CSE 664: Applied Cryptography and Computer Security

Spring 2014
Department of Computer Science and Engineering
University at Buffalo, SUNY

Time: Tuesday & Thursday 2:00 pm - 3:20 pm
Location: Frnczk 454
Instructor: Dr. Kui Ren (kuiren@buffalo.edu)
Office: Davis Hall 317 (x645-1587)
Office Hours: Tuesday & Thursday, 12:15pm – 1:45pm and by appointment (email)

Prerequisites: Background in engineering math, computer networks, etc. Having taken CSE 565 is highly recommended

Text book: N/A

Course webpage: Blackboard@UBLearns

Course Description and Objectives

The first goal for students in this course is to learn the fundamentals of applied cryptography, computer & network security, including:

Basic cryptography

- Secret key cryptography, i.e., DES, AES.
- Hash and message digest, MACs
- Public key cryptography, e.g., RSA, Rabin, etc.

Security protocols

- Kerberos, SSL, IPsec
- Key management, PKI
Advanced cryptography

- Zero-knowledge proof, PIR, etc.

Internet security

- Browser security, DNS security
- Case study: Amazon, skype

Wireless and mobile security

- 3G, LTE, WLAN security, RFID security
- Location privacy, Mobile social networks

Project

Course projects fulfill the other two important goals of the course, i.e., 1) the ability to conduct research in the field and 2) the ability to communicate effectively. Two projects will be assigned to each students and/or student groups during the semester. Project result presentation will be required for each student to demonstrate to the class the project outcome.

The projects will be posted through blackboard within the first two weeks of the course.

Exams

There will be two midterm exams, which will be close-book and close-note. Details will be discussed one week prior to the exam. Exam grades will be returned within two weeks after the exam date. There will be NO final exam.

Homework

Four sets of homework will be assigned during the semester. The problem set will be posted via Blackboard system and announced in class. Homework will NOT be collected for grading.

Grading Policy

Your grades will be determined as follows:

<table>
<thead>
<tr>
<th>Component</th>
<th>Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exam I, II</td>
<td>25%</td>
</tr>
<tr>
<td>Project Reports I, II</td>
<td>15%</td>
</tr>
<tr>
<td>Project II Presentation</td>
<td>15%</td>
</tr>
<tr>
<td></td>
<td>50%</td>
</tr>
</tbody>
</table>
Letter grades will be assigned only at the end of the semester. Grade Assignment: (91-100 = A, 85-90 = A-, 83-84 = B+, 81-82 = B, 79-80 = B-, 77-78 = C+, 71-76 = C, 66-70 = C-, 60-65 = D, 1-59 = F). Curving may be applied if deemed appropriate by the instructor.

Completed homework and projects are to be submitted at the beginning of the class on the due date.

Late policy: Late submissions will result in a 20% penalty per day. A day is defined as 24 hours after the day/time the assignment is due (including weekends and holidays). Maximum such delay allowed is 2 days (unless otherwise stated). In addition, no help will be available for a project after its scheduled due date. Projects and exams may be submitted for re-grading no later than two days after they are returned. If you don't pick them up on the day they are returned, it does NOT extend the re-grading deadline. Re-grading requests must be clearly written and attached to the assignment. Work done in pencil cannot be considered for re-grading. When work is submitted for re-grading, the entire work may be re-graded. Note that Project II report will Not be returned to the students.

Incompletes: As per departmental and University policy, Incomplete (I) grades are only given in cases where the student has done satisfactory work, but only lacks one or two assignments/exams because of a type of unexpected emergency or serious illness at the end of the semester and documented. Do not request an "I" grade unless you believe that you actually fall into this category, and you are prepared to present evidence. Incompletes are given only in these very rare circumstances.

Class Attendance

The primary teaching method will be class lectures and discussions. The lectures will discuss topics presented in the syllabus and cover additional material. Class attendance is expected in every class.

Disabilities

If you have a diagnosed disability (physical, learning, or psychological) that will make it difficult for you to carry out the course work as outlined, or that requires accommodations such as recruiting note-takers, readers, or extended time on exams or assignments, please advise the instructor during the first two days of the course so that we may review possible arrangements for reasonable accommodations. In addition, if you have not yet done so, contact the Office of Disability Services.

Academic Honesty Policy

• The value of our courses, grades, degrees and research findings are dependent upon adherence to standards of ethical conduct. Plagiarism and inappropriate collaboration will not be tolerated. In this course we will adhere to the departmental standard for academic integrity, as follows:
As a good rule of thumb, you may discuss any problem in the course as long as no one is using a writing implement (computers included) nor looking at any source code for the assignment. That is, any group work must be verbal only. Obviously you may look at the textbook or class handouts/class notes together. One exception to this rule is that when a friend is having trouble with a small bug, and you notice a typo or other ``silly little mistake", you may point it out to them. More substantive assistance is definitely not allowed, from any source whatsoever, including tutors or friends not enrolled in the course. The professor or teaching assistants will be able to give more help if you are stuck with concepts.

All academic work must be your own. Collaboration, usually evidenced by unjustifiable similarity in assignments, is never allowed. Plagiarism, defined as copying or receiving materials from a source or sources and submitting this material as one's own without acknowledging the particular debts to the source (quotations, paraphrases, basic ideas), or otherwise representing the work of another as one's own, is never allowed. After an appropriate informal review, if any students are found in violation of maintaining academic integrity, sanctions will be imposed, which can be as severe as receiving an F in the course. Especially flagrant violations will be considered under formal review proceedings, which can call for harsher sanctions including expulsion from the University. If you ever have any questions or concerns regarding the policy, particularly as it relates to this course, see your instructor.

Additional information on University-wide policies and procedures is contained in UB Catalog Statement on Academic Integrity

---

**Tentative Lecture Schedule:** course materials access through Blackboard.

Week 1 (Jan. 28, 30): Secret Key Cryptography-DES; Secret Key Cryptography-AES;

Week 2 (Feb. 4, 6): Modes of Operation; Hashes & Message Digests (Projects Posted)

Week 3 (Feb. 11, 13): Number Theory Basics; Public Key Algorithms

Week 4 (Feb. 18, 20): Public Key Algorithms

Week 5 (Feb. 7, 9): Authentication and Key Agreement, Kerberos; PKI, IPsec,

Week 6 (Feb. 25, 27): SSL/TLS, Zero-Knowledge Proof

Week 7 (Mar. 4, 6): PIR, Midterm Exam I (One class lasting 2 hrs)

Week 8 (Mar. 11, 13): DNS Security, Browser Security (Project I Due)
Week 9 (Mar. 18, 20): Spring Break

Week 10 (Mar. 25, 27): E-Commerce Security, Skype Security & SSL Vulnerability

Week 11 (Apr. 1, 3): Cellular, WLAN Security, RFID Security

Week 12 (Apr. 8, 10): Location privacy, Mobile Social Network Security

Week 13 (Apr. 15, 17): Selected Topics, Midterm Exam II (One class lasting 2 hrs)

Week 14 (Apr. 22, 24): Project II Presentation/Demo

Week 15 (Apr. 29, May 1): 04/29 No Class due to Travel, Project II Presentation/Demo

Week 16 (May 6, 8): Project II Presentation/Demo, (Project II Report Due)

* Note: The instructor reserves the right to make changes to this syllabus throughout the semester.