CYBER SECURITY

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 on the Engineering-LAS Online Learning program visit www.eol.iastate.edu. (http://www.eol.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 530	Network Protocols and Security	3
CYBSC 531	Information System Security	3
CYBSC 532	Information Warfare	3
CYBSC 533	Cryptography	3
or CYBSC 535	Steganography and Digital Image Forensics	
or CYBSC 534	Legal and Ethical Issues in Information Assurance	
or CYBSC 536	Computer and Network Forensics	
or CPR E 537	Wireless Network Security	
Total Credits		**12**

For additional information students should visit http://www.iac.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, Supply Chain and Information Systems, 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 information assurance.

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

our Engineering-LAS Online Learning streaming media online education program. (**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 three categories: core, electives, and capstone course. (**Note**: Students pursuing the MENGR do not have a program of study committee and the major professor is the Information Assurance, 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 131: Introduction to Computer Security Literacy
(Cross-listed with CPR E). (1-0) Cr. 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 332: Cyber Defense Competition
(Cross-listed with CPR E). (0-2) Cr. 1. Repeatable. S.
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.

CYBSC 430: Network Protocols and Security
(Dual-listed with CYBSC 530). (Cross-listed with CPR E). (3-0) Cr. 3.
Prereq: CPR E 308 OR COM S 252 OR COM S 352
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.

Courses primarily for graduate students, open to qualified undergraduates:

CYBSC 530: Network Protocols and Security
(Dual-listed with CYBSC 430). (Cross-listed with CPR E). (3-0) Cr. 3.
Prereq: CPR E 308 OR COM S 252 OR COM S 352
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 531: Information System Security
(Cross-listed with CPR E). (3-0) Cr. 3.
Prereq: CPR E 489 or CPR E 530 or COM S 586 or MIS 535
Computer, software, and data security: basic cryptography, security policies, multilevel security models, attack and protection mechanisms, legal and ethical issues.

CYBSC 532: Information Warfare
(Cross-listed with CPR E). (3-0) Cr. 3. S.
Prereq: CPR E 430 or 530
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 information assurance. Emphasis on laboratory experiments.

CYBSC 533: Cryptography
(Cross-listed with CPR E, MATH). (3-0) Cr. 3. S.
Prereq: MATH 301 or CPR E 310 or COM S 230
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.

CYBSC 534: Legal and Ethical Issues in Information Assurance
(Cross-listed with CPR E, POL S). (3-0) Cr. 3. S.
Prereq: Graduate classification; CPR E 531 or CYBSC 531
Legal and ethical issues in computer security. State and local codes and regulations. Privacy issues.

CYBSC 535: Steganography and Digital Image Forensics
(Cross-listed with CPR E, MATH). (3-0) Cr. 3. S.
Prereq: E E 524 or MATH 317 or MATH 407 or COM S 230
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.

CYBSC 536: Computer and Network Forensics
(Cross-listed with CPR E). (3-0) Cr. 3.
Prereq: CPR E 489 or CPR E 530
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 538: Reverse Engineering and Security Testing
(Cross-listed with CPR E). (2-3) Cr. 3. S.
Prereq: COM S 321 or CPR E 381, COM S 352 or CPR E 308
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.

CYBSC 560: Data-Driven Security and Privacy
(Cross-listed with COM S, CPR E). Cr. 3. Alt. S., offered irregularly.
Prereq: CPR E 531; COM S 474 or COM S 573
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.

CYBSC 592: Seminar in Information Assurance
Cr. 1-3. Repeatable.
Prereq: Permission of instructor
Projects or seminar in Information Assurance.

Courses for graduate students:

CYBSC 631: Cyber Security Operations Practicum
(Cross-listed with CPR E). Cr. 3. Repeatable.
Prereq: CPR E 532; CPR E 534; and permission of instructor
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 632: Information Assurance Capstone Design
(Cross-listed with CPR E). (3-0) Cr. 3.
Prereq: CYBSC 531, CYBSC 532, CYBSC 534
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 634: Current Research Problems in Cyber Security
(3-0) Cr. 0. Repeatable. F.S.
Prereq: CPR E 530, CPR E 531, permission of instructor.
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/information assurance 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.

CYBSC 697: Information Assurance Summer Internship
Cr. R.
Prereq: Permission of department, graduate classification
One semester and one summer maximum per academic year professional work period. Offered on a satisfactory-fail basis only.