CSC 512 – WEB SECURITY

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

CATALOG DESCRIPTION

Fundamental coverage of issues and techniques in developing secure web-based applications; related topics such as network security, web server security, application-level security, and web database security.

PURPOSE OF COURSE

Study and practice of fundamental techniques in developing secure web based applications, including vulnerability of web based applications. Learn and apply principles of cyber security to protect applications from attacks. Address advanced cyber security topics such as web attacks and defense, e-commerce security, and collaborative web-based applications. Complete a research paper on an instructor-approved topic.

EDUCATIONAL OBJECTIVES

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

1. Demonstrate an understanding of security-related issues in Web-based systems and applications.
2. Demonstrate an understanding of the fundamental security components of a computer system.
3. Be able to evaluate a Web-based system with respect to its security requirements.
4. Demonstrate an understanding of the process of developing secure networked systems.
5. Demonstrate an understanding of the fundamental mechanisms of securing a Web-based system.
6. Be able to implement security mechanisms to secure a Web-based application.
7. Be able to evaluate security issues and common controls in electronic commerce systems

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 **Hours**

Introduction to Web-based security 6
- Overview of ISO and N-tier web models
- Typical components and mechanisms
- HTTP vs. HTTPS security

Proxy Servers, Firewalls, NAT 9
- Use of proxy servers for security
- Effectively using Firewalls
- Address translations

Internet Security Protocols 12
- ISO security vs. TCP/IP
- SSL
- Man in the middle attacks

Database Security 6
- Oracle and SQL
- Coding security into applications

Electronic Payment Systems and coding 6
- Signing and certificates
- Client and server side security
- Risk Management

Exams (plus final) 6

TOTAL 45

REFERENCES

Oppliger, Security Technologies for the World Wide Web, 2nd Ed. Artech, 2002

Leblanc and Messerschmid, Identity and Data Security for Web Development: Best Practices O'Reilly, 2016

Stuttard and Pinto , The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws Wiley, 2011

RELATED DOCUMENTS

- Man in the middle attack
- VeriSign Technical Brief. "Building an E-Commerce Trust Infrastructure: *SSL Server Certificates* and Online Payment Services"
- www.cybercrime.gov: Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division of the US Dept. of Justice
- https://www.justice.gov/criminal-ccipscc.html
- The archived World Wide Web Security FAQ: http://www.w3.org/Security/faq/
- Cryptography FAQ Index: http://www.faqs.org/faqs/cryptography-faq/
- Cryptography.org: http://www.cryptography.org/
- The Open SSL Project (SDKs for free download): http://www.openssl.org/
- Discussion about Windows Security: http://www.windowsitpro.com/categories/category/security