Information Assurance, PhD

A research-based, interdisciplinary Doctor of Philosophy (PhD) in Information Assurance combines a strong security technical foundation with a security policy and social sciences perspective. It seeks to prepare graduates to advance the state-of-the-art of security in systems, networks, and the internet in industry, academia, and government. The interdisciplinary nature of the program distinguishes it from traditional doctoral degree programs in computer science, engineering, or social sciences and makes it unique in the Boston area.

Students who choose the PhD in information assurance program have a strong desire to pursue academic research solving critical cybersecurity challenges facing today's society. The PhD program is a natural path for students in the college's Master of Science in Information Assurance and Cybersecurity (http://www.ccs.neu.edu/graduate/degree-programs/m-s-in-information-assurance)program who want to pursue research and students with bachelor's degrees and an interest in research-focused careers. Students who pursue careers in advancing the state-of-the art of cybersecurity have an opportunity to gain:

- A strong technical foundation in cybersecurity and an interdisciplinary perspective based on policy and social science
- A path to a research-focused career coupled with depth in information assurance research at a leading institution, one of the earliest designees by NSA/DHS as a National Center of Academic Excellence (http://www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml) in Information Assurance Research, Information Assurance/Cyber Defense, and Cyber Operations
- The opportunity to work with and learn from faculty who are recognized internationally for their expertise and contributions in information assurance from Northeastern's College of Computer and Information Science, the Department of Electrical and Computer Engineering, and the College of Social Sciences and Humanities
- Access to research projects at Northeastern's research centers focused on security:
  - The Cybersecurity and Privacy Institute (https://cyber.ccis.northeastern.edu/about): The mission of Northeastern's Cybersecurity and Privacy Institute is to safeguard critical technology. Forging partnerships with experts in industry, government, and academia worldwide, the Institute's faculty and students develop, protect, and enhance technologies on which the world relies—from mobile devices and "smart" IoT applications to tomorrow's self-driving cars and delivery drones. Their expertise spans algorithm auditing, cloud security, cryptography, differential privacy, embedded device security, Internet-scale security measurements, machine learning, big data, and security, malware and advanced threats, network protocols and security, Web and mobile security, wireless network security.
  - The International Secure Systems Lab (http://www.iseclab.org), affiliated with Northeastern, a collaborative effort of European and U.S. researchers focused on web security, malware and vulnerability analysis, intrusion detection, and other computer security issues
  - The ALERT Center (http://www.northeastern.edu/alert), where Northeastern is the lead institution, a multiuniversity Department of Homeland Security Center of Excellence involved in research, education, and technology related to threats from explosives

The benefits of the Boston area:

- World-renowned for academic and research excellence, the Boston area is also home to some of the nation's largest Department of Defense contractors and government and independent labs such as MIT Lincoln Lab, MITRE, and Draper Lab

Degree Requirements

The PhD in information assurance degree requires completion of at least 48 semester credit hours beyond a bachelor's degree. Students who enter with an undergraduate degree will typically need four to five years to complete the program, and they will be awarded a master's degree en route to the PhD.

Doctoral Degree Candidacy

A student is considered a PhD degree candidate after completing the core courses with at least a 3.400 grade-point average (GPA) and either publishing a paper in a strong conference or journal or passing an oral exam that is conducted by a committee of three information assurance faculty members and based on paper(s) written by the student.

RESIDENCY

One year of continuous full-time study is required after admission to the PhD candidacy. During this period, the student will be expected to make substantial progress in preparing for the comprehensive examination.

DISSERTATION ADVISING

The doctoral dissertation advising team for each student consists of two information assurance faculty members, one in a technical area. When appropriate, the second faculty advisor will be from the policy/social science area.

DISSERTATION COMMITTEE

A PhD student's dissertation committee consists of the two members of the dissertation advising team plus two others: One is a member of the information assurance faculty, and the other is an external examiner who is knowledgeable about the student's research topic.

COMPREHENSIVE EXAMINATION

A PhD student must submit a written dissertation proposal and present it to the dissertation committee. The proposal should identify the research problem, the research plan, and the potential impact of the research on the field. The presentation of the proposal will be made in an open forum, and the student must successfully defend it before the dissertation committee after the public presentation.

DISSERTATION DEFENSE

A PhD student must complete and defend a dissertation that involves original research in information assurance.

AWARDING OF MASTER'S DEGREES

Students who enter the PhD in information assurance program with a bachelor's degree have the option of obtaining a master's degree from one of the departments participating in the program. To do so, they must meet all of the department's degree requirements.

Program Requirements

Bachelor's Degree Entrance

Complete all courses and requirements listed below unless otherwise indicated.

Milestones

Qualifying exam and area exam
Annual review
Dissertation proposal
Dissertation committee
Dissertation defense

Core Requirements

A cumulative 3.400 GPA is required for the core requirement.

Code	Title	Hours
Fundamentals		
CS 5700	Fundamentals of Computer Networking	4
or EECE 7336	Digital Communications	
Software		
CS 5770	Software Vulnerabilities and Security	4
Security and Cyberlaw		
CS 6740	Network Security	4
or CS 6750	Cryptography and Communications Security	
IA 5200	Security Risk Management and Assessment	4
IA 5240	Cyberlaw: Privacy, Ethics, and Digital Rights	4

Electives and Specializations

Code	Title	Hours
Complete 28 semester hours from the following:		28
Consult faculty advisor for other acceptable courses.		
Track 1: Network/Communication Security		
CS 6710	Wireless Network	
EECE 5666	Digital Signal Processing	
Track 2: System Security		
CS 5600	Computer Systems	
or EECE 7352	Computer Architecture	
IA 6120	Software Security Practices	
Track 3 Policy/Society		
CRIM 7246	Security Management	
POLS 7341	Security and Resilience Policy	
General Electives		
CS 5500	Managing Software Development	
CS 6140	Machine Learning	
CS 6200	Information Retrieval	
EECE 7204	Applied Probability and Stochastic Processes	
EECE 7205	Fundamentals of Computer Engineering	
EECE 7337	Information Theory	
SOCL 7211	Research Methods	
or CS 6350	Empirical Research Methods	

Dissertation

Code	Title	Hours
Complete the following (repeatable) course twice:		
IA 9990	Dissertation	
Complete the following (repeatable) course until graduation:		
IA 9996	Dissertation Continuation	

Program Credit/GPA Requirements

48 total semester hours required
Minimum 3.000 GPA required