TCOM 557 Network Security Fundamentals (3.0:3.0:0)
   (b) Prerequisites: TCOM 500
   (c) Catalog Description: An introduction to the full spectrum of network security. Topics include Taxonomy - language commonality in incident handling; National Strategy to Secure Cyberspace; Cybersecurity Organizations - organizational structure for network defense; Best Practices, Security Policy, Threats; actors and tools, countermeasures, vulnerability identification/correction, intrusion detection, and impact assessment; Firewalls and Intrusion Detection Systems; Anti-Virus Software; Active Defense; Disaster Recovery; and Law Enforcement and Privacy Issues. The course reviews threats and vulnerabilities in network systems based on reports, case studies available in the literature, and actual experience.

2. JUSTIFICATION
   (a) Course Objectives:
       This course is intended to provide an introduction to computer system and network security fundamentals. Students will learn about the issues involved in providing secure communications and will leave the course understanding the fundamentals of how systems are developed, installed, protected, and maintained for secure computer systems and communications links. The course is designed as an introductory element treating network security issues in more depth.
   (b) Course Necessity:
       The proposed course is a broad-based introduction to security and assured connectivity issues, which are becoming increasingly important for near instantaneous information sharing. It is designed as a basic course for both systems-oriented students and network-oriented students and so would be offered in Modules 1 and 2 (Network-oriented elements) as well as in Modules 4 and 5 (Systems Engineering-oriented elements) of the TCOM program. Network security is a growing element in all aspects of transfer of information over commercial or government links, and understanding the basic terminology, potential threats, and suitable countermeasures is critical.
   (c) Relationship to Existing Courses:
       This is a new course in the TCOM program that has been designed as a companion course for the pair of 1.5 credit hour courses TCOM 548/556 Security and Privacy Issues in Telecommunications/Cryptography and Network Security, respectively. TCOM 548/556 introduce the broad background to security issues and cryptography while TCOM 557 focuses on specific threats and countermeasures. They are designed as companion courses that may be taken in any order. More advanced courses on the subject of network security issues are given in the Information Systems and Software Engineering programs, e.g. INFS 765 Database and Distributed Systems Security, INFS 762 Information Systems Security, INFS 766 Internet Security Protocols, and INFS 767 Secure Electronic Commerce.
3. APPROVAL HISTORY

ECE Department Date: June 2003
IT&E Graduate Committee Date: June 2003
IT&E Dean Date:

4. SCHEDULING
Every fall semester, starting in 2003 and every fall thereafter. It would be a natural precursor to the pair of courses, TCOM 548/556, which are offered every spring. Proposed Instructors: Jeremy Allnutt, Jerry Martin, and suitably qualified faculty and adjunct professors.

5. COURSE OUTLINE

Syllabus for Network Security Fundamentals


Overview and a Common Language: COMPUSEC taxonomy: standardizing terminology, categorization, identification, and response.


Protecting the National Infrastructure: An investigation and review of the published direction the administration has chosen to safeguard national assets.

Week 3 (reading: National Strategy to Secure Cyberspace, www.whitehouse.gov)

Best Practices: A review and discussion of best practices from backbone ISP perspective down to individual home user. Case Study #1 (from bsp.cio.gov) due.

Week 4 (reading: ISO/IEC JTC1 ’Guidelines for the Management of IT Security (GMITS)’ TR 13335 Parts 1 to 5)

Security Policy: The development of comprehensive organizational policies and the importance of implementation and enforcement.

Week 5 (reading: TBD)

**Week 6** (reading: TBD)

**Threats**: DoS attacks: tools, availability, concept, targeting, goals, actors. DDoS attacks: concept, objectives, tools, actors.
Case Study #2 (from bsp.cio.gov) due.

**Week 7** (reading: TBD)

**Threats**: DNS cache poisoning, BGP table corruption, concept, objectives, tools, actors.

**Week 8**

Midterm

**Week 9** (reading: Intrusion Detection Systems, Robert Winkler, December 9, 2000)

Firewalls and Intrusion Detection Systems
Case Study #3 (from bsp.cio.gov) due.

**Week 10** (reading: TBD)

**Anti-Virus protection**: tools, availability, concept, goals

**Week 11** (reading: TBD)

**Threats**: DNS cache poisoning, BGP table corruption, concept, objectives, tools, actors.

**Week 12** (reading: Know Your Enemy: Defining Virtual Honeynets


04 September, 2002)

**Active Defense.** Techniques, tools and procedures to proactively respond to cyber attacks.

**Week 13** (reading: TBD)

**Disaster Recovery.** Techniques and activities to recover from major cyber attacks.


**Law Enforcement and Privacy Issues.** Law enforcement: applicable laws, jurisdiction, forensics, international law. 7 – 10 page paper due.

**Challenges for the Future.**
Week 15

Final

(a) Reading and Reference Material

Listed by week

(b) Student Evaluation Criteria

Homework: 15%
Midterm: 35%
Paper: 15%
Final: 35%