CYBER SECURITY GRADUATE PROGRAMS

INTERDEPARTMENTAL GRADUATE MAJOR

Iowa State University has been offering courses in cyber security since 1995 and has one of the largest programs in the country. Graduate degrees can be obtained in a traditional on campus setting or as an on-line program. For information about the online Cyber Security program visit Iowa State Online (https://iowastateonline.iastate.edu/).

Students graduating from the major will help to fill the need for well-educated system security specialists in the government, private sector, and academia. The program objectives identified as being critical to the accomplishment of this mission are:

1. Impart and enhance knowledge about information infrastructure security
2. Expand and develop the ability to engineer complex systems
3. Instill and nurture social awareness, and the ability to function in a team
4. Instill and nurture a sense of ethics
5. Develop an understanding of strategic and policy issues

We offer 4 different graduate degree options:

1. Masters of Science with thesis
2. Masters of Science without thesis
3. Masters of Engineering (coursework only)
4. Graduate certificate

Graduate Certificate

A graduate certificate in Cyber Security is offered, which consists of four courses (12 credits): The graduate certificate is targeted for off-campus students as a way to either supplement their education or as way to try out online education courses. All of the certificate courses will transfer into the MS or MENGR degree in Cyber Security.

for Certificate in Cyber Security

CYBSC 5300	Network Protocols and Security	3
CYBSC 5310	Information System Security	3
CYBSC 5320	Information Warfare	3
MATH 5330	Cryptography	3
or CYBSC 5350	Steganography and Digital Image Forensics	
or CYBSC 5340	Legal and Ethical Issues in Cyber Security	
or CYBSC 5360	Computer and Network Forensics	
or CPRE 5370	Wireless Network Security	
Total Credits		**12**

For additional information students should visit https://www.cyio.iastate.edu/. (http://www.iac.iastate.edu)

Master of Science with & without thesis

The degree Master of Science with a major in Cyber Security is under a cooperative arrangement with various home departments including Electrical and Computer Engineering, Political Science, Information Systems and Business Analytics, and Mathematics.

The degree Master of Science with thesis is recommended for students who intend to continue toward the Doctor of Philosophy degree or to undertake a career in research and development. The non-thesis Master of Science degree requires a creative component and is intended for students interested in a career in cybersecurity.

Students interested in the interdepartmental major apply and are admitted to both a home department (the department that is most closely aligned with the student's research interest and background) and to the program. The home department sets the admission standards, course requirements, and thesis standards. (**Note:** Electrical and Computer Engineering is the only home department for off-campus students pursuing the Master of Science in Cyber Security).

The program is broadly based and uses courses in the various departments. The program will consist of 24 course credits with 6 credits of research work for a Master of Science with thesis. A non-thesis Master of Science will consist of 27 credits of courses and 3 credits of creative component. The courses are divided into three categories: core, electives, and thesis research. A student's Program of Study Committee, in consultation with the student, determines the elective courses to be taken and the acceptability of transfer credits. The major professor will be selected from the discipline where the student is admitted (home department).

The basic prerequisite for admission to this program is a baccalaureate degree in engineering, mathematics, computer science, management information systems, political science, or closely related field. The GRE or GMAT examination may be required based on the standards of the home department. If the GRE or GMAT is not required it will be considered in admissions decisions if offered. Potential students with baccalaureate degrees in the physical sciences, statistics, or other related fields will be considered on an individual basis, possibly with provisional admission.

Master of Engineering

The Master of Engineering (MENGR) in Cyber Security degree is only offered to off-campus students. This program is designed to assist all individuals who already have a bachelor's degree in computing or related

areas to pursue an in-depth study in information assurance. The Master of Engineering program is based on coursework credits only (a thesis or creative component is not required). Courses are offered via digital streaming video. (**Note:** Electrical and Computer Engineering is the only home department for the Master of Engineering in Cyber Security).

A coursework only Master of Engineering degree in Cyber Security consists of 30 credits. The courses are divided into two categories: core and electives. (**Note**: Students pursuing the MENGR do not have a program of study committee and the major professor is the Cyber Security, Director of Graduate Education (DoGE)

Students interested in the MENGR in Cyber Security degree apply and are admitted to Cyber Security (CYBSC) with ECpE as the home department. The admission requirements for students entering the program without work experience are the same as the admission requirements for the ECpE department. For students with 3 or more years of work experience in a computer related position the GRE and GPA minimum may be waived. Students with an undergraduate degree in a non computing field that have at least 3 years of work experience in an information technology field may be admitted to the program.

