COMPSCI 461/661:
Secure Distributed Systems
SYLLABUS

Prof. Andrew Stone with Brian Levine

Last revised: September 2, 2022

1 Important Details

Credits: 3

Teaching Assistant:
TBD
Undergraduate Class Assistant:
TBD

Piazza (discussion):
`https://piazza.com/class/l798fbw7p8sw9`

Moodle (course materials):
`http://compsci461661.andrewstone.space`

Readings: There is no textbook for this class. Instead, we will be using prepared notes authored by Brian Levine and myself supplemented by selected research papers.

Office Hours: Tuesdays by appointment. Set it up with me on Piazza. Held in my office, TBD.
Office hours will also be offered by the teaching assistants, times and places TBA.

Prereqs 661: You must be a graduate student in Computer Science or have instructor permission. **Prereqs 461:** (CMPSCI 220 or CMPSCI 230) and CMPSCI 240.

2 Introduction

This class is devoted to the study of securing distributed systems. Our goal is to explore a broad collection of classic topics in security, network, and distributed systems. Blockchains will serve as a common thread and cohesive structure for us, however, many topics that we will cover are applicable well beyond blockchains and similar distributed, open ledgers. A blockchain is a novel distributed system that (probabilistically) provides secure computation and storage by carefully orchestrating economic incentives among a set of untrusted peers. Unlike other distributed systems, economic value is an integral component of blockchains.

We will start with describing blockchain operation and theory. We'll also look at the efficiency of the network architectures for peer-to-peer communication and attacks on their security (e.g., eclipse/denial-of-service attacks). And we'll review the operation of applied cryptography including hash functions and elliptic curves (used to validate transactions). We will look at other consensus systems and understand fundamental results from Lamport, Fischer, and Douceur, and see how these results inform the design of consensus systems. Other topics include secure network protocol design, secure distributed programming (via Solidity), probabilistic data structures, privacy, economics, and finance. In examining these concepts, we'll make use of notions from basic probability, Monte Carlo simulation methods, and some proofs on the correctness of algorithms.

Assignments will include advanced programming projects and reading research papers. Students will complete these readings, several take-home assignments based on the readings, and participate in a lively class discussion. In addition, there will be a midterm and final exam. Students will be asked to express an opinion on many topics and challenge the instructor's views and analyses.

The specific objectives for the course are as follows:

- To gain a deep understanding of secure distributed systems, with attention paid to underlying theory as well as the practical blockchain technologies that are in wide use today.
- To gain an understanding of recent research.
- To gain experience in making well-reasoned arguments during class discussion.

Because of the programming assignments, students will need prior experience programming. You must use Python for these assignments. We'll also write Ethereum software contracts in a language called Solidity that I don't expect you to have used before (it's similar to

java/python/C), and Bitcoin Script which is essentially a stack-only assembly language.

2.1 Flipped Class

This course will be making use of a "flipped classroom" model. Lectures will be pre-recorded and available online and will be provided with accompanying written notes. We meet once a week in person for discussion. Discussions will be carried out assuming that students have completed readings and assignments and viewed pre-recorded lectures. There will be some work assigned and completed during discussions (included in "written assignments" portion of the grade). Students who do not attend discussion will lose points towards their final grade.

2.2 List of Topics

Below are an overview of topics covered in this course. The course moodle web site has more specifics and last-minute changes.

