COURSE DESCRIPTION

Dept., Number	**CS 4351** **Selected Elective**	Course Title	Computer Security
Semester hours	45 hours	Course Coordinator	Luc Longpré

Current Catalog Description

General concepts and applied methods of computer security, especially as they relate to confidentiality, integrity, and availability of information assets. Topics include system security analysis; access control and security models; identification and authentication; protection against external and internal threats; communication protocols; Internet security.

Textbook:

Gollmann, D. (2011), *Computer Security*, 3rd edition.

Course Outcomes:

Level 3: Synthesis and Evaluation:

Level 3 outcomes are those in which the student can apply the material in new situations. This is the highest level of mastery.

On successful completion of this course, students will be able to:

1. Appraise a given code fragment for vulnerabilities.
2. Assess risk for a given network system using publicly available tools and techniques.
3. Appraise a given protocol for security flaws.

Level 2: Application and Analysis:

Level 2 outcomes are those in which the student can apply the material in familiar situations, e.g., can work a problem of familiar structure with minor changes in the details. Upon successful completion of this course, students will be able to:

1. Set up file protections in a Unix or Windows file system to achieve a given purpose.
2. Understand security evaluation toolsets and their purpose and usage.
3. Describe different encryption techniques and their applications.
4. Explain the various controls available for protection against Internet attacks, including authentication, integrity check, firewalls, intrusion detection systems.
5. Understand security evaluation toolsets and their purpose and usage.

Level 1: Knowledge and Comprehension

Level 1 outcomes are those in which the student has been exposed to the terms and concepts at a basic level and can supply basic definitions. On successful completion of this course, students will be able to:

1. Identify potential security issues and solutions for state-of-the-art and future technologies.

2. Describe legal, privacy and ethical issues in computer security.
3. Enumerate programming techniques that enhance security.
4. Describe the functioning of various types of malicious code, such as viruses, worms, trapdoors.
5. Explain the various controls available for protection against Internet attacks, including authentication, integrity check, firewalls, and intrusion detection systems.
6. Describe the different ways of providing authentication of a user or program.
7. Describe the mechanisms used to provide security in programs, operating systems, databases and networks.
8. Describe the background, history and properties of widely used encryption algorithms.
9. List and explain the typical set of tasks required of a security analyst.

Student Outcomes:

Not applicable

Prerequisites by Topic:

CS 3331 with a grade of "C" or better.