CIS 6370 Computer Data Security

Credits: 3 credits

Text book, title, author, and year: E. B. Fernandez, class notes (provided in Canvas)

Reference materials: 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:

1. **Introduction**: Motivation and definitions. Internet and Intranet-- Structure, growth, possibilities. Environment for security. Related subjects. The Internet and its threats. Vulnerabilities and threats: Viruses, worms, denial of service, attackers.
2. **Security policies and models**: Institution, legislation, and privacy policies. Compliance. Forensic policies. Access matrix, multilevel, mandatory, discretionary models. Role-Based Access Control. Patterns for models.
3. **Cryptography** : Symmetric ciphers, DES and AES. Public key systems, digital signatures, hashing, steganography.
4. **Security in hardware and operating systems**: Effect of hardware on security. Process and memory protection. Virtualization. Vulnerabilities. Unix, Linux,Windows. Hardened operating systems. Authentication.
5. **Program and Application security** : Malicious software. Language problems, buffer overflow, remote execution, Java security. Application/content firewalls. Components.
6. **Database security**: Using views for authorization in relational databases. Authorization systems in Oracle and similar systems. SQL injection and other attacks.NoSQL databases. Data intensive systems security.
7. **Network Security**: Attacks. Secure layers. SSL/TLS, Kerberos, VPNs, Firewalls. Intrusion Detection. Wireless systems
8. **Distributed systems**: Web security, Cross-script attacks. Security in Web Services and in cloud computing.
9. **Developing secure software and systems**: Secure system design methodology. Use of patterns. Formal methods, model checking. Code-based secure lifecycles. Evaluation of security.