COMPUTER AND INFORMATION SYSTEMS SECURITY (CISS)

CISS 609. Advanced Computational Intelligence. 3 Hours.
Semester course; 3 lecture hours. 3 credits. Prerequisite: an undergraduate course in artificial intelligence, or equivalent background with permission of instructor. Exploration of issues related to application of computational intelligence techniques to system security, particularly in the detection of anomalous system behavior. Of particular interest are issues associated with the automated detection of anomalies caused by authorized users through intended malicious behavior or through accidental misuse, and issues associated with automated user authentication. Crosslisted as: CMSC 609.

CISS 616. Data Warehousing. 3 Hours.
Semester course; 3 lecture hours. 3 credits. Prerequisite: INFO 610. Covers important concepts and techniques in the design and implementation of a data warehouse. Topics include the data warehouse architecture, the logical and physical design issues in the data warehousing development process, technical factors (i.e., hardware, client/server technology, data warehousing and DBMS technologies) and implementation considerations (i.e., data extraction, clean-up and transformation tools). Introduces online analytical processing and data mining. Crosslisted as: INFO 616.

CISS 618. Database and Application Security. 3 Hours.
Semester course; 3 lecture hours. 3 credits. Theory and practice of database and software security focusing in particular on some common database software security risks and on the identification of potential threats and vulnerabilities. Crosslisted as: CMSC 618.

CISS 622. Network and Operating Systems Security. 3 Hours.
Semester course; 3 lecture hours. 3 credits. Prerequisite: CISS 624. Studies the principles of network security and secure operating systems. Included are topics relating to the use of intrusion detection, intrusion prevention and other related tools. Crosslisted as: CMSC 622.

CISS 624. Applied Cryptography. 3 Hours.
Semester course; 3 lecture hours. 3 credits. Provides a comprehensive survey of modern cryptography. Included are techniques of enciphering and deciphering messages using cryptographic algorithms, block ciphers and block cipher modes, hash functions and message authentication codes, public key cryptography and digital signatures, and steganography. Crosslisted as: CMSC 620.

CISS 634. Ethical, Social and Legal Issues in Computer and Information Systems Security. 3 Hours.
Semester course; 3 lecture hours. 3 credits. Analyzing socio-political and ethical issues surrounding computer and information systems security. Topics include privacy laws, identity theft, information collection and retention policies, and enforcement.

CISS 644. Principles of Computer and Information Systems Security. 3 Hours.
Semester course; 3 lecture hours. 3 credits. Prerequisite: INFO 640 or INFO 661. Explores issues related to protecting information resources of a firm. Various tools and techniques useful for assessing CISS security concerns in organizations are introduced. Principles and models for CISS security and security management are presented and selected computer and CISS security topics are introduced. Material is presented and discussed from a management frame of reference. Crosslisted as: INFO 644.