TOWSON UNIVERSITY

COSC 647 Application Software Security

Instructor: **Nam Nguyen**
Email: npnguyen@towson.edu
Office: York 7800, Room 445
Class time: Tue 7 – 9:40pm. Room 405.
Office hours: Mon, Tues, Wed 10 – 12:00pm (or by appointment)
Final Exam: Wed, Dec 16th 2014, 7:30 – 9:30pm YR 405.

===

Course website

Course materials are available online on BlackBoard @ bbweb.towson.edu.

Prerequisites

Database Systems, Advanced Data Structures and Algorithms Analysis.

Course description

A study of security concepts in developing software applications. This course discusses design principles for secure software development, and some of the security issues in current programming languages, database systems and web applications.

Course objectives

Upon completion of this course students should be able to:

- Understand principles of application software security.
- Understand the basic concepts of threats modeling and risk analysis.
- Understand the most critical and prevalent web application security risks and vulnerabilities.
- Understand and demonstrate the use of software security application techniques and tools used to discover compromised systems, and develop secure systems.

Topics

1. Application Software Security Principles
2. Threat modeling
3. Buffer overflow
4. Heap overflow
5. Integer overflow
6. Format string vulnerability
7. Authentication & access control
8. SQL injection
9. Cross site scripting
10. Cross site request forgery
11. Penetration testing

References

1. Jon Erickson. Hacking: The Art of Exploitation, 2nd Edition. 2008
2. Matt Bishop. Computer Security: Art and Science. 2003
3. Matt Bishop. Introduction to Computer Security. 2005
4. Micheal Howard, David LeBlanc, and John Viega. 19 Deadly Sins of Software Security. 2009
5. John Viega and Gary McGraw. Building Secure Software. 2002
6. Micheal Howard and David LeBlanc. Writing Secure Code. 2003
7. Gary McGraw. Software Security: Building Security In. 2006
8. Robert C. Seacord. Secure Coding in C and C++. 2005
9. Greg Hoglund and Gary McGraw. Exploiting Software: How to break code. 2004
10. James A. Wittaker and Herbert H. Thompson. How to Break Software Security. 2004
11. www.owasp.org
12. SOAR Software Security Assurance
13. www.cert.org
14. www.sans.org
15. www.securityfocus.com

16. www.phrack.org
17. slashdot.org

Additional readings and materials will be provided by the instructor.

Term project

The goal of this project is to further explore and learn about a related topic to application software security. Each project should have research, implementation, and evaluation components. However, each of these components can vary based on the specific chosen topic. The project final report will be an 8-10 page paper in the ACM SIG conference publications format. This paper should include an abstract, introduction, description of the major components of your system, screen shots, and other information necessary to summarize what you've done, and how you've done it. These will also be conference style presentations with slides, demos, and other materials designed to convey your points to others during the last week of class.

Literature review

Article from ACM & IEEE journals relevant to the topics covered in this course are assigned weekly. You are expected to write a one-page review and to be prepared to discuss the article in class.

Projects

There will be several individual and team projects related to software security.

Exams

Midterm and Final exams.

Academic Integrity

Cheating and plagiarism of any kind are unacceptable. Do not turn in work that has been copied from somebody else, even from the Internet. Do not let your work to be copied. Anyone found cheating will receive a grade of F of the course. A statement of cheating and plagiarism may be found in the Undergraduate Catalog, Apendix F.

Class attendance

Class attendance is expected. If you miss a class, you are responsible for the material presented in lectures and for obtaining information about assignments and handouts from classes you miss.

Grading Policy

- Literature review:	5% (5 assigned papers)
- Quizzes:	5% (5 quizzes)
- Assignments:	20% (4 homework)
- Term project & Presentation:	20% (Report 1: 3%, Report 2: 7%, Final report 10%)
- Midterm exam:	20%
- Final Exam:	30%
- Bonus:	20pts (equals 5% extra)

Grade Letters

A [93, 100], **A-** [90, 93)

B+ [87, 90), **B** [83, 87), **B-** [80, 83)

C+ [77, 80), **C** [74, 77), **C-** [70, 74)

D+ [67, 70), **D** [63, 67), **D-** [60, 63)

F [0, 60).

Makeup Policy

If a student must miss an exam it is the student's responsibility to provide sufficient documentation of the reason for the absence. Otherwise, a grade of zero will be assigned.

University Policy

- Students may appeal any charges of cheating or plagiarism
- Students may not repeat a course more than once without prior permission of the Academics Standards Committee.

Disability Accommodation

If you may need an accommodation due to a disability please contact me privately to discuss your specific needs. A memo from Disability Support Services (DSS) authorizing your accommodation will be needed.

Class policy

- It is expected that students will make every attempt to arrive to class on time.
- Cell phones are to be turned OFF during class.
- Food and drinks are prohibited from lab rooms.