Course Number and Title: CS 5435: Security and Privacy Concepts in The Wild

Professor: Ari Juels

Credits: 3

Catalog Description:

This course will impart a technical and social understanding of how and why security and privacy matter, how to think adversarially, how (and how not) to design systems and products. Less attention will be paid to specific skills such as hacking, writing secure code, and security administration. Topics will include user authentication, cryptography, malware, human factors in security, privacy and anonymity, side channels, decoys and deception, and adversarial modeling. We will explore these concepts by studying attacks and defenses in real-world systems, covering blockchains, Stuxnet, retailer breaches, implantable medical devices, and much more.

Course Frequency:

Offered every fall

Prerequisites:

CS 2800 or CS 4820 or permission of instructor

Corequisites:

NONE

Preparation Summary:

Computer Science: Students must have basic facility with programming and a familiarity with Python.

Math: Students must be comfortable with basic concepts in discrete mathematics, including graph theory, combinatorics, and discrete probability.

Textbook(s) and/or Other Required Materials:

- Selected readings assigned via CMSX
- Ross Anderson, *Security Engineering*, 2nd Edition (available online at http://www.cl.cam.ac.uk/~rja14/book.html)

Class and Laboratory Schedule:

Lectures: 3 hrs/wk

Recitations: None.

Labs: None.

Assignments, Exams and Projects:

Homework: Five assignments

Exams: Final exam

Project: None required

Typical Topics Covered:

- Biometrics: various forms, from fingers to ears; spoofing attacks; false acceptance and rejection rates; secure storage and use
- Passwords: security metrics; composition policies; breaches; secure password storage
- Deception: honey objects, decoys, and steganography
- Basic cryptographic primitives: hash functions, commitment schemes, symmetric-key encryption, and message authentication codes
- Public-key cryptography: public-key encryption and digital signatures
- Authentication devices: one-time passcode tokens; RFID/NFC devices
- Adversarial modeling: cryptographic experiments; attack trees
- Anonymity networks: mixnets and their applications, dining cryptographers (DC) nets; Tor
- Cloud security: virtualization and storage security
- Medical security: implantable medical devices; hospital information security practices
- Cyberwarfare: zero-days; Stuxnet; advanced persistent threats (APTs)
- Blockchains: consensus algorithms, cryptocurrencies, smart contracts; Bitcoin and Ethereum

Student Outcomes:

1. Demonstrate a basic ability to understand security considerations in system design and perform common forms of adversarial modeling.
2. Demonstrate understanding of and applicability of basic cryptographic primitives.
3. Demonstrate knowledge of various types of user authentication (the three classical factors), their use and misuse, and how to evaluate their security.
4. Demonstrate ability to identify privacy weaknesses across a variety of settings and familiarity with techniques that might be used to address them.
5. Demonstrate basic familiarity with blockchain technologies and cryptocurrencies, including suitable (and unsuitable) application scenarios.

Academic Integrity:

Each student in this course is expected to abide by the Cornell University Code of Academic Integrity. Any work submitted by a student in this course for academic credit will be the student's own work. The policy can be found on the university’s website here: https://theuniversityfaculty.cornell.edu/academic-integrity/. For this course, collaboration on certain homework assignments is permitted *when specifically indicated by the instructor*.

You are encouraged to study together and to discuss information and concepts covered in lecture and the sections with other students. You can give "consulting" help to or receive "consulting" help from such students. However, this permissible cooperation should never involve one student having possession of a copy of all or part of work done by someone else, in the form of an e-mail, an e-mail attachment file, a diskette, or a hard copy.

Should copying occur, both the student who copied work from another student and the student who gave material to be copied will both automatically receive a zero for the assignment. Penalty for violation of this Code can also be extended to include failure of the course and University disciplinary action.

During examinations, you must do your own work. Talking or discussion is not permitted during the examinations, nor may you compare papers, copy from others, or collaborate in any way. Any collaborative behavior during the examinations will result in failure of the exam, and may lead to failure of the course and University disciplinary action.

- **Academic Misconduct.** A faculty member may impose a grade penalty for any misconduct in the classroom or examination room. Examples of academic misconduct include, but are not limited to, talking during an exam, bringing unauthorized materials into the exam room, and disruptive behavior in the classroom.

Students with Disabilities

Your access in this course is important. Please give the instructor or TA your Student Disability Services (SDS) accommodation letter early in the semester so that we have adequate time to arrange your approved academic accommodations. If you need an immediate accommodation for equal access, please speak with me after class or send an email message to me and/or SDS at sds_cu@cornell.edu. If the need arises for additional accommodations during the semester, please contact SDS. You may also feel free to speak with Student Services at Cornell Tech who will connect you with the university SDS office.