Information Assurance

Interdepartmental Graduate Major

Work is offered for the degree Master of Science with a major in information assurance under a cooperative arrangement with various departments including Electrical and Computer Engineering, Computer Science, Political Science, Supply Chain Management, 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. The Master of Engineering degree is coursework only.

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 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

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.

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 coursework only Master of Engineering degree in Information Assurance consisting of 30 credits is also offered.

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.

A graduate certificate in Information Assurance is offered, which consists of four courses (12 credits):

INFAS 530	Advanced Protocols and Network Security	3
INFAS 531	Information System Security	3
INFAS 532	Information Warfare	3
INFAS 533	Cryptography	3
or INFAS 535	Steganography and Digital Image Forensics	
or INFAS 534	Legal and Ethical Issues in Information Assurance	
or INFAS 536	Computer and Network Forensics	
or CPR E 537	Wireless Network Security	
Total Credits		12

For additional information students should contact the chair of the Supervisory Committee, 2215 Coover Hall, ISU, Ames, Iowa 50011, or visit http://www.iac.iastate.edu . (http://www.iac.iastate.edu.)

Courses primarily for undergraduates:

INFAS 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.

Courses primarily for graduate students, open to qualified undergraduates:

INFAS 530. Advanced Protocols and Network Security.
(Cross-listed with CPR E). (3-0) Cr. 3. *Prereq: CPR E 381*
Detailed examination of networking standards, protocols, and their implementation. TCP/IP protocol suite, network application protocols, IP routing, network security issues. Emphasis on laboratory experiments.

INFAS 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 and network security: basic cryptography, security policies, multilevel security models, attack and protection mechanisms, legal and ethical issues.

INFAS 532. Information Warfare.
(Cross-listed with CPR E). (3-0) Cr. 3. S. *Prereq: CPR E 531*
Computer system and network security: implementation, configuration, testing of security software and hardware, network monitoring. Authentication, firewalls, vulnerabilities, exploits, countermeasures. Ethics in information assurance. Emphasis on laboratory experiments.

INFAS 533. Cryptography.
(Cross-listed with CPR E, MATH). (3-0) Cr. 3. S. *Prereq: MATH 301 or CPR E 310 or COM S 330*
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.

INFAS 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 INFAS 531*
Legal and ethical issues in computer security. State and local codes and regulations. Privacy issues.

INFAS 535. Steganography and Digital Image Forensics.
(Cross-listed with CPR E, MATH). (3-0) Cr. 3. S. *Prereq: E E 524 or MATH 307 or COM S 330*
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.

INFAS 536. Computer and Network Forensics.
(Cross-listed with CPR E). (3-0) Cr. 3. *Prereq: CPR E 381 and 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.

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

Courses for graduate students:

INFAS 632. Information Assurance Capstone Design.
(Cross-listed with CPR E). (3-0) Cr. 3. *Prereq: INFAS 531, INFAS 532, INFAS 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 attach 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, and an oral report.

INFAS 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.