1. Applied cryptography [**?**]
   - Definition of security
   - Cryptograph hash functions and hash-based protocols
   - Merkle trees, a secure data structure
   - public/private key crypto using elliptic curves
2. Blockchains
   - Nakamoto consensus [**?**] [**?**]
   - Doublespend attacks (including Gambler's Ruin) [**?**]
   - Selfish mining attacks [**?**] [**?**]
   - Eclipse attacks [**?**]
   - Details of Bitcoin: transactions, blocks, p2p networking [**?**]
   - Ethics
3. Distributed Systems
   - Doucer's Sybil attack (impossibility result) [**?**]
   - Clocks: NTP and Lamport clocks [**?**]
   - Lamport's Byzantine Generals result [**?**]
   - Fischer, Lynch, and Paterson's (FLP) impossibility result [**?**]
4. Engineering Security and Performance
   - Difficulty adjustment (inter-block timing) algorithms
   - Hashrate estimation (quantifying security)
   - Distributed protocols for Fair Exchange and or other services [**?**]
   - Lightning networks
5. Ethereum [**?**]
   - The Ghost protocol (for when interblock times are close to network propagation delay) [**?**]
   - ETHASH (memory bound PoW)
   - Patricia Merkle Trees (authenticated data structures)
   - DAPPS (secure cloud computing)
   - Programming Ethereum with Solidity (`https://cryptozombies.io/`)
6. Finance [**?**]
   - basic overview of economic metrics
   - basic overview of financial instruments (e.g., futures)
   - Initial Coin Offerings
7. Improving Blockchain performance
   - Bloom filters [**?**]
   - Invertible Bloom Lookup Tables (IBLTs) [**?**]
   - Compact Blocks
   - Graphene (optimal application of Bloom filters) [**?**]
   - Low-variance mining with Bobtail [**?**]
   - Proof of stake (avoids carbon pollution; applies game theory and finance to distributed consensus) [**?**]
8. Recent research
   - If time, TBA

3 Inclusive Discussion

In this course, each voice in the classroom has something of value to contribute. Please take care to respect the different experiences, beliefs and values expressed by students and staff involved in this course. I support the commitment of the UMass Amherst College of Information and Computer Sciences to diversity, and welcome individuals of all ages, backgrounds, citizenships, disability, sex, education, ethnicities, family statuses, genders, gender identities, geographical locations, languages, military experience, political views, races, religions, sexual orientations, socioeconomic statuses, and work experiences.

4 Grading

Your overall grade for the course will be derived from three components. At a high-level grading is based on the following formula:

- 50% Written Assignments (including assignments completed during discussion)
- 20% Midterm Exam (evening exam, date TBA)
- 20% Final Exam (during finals week)
- 10% Class participation (including attendance in discussion and online participation)

Additionally, without a grade of 50% or higher on each of the two exams, students cannot pass the class.

Each assignment will have a slightly different number of points. Your score will be the total number of points earned over total number of points available for all assignments. Late homeworks are NOT accepted.

I will assign a `B` grade to students with a final numeric grade equal to the mean of the class. The range of each letter will be based on the standard deviation (sd) of the class grades. An `A` is 1 sd above `B`; `A-` is 0.7 sd above; `B+` is 0.3 above; `C+` is 0.7 below; `C` is 1 sd below. Graduate students at UMass cannot be assigned a grade below a `C` other than a failing grade. I may curve grades or assignments. In previous semesters, a `B` has been about an 85%.

Don't underestimate the *Class Participation* component — full credit versus none can move your final grade by quite a bit. Furthermore, in-class exercises that are missed due to unexcused absences will lower your grade.

4.1 Homeworks

I will use gradescope to accept assignments, which must be in the form of a PDF (no word, text, or other formats), with your name clearly visible. In the case that an assignment involves code, please submit a tar-ball or zip file. I will not accept assignments late, and I will assign a score of zero for work that is not submitted on time (or at all).

If class participation is generally low, or if I get the sense that students aren't reading, or if it seems like good preparation for the midterm or final exams, I will give in-class quizzes. These quizzes may not be pre-announced. They will become part of the homework component of your grade.

Assignments that do not compile will receive no credit.

4.2 Exams

There will be a midterm exam and a final exam. The final will focus on material presented after the midterm, but questions that pull in pre-midterm material are inevitable and are to be expected.

4.3 Class Participation

I will assign this portion of your grade on the basis of your presence and participation in class. Obviously, I expect you to always attend class. Further, I expect you to participate in class discussion, posing and answering questions as appropriate. Also, I expect that you'll leave room for others to speak their minds as well. I will provide feedback about halfway through the semester as to the status of this portion of your grade.

If I have outside experts join us in class, not attending on these days will weigh more heavily against your participation grade.

Fully remote students should participate strongly in Piazza discussions, and occasionally meet with the instructor via video chat as may be determined based on the level of full-remote enrollment.

5 Policies

Cell phones, laptops, and similar devices may not be used during in-class session.

5.1 Collaboration and Plagiarism

Please come see me if you are unable to keep up with the work for this class, for any reason, and I will work something out. Obviously, there isn't anything I can do when the semester has already ended. I want to see you succeed and will do everything I can to help you out. The earlier you let me help, the more help I can offer. I've been here since last millennium and I've seen it all; please come by.

