Updates for the B.S. in Computer and Cybersecurity Engineering Curriculum

February 2023

- A new required course is introduced in the sophomore year:
    - ECE 222 - Introduction to Cybersecurity (see attached syllabus)
    - Replaces the Career Elective II in the curriculum

- Additional curriculum updates:
    - Cybersecurity Software Engineering Elective replaces ECE 442:
        - Electives: ***ECE442*** - *Internet of Things and Cyber Physical Systems,* ***ECE 448*** - *Application Software Design*, ***ECE 449*** - *Object-Oriented Programming and Machine Learning* and ***ECE 473*** - *Cloud Computing and Cloud Native Systems*
        - More options for students
    - Additional LAW elective (LAW 379 Blockchain and the Law) for BSCCSE
        - Electives: LAW 252, LAW 285, LAW 295, **LAW379** or LAW 478
        - More options for students
    - Remove the CS470 substitution for ECE485 in BSCPE/BSCCSE
        - Course content is different.
- No change in total credit hours
- See the revised curriculum sheet for changes highlighted in yellow.

B.S. in Computer and Cyber Security Engineering Curriculum Sheet (Total Credits : 133-134)

Name:				**CWID:**			
PIN:							
First Semester		Term Taken	Grade	**Second Semester**		Term Taken	Grade
ECE 100 Intro to the Profession I	3			MATH 152 Calculus II	5		
MATH 151 Calculus I	5			PHYS 123 Physics I: Mechanics	4		
CHEM 122 Chemistry I w/o Lab	3			CS 116 Object-Oriented Programming II	2		
CS 115 Object-Oriented Programming I	2			Social Sciences Elective	3		
Humanities (200-level)	3			Career Elective I [1]	3		
TOTAL	**16**			**TOTAL**	**17**		
Third Semester		Term Taken	Grade	**Fourth Semester**		Term Taken	Grade
MATH 252 Intro to Differential Equations	4			MATH 251 Multivariate & Vector Calc.	4		
PHYS 221 Physics II: Electr. & Magnetism	4			ECE 222 Introduction to Cybersecurity	3		
ECE 211 Circuit Analysis I	3			ECE 213 Circuit Analysis II	4		
ECE 218 Digital systems	4			ECE 242 Digital Compt. & Computing	3		
CS 331 Data Structures & Algorithm	3			CS 330 Discrete Structures	3		
TOTAL	**18**			**TOTAL**	**17**		
Fifth Semester		Term Taken	Grade	**Sixth Semester**		Term Taken	Grade
ECE 308 Signals & Systems	3			CS 450 Operating Systems	3		
ECE 311 Engineering Electronics	4			ECE 407 Intro to Computer Networks w/Lab	4		
CS 351 Systems Programming	3			MATH 333 or MATH 350	3		
ECE 443 Intro.to Computer Cyber Security	3			IPRO Elective I	3		
Humanities Elective (300+)	3			Social Sciences Elective (300+)	3		
TOTAL	**16**			**TOTAL**	**16**		
Seventh Semester		Term Taken	Grade	**Eighth Semester**		Term Taken	Grade
ECE 497 Special Problems [2]	3			ECE 441 Smart & Connected Emb. Sys. [3]	4		
ECE 485 Comp. Arch. & Org.	3			Cybersecurity Software Eng. Elective [4]	3		
MATH 374 Probability/Stat. for ECE	3			ECE 444 Computer Network Security	3		
IPRO Elective II	3			Cyber Security Law Elective [5]	2-3		
Additional Hum. or Soc. Sci. Elective	3			Social Sciences Elective (300+)	3		
Humanities Elective (300+)	3						
TOTAL	**18**			**TOTAL**	**15-16**		

[1] Career Electives: Advisor-approved course from engineering, science, math, computer science, business, and law that is more advanced than the academic level of the student.

[2] ECE 497 with a project related to cyber security topics such as smart grid, Internet of Things, cloud computing, hardware security, or cryptography. Please see your academic adviser for more details.

