INFORMATION ASSURANCE (INFAS)

Any experimental courses offered by INFAS can be found at:
registrar.iastate.edu/faculty-staff/courses/explistings/ (http://www.registrar.iastate.edu/faculty-staff/courses/explistings)

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.

INFAS 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.

INFAS 430: Network Protocols and Security
(Dual-listed with INFAS 530). (Cross-listed with CPR E). (3-0) Cr. 3.
Prereq: CPR E 381 or equivalent
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:

INFAS 530: Network Protocols and Security
(Dual-listed with INFAS 430). (Cross-listed with CPR E). (3-0) Cr. 3.
Prereq: CPR E 381 or equivalent
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.

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, software, and data 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. Study and use of attack tools. 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 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.

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 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.

INFAS 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.

INFAS 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.

INFAS 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.

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 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.

INFAS 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.

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.