CIS 6370 DATA AND INTERNET SECURITY

Credits: 3 credits


Reference materials: Notes on patterns (E. Fernandez), Selected papers

Specific course information

Catalog description: Overview of technical aspects of data security with emphasis on the Internet and the design of secure systems. 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. Emphasis on a holistic approach to security, as opposed to details of security mechanisms. The course is updated yearly to reflect the latest advances in this topic. Its orientation is strongly practical with emphasis on systems design and evaluation.

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

Specific goals for the course: Understanding of the security problems that arise in the combination of the Internet with Intranets. Need to protect all architectural levels to achieve security. Understanding of how to coordinate hardware and software to provide data security against internal and external attacks. Modeling of the systems involved through the use of object-oriented patterns. Understanding of the security problems introduced in the combination of the Internet with Intranets.

Understanding of how all aspects of a computer system contribute to security.

Providing a perspective on how a variety of mechanisms should work together to defend a system

Developing ability to evaluate and compare diverse systems or mechanisms with respect to their security.

Basic understanding of the theoretical and conceptual aspects that are needed to build secure systems

Proficiency in reading UML models

Brief list of topics to be covered:


Patterns for models.

3. **Cryptography**: Symmetric ciphers, DES and AES. Public key systems, digital signatures, hashing, steganography.