[3] Major Design Experience (M) course

[4] Choose from the following courses: ECE442, ECE448, ECE449 and ECE473

[5] Choose from the following courses: LAW 252, LAW 285, LAW 295, LAW379 or LAW 478

ECE 222 – Introduction to Cybersecurity Engineering
Department of Electrical and Computer Engineering
Illinois Institute of Technology

Course Description:

Students will receive an introductory overview of major issues related to offensive and defensive cybersecurity. Key topics for this course include ethical hacking tools, penetration testing basics, exploit development, intrusion detection, cyber forensics, and cybersecurity law and regulations. Course projects will provide a hands-on experience using open-source tools and software to support concepts taught during the lecture.

Prerequisites:

Basic Programming Skills

Required Textbook:

- "*Computer Security Fundamentals (Pearson IT Cybersecurity Curriculum) 4th Edition*", W. Easttom II, 2019
  - ISBN-13: 978-0135774779

Recommended Textbooks:

- Command Line References:
  - "*Blue Team Field Manual*" A. White and B. Clark, 2017
    - ISBN-13: 978-1541016361
  - "*Red Team Field Manual*" B. Clark and N. Downer, 2022
    - ISBN-13: 978-1075091834
- "*Operator Handbook: Red Team + OSINT + Blue Team Reference*", J. Picolet, 2020
  - ISBN-13: 979-8605493952
- "*Cybersecurity: The Beginner's Guide: A comprehensive guide to getting started in cybersecurity*" E. Ozkaya
  - ISBN-13: 978-0134794105
- "*Computer Security: A Hands-on Approach (Computer and Internet Security)*", W. Du
  - ISBN-13: 978-1733003957

Additional Resources:

- TryHackMe "Introduction to Cyber Security" Path - https://tryhackme.com/paths
- National Cyber League - https://nationalcyberleague.org/
- Cybersecurity Challenges - https://overthewire.org/wargames/ (Command Line – Bandit)
- "The Cyber Mentor" "Zero to Hero Pentesting" YouTube Playlist
- "Getting Started with ATT&CK"
  - Available online - https://www.mitre.org/sites/default/files/2021-11/getting-started-with-attack-october-2019.pdf

Computer Requirement:

A computer desktop or laptop that is able to run VirtualBox is required for this course. Computers with solid-state drives, at least 16 GB of memory and at least 4 physical processor cores are recommended.

ECE 222 Grading:

Assignments	**A** ≥ 90%
Homework – 10%	90% > **B** ≥ 80%
Projects – 40%	80% > **C** ≥ 70%
Midterm Exam – 20%	70% > **D** ≥ 60%
Final Exam - 30%	60% > **E**

Homework and Project Policy:

Late homework and project reports will not be graded. Discussion on homework and projects is encouraged, but copying will call for disciplinary action.

Exam Policy:

Closed book, closed notes exams. A single-page handwritten page (front and back) is allowed. Makeup exams will NOT be given, except for extraordinary reasons approved by the instructor.

Lecture Schedule (tentative):

No.	**Date**	**Topic**	**Text Chapters**	**HW Due**	**Project Due**
1, 2	8/22, 8/24	Syllabus & Cybersecurity Basics	1		
3, 4	8/29, 8/31	Introduction to Kali Linux & the Command Line			
5	9/7	Networks Basics & Protocols	2	HW #1	
6	9/12	Network-Based Attacks	2		
7	9/14	Open-Source Intelligence (OSINT) & Scanning			
8, 9	9/19, 9/21	Penetration Testing 1 – Procedures	6	HW #2	
10, 11	9/26, 9/28	Penetration Testing 2 – Tools & Tactics	6		PRJ #1
12, 13	10/3, 10/5	MITRE ATT&CK Framework	LINK	HW #3	
	10/12	**Midterm Exam**			
14, 15	10/17, 10/19	Malware 1 – Assembly Intro	5		PRJ #2
16, 17	10/24, 10/26	Malware 2 – Architecture & Design	5		
18, 19	10/31, 11/2	Defense Tools 1 – Basic Tools	9	HW #4	
20, 21	11/7, 11/9	Defense Tools 2 – Intrusion Detection & Prevention	10		PRJ #3
22, 23	11/14, 11/16	Cyber Law Intro	3	HW #5	
24	11/21	Intro to Forensics 1 – Windows	14		
25, 26	11/28, 11/30	Intro to Forensics 2 – Linux	3	HW #6	
		Final Exam			PRJ #4

