Course Name: INFSCI 2935 Developing Secure Systems
Special Topic: System & Technology-System Design
(Soon to be a regular IS course)

Class time: Mondays; 6:00 - 8:50PM;
Room: IS 502

Instructor: James B D Joshi
jjoshi@mail.sis.pitt.edu
Room 706 A
412-624-9982

Course URL: http://www.sis.pitt.edu/~jjoshi/Devsec/

Development of this course has been supported by a grant from the National Science Foundation

Course Description

Development of high-assurance software systems is a growing challenge in emerging complex systems. *Secure by design* is emerging as a basic principle for trustworthy computing and as a preferred way to ensure the security of networked information systems and infrastructures. This course will focus on this issue and fosters the design and implementation of secure software systems and architectures. A key coverage will include principles and practices of secure and high assurance software development process, including security development lifecycle models, and secure design using Unified Modeling Language, etc. Secure design of operating systems and network services, databases and application environments will be studied, including security in web services, COTS-based and service oriented systems. Tools and techniques for code analysis and testing, and evaluation and certification of software will be emphasized. The course will also cover secure programming principles using different languages, with particular focus in secure software development using Java and .NET platforms. This is one of the SAIS elective courses.

Pre-requisite:

- IS 2150/TEL 2810 Introduction to Computer Security
- Following courses are preferred but not required:
    - IS 2170/TEL 2820 Cryptography; TEL 2821 Network Security
    - IS 2511 or 25 40
    - Talk to the instructor if you are not sure of the background

Course references

As the topic is new, there exists no single book that provides all the material required for this course. Several books will be used as reference material, supplemented by published articles to make sure the coverage is current. Following books are good source of materials to be covered.

- *Building Secure Software: How to avoid the Security Problems the Right Way, John Viega, Gary McGraw, Addison-Wesley, 2002*
- *Enterprise Java Security: Building Secure J2EE Applications* – Marco Pistoia, Nataraj Nagaratnam, Larry Koved, Anthony Nadalin, Addition-Wesley, 2004
- *Secure Systems Development with UML* – Jan Jurjens, Springer-Verlag, 2005.
- *Securing Web Services with WS-Security: Demystifying WS-Security, WS-Policy, SAML, XML Signature, and XML Encryption* – Jothy Rosenberg, David Remy, 2004, Sams Publishing, 2004.
- *High Assurance Design: Architecting Secure and Reliable Enterprise Applications* – Clifford J. Berg, Addison-Wesley, 2006.
- *Core Security Patterns: Best Practices and Strategies for J2EE, Web Services, and Identity Management*; Christopher Steel, Ramesh Nagappan, Ray Lai; Prentice-Hall
- *How to Break Software Security* - James Whittaker, Herbert Thompson, Addition Wesley, 2003.
- Secure Coding in C and C++, Robert C. Seacord, Addition-wesley, 2006
- *Computer Security: Art and Science by Matt Bishop* (ISBN: 0-201-44099-7), Addison-wesley 2003.
- Papers; MSDN, US-CERT etc.

Grading (Tentative)

Homework/Quiz/:	40%
Presentation/Review	10%
Exams	20%
Project	30%

Course Policy

- Your work MUST be your own
- Zero tolerance for cheating/plagiarism
- You get an F for the course if you cheat in anything however small – NO DISCUSSION
- Discussing the problem is encouraged
- Homework
    - Penalty for late assignments (15% each day)
    - Ensure clarity in your answers – no credit will be given for vague answers
    - Homework is primarily the GSA's responsibility
- Check webpage for everything!
    - You are responsible for checking the webpage for updates