University of Connecticut
Department of Computer Science & Engineering

Instructor: Dr. Walter O. Krawec
Instructor's Office: ITE 245
E-mail: walter.krawec@uconn.edu
Phone: 860-486-5523
Instructor's Office Hours: Tuesday/Thursday: 4-5pm; and by appointment
Class Meeting: Tu/Th 12:30pm-1:45pm
Classroom: MCHU 301

CSE 3400/5850: Introduction to Computer and Network Security

Introduction to computer security and the design of secure computer systems. Introduction to applied cryptography, including basic elements of symmetric-key and public-key ciphers, authentication, and key exchange. Security issues in operating systems, software, databases, and networks. Attacks and countermeasures. Ethical, legal and business aspects.

Prerequisite: CSE 2500 and 3100; open only to students in the School of Engineering and declared Computer Science minors.

Required Textbooks:

1. Foundations of Cybersecurity: Applied Introduction to Cryptography, by Amir Herzberg. Available on Husky CT.

Recommended Textbooks:

1. Introduction to Modern Cryptography, by J. Katz and Y. Lindell (2E). ISBN: 978-1466570269

Course Outcomes:

1. Develop an appreciation for modern Cybersecurity and Applied Cryptography.
2. Learn how to construct suitable definitions of security for various security tasks and the difficulty in doing so correctly.
3. Identify the appropriate uses of various symmetric and asymmetric cryptographic primitives.
4. Develop a sense as to how protocols are proven secure or insecure.

Course Grading:

Assignments: 45%

- Several take-home assignments will be given throughout the semester. Unless otherwise specified by the instructor, you may work in groups of 2-3 on these assignments. If you choose to work in groups, all members of that group should have their names clearly printed on the first page of the assignment. Furthermore, all members of the group must submit the same document (see below for hand-in policy). Group members will be given the same grade for the assignment.

Midterm Exam: 25%

- More information on the topics covered on the exam will be provided as the test day approaches.

Final: 25%

- More information on the topics covered on the exam will be provided as the test day approaches.

Class Participation: 5%

- All students are expected to show up for every class on time and to participate in discussions. If you miss a class, you are responsible for finding what, if any, work has been assigned and what the due dates are.

Submission Policy:

All written assignments must be submitted electronically to HuskyCT as **PDF** files ***(no other format will be accepted!)***. They should either be typed and submitted as a PDF file, or scanned and submitted ***(photos of assignments will not be accepted – use a real scanner!)***. If you scan your document, make sure to check it is legible. **The instructor reserves the right to give a 0 to any answer that is not legible.**

For programming assignments, source code must be provided in a ZIP file (no other format will be accepted). Do not zip binary files – just the source code along with instructions on how to compile it (and/or a Makefile if appropriate).

If you work in a group, all members of that group should have their names listed clearly on the assignment hand-in. Furthermore, all members of the group should upload the same submission to HuskyCT. All members of the group will be given the same grade.

Course Outline (tentative):

1. Introduction and Background
    - **Recommended Reading:** Chapter 1 and 2.1
    - Basics of Cybersecurity and Cryptography
    - Basic primitives: Encryption, MAC, Signature
    - Defining Security
2. Private Key Encryption
    - **Recommended Reading:** Chapter 2
    - Historical Ciphers
    - Building Blocks: PRG's PRF's PRP's
    - Attack Models
    - Modes of Operation
    - Implementations
3. Public Key Encryption
    - **Recommended Reading:** Chapter 6 (up to and including 6.5)
    - Number Theory Review
    - Attack Models and Definitions
    - RSA and El Gamal
4. Message Authentication Codes
    - **Recommended Reading:** Chapter 3.1-3.5
    - Security Definition
    - Applications

5. Digital Signatures
    - **Recommended Reading:** Chapters 6.1.2, 6.5.2, 6.6
    - Security Definition + constructions
    - Applications
6. Advanced Protocols: TLS/SSL
    - **Recommended Reading:** Chapter 7
    - Protocol and Security
    - Design considerations
7. Quantum Security
    - **Recommended Reading:** TBD
    - Qubits vs. Classical Bits
    - Measurements
    - Quantum Key Distribution
    - Post-Quantum Cryptography

Course Policies:
All students are expected to know and follow all UConn policies including those listed on http://ecampus.uconn.edu/policies.html

Academic Honesty: Students are expected to act in accordance with the Guidelines for Academic Integrity at the University of Connecticut.

Student Conduct Code: Students are expected to conduct themselves in accordance with UConn's Student Conduct Code.

Final Exam Policy: Students are required to be available for their final exam and complete any assessment during the time stated. If you have a conflict with this time, you must obtain official permission to schedule a make-up exam with the Office of Student Support and Advocacy (OSSA).