Projects

- Project #1 – Environment Basics & Scanning
  - Students will familiarize themselves with Kali Linux and basic scanning tools. Scans will be conducted against a vulnerable machine.
  - Deliverables – A report detailing key components of Kali Linux along with analysis of the scanning tool results. Screenshots of scanner results must be included for full points.
- Project #2 – Penetration Test
  - Students will conduct a penetration test against the machine they scanned in Project #1. The objective of the test will be to gain root access to the target machine.
  - Deliverables – A report detailing the steps completed as part of the Penetration Test along with analysis of the CVE used to exploit the target. Screenshots of steps taken and the root flag must be included for full points.
- Project #3 – Buffer Overflow Analysis
  - Students will examine the provided C code to identify and exploit a buffer overflow vulnerability in the code.
  - Deliverables – A report detailing the provided code and vulnerability along with a screenshot proving successful exploitation.
- Project #4 – Intrusion Detection Basics
  - Students will learn how to write basic Snort rules for identifying basic attacks against a host-based IDS. Students will launch attacks against the target to verify the ruleset worked.
  - Deliverables – A report detailing the rules that were created along with screenshots showing detection of the launched attacks.

ECE 222 Course Objectives (ABET):

After completing this course, the student should be able to do the following:

1. Identify network-based cyberattacks, such as Denial of Service (DoS), Man-in-the-Middle (MitM), and ARP Spoofing.
2. Utilize open-source tools to map network resources and identify vulnerabilities.
3. Explain and execute the steps involved in the penetration testing process.
4. Describe the MITRE ATT&CK Framework and apply it to a cyber kill chain.
5. Identify and exploit buffer overflow vulnerabilities.
6. Develop basic rulesets for an Intrusion Detection System (IDS).
7. Outline anti-hacking laws and industry-specific cybersecurity regulations within the United States.
8. Understand the steps needed to conduct forensics on a Windows and Linux Operating System.

ADA Statement:

Reasonable accommodations will be made for students with documented disabilities. In order to receive accommodations, students must obtain a letter of accommodation from the Center for Disability Resources and make an appointment to speak with me as soon as possible. The Center for Disability Resources is located in the Life Sciences Building, room 218, 312-567-5744 or disabilities@iit.edu

Sexual Harassment and Discrimination Information:

Illinois Tech prohibits all sexual harassment, sexual misconduct, and gender discrimination by any member of our community. This includes harassment among students, staff, or faculty. Sexual harassment of a student by a faculty member or sexual harassment of an employee by a supervisor is particularly serious. Such conduct may easily create an intimidating, hostile, or offensive environment. Illinois Tech encourages anyone experiencing sexual harassment or sexual misconduct to speak with the Office of Title IX Compliance for information on support options and the resolution process. You can report sexual harassment electronically at iit.edu/incidentreport, which can be completed anonymously. You may additionally report by contacting the Title IX Coordinator, Virginia Foster at foster@iit.edu or the Deputy Title IX Coordinator at eespeland@iit.edu. For confidential support, you may reach Illinois Tech's Confidential Advisor at (773) 907-1062. You can also contact a licensed practitioner at Illinois Tech's Student Health and Wellness Center at student.health@iit.edu or (312) 567-7550. For a comprehensive list of resources regarding counseling services, medical assistance, legal assistance and visa and immigration services, you can visit the Office of Title IX compliance website at https://www.iit.edu/title-ix/resources.

