Basic Course Information CS 5500

Course Title: Advanced Information Security

Units: 3

C/S Classification #: C-2

Component (select one): Lecture

Instructional Mode (select all appropriate choices): Face-to-Face and web-assisted

Grading Basis (select one): Graded only

Repeat Basis (select one): May be taken only once

Cross listed Course (if offered with another department):

Dual-listed Course (if offered as lower/upper division or undergraduate/graduate):

Major course/Service course/GE course (select all appropriate choices): Major course

Prepared by: Mohammad Husain

I Catalog Description

Advanced information security issues in wireless networks, web applications, databases, and cloud computing.

II Required Coursework and Background

Pre-requisite(s): CS 3800 or consent of instructor

III Expected Outcomes

On successful completion of this course, students will be able to:

1. Comprehend major security challenges in existing and emerging technology
2. Master techniques that scientists use to protect a system from security attacks including their advantages and disadvantages
3. Analyze, identify and address security issues in wireless networks
4. Write secure applications for mobile and web
5. Secure databases from unauthorized access and manipulation
6. Design secure applications for computation and storage in the cloud and virtual environment
7. Learn how to evaluate and present existing security literature
8. Learn how to formulate and solve a systems security research problem

Outcomes of this course will build student capacity in each of the following areas as defined by programmatic objectives for the computer science major.

P-SLO 3. An ability to build applications, either individually or in a team, that are robust, reliable, and maintainable.

P-SLO 4. A breadth of advanced knowledge and skills in applied areas of computer science.

IV Instructional Materials

Texts may vary with instructor and over time. Examples of possible texts include:

Computer Security, Dieter Gollmann, 3rd Edition, 2011, John Wiley & Sons

V Minimum Student Material

Course textbooks

VI Minimum College Facilities

Computer laboratories with Linux operating systems, library, Blackboard, classroom with a projection system

VII Course Outline

* Review of information security basics: confidentiality, integrity, authentication and access control
* Review of basic wireless networking concepts
* Eavesdropping and denial-of-service attacks and mitigation techniques
* Review of mobile and web applications design
* Remote code execution and cross site scripting attacks, and mitigation techniques
* Review of web application interaction with databases
* SQL injection attack and mitigation techniques
* Review of computation and storage techniques on the cloud and virtual environment
* Unauthorized access and manipulation of computation and storage attacks, and mitigation techniques

VIII Instructional Methods

Lecture

Problem-solving

Discussion

Project-based learning

Team presentation

IX Evaluation of Outcomes

A Student Assessment

i homework assignments and projects

ii mid-term

iii final

iv quizzes

v presentation and report

B. Meaningful Writing Assignment

Short answer essay questions on exams and reports will require students to explain and justify their response in writing.

C. A Matrix of Course Student Learning Outcomes vs Methods of Assessment

If the course is being evaluated for accreditation purposes, approved department accreditation assessment tools will additionally be utilized.

|  |  |  |  |
| --- | --- | --- | --- |
| Course Learning Outcomes | Methods of Assessment | | |
| Assignments/  Projects | Quiz/  Exam | Presentation/  Report |
| 1 Comprehend major security challenges in existing and emerging technology | x | x |  |
| 2 Master techniques that scientists use to protect a system from security attacks including their advantages and disadvantages | x | x |  |
| 3 Analyze, identify and address security issues in wireless networks | x | x |  |
| 4 Write secure applications for mobile and web | x | x |  |
| 5 Secure databases from unauthorized access and manipulation | x | x |  |
| 6 Design secure applications for computation and storage in the cloud and virtual environment | x | x |  |
| 7 Learn how to evaluate and present existing security literature |  |  | X |
| 8 Learn how to formulate and solve a systems security research problem |  |  | X |