Information Assurance (IA)

Courses

IA 241 Cyberlaw and Cybercrime 3 Cr.
This course includes extensive discussion of the legal constraints, both civil and criminal, that underlie acceptable behavior using computers and networks today. Cross-listed as CJ341. Prerequisite: CJ 101 or instructor permission.

IA 340 Introduction to Information Assurance 3 Cr.
This course introduces the foundations of information assurance, with focus on concepts and terminology used in describing, analyzing, and implementing information security. Topics include the history and mission of information assurance, history of computer crime, modern and historical cryptology, information warfare, penetrating computer systems and networks, malware, social engineering, spam, phishing, physical and facilities security, network security, identification and authentication, securing stored data, data backups and archives, patch management, and protecting digital rights. 3 hours; laboratory 2 hours. Prerequisite: C or higher in IS 131 or CS 140 or permission of instructor.

IA 342 Management of Information Assurance 3 Cr.
This course focuses on management of the information assurance process. Topics include human factors in reducing security breaches, security incident detection and response, remediation, management's role in information assurance, and other considerations in framing and implementing information assurance policies. The final section reviews current topics of particular interest and activity in the field of information assurance. Prerequisite: IS 340 or IA 340 or permission of instructor.

IA 360 Network Security 3 Cr.
This course focuses on the concepts, terminology and practice of network security. Topics include the fundamental goals of network security and practical applications of wired and wireless network security techniques such as applications of cryptology in network protocols, authentication, access control, network security devices such as firewalls and intrusion detection and prevention systems, incident response, log analysis, honeypots and honeynets. Classroom 3 hours, laboratory 2 hours. Prerequisite: IS 460 or CS 260.

IA 455 Contemporary Issues in Information Assurance 3 Cr.
A capstone seminar for Computer Security and Information Assurance majors which will vary every term in accordance with the current issues of the time. Students work with the instructor as they explore today's issues and trends in preparation of a thesis or project. Emphasis is placed on critical thinking, research and evaluation of current issues. A comprehensive computer security exam is included in this course. Prerequisites: IA 340, IA 342. Open to CSIA Junior 2 or higher, or by instructor permission.

IA 456 Cyber Defense Practicum 3 Cr.
This course provides practical application of the concepts learned over the course of the CSIA program. This is the technical capstone for the program and is a required course. The class is divided into three teams. Each team rotates through red (attack), blue (defend) and white (monitor/analyze) cells over the semester. Network attack analysis, intrusion detection systems and the use of network forensics in attaché analysis and defense are covered. Several open source and commercial tools during the class are used. Scenarios on a variation of the virtual network are ran. Blue teams harden the devices on the network to resist attack and are scored on how successful they are. Red teams develop a suite of attacks that allow completion of the scenario and are scored on the completeness of attack preparations. White teams analyze the read attacks and the blue responses and present analysis to the class at the close of the exercise. The scenario changes slightly for the iterations presented. This is a100% lab class. Prerequisites: IS 340 or IA 340 and IS 460 or CS 260.