Cosc 647
Application Software Security
Class Policies

Mike O'Leary
Office: 316K Stephens Hall
Office Phone: 410-704-4747
Email: moleary@towson.edu
Office Hours: MWF 2:00 – 3:00

Fall 2006
MW: 4:00-5:15 p.m., YR 405
Section: 101

Prerequisites: COSC 578, COSC 600.

Catalog 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 and scripting languages, database systems and web servers.

Learning Objectives:

1. To understand buffer overflows, including stack-based overflows and heap-based overflows.
2. To understand format string vulnerabilities.
3. To understand race conditions, especially in the file system.
4. To understand remote code injection vulnerabilities.
5. To understand SQL injection attacks.
6. To understand cross site scripting attacks.

Academic Integrity: The nature of graduate studies requires that students adhere to accepted standards of academic integrity. Violations of academic integrity include cheating, plagiarism, falsification and fabrication, complicity in academic dishonesty, personal misrepresentation and proxy, bribes, favors and threats. Cheating is a serious offense that will have grave consequences for your academic life.

Students who violate these standards will either fail the course outright or, at the instructor's discretion, may merely receive a zero on any assignment for which the student receives inappropriate assistance. Particularly serious violations of these standards will be referred to the administration for possible additional action.

Instructional Material: The primary required texts are

- *Secure Coding in C and C++*, R.C. Seacord, Addison Wesley, 2006
- *Pro PHP Security*, C. Snyder & M. Southwell, APress, 2005.

Strongly recommended books include

- *Building Secure Software* by J. Viega and G. McGraw
- *Writing Secure Code*, M. Howard and D. LeBlanc, Microsoft Press, 2003.
- *Secure Programming for Linux and Unix HOWTO,* D. Wheeler. Online: http://www.dwheeler.com/secure-programs/
- Professional Assembly Language, R. Blum, Wrox, 2005.

There are a number of other books that would be very useful, including

- *Hacking, Jon Erickson,* No Starch Press, 2003.
- *Buffer Overflow Attacks, James Foster et.al.,* Syngress, 2005.
- *Sockets, Shellcode, Porting & Coding, James Foster et.al.,* Syngress, 2005.
- *The Shellcoder's Handbook*, Jack Koziol et.al., Wiley, 2004.
- *Exploiting Software. How to Break Code*, Greah Hoglund & Gary McGraw, Addison-Wesley 2004.
- *Hacker Disassembly Uncovered*, Kris Kaspersky, A-List, 2003.
- *The .NET Developers Guide to Windows Security*, Keith Brown, Addison-Wesley 2005.

Attendance: Attendance is expected; you should only miss a class for a compelling reason. If you do miss a class, you are responsible for any material that you miss, including any homework assignments given in that class. Unexcused absences can result in a lower grade.

Evaluation: Regular assignments will be given in class; these will include readings, exercises, analyses, and complete programs. Together, these problems will be worth 70% of the final grade. The remainder of the course grade will be determined by the final exam.

Final Exam: The Final Exam is scheduled for **Wednesday, December 13, from 5:15-7:15 pm.** The final exam will not be rescheduled. Attendance is expected; a make-up exam will not be given without an extremely compelling reason. The final exam shall be comprehensive.

Withdraw: The last day to withdraw from the course with a grade of "W" is November 8.

Help: If you have difficulty completing a homework assignment, do not hesitate to ask for help, either from your friends, or from me. You are welcome to stop by my office, for whatever reason, and at whatever time, even if there are no office hours scheduled then. If you wish, you may also simply send an e-mail message.