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: 662

Full Course Title: Advanced Secure Networking

Abbreviated Course Title (24 characters max.): Adv. Secure Networking

Credit hours: 3.0  

Program of Record: MS in Telecommunications

Repeatable for Credit?  ___ D=Yes, not within same term  Up to hours  

___ T=Yes, within the same term  Up to hours  

___ N=Cannot be repeated for credit

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

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

__ Seminar (SEM)

Catalog Credit Format  3.0: 3.0: 0  

Course Level: GF(500-600) ___X__ GA(700+) ___

Maximum Enrollment: 35  

For NEW courses, first term to be offered: Spring 2005

Prerequisites or co-requisites:  prerequisite course TCOM 509 and TCOM 562

Catalog Description (35 words or less)  Please use catalog format and attach a copy of the syllabus for new courses: Examines adv. technologies in network security; network perimeter defense; components for complete layered defense. Examines component and technological vulnerabilities of TCP/IP, router access control list (ACL), dynamic ACL, firewall, network address translation (NAT), virtual private network (VPN), IPSec tunnels, intrusion detection system (IDS), routing protocol security, denial-of-service (DOS) attack, DOS detection and mitigation techniques.

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:  _Oct. 18th, 2004___

College Committee:  

Date:  __Oct. 21st, 2004___

Graduate Council Representative:  

Date:  ____________________
GEORGE MASON UNIVERSITY  
Course Coordination Form

Approval from other units: Not Applicable

Please list those units outside of your own who may be affected by this new, modified, or deleted course. Each of these units must approve this change prior to it being submitted to the Graduate Council for approval.

<table>
<thead>
<tr>
<th>Unit:</th>
<th>Head of Unit’s Signature:</th>
<th>Date:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Graduate Council approval: ___________________________________________ Date: __________

Graduate Council representative: __________________________ Date: __________

Provost Office representative: ___________________________ Date: __________
1. CATALOG DESCRIPTION
   (a) TCOM 662 Advanced Secure Networking (3:3:0)
   (b) Prerequisites: TCOM 509 (TCP/IP) and TCOM 562 (network Security Fundamental) and a working knowledge of network routing protocols
   (a) Catalog Description:
   This course deals with the advanced technologies in network security that can be applied to enhance enterprise and ISP’s network security. It covers the network perimeter defense concept and the various components for a complete layered defense system. It examines each component and its technologies, including TCP/IP protocol vulnerabilities, router access control list (ACL), dynamic ACL, firewall, network address translation (NAT), virtual private network (VPN), IPSec tunnels, intrusion detection system (IDS), routing protocol security, denial-of-service (DOS) attack, DOS detection and mitigation techniques.

2. JUSTIFICATION
   (a) Course Objectives:
   At the conclusion of this course, the student will have learned the concept of perimeter security, the components of a layer defense system, and the skills to apply these techniques to design and to implement real-world network security. It provides students with the opportunity to understand all potential network vulnerabilities, the ability to examine and compare technologies that enhance the network defense, and to evaluate evolving new standards and procedures.
   (b) Course Necessity:
   Since the explosion of the Internet with the World Wide Web, our increasingly internetwork-dependent society has been under attack by those who would subvert the Internet for political, economic, and/or personal gain. The field of network security represents the defense components to prevent, detect, analyze, and mitigate these attacks. New technologies emerge and new standards are being proposed to defend against these constantly changing attack procedures. This course will provide students with an understanding of the current state-of-art in network security as well as the ability to examine and study emerging defense procedures and new standards.
   (c) Relationship to Existing Courses:
   This is a new course in the TCOM program that has been designed to provide a body of knowledge that is directly applicable to the needs of the telecommunications industry. It builds on other courses within the program (TCOM 501/502, TCOM 509/519, TCOM 548/556, and TCOM 562) with the goal of applying network-engineering skills to the field of network security and attack forensics. This course will work on the base of TCOM 562 and work hand in hand with proposed new forensics courses TCOM 660 and TCOM 661 as part of core courses within a network forensics and security certificate. Since it mostly deals with network devices, routing protocols security and the routing techniques instead of applications and servers, it will not significantly overlap, but be complementary to, courses currently offered in Information Systems in the security assurance area.

