SY486C: Anonymous Communication
Course Policy

Spring 2020

Dr. Ellis Fenske Leahy 102 fenske@usna.edu

Course Content

Anonymous Communication protocols are protocols designed to allow users to communicate without leaking identity metadata, obscuring the relationship between sender and receiver of messages. The course will cover:

- The basic well-known tools for providing anonymity: onion routing including Tor, Mixnets, and the Dining Cryptographers protocol.
- Practical attacks and vulnerabilities specific to anonymity protocols: fingerprinting, traffic correlation, intersection attacks, Sybil attacks, related ciphertext attacks
- Steganography
- Data anonymization at rest and differential privacy
- Policy and law around anonymity services
- Selected modern proposed anonymity protocols

Learning Objectives

After the conclusion of the course, students should be able to:

1. Recognize the importance of metadata and discuss design decisions to prevent metadata leakage
2. Implement some basic multiparty anonymity protocols and corresponding attacks
3. Read, understand, and explain modern academic research papers on technologies for security and privacy
4. Write and present a summary of technical work
5. Discuss anonymity in the technical context of the modern Internet and how this intersects with social policy.

Course Resources

There is no textbook for this material, so all materials will be provided on the course website and through notes in class. Academic papers and summaries will be posted for every lecture as references, and students will be expected to take thorough notes and ask plenty of questions in lecture.

Collaboration Policy

Submitted work falls under one of the following collaboration policies:

1. Group work. Students will be paired or assigned to groups and may turn in one assignment on behalf of the group. It is expected that all students in the group participate in these assignments. Discussion of the work outside the group should be limited to verbal, broad comments about stragegies or approaches and not details.

2. Individual work. Students are expected to complete this on their own, though they may discuss the problems with each other. Students should not distribute copies of their work to anyone, and may under no circumstances copy.

3. Final Paper. Students are free to discuss their work and topics with each other, but must write the paper themselves.

Grading Policy

Homework will be given generally every two weeks and may include questions on the readings, short essays, programming assignments, or mathematics. Short quizzes, discussions, and summaries of papers will be given regularly to assess and encourage regular student engagement with the material. Two-thirds of the way through the semester, students will be expected to select a paper topic and write a technical summary of a protocol not covered in class (a list will be provided), a policy paper on a specific topic, or a topic of the student's choice subject to approval. Students will present their papers to each other in the last few class periods, and will submit brief summaries of their peers' presentations.

Category	**Proportion**
Homework	35%
Quizzes, Readings, Participation	15%
Paper	15%
Presentation and Summaries	15%
Final Exam	20%