Courses primarily for undergraduates:

CYBSC 1310: Introduction to Computer Security Literacy
(Cross-listed with CPRE 1310).
Credits: 1. Contact Hours: Lecture 1.
Basic concepts of practical computer and Internet security: passwords, firewalls, antivirus software, malware, social networking, surfing the Internet, phishing, and wireless networks. This class is intended for students with little or no background in information technology or security. Basic knowledge of word processing required. Offered on a satisfactory-fail basis only.

CYBSC 3320: Cyber Defense Competition
(Cross-listed with CPRE 3320).
Credits: 1. Contact Hours: Laboratory 2.
Repeatable.
Participation in cyber defense competition driven by scenario-based network design. Includes computer system setup, risk assessment and implementation of security systems, as well as defense of computer and network systems against trained attackers. Team based. Offered on a satisfactory-fail basis only. (Typically Offered: Spring)

CYBSC 3700: Fundamentals of Network Security
Credits: 3. Contact Hours: Lecture 3.
Fundamentals of network security, including common network protocols, potential security risks, and countermeasures. Network routing and its impact on security.

CYBSC 3710: Adversarial Thinking
Credits: 2. Contact Hours: Lecture 2.
Mindset and tactics of cyber adversaries. Anticipating and countering cybersecurity threats. Analyzing and predicting the strategies of cyber adversaries, including understanding their motives, methods, and techniques to evade detection. Multi-week team project where students will assume the role of attackers and plan an attack against a fictitious target.

CYBSC 3720: Fundamentals of Data Security and Privacy
Credits: 2. Contact Hours: Lecture 2.
Introduction and application of basic mechanisms for protecting data. Security issues related to safeguarding sensitive personal and corporate information against inadvertent disclosure. Real-world effects of data breaches on individuals and businesses and the balancing of interests among individuals, government, and enterprises. Emerging technologies that may affect security and privacy concerns. Issues related to developing enterprise data security programs, policies, and procedures that consider the requirements of all relevant constituencies, e.g., technical, business, and legal.

CYBSC 4300: Network Protocols and Security
(Dual-listed with CPRE 5300/ CYBSC 5300). (Cross-listed with CPRE 4300).
Credits: 3. Contact Hours: Lecture 3.
*Prereq: (*CPRE 3080*,* COMS 2520*, or* COMS 3520*) or* CPRE 2880
Detailed examination of networking standards, protocols, and their implementation. TCP/IP protocol suite, network application protocols. Network security issues, attack and mitigation techniques. Emphasis on laboratory experiments.

CYBSC 4600: Application of Security Literacy
Credits: 1. Contact Hours: Lecture 1.
Prereq: ENGL 3140 *or* ENGL 3140H
Training of teaching of basic cybersecurity concepts and running effective security awareness campaigns. Communication strategies, collaboration with departments such as HR, and promoting a security culture within organizations. Preparation to become advocates for security awareness in professional settings.

CYBSC 4610: Cyber Exercise Design
Credits: 1. Contact Hours: Lecture 1.
Prereq: ENGL 3140 *or* ENGL 3140H
Introduction to designing and facilitating cybersecurity exercises, including tabletop exercises and livesimulations. Creation of tabletop exercises and live simulations that enhance cybersecurity awareness,preparedness, and response capabilities. Scenario planning, facilitation skills, post-exercise evaluation,adaptation for various roles, and evaluation using federal guidelines.

CYBSC 4700: Threat Hunting and Intelligence
Credits: 2. Contact Hours: Lecture 2.
Prereq: CYBSC 3710 *and* CYBSC 3720 *and* CYBSC 4300
Tools and methods for threat hunting and intelligence gathering to strengthen organizational defense. Techniques for identifying and mitigating cyber threats, utilizing various security tools and intelligence sources.

CYBSC 4710: Digital Forensics and Incident Response
Credits: 2. Contact Hours: Lecture 2.
Prereq: CYBSC 3710 *and* CYBSC 3720 *and* CYBSC 4300
Fundamentals of digital forensics and incident response, including evidence collection, analysis, andresponse planning techniques. Preparation to handle security incidents effectively, covering forensicanalysis techniques, evidence collection and handling, response planning, and incident response policydevelopment.

CYBSC 4720: Applications of Cryptography
Credits: 2. Contact Hours: Lecture 2.
Prereq: CYBSC 3710 *and* CYBSC 3720 *and* CYBSC 4300
Cryptographic methods for information security, privacy assurance, and authenticity verification.Encryption techniques, cryptographic protocols, secure key management, and digital signatures,emphasizing practical applications in cybersecurity.

