CNT 4403 Introduction to Data and Network Security

Credits: 3

Text book, title, author, and year: E.B.Fernandez, Ehud Gudes, Martin Olivier, "The design of secure systems", to appear W. Stallings and L. Brown, Computer Security: Principles and practice (2nd Ed.), Pearson 2012.

a. **Supplemental materials:** none.

Specific course information

- **Catalog description:** Overview of technical aspects of data security with emphasis on the Internet. Attacks and defenses. The design of secure systems.
- **Prerequisites:** COP 4610
- **Required, elective, or selected elective:** elective

Specific goals for the course

Specific outcomes of instruction: By the end of the course students will be able to: *(i) Understand the security problems introduced by the combination of the Internet with Intranets, mobile devices, and sensors. ii) Understand how all aspects of a computer system contribute to security. iii) Obtain a perspective on how a variety of mechanisms should work together to defend a system iv) Develop ability to evaluate and compare diverse systems or mechanisms with respect to their security. v) Develop a basic understanding of the theoretical and conceptual aspects that are needed to build secure systems; vi) Learn a basic use of patterns and UML to describe complex systems*

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, Java security. Application/content firewalls. Components. Security in .NET and Sun ONE.
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.