CSCE 522 - Information Security Principles

- **Credit Hours:** 3 hours
- **Contact Hours:** 3 lecture hours
- **Instructor:** Dr. Csilla Farkas
- **Required Textbooks:** Charles P. Pfleeger and Shari Lawrence Pfleeger, Security in Computing (5th Edition) (Hardcover), Prentice Hall, 2015.
- **Bulletin Description:** Threats to information resources and appropriate countermeasures. Cryptography, identification and authentication, access control models and mechanisms, multilevel database security, steganography, Internet security, and intrusion detection and prevention.
- **Prerequisites:** CSCE 146; MATH 374 or MATH 174
- **Required Course** in CIS and Selected Elective in CE,CS
- **Course Outcomes:** Students will be able to:
  1. Identify common risks, threats, and countermeasures related to computing systems.
  2. Apply knowledge of computer security to personal computer use.
  3. Analyze computing situations with respect to security risks, threats, and countermeasures, including the tradeoffs between security and system functionality.
  4. Work with others to design and/or implement security measures.

- **Student Outcomes addressed by course**

Program	Student Outcomes Addressed
Computer Engineering	N/A
Computer Information Systems	1, 2, 6
Computer Science	1, 2

- **Topics covered**
  1. Basic security concepts
  2. Cryptography, Secret Key
  3. Cryptography, Public Key
  4. Identification and Authentication, key-distribution centers, Kerberos
  5. Security Policies -- Discretionary Access Control, Mandatory Access Control
  6. Access control -- Role-Based, Provisional, and Logic-Based Access Control
  7. The Inference Problem
  8. Program Security -- Viruses, Worms, etc.
  9. Network and Internet Security, E-mail security, User Safety
  10. Firewalls
  11. Intrusion Detection, Fault tolerance and recovery
  12. Information Warfare
  13. Security Administration, Economic impact of cyber attack