UTSA
Department of Electrical and Computer Engineering
EE 5453 – Computer and Network Security
Syllabus – Spring 2020

Part A - Course Outline

Course Description:

3 hours credit.
Introduction to computer and network security: cryptography (symmetric key encryption, public key encryption, digital signature, etc.), authentication, network security protocols, access control, etc.

Prerequisites:

Basic computer programming knowledge (and the ability to learn programming concepts/tools on your own) in any modern language is expected. In particular, part of the final project will require you to develop code.

Major Prerequisites by Topic:

Computer programming.

Course Objectives:

1. Demonstrate basic knowledge in cryptography
2. Demonstrate basic knowledge in network security protocols
3. Demonstrate basic knowledge in access control
4. Demonstrate the ability to apply basic tools and techniques to secure networked systems

Evaluation Methods:

1. Exams
2. Assignments
3. Project
4. Pop quiz
5. Class Participation

Performance Criteria:

Course objectives 1 through 3 will be evaluated using evaluation methods [1 - 5]

Course Content:

Engineering Science: 2 credits (67%)
Engineering Design: 1 credit (33%)

Class/Laboratory Schedule:

2 hours and 30 minutes of lectures per week.

Course coordinator:

Ram Krishnan – Associate Professor of Electrical and Computer Engineering

Part B – General Course Information and Policies

Instructor:

Ram Krishnan (http://engineering.utsa.edu/rkrishnan/)
Microsoft President's Endowed Associate Professor
Department of Electrical and Computer Engineering
University of Texas at San Antonio
Email: Ram.Krishnan@utsa.edu

Lecture hours:

Tuesdays and Thursdays 11:30 AM – 12:45 PM @ MS 2.02.02

Office hours:

Tuesdays and Thursdays 10:00 PM – 11:15 PM. Instructor's office is currently at BSE 1.518.

Course website:

http://engineering.utsa.edu/rkrishnan/teaching/intro-to-computer-and-network-security/

The above website will be used for general info dissemination. Content (slides, assignments, etc.) for this course will be managed through Blackboard.

Recommended Textbook:

Network Security – Private Communication in a Public World by Charlie Kaufman, Radia Perlman, and Mike Speciner (2nd edition).

Reference Textbook:

Information Security: Principles and Practice by Mark Stamp

Topics:

1. Cryptography basics
   a. Symmetric key cryptosystems: Block encryption, Block encryption modes, Multiple encryptions, etc.
   b. Public key cryptosystems: Diffie-Hellman, RSA, etc.
   c. Hashes and Message Digests
2. Network security protocols for authentication, confidentiality and integrity of data (examples below)
   a. Kerberos
   b. SSL/TLS
   c. IPSec

    d. PKI, PGP, etc.
3. Access control
    a. Discretionary Access Control: Access control matrix (ACLs vs capabilities)
    b. Mandatory Access Control: Mutilevel security models (Bell-LaPadula and Biba)

Evaluation methods:

1. Two Exams – 30% (15% mid-term exam + 15% final exam)
2. Assignments – 30%
3. Project – 20%
4. Pop quiz – 10%
5. Class Participation – 10%

Grading:

A letter grade will be determined based on the nature of students' course performance curve.

Attendance:

No penalties will be incurred for absences during regular class hours. However, it is your responsibility to talk to your classmates and keep abreast of topics covered, announcements and assignments given during missed classes.

Late submission policy for assignments and project:

Late submission is not allowed.

Exam policy:

Exams will be held in-class, closed-book and closed-notes. To be fair to all students, there will be no makeup exams. No credit will be given for a missed exam except under extenuating circumstances such as an unexpected major health issue.

Course evaluation:

Each student completing this course is highly encouraged to evaluate the course toward the end of the semester. The evaluation is used for 2 major purposes: (1) The instructor strongly takes the feedback into account to improve his teaching in the future, and (2) The university utilizes the feedback as one measure to evaluate instructor effectiveness. To encourage student participation, the instructor offers a 1% extra-credit for each student who completes his/her course evaluation.

Counseling services, student code of conduct and scholastic dishonesty, etc.:
Please visit this webpage: **http://utsa.edu/syllabus**

****Tentative** course schedule:**

Please take a look at the Spring academic calendar and the Spring final exam schedules in UTSA ASAP. This is a tentative schedule of lecture topics. We will likely calibrate as we move along. In particular, the Mid-Term exam date is tentative (± 1 week).

Part I: Cryptography basics

14 lectures before Mid-Term

Expected date of Mid-Term Exam: Mar 17 (± 1 week)

Lecture #	Date	Topics Covered
1	Jan 21	Course overview. Security policy vs enforcement vs implementation
2	Jan 23	No face to face lecture. Assignment.
3	Jan 28	Intro to symmetric key crypto, Block ciphers: intro
4	Jan 30	Block ciphers: handling multiple blocks
5	Feb 04	Multiple encryption and meet-in-the-middle attack
6	Feb 06	Integrity
7	Feb 11	Intro to public-key cryptosystem
8	Feb 13	RSA
9	Feb 18	Diffie-Hellman
10	Feb 20	Digital signature
11	Feb 25	Hashing
12	Feb 27	Public Key Infrastructure, passwords
13	Mar 03	Random numbers and secret sharing
14	Mar 05	Mid-Term review
	Mar 10	**Spring Break**
	Mar 12	**Spring Break**
	Mar 17	**Mid-Term Exam (Instructor on conference travel)**

Part II: Authentication and Authorization

13 lectures before Final

Expected Project deadline: 05/05
Final Exam: May 12 @ 9:45 AM

Lecture #	Date	Topics Covered
16	Mar 19	Authentication Protocols basics I
17	Mar 24	Authentication Protocols basics II
18	Mar 26	Mid-Term exam solution review
19	Mar 31	Timestamps, and Intro to Needham-Schroeder
20	Apr 02	Needham-Schroeder

21	Apr 07	Zero-Knowledge Proof [Final Project to be posted (tentative)]
22	Apr 09	Kerberos intro
23	Apr 14	Kerberos
24	Apr 16	Final Project discussion
25	Apr 21	TCP/IP overview and SSL
26	Apr 23	IPSec
27	Apr 28	No face to face class: Attend tech Symposium
28	Apr 30	Discretionary Access Control and Mandatory Access Control
29	May 05	Final exam review
	May 12	**Final exam @ 9:45 AM**
	May 18	Course grade due @ 2:00 PM