CYBSC 4730: Fundamentals of Operating Systems Security
Credits: 2. Contact Hours: Lecture 2.
Prereq: CYBSC 3710 *and* CYBSC 3720
Introduction of security principles for operating systems, focusing on securing Windows and Linuxenvironments. Access control, privilege management, file system security, memory management, andsystem hardening techniques to protect against vulnerabilities. Exploring vulnerabilities in operatingsystems, analysis of security features, and defensive strategies for enhancing OS security.

CYBSC 4740: Fundamentals of Cloud Security
Credits: 2. Contact Hours: Lecture 2.
Prereq: CYBSC 3710 *and* CYBSC 3720
Introduction to cloud security concepts, architectural principles, secure cloud design, and best practicesfor cloud service providers and users. Cloud security principles, including secure design, data protection, identity management, and regulatory compliance. Protecting cloud environments from uniquecybersecurity threats.

CYBSC 4750: Fundamentals of Software Security
Credits: 2. Contact Hours: Lecture 2.
Prereq: CYBSC 3710 *and* CYBSC 3720
Overview of secure software development, common vulnerabilities, secure coding practices, and testingmethods. Basic secure coding practices, threat modeling, vulnerability assessment, and techniques formitigating risks such as buffer overflows, injection attacks, and improper input validation.

CYBSC 4760: Fundamentals of Cybersecurity Scripting
Credits: 2. Contact Hours: Lecture 2.
Prereq: CYBSC 3710 *and* CYBSC 3720
Scripting for cybersecurity tasks, focusing on automation and custom tool development. Basics ofscripting languages commonly used in cybersecurity, such as Python and PowerShell. Writing scripts for data parsing, log analysis, and network monitoring, as well as developing custom scripts for security tasks like vulnerability scanning and incident response.

CYBSC 4770: Fundamentals of Cyber Resilience
Credits: 2. Contact Hours: Lecture 2.
Prereq: CYBSC 3710 *and* CYBSC 3720
Strategies for designing systems that can withstand and recover from cyber-attacks, detection, response, and recovery from cyber-attacks while minimizing impact. Resilience planning, incident response, maintaining operational continuity, and strategies to ensure operational continuity under adverse conditions.

CYBSC 4780: Fundamentals of Cyber-Physical and Critical Infrastructure Security
Credits: 2. Contact Hours: Lecture 2.
Prereq: CYBSC 3710 *and* CYBSC 3720
Cybersecurity challenges unique to cyber-physical systems and critical infrastructure sectors. Securingcyber-physical systems, critical infrastructure, threat modeling, risk management, and incident response. Emphasizes security challenges in energy, manufacturing, agriculture, and transportation sectors.

CYBSC 4790: Fundamentals of Web Security
Credits: 2. Contact Hours: Lecture 2.
Prereq: CYBSC 3710 *and* CYBSC 3720
Securing web applications by addressing vulnerabilities such as SQL injection and cross-site scripting.Fundamental principles of web security and secure applications. SQL injection, cross-site scripting(XSS), authentication and session management, and the Open Web Application Security Project(OWASP) Top Ten.

CYBSC 4890: Cybersecurity Capstone
Credits: 3. Contact Hours: Lecture 3.
Prereq: CYBSC 3710*,* CYBSC 3720*,* CYBSC 4300*, and 8 additional credits CYBSC courses*
Culminating capstone experience. Development a cybersecurity solution, including threat assessment,architecture design, incident response plan, and final plan presentation.

Courses primarily for graduate students, open to qualified undergraduates:

CYBSC 5300: Network Protocols and Security
(Dual-listed with CPRE 4300/ CYBSC 4300). (Cross-listed with CPRE 5300).
Credits: 3. Contact Hours: Lecture 3.
Prereq: Graduate Standing or Permission of Instructor
Detailed examination of networking standards, protocols, and their implementation. TCP/IP protocol suite, network application protocols. Network security issues, attack and mitigation techniques. Emphasis on laboratory experiments.

CYBSC 5310: Information System Security
(Cross-listed with CPRE 5310).
Credits: 3. Contact Hours: Lecture 3.
Prereq: Graduate Standing or Permission of Instructor
Computer, software, and data security: basic cryptography, security policies, multilevel security models, attack and protection mechanisms, legal and ethical issues.

