NEW UNDERGRADUATE PROGRAM PROPOSAL

ILLINOIS INSTITUTE OF TECHNOLOGY

The following information is required by the Undergraduate Studies Committee to approve new programs. After approval by UGSC this form should be routed to Faculty Council for approval and then the Provost's office.

College(s): Armour College of Engineering

Department(s): Electrical and Computer Engineering

Date: 01/19/2018

Approvals Required

(1) Academic Unit Head(s): Chair, Electrical and Computer Engineering

(2) Dean(s): Dean, Armour College of Engineering

(3) Other: Undergraduate Studies Committee, University Faculty Council

GENERAL INFORMATION

Program Title: Bachelor of Science in Computer and Cybersecurity Engineering

Program Scheduling: Fall 2018

Total Program Credit Hours: 131 / 132

Program Description: *Provide a brief narrative of the program content (use as much space as needed).*

Bachelor of Science in Computer and Cybersecurity Engineering (CCSE) is a degree program that prepares students for an engineering career that involves design and application of secure and resilient computer hardware and software systems. This is a unique program that combines computer engineering and cybersecurity topics into one major. The program emphasizes the cybersecurity engineering of cyber-physical systems which are becoming more prevalent every day. It is concerned with detection and elimination of vulnerabilities and safe operation of Internet of Things, cloud computing, healthcare, smart/micro grid power systems, computer networks, and wireless communications.

Joint Task Force on Cybersecurity Education[1] defines the cybersecurity discipline as:

> *"A computing-based discipline involving technology, people, information, and processes to enable assured operations in the context of adversaries. It involves the creation, operation, analysis, and testing of secure computer systems. It is an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management"*

Therefore, CCSE students must also know about human factors, ethical issues and law in addition to the detailed knowledge of secure hardware/software components to design and build systems for security applications. CCSE program is built on a very strong Computer Engineering program within the ECE Department and is tailored to expand knowledge to counter cyber threats by providing both theoretical fundamentals and actual implementation of cyber infrastructure. Interdisciplinary component of the program is satisfied with the courses that CCSE students can select from Department of Computer Science and Chicago-Kent School of Law.

[1] https://www.csec2017.org/

Program Purpose/ Program Benefits: *Provide details on the intent of the program and its relation to other programs. State the impact of the program for students and for IIT.*

All major industries such as defense, energy, finance, transportation, infrastructure, healthcare are impacted by cybersecurity challenges. There is great need for educated workforce who can help build the safety measures, protect all forms of digital assets and also understand ethical and legal issues in cybersecurity. However, cybersecurity job market is still straining to find enough trained workers. Demand for talent in the cybersecurity job market outstrips the supply of available workers. US Department of Labor's outlook for "Information Security Analysts" predicts growth by 28% for years 2016-2026[2]. In fact, according to Burning Glass data[3], Chicago metropolitan area had 10,670 cybersecurity job openings during the 12-month period that ended in September 2017 which was among the highest in large metropolitan areas.

Clearly, cybersecurity education is an important opportunity for Illinois Institute of Technology to attract highly qualified students interested in science and engineering. It is essential to provide a carefully designed, rigorous degree program which can establish IIT as a leading cybersecurity institution. Department of Electrical and Computer Engineering have substantial critical mass and resources to achieve this goal. Multiple tenured/tenure track faculty are directly involved in research related to cybersecurity topics and their research has been funded by federal agencies and industry. ECE research on security topics cover a broad spectrum, including cloud computing, healthcare and body area networks, secure networking protocols, cryptography, smart grid power systems and big data. In addition to funded research and graduate theses & dissertations, ECE has been offering cybersecurity courses at both undergraduate and graduate level. Overall, ECE is ready and well-poised for a new degree program addressing the curriculum challenges identified by the Joint Task Force on Cybersecurity Education (JTF is a collaboration between major international computing societies: Association for Computing Machinery (ACM), IEEE Computer Society (IEEE CS), Association for Information Systems Special Interest Group on Security (AIS SIGSEC), and International Federation for Information Processing Technical Committee on Information Security Education).