Curriculum changes to ECE Programs (EE, CPE, CCSE) since 2018

02/22/2022

Information Item:

The ECE Department recently approved curriculum changes for all three undergraduate degree programs (B.S. in Electrical Engineering; B.S. in Computer Engineering and B.S. in Computer and Cybersecurity Engineering). The objective of this curriculum update is to create program flexibility with a balance between wider breadth of knowledge and strong foundation in core areas while providing a personalized learning experience for students consistent with their interest and potential.

This proposal introduces "Career Elective" courses in multiple semesters (four in EE, three in CPE and two in CCSE). A career elective course is defined as "an advisor-approved course from engineering, science, math, computer science, business, and law that is more advanced than the academic level of the student"

The following document includes the summary of changes, current and revised curriculum sample sheets for all three programs. Additional documents include curriculum guidelines for reference and the history of the ECE program changes.

Objectives:

- Position our students to be competitive in research and industry careers by
  - creating program flexibility and program tracks with a balance between wider breadth of knowledge and strong foundation in core areas;
  - providing an effective learning experience to students consistent with their interest and potential;
  - upgrading our undergraduate program consistent with advances in Electrical and Computer Engineering and being more competitive with peer universities in a timely fashion.
- Position our undergraduate program as an attractive one for incoming students.
  - Maximize flexibility for transfer students and flexibility to pursue co-curricular and extra-curricular activities, co-terminal and interdisciplinary masters, etc. Minimize pre- and co-requisite requirements where possible.

Restructuring Highlights

- Career Electives I, II, III and IV in Freshman, Sophomore, Junior and Senior years create opportunities for options for minors, increased emphasis within major tracks, and depth and breadth across technical disciplines.
- Remove specific course requirements that are less relevant to today's ECE work and replace with more flexible options.
  - MMAE 200/320, Science Elective, Physics III are replaced by Career Electives

02/09/2021

Information Item:

Update for the ECE Curriculum

ABET has reported a shortcoming in the Criteria 5 (Curriculum) with respect to “culminating major engineering design” for both EE and CPE programs. ECE department meets this requirement through two elective laboratory design courses with senior design projects. ABET audit summary reports that “Program lab courses, either individually or collectively, is not culmination of years of student learning and experience.”

Based on the feedback received from ABET, ECE Department has decided to designate one of the senior professional elective courses required as a Major Design Experience (M) course. Major Design Experience courses are designed to meet the ABET requirements (see below).

Curriculum change for ECE Programs (EE, CPE and CCSE)

> Professional ECE electives may be chosen from any of the 400-level ECE courses identified with (P) in the course descriptions. At least two of the electives must contain laboratories. At least one of the elective courses must be identified as Major Design Experience (M) course.

Revised ECE441 Course designated as a Major Design Experience (M) course:

> ECE441 is now a 100% project-based course with students working in teams on implementation of a smart and connected system targeting different application domains. Restructured ECE441 schedule include several project milestones that need to be met by students including project proposal, midterm progress reports, final report and presentations

11/24/2020

Information item:

All ECE 400-level courses are to be denoted as Professional Electives and designated as such by the addition of the letter (P) in the bulletin. This formalizes an existing practice within ECE.

09/25/2018

Program changes to BS EE

Consolidation of *ECE 211 Circuit Analysis I*, *ECE 213 Circuit Analysis II*, *ECE 311 Engineering Electronics*, and *ECE 312 Electronics Circuits* is part of an effort by the ECE to restructure our BS curricula to position our students to be competitive in research and industry careers by

- creating program flexibility and program tracks with a balance between wider breadth of knowledge and strong foundation in core areas;
- providing an effective learning experience to students consistent with their interest and potential; and

- upgrading our undergraduate program consistent with advances in Electrical and Computer Engineering and being more competitive with peer universities in a timely fashion.

In short, changes are as follows:

- **ECE 211, ECE 213, and ECE 311 course contents are revised to remove any redundancy and cover the important topics from ECE 312.**
- **ECE 312 (4 hours) was therefore eliminated in the BS EE and is now replaced by a Free Elective (3 hours).**
- The range of total credit hours is thus reduced from 131-134 to 130-133.