3. APPROVAL HISTORY
   ECE Department Date: October 18th, 2004
   IT&E Graduate Committee Date: October 21st, 2004
4. **SCHEDULING**
Every spring semester, starting spring 2005 and every spring thereafter.
Proposed Instructors: Dr. Jeremy Allnutt, Dr. Yunqing Wu, Mr. Scott Robohn and other suitably qualified faculty.

5. **COURSE OUTLINE**
(a) Syllabus

**Week 1**
*Course overview*: Introduction to the course and review of TCP/IP; TCP/IP protocol vulnerabilities, review of general attack, defense techniques and recent trends.

*Project discussion*

**Week 2**
*Perimeter security and layered defense model, router ACL*: perimeter security model, each component of layered defense system, first layer of defense: perimeter router, router access control list (ACL), Cisco router ACL configurations and router ACL defense case study

**Week 3**
*Advanced filtering and deep packet scan*: communication states, stateful filtering, dynamic ACL, reflexive ACL, content-based ACL, deep packet scan

**Week 4**
*Firewall and NAT/PAT*: The role of firewall, different type of firewalls, network address translation (NAT), port address translation (PAT), firewall case study, PIX firewall and enterprise network security case study

*Course project initiated*

**Week 5**
*VPN and IPSec tunnels*: VPN concept, different types of VPN, remote access VPN, GRE tunnels, MPLS layer 2 and Layer 4 VPN, review of public vs. private key encryption techniques, IPSec VPN

**Week 6**
*IPSec VPN and enterprise network security case study*: continued IPSec VPN discussion, Cisco configuration, enterprise network layered defense case study

**Week 7**
*Intrusion detection system (IDS) and mid-term review*: IDS introduction, IDS types: host-based IDS and network-based IDS, IDS architecture, IDS roles, mid-term examination review

**Week 8**
*Mid-term examination and project progress discussion*

**Week 9**
**IDS continued: Snort system:** Snort architecture, preprocessors, Snort rule set, snort deployment, example rules, Snort enhancement and other post Snort projects

**Week 10**
**Router security and routing protocol security:** role of router, router hardening, routing protocol security: EIGRP, OSPF, BGP, BGP with MD5 and other BGP security proposals (sBGP, soBGP, TTL hack etc)

**Week 11**
**Router security continued and ISP packet filtering:** protecting routing engine: Cisco rACL and Juniper firewall rules, BGP TTL hack, dynamic ACL filtering and rout-map, anti-spoofing ACL, RPF (Reverse path forwarding) and uRPF (unicast reverse path forwarding)

**Week 12**
**ISP network security and DOS attack:** DOS attack, different types of DOS attack, DDOS (Distributed Denial-of-services), ISP security response procedure, typical ISP attack identification and classification techniques, classification ACL, blackhole filtering

**Student projects due**

**Week 13**
**DOS attack detection and mitigation:** remotely triggered blackhole filtering, sink hole network, backscatter traceback techniques, netflow traceback, BGP policy accounting traceback, DOS mitigation: ACL, uRPF, CAR (committed access rate) and blackhole filtering

**Week 14**
**Special topics in network security, project discussion, and final exam review:** home-network security, wireless network security, VoIP security, email anti-spamming, selected project discussion, and final review

**Week 15**
Final exam

(b) Required Reading and Reference Material

- **Mandatory textbook:**

- **Reference books:**
Online Resources:
- [http://cert.org](http://cert.org)
- [http://www.sans.org](http://www.sans.org)
- [http://www.insecure.org](http://www.insecure.org)
- [http://www.snort.org](http://www.snort.org)
- [http://www.ietf.org](http://www.ietf.org)

(c) Student Evaluation Criteria

<table>
<thead>
<tr>
<th>Evaluation</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mid-term:</td>
<td>35%</td>
</tr>
<tr>
<td>Project:</td>
<td>30%</td>
</tr>
<tr>
<td>Final:</td>
<td>35%</td>
</tr>
</tbody>
</table>