Secure Embedded Systems PhD Program Overview

Program Description

The Internet of Things (IoT) is an excellent opportunity for the progression of embedded systems. IoT mobile devices like smartphones, tablets, and wearables are already ubiquitous. As the IoT market expands, the volume and pervasiveness of IoT will grow exponentially. With each passing day, embedded systems are getting smaller and smarter, enabling us to get more things done than before. As we embed more functionality into smaller device footprints, there is an upsurge in security concerns. We present the Ph.D. in Secure Embedded Systems to address the security concerns. The Ph.D. program in Secure Embedded Systems targets highly motivated students with a bachelor's or master's degree and a strong desire to pursue career opportunities in academia, commercial industry, defense, government laboratories, federal agencies, consulting, military, or research.

Program Objectives

The Program targets highly motivated students who have already obtained a bachelor's or master's degree and desire to seek career opportunities in education, consulting, research, or administration, to name a few.

Expected Student Learning Outcomes

Upon completing the Program, students will have gained a broad technical and interdisciplinary background that enhances their ability to identify and tackle critical cybersecurity problems related to embedded system hardware and software. Specifically, upon completing the Program, students will be expected to:

1. Demonstrate a breadth of knowledge in advanced cybersecurity, cryptography, networking, and reverse engineering; and exhibit deep expertise in any one or combination of the core breadth areas, such as lightweight cryptography for embedded systems, side-channel analysis, digital forensics;
2. Apply mathematics, systems theory, principles of engineering, planning/or management in solving complex cybersecurity problems;
3. Design independently and execute high-level research; and
4. Communicate effectively orally and in written form and function on an interdisciplinary team, particularly in a laboratory setting.

General Requirements

Students enrolled in the Program will be required to satisfy the following requirements:

1. Form a doctoral advisory committee comprising four members, among whom at least three should be tenured or tenure-track faculty members. The committee chair must be a member of the graduate faculty and the ECE department or CAP faculty. A minimum of two ECE or CAP faculty must serve on the committee. The students form an advisory committee no later than the end of the first year. The committee approves the student's Program of study and guides the student's research activities;
2. Complete a minimum of 36 graduate credit hours (including 18 hours of dissertation-related research) of study beyond the Master's degree or a minimum of 48 graduate credit hours (including 18 hours of dissertation-related research) beyond the Bachelor's degree.
3. Pass a written qualifying exam within the first two years of study (one attempt within the first year), doctoral candidacy examinations (no sooner than a year of passing the qualifying exam), administered by the dissertation committee, on the core subjects and declared concentration; DocuSign
4. Develop and defend a dissertation proposal within the first four years of admission and
5. Complete and successfully defend a dissertation based on timely and original research in a relevant area of Secure Embedded Systems within six years of enrollment;
6. The dissertation committee chair must determine the original contribution of the dissertation work.

To maintain good academic standing and remain in the Program, the student may not have course grades lower than B in any required core courses and must maintain a cumulative GPA of 3.5. Failure to meet these requirements will lead to academic probation for one academic year.

Admission

The Program welcomes exceptional students with at least a 3.3 cumulative GPA (on a scale of 4.0) for all undergraduate and graduate work completed. Other requirements include a resume or curriculum vitae documenting current and previous professional activities, achievements, planned career goals, a statement of research interest, and three letters of recommendation from professors or supervisors familiar with the applicant's academic background. All application materials must be sent directly to the School of Graduate Studies through the application system for preliminary screening. Eligibility to be a student within the School of Graduate Studies is a prerequisite for admission into the Program.

Program of Study

The required minimum coursework for the Ph.D. in Secure Embedded Systems is 60 graduate credits beyond the Bachelor's degree and 36 graduate credits beyond the Master's degree. Up to four courses (not to exceed 12 credits) from other accredited institutions may be accepted for transfer toward the Ph.D. degree, assuming that students do not use transfer courses to satisfy the academic requirements of the former Program.