Syllabus

Instructor: Christina Garman (clg@purdue.edu)

Course Webpage: `https://www.cs.purdue.edu/homes/clg/CS590/`

1 Overview

In 2016 more than 2 billion records and $450 billion were lost due to publicly-reported criminal and nation-state cyberattacks across the globe, and over 100 million medical records were stolen in the United States alone. The failure of our existing security infrastructure motivates the need for improved technologies, and cryptography provides a powerful tool for doing this. Over the past several years though, we have seen a number of serious vulnerabilities in the cryptographic pieces of systems, some with large consequences.

This course will cover cryptography as it is applied to real world systems, both in how to build secure systems as well as examining flaws and "breaks" in already deployed systems. We will also discuss the mistakes that led to these flaws, how these flaws could have been prevented, and various tools and techniques that exist for building cryptographic systems in practice. Students will have the opportunity to implement cryptographic schemes and explore cryptographic failures in practice, as well as engage in a semester-long research project related to applied cryptography. The course will consist of a combination of lectures and paper reading/discussions.

Time: Tu/Th 1:30pm-2:45pm
Location: Lawson B134

Prerequisites:

- CS 526 (Information Security) or CS 426 (Computer Security) or permission of the instructor
- Programming experience: Some of the assignments will require programming knowledge and we will be implementing cryptographic schemes, so you should be comfortable programming.
- Strongly recommend either: CS 355 (Introduction to Cryptography) or CS 555 (Cryptography and Data Security) but not required.

2 Office Hours

TBA

I will be available by appointment as well.

3 Grading

The course will consist of a combination of lectures and paper reading/discussions. Each student will be expected to present at least one paper and lead a discussion on the paper. We will also have a few projects, both in implementing cryptographic schemes as well as exploring cryptographic failures in practice. Finally, there will be a semester-long research project related to applied cryptography.

Because this is a seminar-style course and discussion will be important, part of your grade will include a participation component. So please attend class! If you cannot make class for any reason (such as job interviews, etc.), please let me know as you will not be penalized for this.

- Assignments: 50%
- Presentation(s): 10%
- Midterm: 15%
- Course Project: 15%
- Class participation: 10%

Assignments are due at the beginning of class at 1:30pm on the stated due date. Late assignments will be penalized 5 percentage points per day. There is no collaboration allowed on exams. You must do only your own work. There are no textbooks, notes, or computers allowed during exams.

Final grades will be assigned on a curve at the end of the course.

4 Schedule

Please refer to the course webpage for the most up-to-date schedule as it is subject to change.

5 Additional Resources

We will be using Blackboard to submit assignments.

Students are expected to have read the associated paper(s) BEFORE each class.

If you have any suggestions for papers that you would like to present, please let me know!

No textbook is required, but if you would like additional resources the following may be useful:
Handbook of Applied Cryptography by Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone (`http://cacr.uwaterloo.ca/hac/`)
Modern Cryptography: Theory and Practice by Wenbo Mao
Introduction to Modern Cryptography by Jonathan Katz and Yehuda Lindell (`http://www.cs.umd.edu/~jkatz/imc.html`)

6 Computer Science Department Academic Integrity Policy

The Department of Computer Science expects and enforces the highest standards of academic integrity and ethics. The Department takes severe action against academic dishonesty, which may include failing grades on an assignment or in a course, up to a recommendation for dismissal from the University.

Academic dishonesty is defined as any action or practice that provides the potential for an unfair advantage to one individual or one group. Academic dishonesty includes misrepresenting facts, fabricating or doctoring data or results, representing another's work or knowledge as one's own, disrupting or destroying the work of others, or abetting anyone who engages in such practices.

Academic dishonesty is not absolute because the expectations for collaboration vary. In some courses, for example, students are assigned to work on team projects. In others, students are given permission

to collaborate on homework projects or to have written materials present during an examination. Unless otherwise specified, however, the CS Department requires all work to be the result of individual effort, performed without the help of other individuals or outside sources. If a question arises about the type of external materials that may be used or the amount of collaboration that is permitted for a given task, each individual involved is responsible for verifying the rules with the appropriate authority before engaging in collaborative activities, using external materials, or accepting help from others.

A student accused of academic dishonesty must be afforded due process as defined by Purdue University procedures. The Dean of Students Office may be notified concerning an academic dishonesty incident as provided by Purdue University procedures.

7 University Academic Integrity

Academic integrity is one of the highest values that Purdue University holds. Individuals are encouraged to alert university officials to potential breeches of this value by either emailing integrity@purdue.edu or by calling 765-494-8778. While information may be submitted anonymously, the more information that is submitted provides the greatest opportunity for the university to investigate the concern.

