CSC 522 – DEFENSIVE CODING AND SECURITY

CREDIT HOURS: 3
PREREQUISITES: CSC 241 or 331, CSC 455 or 447; or Instructor Permission. CSC 562 recommended.
GRADE REMINDER: Must have a grade of C or better in each prerequisite course

CATALOG DESCRIPTION

Provides a foundation for building secure software by applying security principles to the software development lifecycle. Topics covered include: security in requirements engineering, secure designs, risk analysis, threat modeling, deploying cryptographic algorithms, defensive coding, penetration testing, fuzzing, static analysis, and security assessment. Includes case studies, data protection via coding and secure access methodology, and vulnerability identification, and modern security coding techniques.

PURPOSE OF COURSE

To study and practice fundamental techniques in developing secure coding practices, along with identifying and mitigating security risks in code. To discuss security concerns vs. design tradeoffs at various levels of coding abstraction. Learn the practical skills for developing and testing for secure software while also learning sound security fundamentals from real-world case studies.

EDUCATIONAL OBJECTIVES

Upon successful completion of the course, students should be able to:

1. Apply contemporary formal mathematical modeling techniques to model and analyze the security of a software system
2. Identify project security risks and selecting risk management strategies.
3. Use statistical methods to collect and analyze metrics for assessing and improving the security of a product, process, and project objectives.
4. Describe and discuss security concerns and designs at multiple levels of abstraction.
5. Demonstrate how to comply with data privacy and security requirements when designing a software system.
6. Design a software solution with secure access and protection of data.
7. Use quality assurance activities and strategies that support early vulnerability detection and contribute to improving the development process.
8. Develop secure coding techniques.

CONTENT

Introduction to Defensive Coding and Security .................................................................................................................................................................................. 3
   Overview and course introduction
   Coding Lifecycles

Misuse, Ignorance and Abuse of Coding ..................................................................................................................................................................................... 12
Case studies
Violating good coding practices
Threat modeling
Test planning

Coding

Defensive Coding
Case Studies
Code reviews and inspection

Cryptography

Theory of cryptography
Cryptography in practice
Methods used to subvert cryptography

Miscellaneous Threats

Distribution and deployment of code
Insider threats
CVSS
Usability

Exams (plus final)

REFERENCES

