Information Security Engineering Courses (Core Breadth)

IS201 Introduction to Information Security Engineering				
Credit Hours:	3-0-3	**Prerequisites**	Nil	
Course Learning Outcomes:				
S No	**CLO**	**Domain**	**Taxonomy Level**	**PLO**
1	Understand the basic concepts of information security engineering and role of risk assessment methodologies	Cognitive	2	1
2	Apply the basic principles of confidentiality, integrity, availability, authentication and access control in designing and analyzing secure systems	Cognitive	3	3
3	Understand the concepts of secure systems evaluation and assurance and impact of standards / best practices on this process	Cognitive	2	2

Course Content:

Introduction to the principles, applications, and practice of information security engineering. Role of computer as a general-purpose information processing tool, role of operating system, how sensors and actuators can be interfaced to a computer at the hardware and software level. Role of probability as the mathematical tool for modelling uncertainty in sensors and how to use Bayes rule/ conditional probability as means to combine sensor measurements. Understand data capture, its analysis and the related controlling system. How to discretize continuous controllers. The nature and basic concepts of information security - assets, risks, threats, vulnerabilities, security measures. Different security and risk assessment methodologies, solving the security task. Usability and Psychology, Attacks Based on Psychology, Passwords and associated system issues, Security protocols, Access control, Authentication and authorization. Multilateral Security, Physical protection, Monitoring and metering, Security printing and seals. Biometrics and Physical tamper resistance, Emission Security, Electronic and Information warfare, Copyright and DRM, System evaluation and assurance. Secure programming, network security. Web Application Security, OWASP. Cyber hygiene. Ethical and legal aspects of security, protection of personal data. Distributed Systems Security

Teaching Methodology:

Lectures, Written Assignments, Semester Project, Presentations

Course Assessment:

Midterm Exam, Home Assignments, Quizzes, Project, Presentations, Final Exam

Reference Materials:

1. Ross Anderson. Security engineering: A guide to building dependable distributed Systems, 2nd Edition, 2010
2. Nancy R. Mead and Carol Woody. Cyber Security Engineering: A Practical Approach for Systems and Software Assurance. 1st Edition, 2016
3. Edward Griffor. Handbook of System Safety and Security. Elsevier, 2016
4. Micki Krause Nozaki, and Harold F. Tipton. Information Security Management Handbook, 6th Edition, CRC Press, 2016

(In addition, there will be lecture notes and selected articles).