Incidents of academic misconduct in this course will be addressed by the course instructor and referred to the Office of Student Rights and Responsibilities (OSRR) for review at the university level. Any violation of course policies as it relates to academic integrity will result minimally in a failing or zero grade for that particular assignment, and at the instructor's discretion may result in a failing grade for the course. In addition, all incidents of academic misconduct will be forwarded to OSRR, where university penalties, including removal from the university, may be considered.

From the University: Purdue prohibits "dishonesty in connection with any University activity. Cheating, plagiarism, or knowingly furnishing false information to the University are examples of dishonesty." [Part 5, Section III-B-2-a, Student Regulations] Furthermore, the University Senate has stipulated that "the commitment of acts of cheating, lying, and deceit in any of their diverse forms (such as the use of substitutes for taking examinations, the use of illegal cribs, plagiarism, and copying during examinations) is dishonest and must not be tolerated. Moreover, knowingly to aid and abet, directly or indirectly, other parties in committing dishonest acts is in itself dishonest." [University Senate Document 72-18, December 15, 1972]

Please refer to Purdue's student guide for academic integrity: `https://www.purdue.edu/odos/academic-integrity/`

8 Purdue Honors Pledge

"As a boilermaker pursuing academic excellence, I pledge to be honest and true in all that I do. Accountable together - we are Purdue." `https://www.purdue.edu/provost/teachinglearning/honor-pledge.html`

9 Emergencies

In the event of a major campus emergency, course requirements, deadlines and grading percentages are subject to changes that may be necessitated by a revised semester calendar or other circumstances beyond the instructor's control. Relevant changes to this course will be posted onto the course website or can be obtained by contacting the instructors or TAs via email or phone. You are expected to read your @purdue.edu email on a frequent basis.

See the University's website for additional information: `https://www.purdue.edu/ehps/emergency_preparedness/`

10 Accessibility and Accommodations

Purdue University strives to make learning experiences as accessible as possible. If you anticipate or experience physical or academic barriers based on disability, you are welcome to let me know so that we can discuss options. You are also encouraged to contact the Disability Resource Center at: drc@purdue.edu or by phone: 765-494-1247.

11 CAPS Information

Purdue University is committed to advancing the mental health and well-being of its students. If you or someone you know is feeling overwhelmed, depressed, and/or in need of support, services are available. For help, such individuals should contact Counseling and Psychological Services (CAPS) at (765)494-6995 and http://www.purdue.edu/caps/ during and after hours, on weekends and holidays, or through its counselors physically located in the Purdue University Student Health Center (PUSH) during business hours.

12 Nondiscrimination

From the University: "Purdue University is committed to maintaining a community which recognizes and values the inherent worth and dignity of every person; fosters tolerance, sensitivity, understanding, and mutual respect among its members; and encourages each individual to strive to reach his or her own potential. In pursuit of its goal of academic excellence, the University seeks to develop and nurture diversity. The University believes that diversity among its many members strengthens the institution, stimulates creativity, promotes the exchange of ideas, and enriches campus life.

Purdue University prohibits discrimination against any member of the University community on the basis of race, religion, color, sex, age, national origin or ancestry, genetic information, marital status, parental status, sexual orientation, gender identity and expression, disability, or status as a veteran. The University

will conduct its programs, services and activities consistent with applicable federal, state and local laws, regulations and orders and in conformance with the procedures and limitations as set forth in Executive Memorandum No. D-1, which provides specific contractual rights and remedies. Any student who believes they have been discriminated against may visit University's website (www.purdue.edu/report-hate) to submit a complaint to the Office of Institutional Equity. Information may be reported anonymously."

Please refer to Purdue's nondiscrimination statement: `http://www.purdue.edu/purdue/ea_eou_statement.html`

13 Grief Absence Policy for Students

Purdue University recognizes that a time of bereavement is very difficult for a student. The University therefore provides the following rights to students facing the loss of a family member through the Grief Absence Policy for Students (GAPS). GAPS Policy: Students will be excused for funeral leave and given the opportunity to earn equivalent credit and to demonstrate evidence of meeting the learning outcomes for misses assignments or assessments in the event of the death of a member of the student's family.

See the University's website for additional information: `http://www.purdue.edu/studentregulations/regulations_procedures/classes.html`

14 Violent Behavior Policy

Purdue University is committed to providing a safe and secure campus environment for members of the university community. Purdue strives to create an educational environment for students and a work environment for employees that promote educational and career goals. Violent Behavior impedes such goals. Therefore, Violent Behavior is prohibited in or on any University Facility or while participating in any university activity.

See the University's website for additional information: `http://www.purdue.edu/policies/facilities-safeiva3.html`