With the introduction of CCSE degree, ECE department will be able to recruit students who want to be engineers while focusing on cybersecurity. We anticipate total enrollment in ECE programs will increase gradually with the CCSE degree. This may also boost the ECE graduate programs (including a potential Master of Cybersecurity Engineering degree which is under preparation) and result in higher visibility and healthy growth for the ECE Department.

Classification of Instructional Programs (CIP) Code _1_ _4__ . _0_ _9_ _9_ _9_

Currently, there is no specific code for a Cybersecurity degree under the Engineering discipline. However, the proposed program is closely related to the Computer Engineering with a four digit code of 14.09. Last two digits 99 indicates "Other" degree.

Required to make the program US Financial Aid Eligible - The CIP code takes the following structure: xx.xxxx Where each x is a number between 0 and 9. This 6-digit code identifies, to the greatest specificity possible, an entire instructional program. The classification scheme seeks to comprehensively address all areas of study. Because of the dynamic nature of education, however, new CIP codes are frequently added to the list. The first 2-digits are the first cut off of detail and describe the general discipline of the program. For example, any program with a CIP that starts with 14 is within the Engineering discipline; anything with a 22 is within the legal discipline. The next 2 digits increase the level of detail, and the final 2-digits provide the highest level of detail.
Find CIP codes at http://nces.ed.gov/ipeds/cipcode

[2] https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm
[3] http://burning-glass.com/track-cybersecurity-job-market-cyberseek/

PROGRAM VIABILITY

Competitive Programs: *Indicate other similar programs locally and nationally detail their success.*

Although a large number Cybersecurity programs exist at the graduate level (most of them online), undergraduate degrees are not common. This is expected to change rapidly soon with the formal accreditation process in place by ABET. Several schools have started their pilot programs or expressed interest in offering undergraduate cybersecurity degrees.

Nationwide, similar competitive programs include:

- George Mason University, B.S. in Cybersecurity Engineering
- Stevens Institute of Technology, B.S. in Cybersecurity
- Rochester Institute of Technology, B.S. in Cybersecurity

In Illinois, there are several competitive programs. Closest competition would be at UIUC:

- University of Illinois at Urbana-Champaign; (Information Trust Institute)
  Bachelor of Science in Computer Engineering – Illinois Cyber Security Scholars Program
  Bachelor of Science in Computer Science (Engineering) – Illinois Cyber Security Scholars Program

The following programs are more closely associated with Computer Science rather than engineering:

- Illinois State University;
  BS in Information Systems with a specialization in Information Assurance and Security
- Northeastern Illinois University;
  Bachelor of Science in Computer Science – Computer Networks and Security concentration
- Southern Illinois University, Carbondale, Illinois
  Bachelor of Science in Computer Science – Computer Networks and Security concentration
- DePaul University;
  BS in Cybersecurity

Market Analysis for Recruiting Students: *Detail what work has been done with UG Admissions to identify and recruit potential students.*

One of the potential challenges for UG admissions would be to distinguish the multiple cybersecurity programs offered across multiple colleges at IIT. ECE Department will prepare and provide marketing materials for the UG Admissions, emphasizing the engineering focus with the proposed cybersecurity program. ECE department will also collaborate with other departments to coordinate the IIT's push for leadership in cybersecurity education. Our open house and recruitment events will highlight ECE faculty's research projects related to the cybersecurity fields.

Market Analysis for Graduates: *Detail what work has been done with the Career Management Center to identify potential employment opportunities for graduates*.

According to Bureau of Labor Statistics, Greater Chicago area has the 5th highest employment of Information Security Analysts with an annual mean wage of $97,320[4]. Furthermore, Illinois has several major firms listed in the top 500 hottest cybersecurity companies, based on the Cybersecurity Ventures[5] report in 2017. Among them are Cimcor (#75) at Chicago; NowSecure (#124) at Oak Park; Trustwave (#157) at Chicago; Flexera Software (#174) at Itasca; Kenna (#338) at Chicago and MailControl (#404) at Chicago. Multiple Fortune 500 companies in Illinois such as Boeing, United, State Farm, Abbot Laboratories, Caterpillar Inc, etc. increasingly need cybersecurity professionals to prevent security breaches and provide security protection for their customers.

