CSE 664: Applied Cryptography and Computer Security

Spring 2016
Department of Computer Science and Engineering
University at Buffalo, State University of New York
Last updated: January 29, 2016

1 Course Information

<table>
<thead>
<tr>
<th>Time</th>
<th>Tuesday and Thursday (11:00 – 12:20)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>NSC 216</td>
</tr>
<tr>
<td>Instructor</td>
<td>Dr. Aziz Mohaisen (<a href="mailto:mohaisen@buffalo.edu">mohaisen@buffalo.edu</a>)</td>
</tr>
<tr>
<td>TA</td>
<td>Hayreddin Ceker (<a href="mailto:hayreddi@buffalo.edu">hayreddi@buffalo.edu</a>)</td>
</tr>
<tr>
<td>Assistant</td>
<td>Dr. Ah Reum Kang (second half of the semester)</td>
</tr>
<tr>
<td>Textbook</td>
<td>No assigned textbook</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>CSE 565 (highly recommended), engineering math, computer networks.</td>
</tr>
<tr>
<td>Phone</td>
<td>716-645-1592</td>
</tr>
<tr>
<td>Office</td>
<td>323 Davis</td>
</tr>
<tr>
<td>Office hours</td>
<td>Tuesday and Thursday (10:00 – 11:00) or by appointment (email)</td>
</tr>
</tbody>
</table>

2 Recommended Reading


Topics covered in applied cryptography are mostly following Katz and Lindell’s and the topics covered in computer security are partly following Goodrich and Tamassia. You do not have to buy any of those books to do well in this course, though.

3 Course Description and Objectives

This course is intended for graduate students only. Students are expected to attend most of the lectures to do well in this course.

In this course, students will learn topics in applied cryptography and computer security. Topics taught in the class and specific contents are focused on various topics in the aforementioned areas and are below. The course combines both lecture-based and project-based approaches. Semester-long projects are the major theme of this course, and require a lot of hacking (details are below).

Attendance of the in-class lectures is not mandatory, and no points are assigned to it, but students are expected to do all lectures to do well in the class. Projects, assignments, and (take home) tests will be discussed only in class.
3.1 Grading

The grading of the course will follow the following grade distribution.

<table>
<thead>
<tr>
<th>Item</th>
<th>Grade</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project</td>
<td>40%</td>
<td>3 deliverables</td>
</tr>
<tr>
<td>Midterm I</td>
<td>20%</td>
<td>take home</td>
</tr>
<tr>
<td>Midterm II</td>
<td>20%</td>
<td>in class</td>
</tr>
<tr>
<td>Assignments</td>
<td>20%</td>
<td>2 assignments</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
<td></td>
</tr>
</tbody>
</table>

- Grade interpretation: $A \geq 90$, $B \geq 80$, $C \geq 70$, etc.

3.2 Project

A large component of the course is a project. The project will be done by a group of 3-4 students. The research project should address a problem related to applied cryptography and computer security. This may include:

- A nontrivial attack on a recently published design, or a widely used system.
- A meaningful defense against a nontrivial attack or vulnerability.
- A design of a protocol, algorithm, or system that improves security/privacy of a prior work.
- An implementation of a recently published work demonstrating previously unknown aspects of it that are equally interesting and unique
- A security analysis of a system or protocol that is not intended as a secure system (or protocol), and highlighting ways to make secure.
- Analyzing a dataset that would result in understanding behavioral traits, use patterns, etc., and can be used for applications of security and privacy.

The work presented as a project for this course has to be done solely for this course, and should not have been submitted for any prior course nor will be used for any future course. Literature surveys are not allowed as a course project.

**Project selection.** It is the responsibility of the students to select their projects and come up with a team. The instructor should be informed of the team members as soon as possible, and no later than the deadline for the project proposal. During the first two weeks of the course, and until the deadline of the project proposal, feel free to use the instructor’s office hours to discuss potential ideas and topics for the project. Before submitting the proposal, make sure that the instructor is aware and approving of the project topic.

**Project deliverables.** Each project will have three (3) deliverables: a proposal, a midterm, and a final report (see below for grading). Each proposal has to be discussed with the instructor before its submission. Such discussion should optimally take place during the office hours. Beside the required deliverables, students have to meet at least three times during the semester (office hours) with the instructor to report progress. The three meetings are expected to align with the deliverables (proposal meeting, midterm meeting, and final meeting). Teams, project topics, and proposals will be posted online (via piazza) after the proposal deadline.

**Project grading and deadlines.** Project deliverables are due on 2/4 (February 4th; proposal), 3/13 (March 13th; midterm report), and 4/28 (April 28th; final report). The first deliverable
(proposal) is worth 2%, the second deliverable (midterm report) is worth 8%, and the final report (including code, data – if you are doing a user study, etc.) is worth 30%. Exceptional project will have up to 5% of extra points.

3.3 Exams and Assignments

The second largest component (tied) of this course is exams. In this course, you will have two “midterm” exams, and we will not use the officially assigned final time slot. Both exams (combined) are worth 40% of the grade. The first midterm is at the end of the first part and the second midterm is at the end of the second part of the course. The first midterm is to take home and is due in three (3) days after its release. The second midterm is in class, and will be closed book exam. The second midterm exam will be held on 5/5 (May 5th) during the lecture time.

The last component in this course is assignments. We will have two assignments that are combined worth 20% of the grade. The purpose of the assignments is to ensure that you learn the core concepts taught in the course, and prepare you for both exams. Both assignments are take home and are due in 7 days from their release. Their release date is to be announced later. All answers to assignments have to be typed in, emailed to the instructor and TA before the deadline, and a printed copy should be delivered during the lecture.

4 Contents and Schedule

Note: 14 weeks of lectures. The week of March 14 to March 19 is the spring break.

Part I: Applied cryptography

• Symmetric key cryptography (1 week): computational cryptography, computational security, pseudorandomness and associated notions, security against CPA and CCA
• Message authentication codes and hash functions (1 week): message integrity, encryption vs message authentication, CBC-MAC, collision resistance and other notions, NMAC and HMAC.
• Pseudorandom permutations (1 week): Feistel networks, DES and its security, AES and its security, introduction to crypto analysis
• Public key cryptography (1.5 weeks): number theory, primes, factoring, and RSA, groups and assumptions in groups, cryptographic applications of number theory
• Public key encryption (1.5 weeks): definitions of security and notions, hybrid encryption schemes, RSA, El Gamal, trapdoor permutations, other cryptosystems; Goldwasser-Micali, Rabin, Paillier, and ABE.
• Digital signatures (1 week): notions and definitions, RSA, hash-and-sign, Lamport’s and recent applications, DSS, certifications, and PKI standards

Part II: Computer Security.

• Networks Security (5 weeks); Transport security: HTTPS, SSL, TLS, RPKI, BGPSEC, IPSEC, DNSSEC; Network attacks and defenses: DDoS, botnets, defenses, passwords, offline attacks, online attacks, reflectors, etc.; Application security: bugs, shellcodes, viruses, worms, viruses, spyware; Web security: cookies, tracking, XSS, SQL injection, defenses; Advanced threats: cyber warfare and APTs
• Privacy (2 weeks): TOR, OTR, GPG, Anticensorship, Social networks, Advanced topics