CIS 6370 COMPUTER DATA SECURITY

President Obama has declared computer network warfare to be one of the highest priorities in national defense. Cyberwarfare is now the fastest growing area of government and military spending.

The Air Force new military command for computer network offense and defense, based in San Antonio, TX, will hire 5500 to 7000 employees, including civilians and contractors.

The US Department of Homeland Security has announced that it plans to hire up to 1,000 cyber security experts over the next three years.

Both intelligence and law enforcement agencies have uncovered evidence of penetrations of government and commercial organizations resulting in loss of highly sensitive national defense and business information. The result is a massive shift in demand for security people away from those who can write reports to those who can find the flaws, see the attacks, and secure the networks.

Security is a fundamental issue in current systems and there is a strong demand for software engineers who can develop secure software and maintain secure systems. This course exposes the required concepts and points the directions for further specialization. We use security patterns and UML models to describe designs. The course is updated yearly to reflect the latest advances in this topic. Its orientation is strongly practical with emphasis on systems development and maintenance. It is appropriate for undergrad students who know some UML.

This course will be taught by Dr. Ed Fernandez. He developed the course, is the author of three books on security and a world-recognized expert on software systems and software security. Among other assignments, he spent two weeks in July 2008 and a week in March of 2009 in Tokyo by invitation of the Japanese Government to work on software security. He also spent a week in June 2009 in Israel to work on database security. He has taught short courses on security in Argentina, Chile, Paraguay, China, Japan, Mexico, Austria, and other places. His biography can be found in: http://www.cse.fau.edu/~ed

Catalog description: Prerequisite: general background on operating systems, architecture, and languages, as well as basic knowledge of object-oriented design. Overview of technical aspects of data and network security with emphasis on the Internet. Emphasis on design as opposed to just description or use of systems.

Textbooks: E.B.Fernandez, E.Gudes, and M. Olivier, *The Design of Secure Systems*, under contract with Addison-Wesley. Draft version available as Blackboard notes. .

Instructor: Dr. Eduardo B. Fernandez, Professor of Computer Science and Eng.

E-mail: ed@cse.fau.edu
Web page: http://www.cse.fau.edu/~ed
Telephone: 561-297-3466 **Fax:** 561-297-2800

Goals: Security problems in the combination of the Internet with Intranets. Need to protect all architectural levels. Understanding of how to coordinate hardware and software to provide data and network protection against internal and external attacks. Modeling of the systems involved through the use of UML object-oriented patterns and formal models.

Prerequisite by topic: General concepts of operating systems, computer systems architecture, and languages. Some knowledge of object-oriented concepts, in particular UML modeling.

Outline :
1. Introduction: motivation, definitions, attacks, defenses. UML as a security language.
2. Security Policies and Models: Institution and system policies. Security models: Access Matrix, Role-Based Access Control, Multilevel. Patterns for models.
3. Cryptography. Classical ciphers. Symmetric ciphers (DES and its variants, AES), Asymmetric encryption (Public key systems, Digital signatures and hashing functions)
4. Security in Hardware and Operating systems: System architecture, Process and resource protection (modes, rings). Memory protection, File protection. Virtualization.
5. Program and application security: Malicious software: Trojan horses, Viruses, and worms, the buffer overflow problem. Security in languages and components.
6. Security in database systems: . Basic architecture and concepts of database management systems (DBMSs), security in Relational and SQL-based databases.
7. Network Security: Network attacks. Firewalls. Secure layers. Secure applications. Intrusion detection (IDS). Wireless systems.
8. Internet and distributed system security: Web security. Web Application Servers and their protection. Web services security. Cloud computing security.
9. Developing secure software: The development of secure systems: traditional and modern approaches. The software engineering cycle. Formal and semiformal design methods. Formal verification and proving correctness. Evaluating security

Grading: 30% assignments (3 or 4), 70% project (selected from a set of topics or your own proposal).