ECE Department will work closely with the Career Management Center to provide the CCSE program details and highlight the potential companies and industry liaisons.

[4] https://www.bls.gov/oes/current/oes151122.htm#st
[5] https://cybersecurityventures.com/cybersecurity-500-list/

ACADEMIC INFORMATION

Enrollment Estimates: *Are there enrollment estimates for this program, and if so, what are they and what are they based on? What is the minimum number of students necessary in the program to make the program viable (i.e.to offer classes unique to the program often enough)?*

We are targeting 20-25 students each year. This estimate is based on i) feedback from open house, admissions and recruiting events, ii) the popularity of the existing security related courses within the ECE degrees; iii) current number of ECE graduate students working on security related topics and theses.

Proposed CCSE program can be run with fewer students without any major issues since it is largely based on the *Bachelor of Science in Computer Engineering* program. New and modified courses that are offered under CCSE are viable options as elective courses for both Computer and Electrical Engineering students.

Enrollment in the ECE undergraduate programs has been fairly stable through the years and ECE department has enough faculty members and resources for this new program. Cybersecurity is a vastly expanding and dynamic field and ECE Department is prepared to handle the Cybersecurity curriculum demands.

Advising Strategy: *Since quality advising is a key component of good retention, graduation and career placement, how will students be advised and mentored? Specifically for interdisciplinary programs, how will advising responsibilities be shared? What student professional organizations will be formed? How will the department work with the Career Management Center to develop industry connections?*

Existing advising procedures and strategies in the ECE Department will continue in this new degree program. Each student will have an academic advisor assigned in their first semester. Mandatory advising meetings will be enforced. For CCSE degree students, advising faculty will be selected among those that have expertise in cybersecurity, cyber-physical systems, internet of things and computer networks. About half of the current ECE faculty (12) can be considered in this category. With potential enrollment of 25 students in CCSE, advising load for each faculty member will be feasible.

CCSE students can benefit from multiple student organizations that already exist within the ECE Department, including the IIT chapter of world's largest professional organization, IEEE, and its' honor society Eta Kappa Nu. These are well-established and well-run student organizations that are attractive for students that are interested in cybersecurity topics.

Course Requirements: *Detail the courses needed for the program including courses currently offered, new courses to be developed (including syllabi), and dependence on courses from other academic units with their commitments to provide these courses on a long-range basis. Include descriptions of laboratories that will need to be developed along with equipment and facilities requirements.*

Most of the courses are already available/offered under the B.S. in Computer Engineering program. Additional coursework for Cybersecurity engineering will be offered through new courses, modification of existing courses and collaboration with other academic units (in particular, College of Science and Chicago-Kent School of Law). No new laboratory will be established, existing laboratory resources in the Computer Engineering program will meet the expected demand.

Coursework listed below is designed to meet the ABET requirements (currently in draft form)[6] for Cybersecurity programs which necessitate at least 45 semester credit hours (or equivalent) of computing and cybersecurity course work covering:

- Data Security
- Software Security
- System Security

[6] https://www.surveymonkey.com/r/cybersecuritycriteria

- Human Security
- Organizational Security
- Societal Security

New courses:

ECE 442: Internet of Things & Cyber Physical Systems
Course objective is to introduce students to the fundamentals of Internet of Things (IoT) and embedded computing by exploring real-world IoT application scenarios

Course topics include IoT applications and embedded computing, Wireless protocols, Wearable sensors, Home environment sensors, Behavior detection sensors, Data fusion, processing and analysis, Data communications and communication methods, Architectural design issues of IoT layers (Perception, Network, Middleware, Application), Security and privacy issues in IoT. Please see the attached syllabus for more detail.

