TCN4081 - Telecommunications Network Security

Three Credits, Four and a half hours, Engineering Topic.

Instructor: Dr. Yu Du

Textbook: Mark Ciampa, Security+ Guide to Network Security Fundamentals, Fifth Edition. Course Technology, Cengage Learning, 2015, ISBN 13: 978-1-305-09391-1.

Specific Course Information:

This course is intended to provide students with the security aspects that are associated with various types of networks. It introduces the fundamentals of network security, including compliance and operational security; threats and vulnerabilities; application, data, and host security; access control and identity management; and cryptography. The course covers new topics in network security as well, including psychological approaches to social engineering attacks, Web application attacks, penetration testing, data loss prevention, cloud computing security, and application programming development security. Students will also engage in activities that link to the Information Security Community Site. The students will be exposed to Number Theory, Steganography, Encryption Design Principles and Algorithms, Message Authentication and Digital Signature Principle and Designs, and Network System Security Design. This course offers a comprehensive guide for anyone wishing to take the CompTIA Security+ SY0-301 Certification Exam.

Specific Goals for the Course

a. Specific outcomes of instruction

Upon successful completion of this course, the student will:

1.Describe many of the vulnerabilities associated with network attacks
2.Identify Malware and Social Engineering Attacks
3.Conduct Vulnerability Assessment and Attack Mitigation
4.Determine the requirements for Wireless network security
5.Describe and use various Cryptographic methods
6.Apply concepts in Number Theory in cypher techniques
7.Use the concept of Steganography to hide information in different mediums.

b. Explicitly indicate which of the student outcomes listed in Criterion 3 or any other outcomes are addressed by the course.

In this course the student will have to show

(a) an ability to apply knowledge of mathematics, science, and engineering (X)
(b) an ability to design and conduct experiments (simulations), as well as to analyze, interpret data (X)
(c) an ability to design a system, component, or process to meet desired needs (X)
(d) an ability to function in multi-disciplinary teams (N/A)
(e) an ability to identify, formulate, and solve engineering problems (homework) (X)
(f) an understanding of professional and ethical responsibility (X)
(g) an ability to communicate effectively (through project reports) (N/A)
(h) the broad education necessary to understand the impact of engineering solutions in a global and societal context (X)

(i) a recognition of the need, and an ability to engage in life-long learning (N/A)
(j) a knowledge of contemporary issues (X)
(k) an ability to use the techniques, skills, and modern engineering tools necessary for engineering practice (X)
(l) a knowledge of probability and statistics (X)

Brief list of the topics to be covered

1. Introduction to Security & Malware and Social Engineering
2. Application and Network Attacks & Vulnerability Assessment & Host, Application and Data Security
3. Basic Cryptography & Advanced Cryptography & Network Security Fundamentals
4. Administering a Secure Network & Wireless Network Security
5. Mobile Device Security & Access Control Fundamentals
6. Authentication and Account Management & Business Continuity
7. Risk Mitigation & Final Exam

GRADING:

Course Requirements	Weight
Discussion Forum Postings/Participation	15%
Self-Assessments	10%
Group Research/Project	15%
Midterm Exam	30%
Final Exam	30%
Overall Grade	100%

Conversion of Numerical Grade to Letter Grade

92<= A <=100	82 <= B< 88	70<= C < 78
90<= A- < 92	80<= B-< 82	60 <= D < 69
88 <= B+ < 90	78 <= C+ < 80	F: Below 60