ITIS 6210/8210 - Access Control and Security Architecture

UNC CHARLOTTE
DEPARTMENT OF SOFTWARE AND INFORMATION SYSTEMS

TUE 6:00 PM - 8:45 PM Atkins 143
Professor Mohamed Shehab
Woodward Hall Room 333F
Course office hours WED 1:00-3:00 PM or by appointment; e-mail all times
E-mail: mshehab (at) uncc (dot) edu (please prefix the subject of your message with ITIS6210)

DESCRIPTION:
ITIS 6210/8210 is a 3-credit course. This course discusses objectives, formal models, and mechanisms for access control, access control on commercial off-the-shelf (COTS) systems, and security architecture for authorization. Topics also include current topics of advanced research in access control. Content varies depending on faculty interests, research developments, and student demand. The course provides the students with hands-on experience in secure system development through a project.

PREREQUISITES:
The official requirement is ITIS 6200 Principles of Information Security and Privacy, and by extension the material required as a prerequisite to IT IS 6200. If you do not have this background you are required to file a “SPECIAL REQUEST” form and get the department approval.

TOPICS:
1. Security Concepts and Principles
2. Access Control Basics
   a. Access Control Matrix
   b. Access Control List
3. Access Control Models
   a. Mandatory Access Control
      i. Chinese Wall Policy
      ii. Biba Model
      iii. Bell-LaPadula Model
      iv. Lattice-based Access Control
   b. Discretionary Access Control
   c. Role Based Access Control
   d. Location Based Access Control
   e. Temporal Based Access Control
4. Delegation Models
5. Policy Specification and Management
   a. SAML
   b. XACML
   c. XML Security
6. Network Firewall Access Control
7. Security Architectures
   a. Trust negotiations and management
   b. Identity Management
   c. Web Services Security

SCHEDULE:
• First Day of Class  8/24/2010.
• Proposal due  9/21/2010.
• Class Presentation Sessions  11/30/2010-12/7/2010.
• Final Exam  12/14/2010.
• Final Report due  12/14/2010.

GRADING POLICY:
Grades are based on research paper critiques (25%), a term project 50% (class presentation and project demo 20% and final report 30%) and a final exam (25%).

TERM PROJECT:
Each project topic should be chosen in mutual agreement with Professor Shehab. Class presentation will be 25 minutes presentation to the whole class and MUST demonstrate the concepts of security topic clearly including some research reasoning. Using 10-pt font, double column text, the final report should be at least 15 pages (double column) including the bibliography. Students should submit a brief proposal (2-3 pages, 10pt, single space) of term project by due date or earlier in class. Student must take initiative to make sure this happens in timely manner. The term paper should contain the following sections:
   • Objectives
   • Project Description
   • Background and related works
   • Your approach and architecture
   • Results or Implementation
   • Discussion and Conclusion
   • Future Work
   • References.

RECOMMENDED TEXTBOOKS:
• Computer Security: Art and Science by Matt Bishop, Addison-Wesley
• Role-based Access Control by David Ferriolo et al., ARTECH
• Security in Computing by Pfleeger, Prentice Hall
• Information Security by Marshall Abrams et al., IEEE
• Fundamental of Computer Security Technology by Edward Amoroso, Prentice Hall
• Secure Electronic Commerce by Warwick Ford, Michael S. Baum, Prentice Hall