Modified/Revised Courses:

ECE 407: Introduction to Computer Networks
Emphasis on the physical, data link, and medium access layers of the OSI architecture. Different general techniques for networking tasks, such as error control, flow control, multiplexing, switching, routing, signaling, congestion control, traffic control, scheduling will be covered along with their experimentation and implementation in a laboratory.

ECE 443: Introduction to Computer Security
Computer security as threats and defense mechanisms. Introductory cryptography and key management. Authentication and authorization. System security. Network security. Cloud and web security. Hardware security. Advanced cryptography topics.

Through other academic units:

- CS 458: Introduction to Information Security
- Software Engineering/Law elective course which can be one of the following:
    - CS 425: Database Organization,
    - CS 487: Software Engineering,
    - LAW 252: Law of Privacy,
    - LAW 285: Cyber Fraud and Privacy Class Actions,
    - LAW 295: Data Privacy and Security,
    - LAW 478: Computer and Network Privacy and Security: Ethical, Legal, and Technical Considerations.

Science and Engineering Science coursework requirements are kept same as the Computer Engineering program. 6 credits of discrete mathematics and statistics requirement for ABET cybersecurity programs are satisfied via MATH 474 and CS 331.

Sample Curriculum/Program Requirements: *Provide a sample semester by semester curriculum and the program requirements, as they would appear in the IIT Undergraduate Programs bulletin*.

Please see attached curriculum sheet.

Program Outcomes and Assessment Process: *Provide the program learning goals and assessment plan (for more information contact the Assessment Office within Academic Affairs).*
Also see https://sites.google.com/a/iit.edu/student-learning-assessment/

The educational objective of the ECE undergraduate computer and cybersecurity engineering program is to produce computer and cybersecurity engineering graduates who are prepared to:

1. Meet the expectations of employers of computer and cybersecurity engineers.
2. Pursue advanced study if they so desire.
3. Assume leadership roles in their communities and/or professions.

Program Learning Outcomes: In order that the CCSE program achieves its objectives, the ECE Faculty expects that a student who completes the program will

a. be able to apply knowledge of mathematics, science, and engineering;
b. be able to design and conduct experiments and analyze and interpret the resulting data;
c. be able to design a system, component, or process to meet desired needs within realistic constraints;
d. be able to function on multi-disciplinary teams;
e. be able to identify, formulate, and solve technical problems;
f. have an understanding of professional and ethical responsibility;
g. be able to communicate effectively both orally and in writing;
h. have the broad education necessary to understand the impact of engineering solutions in a global, economic, environmental, and societal context;
i. have a recognition of the need for, and an ability to engage in, lifelong learning;
j. have a knowledge of contemporary issues;
k. be able to use techniques, skills, and tools of modern engineering practice;
l. *be able to apply security principles and practices to the environment, hardware, software, and human aspects of a system; [Cybersecurity]*
m. *be able to analyze and evaluate systems with respect to maintaining operations in the presence of risks and threat [Cybersecurity]*

Student learning outcomes *l.* and *m.* are specific ABET criteria required for cybersecurity degrees[7].

Assessment of learning outcomes are done regularly through *ECE Undergraduate Program Committee*. Undergraduate course instructors are asked periodically to complete an assessment of their course based on the established rubrics and the performance indicators related to the learning outcomes for a given course.

[7] Joint Task force on Cybersecurity education csec2017 v0.5 report

Computer and Cyber Security Engineering (CCSE) Curriculum

First Semester		Term Taken	Grade
MATH 151 Calculus I	5		
CHEM 122 Prin. Chem. I	3		
CS 115 Object-Oriented Prgm I	2		
ECE 100 Intro. to the Profession I	3		
HUM 200,202,204,206 or 208	3		
TOTAL	**16**		

Second Semester		Term Taken	Grade
MATH 152 Calculus II	5		
PHYS 123 Mechanics	4		
BIOL107, BIOL 115 or CHEM126 or MS 201	3		
CS 116 Object-Oriented Prgm II	2		
Soc Sci Elect [1]	3		
TOTAL	**17**		

