CSCI 454 – Introduction to Network Security (Fall 2015)

INSTRUCTOR
Instructor: Ayankunle Taiwo, Ph.D.
Office: TBA
Office hours: by appointment
Phone: TBA
Email: Ayankunle.Taiwo@tamuc.edu (Please indicate the course number in the email subject line)

CLASS MEETING
Location: TBA
Time: R 4:30–7:10PM (3 credits)

COURSE DESCRIPTION
This course introduces key concepts in network security. Topics include cryptography including symmetric/asymmetric ciphers, cryptographic hash functions, message authentication codes, and digital signatures; mutual trust including key distribution and user authentication protocols; network and Internet security including transport security and IP security; and network system security including firewalls and intrusion detection systems.

EXPECTED STUDENT LEARNING OUTCOMES
• Be able to define basic network security principles.
• Be able to evaluate applied cryptography techniques including symmetric ciphers, public key encryption, hash functions, and digital signatures.
• Be able to state mutual trust methods including key distribution and user authentication protocols.
• Be able to state network and Internet security techniques including transport security and IP security.
• Be able to explain system security tools for network security including firewalls and intrusion detection systems.

PREREQUISITES
• Corequisites C: CSCI 454L
  Prerequisites: Lvl U CSCI 434 Min Grade C, or instructor’s permission required

COURSE MATERIAL:
EVALUATION

Homework 30%
Midterm Exam 30%
Final Exam 40%

GRADING SCALE

A 90-100
B 80-89.x
C 70-79.x
D 60-69.x
F Below 60

LATE POLICY

The deadline for any assignment can be extended with a 15% penalty per day. No deadline can be extended by more than two days. Assignments will NOT be accepted 48 hours after the due date.

MAKEUP POLICY

There will be no makeup exams in general. Makeup exams may be given to students under extreme circumstances, such as hospitalization, serious injury, death in the family, etc, with prior notification and valid documents.

COLLABORATION POLICY

Students are encouraged to talk to each other, to the instructor, or to anyone else about any of the assignments. Any assistance, though, must be limited to discussion of the problem and sketching general approaches to a solution. Each student must write out his or her own solutions to the homework. Consulting another student's or group's solution is prohibited, and submitted solutions may not be copied from any source. These and any other form of collaboration on assignments constitute cheating. If you have any question about whether some activity would constitute cheating, please feel free to ask.

ACADEMIC INTEGRITY

Your commitment as a student to learning is evidenced by your enrollment at Texas A &M University-Commerce. "All students enrolled at the University shall follow the tenets of common decency and acceptable behavior conducive to a positive learning environment." (See Student’s Guide Handbook, Policies and Procedure, Conduct). All phones, pagers, and other communication devices are to be turned off or place on silent mode during class. Instances of academic dishonesty will not be tolerated. Cheating on exams or plagiarism (presenting the work of another as your own, or the use of another person's ideas without giving proper credit) will result in a failing grade and sanctions by the University. For this class, all assignments are to be completed by the individual student unless otherwise specified. Anyone cheating will receive a zero on the work they are doing, and subsequent cheating will result in a failing grade.

STUDENTS WITH DISABILITIES

The Americans with Disabilities Act (ADA) is a federal anti-discrimination statute that provides comprehensive civil rights protection for persons with disabilities. Among other things, this legislation requires that all students with disabilities be guaranteed a learning environment
that provides for reasonable accommodation of their disabilities. If you have a disability requiring an accommodation, please contact:

Office of Student Disability Resources and Services  
Texas A&M University-Commerce  
Gee Library, Room 132  
Phone (903) 886-5150 or (903) 886-5835  
Fax (903) 468-8148  
StudentDisabilityServices@tamu-commerce.edu

**Basic Tenets of Common Decency**

“All students enrolled at the University shall follow the tenets of common decency and acceptable behavior conducive to a positive learning environment.” (Student's Guide Handbook, Policies and Procedures, Conduct.) This means that rude and/or disruptive behavior will not be tolerated.

**Smoke, Vapor & Tobacco Free Environment**

University Procedure 34.05.99.R1 now prohibits the use of vapor/electronic cigarettes, smokeless tobacco, snuff and chewing tobacco inside and adjacent to any building owned, leased, or operated by A&M – Commerce.

**Disclaimer**

This syllabus is meant to provide general guidance of what to expect from this course. The instructor reserves the right to make changes as appropriate based on the progress of the class. All changes made to this syllabus during the semester will be announced. This document has been posted electronically. If you print a copy of it, please be sure to consult the last modified date of the online version to verify that your printed copy is current.
COURSE SCHEDULE (TENTATIVE):

Section1 (Week 1)
Security Basics and Course Overview
Introduction, course overview, and why security is harder than it looks

Section2 (Week 2-4)
Cryptography: Its Uses and Limitations
Introduction to cryptography
JCA; Private-key encryption basics
Private-key encryption, message authentication
Message authentication, hashing, basic number theory
Diffie-Hellman key exchange; the public-key setting; public-key encryption
Public-key encryption, non-malleability
Digital signatures. Crypto pitfalls
Crypto pitfalls and case studies; circumventing crypto; side channel attacks
WEP insecurity:

Section3 (Week 5-6)
System Security
General principles, introduction to systems security
Access control, ACLs vs. capabilities, access control models
Access control models, trusted computing

Section4 (Week 7)
Database Security, Privacy, Anonymity
Database security

Section5 (Week 8-9)
Programming Language Security
Database privacy. Buffer overflow attacks
Buffer overflow attacks, SQL injection attacks

Section6 (Week 10-13)
Network Security
Web security, XSS, XSRF, etc.
Authentication overview; password-based authentication
Authentication protocols, password security
Authentication and key exchange; mediated key exchange
Authentication and key exchange
Protocols for mediated authentication. PKI and certification authorities

Section7 (Week 14-15)
Network Security in Practice
PKI and certification authorities
Intrusion detection and firewalls
Network security protocols in practice. Introduction to Wireshark. SSL, IPsec, and IKE. Course summary.
Revision

Week 16 Final exam