

# ECE 371 Introduction to Security Engineering

Syllabus, Fall 2019

**Course Meetings:** Tuesday and Thursday 1pm-2:15pm, room: Marston 132

**Lab:** Duda Hall, 24/7 card key access.

**Instructor:** Wayne Burleson, Electrical and Computer Engineering

Contact: [burleson@umass.edu](mailto:burleson@umass.edu), Office: Knowles 309B

Office Hours: Tues 12-1pm /Thurs 2:30-3:30pm (tentative)

**Teaching Assistants:** Shayan Moini ([smoini@umass.edu](mailto:smoini@umass.edu)), Jackie Lagasse

([jlagasse@umass.edu](mailto:jlagasse@umass.edu))

## Course Description:

Security is playing an increasing role in computer engineering and society at large. Security engineering crosses several disciplines of computer engineering including hardware, software, cryptography, experimental methods as well as broader topics such as management, economics, risk analysis, forensics, policy and human factors. This new course presents an introduction to the topic of security engineering by building on analytical and experimental computer engineering techniques, and then applying them to security problems. Five labs make up a hands-on aspect of the course which is critical to capture the essence of security engineering. Each lab is preceded by the necessary lectures on security concepts and methods. Contemporary events in the news are used to motivate each section.

## Prerequisites:

- E&C-ENG 241 Programming
- E&C-ENG 231 Embedded Systems
- E&C-ENG 214 Probability and Statistics
- CompSci 250 Intro to Computation

## Calendar:

Date	Week	Lecture	Description	Homework
9/3	Week 1	Intro	Course Overview & Syllabus	
9/5	Week 1	Lab1_doc	Introduction to Lab1	
9/10	Week 2	Lec1	Definition of Security, Terminology	HW0 Deadline
9/12	Week 2	Lec2	Buffer Overflow, History of Worms, Viruses	
9/17	Week 3	Lec3	Cryptography Introduction	Lab1 Deadline
9/19	Week 3	Lec3	Secure Hash, Block Ciphers, DES	HW1
9/24	Week 4	Lab2_doc	Lab 2 Introduction	
9/26	Week 4	Lec4	AES Intro	HW1 Deadline

10/1	Week 5	Lec5	Public Key Encryption	
10/3	Week 5	Lec5	Digital Signature, CA, RSA	Lab2 Deadline
10/8	Week 6	Lec6	Network Security	HW2
10/10	Week 6	Lec6	Block Chains, secure hashing	
10/15	Week 7	-----	Monday Class Schedule	HW2 Deadline, HW3
10/17	Week 7	Lab3_doc	Introduction to lab3	
10/22	Week 8	Lec8	Malware and Software Vulnerabilities	HW3 Deadline
10/24	Week 8	Lec8	Malware, bash/SSL bug, return-to-libc	
10/29	Week 9	Lab4_doc	Introduction to Lab4	Lab3 Deadline
10/31	Week 9	Lec9	Random Number Generation, LFSR	HW
11/5	Week 10	Lec10	Hardware Security Primitives, PUF	
11/7	Week 10	Lec10	Digital Forensics	Lab4 Deadline
11/12	Week 11	Lec11	Hardware Trojans	HW4
11/14	Week 11	Lec11	Hardware Trojan Detection	
11/19	Week 12	Lab5_doc	Introduction to Lab5	HW4 Deadline
11/21	Week 12	Lec12	Side Channel Attack, Power Measurement	HW5
11/26	-----		Thanksgiving	
11/28	-----		Thanksgiving	
12/3	Week 13	Lec13	Security systems, management, economics, policy	Lab5 Deadline, HW5 Deadline
12/5	Week 13	Lec13	Review	

**Grading:**

Labs: 40%  
Midterm Exam: 25%  
Final Exam: 25%

Homework and Quizzes: 10%

**Text Books:**

- Required: Security Engineering, Ross Anderson, Wiley, 2008, 2nd edition.  
<https://www.cl.cam.ac.uk/~rja14/book.html> (available free on-line)
- Recommended: Network Security Essentials, William Stallings, 2017, 6<sup>th</sup> edition

**Accomodation 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/](http://www.umass.edu/dean_students/codeofconduct/acadhonesty/)).

**Inclusivity and Diversity Statement:**

The diversity of the participants in this course is a valuable source of ideas, problem solving strategies, and engineering creativity. If you feel that your contribution is not being valued for any reason, please speak with the instructor privately. If you wish to communicate anonymously, you may do so in writing or speak with Dr. Paula Rees, Director of Engineering Diversity Programs ([rees@umass.edu](mailto:rees@umass.edu), 413.545.6324, Marston 128). We are all members of an academic community where it is our shared responsibility to cultivate a climate where all students/individuals are valued and where both they and their ideas are treated with respect.