Third Semester		Term Taken	Grade
MATH 252 Differential Eqns.	4		
PHYS 221 EM & Optics	4		
ECE 211 Ckt. Analysis I	3		
ECE 218 Digital Systems	4		
CS 331 Data Structures & Alg.	3		
TOTAL	**18**		

Fourth Semester		Term Taken	Grade
MATH 251 Multivariate Calculus	4		
PHYS 224 Thm. & Modern Phys.	3		
ECE 213 Ckt. Analysis II	4		
ECE 242 Dig. Comp. & Comptg.	3		
CS 330 Discrete Structures	3		
TOTAL	**17**		

Fifth Semester		Term Taken	Grade
ECE 308 Signals Systems	3		
ECE 311 Engineering Electronics	4		
CS 351 Systems Programming	3		
MATH 333 Mat.Alg. & Complx.Vars.	3		
Humanities Elect [2]	3		
TOTAL	**16**		

Sixth Semester		Term Taken	Grade
ECE 407 Intro. to Comp Ntwks	4		
CS 450 Operating Systems	3		
MATH 374 Probability/Stat. for ECE	3		
IPRO Interprof. Proj I	3		
Soc Sci Elective [1]	3		
TOTAL	**16**		

Seventh Semester		Term Taken	Grade
ECE 441 Microcomputers &Embedded Sys.	4		
ECE 485 or CS 470 Comp. Arch. & Org.	3		
ECE 443 or CS 458 Comp./Info. Security	3		
Prof. Elect [3]	3/4		
Humanities Elect [2]	3		
TOTAL	**16/17**		

Eighth Semester		Term Taken	Grade
ECE 442 IoT & Cyber Physical Sys.	3		
Software Engineering/Law Elect [6]	3		
IPRO Interprof. Proj II [4]	3		
Hum. or Soc. Sci. El. [5]	3		
Soc Sci Elect [1]	3		
TOTAL	**15**		

Total Credits (BSCCSE) 131/132

[1] **ANTH, ECON**, **PS**, **PSYC**, **SOC** course with (**S**) in course description. Distribution of courses must be from at least two different fields; at least 6 credit hours in 1 field and 3 credit hours in a 2nd field; at least 3 credit hours at 300 level.

[2] **AAH**, **COM**, **HIST**, **LIT**, **PHIL** course with an (**H**) in the course description at 300 level or above. Foreign language courses must be at 200 level or above.

[3] With advisor permission any ECE 4xx with (**P**); CS 4xx; or ECE 541, ECE543, ECE 545, or ECE 546

[4] IPRO with at least 75% Engineering, Science, Mathematics, or Computer Science content and is more advanced than the academic level of the student.

[5] **ECON**, **PS**, **PSYC**, **SOC**, **COM**, **HIST**, **LIT**, **PHIL** course with an (**H**) or (**S**) in course description.

[6] Software Engineering/Law Elective must be ECE 449, CS 425, CS 487, LAW 252, LAW 285, LAW 295 or LAW 478

