CPSC 4600 Biometrics and Cryptography
Fall 2013, Section 0

Course:	CPSC4600, Section 0, CRN 42532		
Title:	Biometrics and Cryptography		
Class Schedule:	EMCS302, MW 2:00 pm-3:15 pm		
Credit:	3		
Faculty:	Dr. Li Yang	Office:	EMCS 314 A
E-mail:	Li-Yang@utc.edu	Phone:	425-4392
Office Hours:	M/T 8:30 am-12:00pm and W 9:00-11:00am		

ADA STATEMENT: Attention: If you are a student with a disability (e.g. physical, learning, psychiatric, vision, hearing, etc.) and think that you might need special assistance or a special accommodation in this class or any other class, call the Disability Resource Center (DRC) at 425-4006 or come by the office, 102 Frist Hall **http://www.utc.edu/Administration/DisabilityResourceCenter/.**
If you find that personal problems, career indecision, study and time management difficulties, etc. are adversely affecting your successful progress at UTC, please contact the Counseling and Career Planning Center at 425-4438 or **http://www.utc.edu/Administration/CounselingAndCareerPlanning/.**

Course Description
The course covers the basic concepts of pattern recognition and biometrics, current major biometric technologies, and then analyzes specific case studies from technical, privacy, and social impact viewpoints. The course also offers a critical study of the cryptographic protocols used in many security applications including authentication, authorization, access control and digital commerce. Both commercial practices and federal government policies for classified information will be explored.

Prerequisites
CPSC 1110, CPSC 3600, and MATH 3030 with a grade of C or better and basic knowledge of information security.

Purpose and Objectives
The purpose of the course is to examine biometric and cryptographic technologies from the viewpoint of systems security administrator, integrator, purchaser, and evaluator. Both biometric and cryptographic systems are very important to the security of systems. So students must understand the fundamentals of these two technologies and be able to competently test and evaluate tools using these technologies, write technical reports on them, do research on them, and understand the process and need of establishing biometrics and cryptographic standards and using them.

Course Requirements
- Regular class attendance.

- Active class and laboratory participation in all discussions; this means spending some quality time reading and preparing for class and lab meetings and discussions
- One mid-term and a comprehensive final examination will be given. Examination make up will be on Reading Day.
- Individual extra credit assignments for the purpose of propping up a bad grade will not be given.
- Students will be required to sign a contract stating that they will not use knowledge acquired in this course for illegal or unethical purposes. This contract may be released to appropriate authorities should the student be suspected of illegal or unethical computer usage.
- Taking notes is encouraged.
- Each student will write a paper and make a technical presentation. Students have the freedom to select topics of interest on the condition that they are related to biometrics or cryptography. You can present your past work, technical reports from industry or selected papers from conferences and journals. You can search the ACM digital library or IEEE Explorer on UTC on-line library. You need to provide a page of abstract and a PowerPoint version of slides for the presentation. All the presentations must address the following questions.

    - How is the problem to be solved?
    - What is the author's solution(s)?
    - How are the solutions to be evaluated?
    - What are the strengths, compared with prior works?
    - Do you think there is any weakness in the proposed work?

* Students are encouraged to present at the ACM Mid-Southeast Conference (November). If your abstract is selected and you present your paper at the conference, you will have 5 points bonus on your final grade. Please go to the following link for more details of the ACM conference: http://www.utm.edu/staff/jclark/midsouth/

Grading Policy

Grades will be based on the following:

Undergraduate
40% Laboratory projects
20% Mid-term examination – covering text material and content of class discussions.
30% Final comprehensive examination – covering text material and content of class discussions
10% a term project that delivers a ppt presentation

Grading Scale

90+ = A; 80-89 = B; 70-79 = C; 60-69 = D; below 60 = F

Primary Texts

- Behrouz A. Forouzan. *Cryptography and Network Security*, McGraw Hill, 2008, ISBN: 0-07-287022-2
- Samir Nanavati, Michael Thieme, Raj Nanavati. *Biometrics: Identity Verification in a Network World*, Wiley, 2002, ISBN: 0-471-09945-7
- Paul Reid. *Biometrics for Network Security*, Prentice Hall, 2004, ISBN 0-13-101549-4

