Applied Cryptography and Computer Security

CSE 664 – Spring 2016

Aziz Mohaisen

University at Buffalo

Basic Information

- Applied cryptography and computer security
- Dr. Aziz Mohaisen (Davis Hall 323)
- Time: Tuesday and Thursday (11:00 – 12:20)
- OH: Tuesday and Thursday (9:30 – 10:30)
- Location (lecture): NSC 216
- TA: Hayreddin Ceker
- Prerequisites: *CSE 565*
  - discrete math, and computer networks.

Basic Information, cont.

- Instructor:
  - Prof. Aziz Mohaisen
  - Davis Hall, 323
  - E-mail: mohaisen@buffalo.edu
  - Phone: 716-665-1592 (no voice mail)
  - Office hours (9:30 – 10:30) before the lecture

Basic Information, cont.

- Textbook: **no textbook is assigned**
- Recommended readings:
  - – Introduction to modern cryptography by Katz and Lindell, CRC, SE 2014
  - – Handbook of applied cryptography by Menezes et al., CRC, FE 1996
  - – Introduction to computer security by Goodrich and Tamassia, Pearson, FE 2010
  - – 19 (or 24) deadly sins of software security: programming flaws and how to fix them. Michael Howard et al, McGraw-Hill (FE) SE 2005 (20xx?)

Basic Information, cont.

- This is a graduate course; stating the obvious
- Objectives of the course
  - Learning in-depth select topics in applied cryptography computer security (50% of time)
  - Learning (in lesser depth) a variety of security topics in computer, networks, and software systems, as well as online privacy.
- Attendance policy: the assumption is that everyone will attend most of the lectures.

Grading Policy

• Project(s)	40%
• Assignments	20% (x2)
• Midterm 1	20% (take home)
• Midterm 2	20% (in class, closed notes)

- A ≥ 90, B ≥ 80, C ≥ 70, D ≥ 60, F < 60.
  - A, A-, B+, B, B-, C+, C, D, F and FX are graded according to http://grad.buffalo.edu/Academics/Policies-Procedures/Grading-Procedures.html

Grading Policy: Projects

- A group of 3-4 students for each project
- Project topics are selected by students in coordination with the instructor
- Deliverables are: proposal, midterm report and final report. Options include:
  - Design a secure protocol
  - Break an existing protocol (security analysis)
  - Implementation a recent work
    - Highlighting new nontrivial and nonobvious findings
  - Data-driven approach to X (security analytics)

Grading Policy: Assignments

- Two assignments for the entire semester.
  - One week window for turning solutions in.
  - Intended to evaluate your understanding of in-class material and to get you to do some active readings/learning out of the class. Midterm prep.
  - Are to be done individually.
    - Academic conduct policies will be strongly enforced
    - Assignments to be typed in. Paper submission.
- Late submission policy:
  - 1h-24h: -25%, 25h-48h: -50%, >48h: -100%

Grading Policy: Midterm 1

- Covers the first half of the course
  - Examines your knowledge of the covered material on applied cryptography
    - May require some coding for solving some of the questions (simple coding)
  - Will be a take-home exam, and any indicators of misconduct will be strongly penalized.

Grading Policy: Midterm 2

- In class midterm. Closed notes exam.
  - – Covers all the material covered in the class
  - – Focuses more on the second half
    - Computer security, network security, software security, and online and data privacy.
  - – Will be held during the last meeting of course

Syllabus

- Part 1: Applied Cryptography (7 weeks)
- Part 2: Applied Security (7 weeks)

Part 1

APPLIED CRYPTOGRAPHY

Syllabus

- Symmetric key cryptography (1 week)
  - Computational cryptography
  - Computational security
  - Pseudorandomness and associated notions
  - Security against CPA and CCA
- MACs/hash functions (1 week)
  - Message integrity
  - Encryption vs message authentication
  - CBC-MAC
  - Collision resistance and other notions
  - NMAC and HMAC

Syllabus, cont.

- Practical constructions and 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

Syllabus, cont.

- 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 2

APPLIED SECURITY

Syllabus, cont.

- Transport security (1 week)
  - HTTPS and IPSEC
  - SSL and TLS
  - RPKI and BGPSEC
  - DNSSEC and DLV
- Network attacks and defenses (1 week)
  - Botnets, DDoS, reflectors
  - Offline and online attacks

Syllabus, cont.

- Application security (1 week)
  - Bugs, shellcodes
  - Viruses, worms, spyware
- Web security:
  - Cookies, tracking
  - XSS, SQL injection, defenses
  - Advanced threats: cyber warfare and APTs
- Privacy (2 weeks):
  - Tor, (anti)censorship, OTR,
  - GPG, social networks, and other advances.

Frequent Asked Questions

1. I did not take CSE 565. Can I take CSE 664?
2. I already took CSE 664. Can I sit in your class?
3. Time conflict. Can I register and not attend?
4. What are you going to teach?
5. Can I do my course project alone?
6. Not attending lectures going to affect my score?
7. If I do well, can you write me a recommendation?
8. Which book should I buy for this course?
9. I cannot attend the midterm. Can you make it up?
10. Can I use the project for a master's thesis?
11. How to compile a X code?
12. Which programming language should I use?
13. Should I do a Ph.D. on topic Y?

More questions?

- Ask now, or
  - Email me on mohaisen@buffalo.edu
  - Come to my office hours (9:30 – 10:30)
  - Call – but no voice mail (I forgot my passwd)