# EEL 4347 Introduction to Cybersecurity

Fall 2020

| | | | |
|---|---|---|---|
| **Instructor:** | C. Harrys Konstantinou | **Time:** | ONLINE |
| **Email:** | konstantinou@eng.famu.fsu.edu | **Place:** | ONLINE |
| **Course webpage:** | eng.famu.fsu.edu/ konstantinou/teaching | **Office:** | B-371 |

**Course Description:** Computer systems have become a vital part of our everyday professional and personal life (e.g., online banking, social networking). These tasks can however expose the users to various security threats (e.g., credit card number theft, personal information leakage). Therefore there is a need for designing secure computer systems. This introductory course teaches both theoretical and practical concepts of cybersecurity. The course will cover an introduction to the most important features of computer security, including topics such as symmetric ciphers, basic number theory, public key cryptosystems, digital signatures, hashes, message authentication codes, key management and distribution, authentication protocols, vulnerabilities and malware, access control, network security.
The course is one of a suite of technical courses that all BS CpE must complete to provide depth within some technical areas of the discipline. Similarly, the course aims to provide depth for graduate students within some technical areas of the CpE discipline. The class will provide students with the necessary tools for designing secure computer systems and programs and for defending against malicious threats (e.g., viruses, worms, denial of service).

**Objectives:** After this course the student:

- Distinguish the broad set of technical, social & political aspects of cybersecurity
- Describe the vulnerabilities and threats posed by criminals, terrorist and nation states to national infrastructure
- Relate the nature of secure software development, operating systems and data base design
- Interpret security guarantees. Assess the level of security provided by a cryptographic protocol.
- Identify the role security management plays in cybersecurity defense
- Explain common vulnerabilities in computer programs, including buffer overflow vulnerabilities, time-of-check to time-of-use flaws, incomplete mediation.
- Identify the security management methods to maintain security protection
- Discuss the legal and social issues at play in developing solutions.
- Apply theoretical concepts in practice by using a programming language to implement attacks and defenses against computer systems.
- Critically analyze a scientific article (graduate students only).

**Undergraduates Prerequisites:**
(1) C/C++ Programming (COP 3014 or CGS 3408 ((FSU,FAMU)).
(2) Digital Logic Design (EEL 3705).
*Permission of instructor is required for graduate students.*
Overall, the course is largely self-contained and will introduce the necessary technologies required for a qualitative (rather than quantitative) understanding of the security landscape of computer systems. HOWEVER, ***students are expected to enter this course with a programming knowledge in C and *nix systems, and basic knowledge of operating systems and data structures***. Some knowledge of assembly and compilers will be helpful, but the relevant information will be covered in the course or in provided references.

**Online Office Hours:**
On Zoom (Invitation on Canvas)

- 13:45–14:45 TR, or
- Other times by appointment only (email instructor).

**Main References:**

- Instructor's lecture notes and handouts.
- Pfleeger, C.P., "Security in Computing" 5th Edition, Prentice Hall, Copyright 2010ISBN 0-13-239077-9

  **In addition to the textbook, students may be given additional reading materials such as research papers. Students are responsible for all assigned reading assignments.*

**Grading Policy for Undergraduate Students (100 points):**

- Online Active Participation (Canvas Discussions) (10).
- Homework (50).
- Midterm Exam (30).
- Final Exam (10).

**Grading Scale for Undergraduate Students:**

- A if $\geq 90$
- B if $\geq 80$ and $\leq 89$
- C if $\geq 70$ and $\leq 79$
- D if $\geq 60$ and $\leq 69$
- F otherwise

**Grading Policy for Graduate Students (120 points):**

- Online Active Participation (Canvas Discussions) (10).
- Homework (50).
- Midterm Exam (30).
- Final Exam (10).
- Project (20).

**Grading Scale for Graduate Students:**

- A if $\geq 105$
- B if $\geq 90$ and $\leq 104$
- C if $\geq 75$ and $\leq 89$
- D if $\geq 60$ and $\leq 74$
- F otherwise

**Course Policy:**

- For the homework students are expected to work independently. Offering and accepting solutions from others is an act of plagiarism, which will be penalized according to the Academic Honesty Policy. Discussion among students is encouraged, but when in doubt, students should direct their questions to the professor or teaching assistant.
- A topic will be assigned bi-weekly (every 2 weeks) on Canvas and students are required to participate in the discussion boards. Participation is: 1) answering questions posed in the topic description, 2) answering questions posed by other students or the instructor, 3) posting interesting/insightful summaries on articles that pertain to the weeks coursework but not necessarily have to be on the topic. Participation is not: 1) simple two sentence responses, 2) linking to articles, 3) copying and pasting.
- You will not receive extensions, unless you contact me ahead of time and make the proper arrangements. Late assignments/projects/etc. will not be accepted.
- Last day to drop a course: Check with your University. No course drops will be allowed after this date except for: medical emergency, military service, administrative correction, and other (consult instructor).

**Academic Honesty:**
The full text of the Academic Honesty Policy is in the *Student Handbook*.

**Resources:**

- Undergraduate students: https://www.eng.famu.fsu.edu/undergraduate/student-handbook
- Graduate students: https://www.eng.famu.fsu.edu/ece/graduate/resources

**ADA and Students with Disabilities:**
Please see the Department and University for Details. Also please let me know if you have any special requirements.

**Registring for this course means your agreement to this class policy and syllabus.**

**COURSE OUTLINE (LIST OF MAJOR TOPICS BY WEEK):**

1. Overview, security mindset, ethics, design principles, threat modeling, attacks, defenses.
2. Basic tools in computer security (authentication, access control).
3. Basic tools in computer security (cryptography: symmetric and asymmetric crypto primitives).
4. Program security (non-malicious programming oversights).
5. Program security (malicious codemalware, countermeasures).
6. Web security (browser attacks, web attacks targeting users, obtaining user/website data, email attacks).
7. Review and Midterm.
8. Operating systems (permissions in Windows/Unix, security in the design, rootkits).
9. Network security (basic internet technology, denial of service, wireless security, crypto, firewalls, IDS/IPS).
10. Databases (security requirements, reliabilit, integrity, disclosure).
11. Cloud computing (concepts, security tools, identity management, securing IaaS).
12. Hardware security (types of vulnerabilities and attacks, hardware Trojan prevention and detection, malicious hardware).
13. Cyber-physical systems security (definition and instances of CPS, vulnerabilities and attacks, defenses).
14. Privacy (concepts, principles and policies, authentication and privacy, privacy on the web).
15. Management and incidents (security planning, handling incidents, risk analysis, dealing with disaster) + Emerging topics (cyber warfare).
16. Final exam & Project Submission.