IS372 Malicious Software and Hardware			
Credit Hours:	2-1-3	**Prerequisites**	IS201

Course Learning Outcomes:

S No	**CLO**	**Domain**	**Taxonomy Level**	**PLO**
1.	Comprehend methodology, technology and application of malware software and hardware analysis techniques	Cognitive	2	1
2.	Analyze contemporary practices of malware and malicious hardware analysis	Cognitive	4	2
3.	Apply the gained knowledge in assessing prevention techniques	Cognitive	3	3
4.	Experiment with malicious techniques and their countermeasures for reinforced learning	Psychomotor	3	5

Course Content:

Various types of malicious software (malware) and hardware's. Malware analysis using virtual machines, sandboxes, process monitors, packet sniffers, de-obfuscation, etc. Reverse Engineering Malware (REM) Methodology, Brief Overview of Malware analysis lab setup and configuration, Introduction to key MA tools and techniques, Behavioral Analysis vs. Code Analysis, Resources for Reverse-Engineering Malware (REM). Introduces hardware Trojans and other forms of malicious hardware. Discusses prevention techniques at the design, fabrication, and post-fabrication level. Introduces various countermeasures against malicious software and hardware

Teaching Methodology:

Lectures, Written Assignments, Semester Project, Presentations

Course Assessment:

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

Reference Materials:

1. Practical Malware Analysis, The hands on Guide to Dissecting Malicious Software by Michael Sikorski and Andrew Honig. 2012
2. Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code, First Edition (2010): Michael Ligh, Steven Adair, Blake Hartstein, and Matthew

Richard.

In addition there will be lecture notes and selected articles.