Department of Electrical and Computer Engineering

EEE 4XXX – Windows Forensics

Catalog Description

This course will show the students to how to analyze different processes running on different versions of Windows operating systems using open-source tools. This course also provides a detailed understanding of the binary structure of Windows Registry and how to perform and live analysis of data contained in the Registry.

Catalog Objectives

- To give the students an understanding of different versions of Windows operating systems.
- To provide a thorough understanding of Windows Registry keeping in mind that Registry is an excellent source of both direct and indirect artifacts.
- To examine the data structures and activities behind different windows processes, and threads.
- To expose the Windows security model to see how it manages access, auditing, and authorization
- To analyze the Windows networking stack from top to bottom
- 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 windows registry forensics.

Prerequisites

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

Textbooks

- Windows Forensic Analysis Toolkit, Third Edition: Advanced Analysis Techniques for Windows 7 by Harlan A. Carvey (Feb 10, 2012)
- Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry by Harlan A. Carvey (Feb 7, 2011)

Topics covered

- Ethical Issues
- Classification of Windows Operating Systems
- Windows Registry Internals
- Analysis of different windows processes

- Windows Security Model
- Windows Networking Stack

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