Department of Electrical and Computer Engineering

EEE 4XXX – Reverse Engineering Malware

Catalog Description

This course will show the students to how to dissect and assess malware threats by performing reverse engineering utilizing practical tools and techniques including variety of system and network monitoring utilities, disassembler, debugger, and other tools. The student will understand how malware operates and determines the type of damage it can perform.

Catalog Objectives

- To give the students an understanding of what Malware is.
- To examine malicious programs include spyware, bots, Trojans, etc.
- To analyze malware by extracting malware's signatures and host-based indicators.
- To reverse engineer web-based malware including JavaScript and Flash files.
- To provide exposure to well-known and novel forensic methods using command-line and graphical open-source analysis tools for examining a wide range of malwares.

Prerequisites

- Knowledge of windows operating system
- EEE-4XXX (Introduction to Digital Forensics Engineering)

Textbooks

- Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software by Michael Sikorski and Andrew Honig (Feb 29, 2012)
- The Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System by Bill Blunden (Mar 16, 2012)

Topics covered

- Ethical Issues
- Classification of Malware
- Dynamic Malware Analysis
- Rootkit detection and analysis
- Attack Cycle
- Covert Channels

Class schedule

Twice a week 75 minutes class with hands-on lab as part of the lectures

Contribution of course to meeting the professional component

Engineering science – 90% (math/science required for creative applications)
Engineering design – 10% (decision making process of devising a system, component or process to meet a desired need).

Relationship of course to program outcomes:

In the course EEE 4XXX – Mobile Device Forensics Engineering, the student will have to show

1. An ability to apply knowledge of mathematics, science, and engineering
2. An ability to design and conduct experiments, as well as to analyze and interpret data
3. An ability to identify, formulate, and solve engineering problems
4. An understanding of professional and ethical responsibility
5. Recognition of the need for, and an ability to engage in life-long learning
6. Knowledge of contemporary issues
7. An ability to use the techniques, skills and modern engineering tools necessary for engineering practice

Person who prepared this description and date of preparation:

Dr. Faisal Kaleem