CYBR - CYBERSECURITY

CYBR 601/CSCE 701 Foundations of Cybersecurity
Credits 3. 3 Lecture Hours.
Foundational concepts and principles of cybersecurity; cryptographic algorithms; hash functions; introduction to cyber-physical systems security; authentication, firewalls, and intrusion detection systems; social constructs and domains of cybersecurity.
Prerequisites: Graduate classification or approval of instructor.
Cross Listing: CSCE 701/CYBR 601.

CYBR 602/CSCE 702 Law and Policy in Cybersecurity
Credits 3. 3 Lecture Hours.
Law and policy issues related to cybersecurity including procurement, operations, maintenance, governance, oversight, protection, defense; analyze law, policies, and regulations domestically and globally.
Prerequisite: Graduate classification.
Cross Listing: CSCE 702/CYBR 602.

CYBR 603/CSCE 703 Cybersecurity Risk
Credits 3. 3 Lecture Hours.
Risks in cybersecurity; avoidance, acceptance, mitigation or transference strategies; developing reliable cybersecurity risk assessments to include analysis, categorization and evaluation; cybersecurity risk audit frameworks.
Cross Listing: CSCE 703/CYBR 603.

CYBR 604/CSCE 704 Data Analytics for Cybersecurity
Credits 3. 3 Lecture Hours.
Introduction to the theoretical foundations, algorithms and methods of data analytics for cybersecurity; societally-critical topic with impacts across computing systems and networks, social and web-based communities, industrial control systems and personal devices, among many others; study and application of data analytics including cluster analysis, supervised machine learning, anomaly detection and visualization; addresses a suite of cybersecurity topics including cyber attacks, anomaly detection, vulnerability analysis, strategic manipulation and propaganda.
Prerequisite: Graduate classification.
Cross Listing: CSCE 704/CYBR 604.

CYBR 630/ECEN 759 Hardware Security
Credits 3. 3 Lecture Hours.
Cryptography and cryptographic algorithms such as AES, DES and others; techniques to optimize hardware implementation of cryptographic systems; different types of side-channel attacks and countermeasures; supply-chain vulnerabilities including hardware Trojans, counterfeits, IP piracy and reverse engineering; security modules for system-on-chip; physical unclonable functions.
Prerequisites: ECEN 468, ECEN 474, or approval of instructor.
Cross Listing: ECEN 759/CYBR 630.

CYBR 660/INTA 690 Cybersecurity Literacy for the Global Arena
Credits 3. 3 Lecture Hours.
Research technical literacy in cybersecurity; exploration of cybersecurity in applied settings to include private and public sector; use of cybersecurity literacy to develop policy guidelines; examination of intent of cyber-actors; technical and policy risk-mitigation strategies.
Prerequisite: Graduate classification or approval of instructor.
Cross Listing: INTA 690/CYBR 660.

CYBR 661/PSAA 608 Cybersecurity Policy, Issues and Operations - A Manager's Guide
Credits 3. 3 Lecture Hours.
Overview related to U.S. homeland defense and homeland security; includes cyber threats; cyberwar; securing cyberspace in public and private sector; protecting data, systems and networks that are connected to the Internet and the Internet of Things.
Prerequisite: Graduate classification.
Cross Listing: PSAA 608/CYBR 661.

CYBR 684 Professional Internship
Credits 0 to 6. 0 to 6 Other Hours.
Directed internship in an organization to provide students with a learning experience supervised by professionals in organizational settings appropriate to the student's professional objectives.

CYBR 685 Directed Studies
Credits 0 to 12. 0 Lecture Hours. 0 Lab Hours. 0 to 12 Other Hours.
Directed individual study in cybersecurity. May be repeated for credit.

CYBR 689 Special Topics in...
Credits 0 to 4. 0 Lecture Hours. 0 Lab Hours. 0 to 4 Other Hours.
Selected topics in an identified area of cybersecurity. May be repeated for credit.

CYBR 691 Research
Credits 0 to 12. 0 Lecture Hours. 0 Lab Hours. 0 to 12 Other Hours.
Research conducted under the direction of faculty member in cybersecurity topics. May be repeated for credit.

CYBR 711/CSCE 711 Introduction to Modern Cryptography
Credits 3. 3 Lecture Hours.
Perfectly secret encryption; one-time pad; pseudorandom generators, functions and permutations; security definitions; block ciphers; stream ciphers; cryptanalysis; message authentication codes; hash functions; factoring, discrete log and the Diffie-Hellman problem; trapdoor functions and permutations; public-key encryption; El Gamal and RSA encryption schemes; digital signatures; DSA and RSA signature schemes; identification schemes; the Fiat-Shamir transform; advanced topics include secret sharing, oblivious transfer, zero-knowledge proofs, secure multi-party computation.
Prerequisites: STAT 211 and CSCE 411; graduate classification.
Cross Listing: CSCE 711/CYBR 711.

CYBR 776/ECEN 776 Unconditionally Secure Electronics
Credits 3. 3 Lecture Hours.
Data security; cryptography; key exchange; conditional security; unconditional (information-theoretic) security; quantum key distribution; the Kirchhoff-law-Johnson-noise (KLJN) key exchange, electronic noise; advanced issues of KLJN including schemes, protocols, attacks, defense, privacy amplification, credit cards, PUF, autonomous vehicles and smart grids.
Prerequisites: ECEN 214, ECEN 303, or STAT 211; graduate classification.
Cross Listing: ECEN 776/CYBR 776.