References

- David Hook. *Beginning Cryptography with Java*, Wiley, 2005, ISBN: 0-7645-9633-0
- Bill Ball. *Linux in 24 hours*, Sams. Free version of this book is available online. http://www.linux-books.us/linux_general_0009.php
- Paul Reid. *Biometrics for Network Security*. Prentice Hall, 2004, ISBN: 0-13-101549-4
- John Chirillo, Scott Blaul. *Implementing Biometric Security*, Wiley, ISBN 0-7645-2502-6
- Bruce Schneier, *Applied Cryptography*, Wiley, second edition, ISBN: 0-471-11709-9

IA resources

Please check this link from the UTC InfoSec center for additional resources for your course work and paper: http://www.utc.edu/center-information-security-assurance/resources.php.

Tentative Course Outline

Week 1	Introduction to Cryptography	Traditional Symmetric-key ciphers
Week 2	Introduction to Modern Symmetric-Key Ciphers	Data Encryption Standard (DES)
Week 3	Advanced Encryption Standard (AES)	Encipherment Using Modern Symmetric-Key Ciphers
Week 4	Asymmetric-Key Cryptography	Message Integrity and Message Authentication
Week 5	Cryptography and Hash Functions	Cryptography and Hash Functions
Week 6	Digital Signature	Digital Signature
Week 7	Entity Authentication	Midterm
Week 8	Key Management	Key Management
Week 9	Security Protocols	Security Protocols
Week 10	Introduction to Biometric Technologies	Fingerprint Biometrics
Week 11	Face Biometrics and PCA, LDA	Voice Biometrics and HMM model
Week 12	Handwriting Analysis	Iris Biometrics and DNA
Week 13	Challenges, Law, and Ethics	Presentation
Week 14	Presentation	Review

Course Website and Communication

You can access lecture notes, assignments, and your grades through Blackboard system. The blackboard system is used to communicate with students. Students can use email to communication with the instructor during the week. Emails received after 10pm or during weekend may not be replied. This includes the night before exams.

Makeup/Late Policy

There will be no make-up tests. The final exam grade will replace an exam you miss. **Failure to take the final exam will result in failing the course.** All assignments are to be turned in on or before the assigned due date. You must demonstrate that your lab or assignment is working properly. To verify you must have your lab assignments signed by the instructor. A 25% penalty will be assessed for late assignments for the first week. **No programming assignments will be accepted after the second late week and a grade of zero will be assigned for that assignment.**

Career Planning

If you find that personal problems, career indecision, study and time management difficulties, etc. are adversely affecting your successful progress at UTC, please contact the Counseling and Career Planning Center at 425-4438.

*UTC's Honor Code

The UTC *Student Handbook* describes the Honor Code (pages 7 - 9), which includes the following examples of violations related to computer usage: (UTC Student Handbook page 7 paragraph B.2)

1. Making use of unauthorized assistance during an examination or in preparing a graded assignment
2. Plagiarism
3. Making unacknowledged use of another's computer program
4. Unauthorized use, or misuse, of the University's computing facilities such as:
    - Logging on to an account without the knowledge and permission of the owner
    - Changing, deleting, and adding to the programs, files and data without authorization of the owner
    - Theft of program data and machine resources
    - Attempts to thwart security of any computer system
    - Attempts to disrupt the normal operations of any computer system

In addition, I will not tolerate the use of cell phones in my class. If you have an emergency situation please let me know so accommodations can be made.

Any suspected Honor Code violation in this course will be forwarded to the Honor Court for action, and an F will be assigned for the course grade. All graded work in this course is subject to the Honor Code, including examinations, programming exercises, and any written work prepared for the course.

Important Dates

Class begins	August 19
Last Day to Withdraw without a W	September 1
Labor Day holiday	September 2
Midterm grade notifications	September 30-October 4 (Monday-Friday)
Last Day to Withdraw	October 20 with a W
Fall Break	October 21-22
Thanksgiving Holiday	November 28-December 1
Last Day of Classes	December 2
Final Exam	December 4-9