CSCI 5322 – DEFENSIVE CODING AND SECURITY

CREDIT HOURS: 3

PREREQUISITES: CSCI 3302 or 3331, CSIT 4355 or CSCI 4347; or Instructor Permission. CSCI 5362 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.

COURSE CALENDAR

This course meets for a minimum of 37.5 lecture contact hours during the semester, including the final exam. Students have significant assignments based on readings from the primary literature, participate in classroom discussions regarding current research topics, complete periodic homework and laboratory/programming assignments, and periodic exams in addition to the final exam. Students are expected to prepare for any class assignments or quizzes over the material covered in class or in the reading.
material. Successful completion of these activities requires at a minimum six additional hours of outside of classroom work each week.

**CONTENT**

<table>
<thead>
<tr>
<th>Hours</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Introduction to Defensive Coding and Security</td>
</tr>
<tr>
<td>12</td>
<td>Misuse, Ignorance and Abuse of Coding</td>
</tr>
<tr>
<td>9</td>
<td>Coding</td>
</tr>
<tr>
<td>9</td>
<td>Cryptography</td>
</tr>
<tr>
<td>6</td>
<td>Miscellaneous Threats</td>
</tr>
<tr>
<td>6</td>
<td>Exams (plus final)</td>
</tr>
<tr>
<td>45</td>
<td>TOTAL</td>
</tr>
</tbody>
</table>

**REFERENCES**

