

CYBR - CYBERSECURITY (CYBR)

CYBR 201/CSCE 201 Fundamentals of Cybersecurity

Credits 3. 3 Lecture Hours.

Basic terminology, concepts, technology, and trends of cybersecurity; foundations of cybersecurity to include cryptography, public key infrastructure, standards and protocols, physical security, network fundamentals; workings of systems, networks, infrastructure; legal and ethical issues in cybersecurity.

Cross Listing: CSCE 201/CYBR 201.

CYBR 285 Directed Studies

Credits 0 to 4. 0 to 4 Other Hours.

Directed individual study in cybersecurity. May be repeated for credit.

CYBR 289 Special Topics in...

Credits 0 to 4. 0 to 4 Other Hours.

Selected topics in an identified area of cybersecurity. May be repeated for credit.

CYBR 291 Research

Credits 0 to 4. 0 to 4 Other Hours.

Research conducted under the direction of faculty member in cybersecurity topics. May be repeated for credit.

CYBR 402 Law and Policy in Cybersecurity

Credits 3. 3 Lecture Hours.

Examination of law and policy issues related to cybersecurity for the spectrum of cybersecurity jobs; includes procurement, operations and maintenance, governance and oversight, protection and defense, analysis, intelligence collection and operation and investigation cybersecurity jobs.

Prerequisites: Junior or senior classification; MARA-403 taught at Galveston campus.

Cross Listing: CSCE 402 and MARA 403.

CYBR 403/CSCE 477 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.

Prerequisite: Grade of C or better in CYBR 201/CSCE 201, CSCE 201/ CYBR 201, or CSCE 221; junior or senior classification.

Cross Listing: CSCE 477/CYBR 403.

CYBR 405 Applied Digital Forensics and Incident Response

Credits 3. 3 Lecture Hours.

Collection of digital evidence; digital evidence analytics; analysis of log data; malware triage; recover damaged digital evidence; write technical reports on malware and incidents; legal and ethical components of digital forensic science.

Prerequisites: Junior or senior classification.

CYBR 466/ECEN 466 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; schemes, protocols, attacks, defense, privacy amplification, credit cards, PUF, autonomous vehicles and smart grids.

Prerequisites: Grade of C or better in ECEN 214; grade of C or better in ECEN 303 or STAT 211; junior or senior classification.

Cross Listing: ECEN 466/CYBR 466.

CYBR 484 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 485 Directed Studies

Credits 0 to 4. 0 to 4 Other Hours.

Directed individual study in cybersecurity. May be repeated for credit.

CYBR 489 Special Topics in...

Credits 0 to 4. 0 to 4 Other Hours.

Selected topics in an identified area of cybersecurity. May be repeated for credit.

CYBR 491 Research

Credits 0 to 4. 0 to 4 Other Hours.

Research conducted under the direction of faculty member in cybersecurity topics. May be repeated for credit.