ECE 442 – Internet of Things and Cyber Physical Systems

Instructor	Professor Jafar Saniie Co-instructor: Dr. Won-Jae Yi
Class Time	XXX
Class Location	XXX
Office Hours	XXX
Prerequisites	ECE 242 and ECE 407 (which may be taken concurrently), or Consent of Instructor, or Graduate Standing. General understanding of writing computer programs and embedded computing. Basic knowledge of computer architecture and network data communication system.
Class Website	IIT Blackboard
Textbooks	“Internet of Things: A Hands-On Approach”, 1st Edition A. Bahga, V. Madisetti, VPT, 2014 ISBN: 978-0996025515
References	"The Internet of Things: Key Applications and Protocols", 2nd Edition O. Hersent, D. Boswarthick, O. Elloumi, John Wiley & Sons, Inc., 2012 ISBN: 978-1119994350 "Internet of Things and Data Analytics Handbook" H. Geng, John Wiley & Sons, Inc., 2016 ISBN: 978-1119173649 "Internet of Things: Principles and Paradigms" R. Buyya and A.V. Dastjerdi, Morgan Kaufmann, 2016 ISBN: 978-0128053959 "Raspberry Pi Sensors" Rushi Gajjar, Packt Publishing, 2015 ISBN: 978-1784393618 "Making Things Talk", 3rd Edition Tom Igoe, Maker Media, 2017 ISBN: 978-1680452150
Topics Covered	IoT applications and embedded computing, Wireless protocols, Wearable sensors, Home environment sensors, Behavior detection sensors, Data fusion, processing and analysis, Data communications and communication methods, Architectural design issues of IoT layers (Perception, Network, Middleware, Application), Security and privacy issues in IoT
Course Objective	To introduce students to the fundamentals of Internet of Things (IoT) and embedded computing To provide understanding of utilizing IoT to build cyber physical systems To understand various data communication methods enabling data mobility in real-time To understand how to analyze and visualize user data To provide comprehensive understanding of IoT by exploring real-world IoT application scenarios

	To gain a better understanding of various technologies that can be utilized for IoT implementations
Grading	Homework Assignments: 20% Design and Research Projects: 30% Midterm Exam: 20% Final Exam: 30%
Academic Honesty	You must acknowledge your work including figures, codes and writings are belonging to you with your signature on the front page of all submitted reports. If any similarity in the code, comments, customized program behavior, report writings and/or figures are found, both the helper (original work) and the requestor (duplicated/modified work) will be called for academic disciplinary action including failure of this course, and student's advisor/department will be notified. IIT Code of Academic Honesty: https://web.iit.edu/student-affairs/handbook/fine-print/code-academic-honesty
ADA Statement	Reasonable accommodations according to American Disability Act (ADA) 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 appoint to speak with as soon as possible. The Center for Disability Resources (CDR) is located in Life Sciences, Room 218, (312) 567-5744 or disabilities@iit.edu

Course Schedule

Week	Topic	Assignment
Week 1	Introduction to Internet of Things (IoT) and Cyber Physical Systems (CPS) • Definition & Characteristics of IoT • Difference between IoT and M2M	
Week 2,3,4	Embedded Systems and Programming • Examples including MCU, FPGA, ASIC • SPI, I2C, PWM, clocks, timers, UART, GPIO, etc. • Introduction to Python programming	HW#1: Arduino and Raspberry Pi Platforms and Programming
Week 5	IoT Perception Layer • Sensing technologies (RFID, WSN, GPS, NFC, etc.) • Wearable sensors, Home environment sensors, Behavior detection sensors	Research Project Release HW#2: Arduino and Raspberry Pi Signal Acquisition, Processing, Analysis and Storage
Week 6	IoT Network Layer • Wireless Protocols (6LoWPAN, CoAP and other protocols) • Broadband Networking Systems for IoT • Hardware Devices, Power Sources, Mobility, Design Issues, Operating Systems	Design Project Release (Encryption and Decryption with Raspberry Pi) HW#3: Wireless Sensing with Bluetooth Connection
Week 7	IoT Middleware Layer • Communication, storage, data management, software, platforms • Real-time analysis, integration, security, monitoring • Cloud computing: web services and interactions, databases, API, service discovery • Analytics and data interpretation	

Week 8	**Midterm Exam**	Research Project Report Due
Week 9,10	IoT Application Layer • Smart devices: Android, IoT gateways, OSes • Real-world Case Studies (transportation, healthcare monitoring, agriculture monitoring, emergency service, etc.)	HW#4: Simple IFTTT Program with Sensors and Server Interactions
Week 11	Security and Privacy Issues in IoT Quality of Service (QoS) Issues in IoT	Design Project Progress Report Due
Week 12, 13	Big data and analytics in IoT Industrial IoT and economic implications Human behavior effects through IoT eco-system	
Week 14	Review Session	Design Project Report Due
Week 15	**Final Exam**	