CYBSC 5320: Information Warfare
(Cross-listed with CPRE 5320).
Credits: 3. Contact Hours: Lecture 3.
Prereq: CPRE 4300 *or 5300*
Computer system and network security: implementation, configuration, testing of security software and hardware, network monitoring. Authentication, firewalls, vulnerabilities, exploits, countermeasures. Study and use of attack tools. Ethics in cyber security. Emphasis on laboratory experiments. (Typically Offered: Spring)

CYBSC 5330: Cryptography
(Cross-listed with CPRE 5330/ MATH 5330).
Credits: 3. Contact Hours: Lecture 3.
*Prereq: Graduate Standing or (*MATH 2300/COMS 2300*,* MATH 3010*, and* CPRE 3100*)*
Basic concepts of secure communication, DES and AES, public-key cryptosystems, elliptic curves, hash algorithms, digital signatures, applications. Relevant material on number theory and finite fields. (Typically Offered: Spring)

CYBSC 5340: Legal and Ethical Issues in Cyber Security
(Cross-listed with CPRE 5340/ POLS 5340).
Credits: 3. Contact Hours: Lecture 3.
Prereq: Graduate Standing or Permission of Instructor
Legal and ethical issues in computer security. State and local codes and regulations. Privacy issues. (Typically Offered: Spring)

CYBSC 5350: Steganography and Digital Image Forensics
(Cross-listed with CPRE 5350/ MATH 5350).
Credits: 3. Contact Hours: Lecture 3.
Prereq: Graduate Standing or Permission of Instructor
Basic principles of covert communication, steganalysis, and forensic analysis for digital images. Steganographic security and capacity, matrix embedding, blind attacks, image forensic detection and device identification techniques. Related material on coding theory, statistics, image processing, pattern recognition. (Typically Offered: Spring)

CYBSC 5360: Computer and Network Forensics
(Cross-listed with CPRE 5360).
Credits: 3. Contact Hours: Lecture 3.
Prereq: CPRE 4890 *or* CPRE 4300 *or* CPRE 5300
Fundamentals of computer and network forensics, forensic duplication and analysis, network surveillance, intrusion detection and response, incident response, anonymity and pseudonymity, privacy-protection techniques, cyber law, computer security policies and guidelines, court testimony and report writing, and case studies. Emphasis on hands-on experiments.

CYBSC 5380: Reverse Engineering and Security Testing
(Cross-listed with CPRE 5380).
Credits: 3. Contact Hours: Lecture 3.
Prereq: Graduate Standing or Permission of Instructor
Techniques and tools for understanding the behavior of software/hardware systems based on reverse engineering. Flaw hypothesis, black, grey, and white box testing as well as other methods for testing the security of software systems. Discussion of counter-reverse engineering techniques. (Typically Offered: Spring)

CYBSC 5600: Data-Driven Security and Privacy
(Cross-listed with COMS 5600/ CPRE 5600).
Credits: 3. Contact Hours: Lecture 3.
Prereq: Graduate Standing or Permission of Instructor
Examination of applications of machine learning and big data techniques to various security and privacy problems, as well as secure and privacy-preserving machine learning algorithms. Offered irregularly. (Typically Offered: Spring)

CYBSC 5920: Seminar in Cyber Security
Credits: 1-3. Contact Hours: Lecture 3.
Repeatable.
Prereq: Graduate Standing or Permission of Instructor
Projects or seminar in Cyber Security. (Typically Offered: Fall, Spring, Summer)

Courses for graduate students:

CYBSC 6310: Cyber Security Operations Practicum
(Cross-listed with CPRE 6310).
Credits: 3. Contact Hours: Lecture 1.
Repeatable.
Practical experience in cyber operations. Cyber security threat analysis, malware analysis, and intrusion detection management. Cyber security data analysis methods. Pen testing tools and techniques. Weekly threat analysis briefings. Offered on a satisfactory-fail basis only.

CYBSC 6320: Cyber Security Capstone Design
(Cross-listed with CPRE 6320).
Credits: 3. Contact Hours: Lecture 3.
Capstone design course which integrates the security design process. Design of a security policy. Creation of a security plan. Implementation of the security plan. The students will attack each other's secure environments in an effort to defeat the security systems. Students evaluate the security plans and the performance of the plans. Social, political and ethics issues. Student self-evaluation, journaling, final written report.

CYBSC 6340: Current Research Problems in Cyber Security
Credits: 3. Contact Hours: Lecture 3.
Repeatable.
Discussion of complex cyber security problems. Students will learn how to apply research techniques, think clearly about these issues, formulate and analyze potential solutions, and communicate their results. Working in small groups under the mentorship of technical clients from government and industry, each student will formulate, carry out, and present original research on complex current cybersecurity problems of interest to the nation. This course will be run in a synchronized distance fashion, coordinating some activities with our partner schools and our technical clients. (Typically Offered: Fall, Spring)

CYBSC 6970: Cyber Security Summer Internship
Credits: Required.
One semester and one summer maximum per academic year professional work period. Offered on a satisfactory-fail basis only.