Please be cognizant of the University's policies on cheating. You may discuss material with others, but your writing must be your own. When in doubt, contact me about whether a potential action would be considered plagiarism. When discussing problems with others, do not show any of your written solutions. When asking others for help, do not take notes about the solution other than to jot down publicly available references. Use only verbal communication.

If you do discuss material with anyone besides the instructors, acknowledge your collaborators in each write-up. If you obtain a key insight with help (e.g., through library work or a friend), acknowledge your source, briefly state the insight, and write up the solution on your own.

I expect to see citations if you use an outside source (other than the assigned articles) to complete an assignment. You may directly quote from a decision in order to complete a brief — provided you surround the text by quotation marks — without citation.

It is never permissible to distribute your completed assignments, my homework solutions, exams, or exam solutions to other persons nor to post these materials to Internet sites, including Github and Course Hero. Of course it is not permissible to use such resources as well. Both are obvious violations of the University's academic honesty policies and I will pursue sanctions even after the course is over.

Never misrepresent someone's work as your own. It must be absolutely clear what material is your original work. You must remove any possibility of someone else's work from being misconstrued as yours.

As a condition of continued enrollment in this course, you agree to submit all assignments to the Gradescope, Turnitin and/or My Drop Box services for textual comparison or originality review for the detection of possible plagiarism. All submitted assignments will be included in the UMass Amherst dedicated databases of assignments at Turnitin and/or My Drop Box. These databases of assignments will be used solely for the purpose of detecting possible plagiarism during the grading process and during this term and in the future. Students who do not submit their papers electronically to the selected service will be required to submit copies of the cover page and first cited page of each source listed in the bibliography with the final paper in order to receive a grade on the assignment.

You can and should read the University's policies on cheating as well at `http://www.umass.edu/ombuds/honesty.php/`. In short, intellectual honesty requires that students demonstrate their own learning during examinations and other academic exercises, and that other sources of information or knowledge be appropriately credited. Scholarship depends upon the reliability of information and reference in the work of others. Student work at the University may be analyzed for originality of content. Such analysis may be done electronically or by other means. Student work may also be included in a database for the purpose of checking for possible plagiarized content in future student submissions. No form of cheating, plagiarism, fabrication, or facilitating dishonesty will be condoned in the University community. (Some portions of the above plagiarized from `http://www.umass.edu/academichonesty/AddressingPlagiarism.html`!)

6 UMass Policies

Accommodation Statement. The University of Massachusetts Amherst is committed to providing an equal educational opportunity for all students. If you have a documented physical, psychological, or learning disability on file with Disability Services (DS), you may be eligible for reasonable academic accommodations to help you succeed in this course. If you have a documented disability that requires an accommodation, please notify me within the first two weeks of the semester so that we may make appropriate arrangements.

Academic Honesty Statement. Since the integrity of the academic enterprise of any institution of higher education requires honesty in scholarship and research, academic honesty is required of all students at the University of Massachusetts Amherst. Academic dishonesty is prohibited in all programs of the University. Academic dishonesty includes but is not limited to: cheating, fabrication, plagiarism, and facilitating dishonesty. Appropriate sanctions may be imposed on any student who has committed an act of academic dishonesty. Instructors should take reasonable steps to address academic misconduct. Any person who has reason to believe that a student has committed academic dishonesty should bring such information to the attention of the appropriate course instructor as soon as possible. Instances of academic dishonesty not related to a specific course should be brought to the attention of the appropriate department Head or Chair. Since students are expected to be familiar with this policy and the commonly accepted standards of academic integrity, ignorance of such standards is not normally sufficient evidence of lack of intent (`http://www.umass.edu/dean_students/codeofconduct/acadhonesty/`).

Audio/Video Recording.

Discussions will be recorded and may be made available. The classroom is equipped with Echo360 and all classroom activity will be recorded. In addition, I may use Zoom or equivalent for remote students' participation and recording of class sessions. These recordings may be made accessible to students enrolled this semester and in subsequent offerings of the class.

In order to comply with Massachusetts's wiretapping statute, all students should be aware and understand that all communications for this class may be recorded. By participating in this course, a student consents to any recordings made as a result of student's activity(s) in the course.