EEL4804 - Introduction Malware Reverse Engineering

Three Credits, Two and a half hours, Engineering Topic.

Instructor: Dr. Asahi Tomitaka.

Textbook:

1.Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software by Michael Sikorski and Andrew Honig (Feb 2012), ISBN: 1593272901

2.The IDA Pro Book: The Unofficial Guide to the World's Most Popular Disassembler by Chris Eagle (Jul 2011), ISBN: 1593272898

Specific Course Information:

The objective of this course is to familiarize students with the practice of performing reverse engineering on suspicious files and firmware by utilizing static and dynamic techniques and procedures. The student will gain an understanding of how firmware is compromised and how to validate and restore its integrity. Analytical information such as environment changes (file, system, network, and process), communication with the rest of the network and the malware's impact on mobile devices will be closely observed and analyzed for actionable information.

This course will consist of 6 modules and 1 project. A project will be completed in groups and portions will be due throughout the semester. Upon completion of this course, students will have learned how to perform malware analysis and reverse engineering to determine malware behavior, propagation, persistency, and other characteristics associated with malware.

Specific Goals for the Course

a. Specific outcomes of instruction

Upon successful completion of this course, the student will:

1.Use Malware Analysis techniques and Reverse Engineering approaches.

2.Apply the latest tools and techniques to find, extract, and analyze malicious code from various types of hardware.

3.Analyze how malware interacts with any associated networks, identifying the type of information being targeted.

4.Describe the manner that malware propagates, becomes resident and executes.

5.Implement malware network signatures to detect and remove their presence.

6.Apply basic static and dynamic analysis for malware identification.

7.Apply advance static and dynamic malware analysis to determine run-time behavior.

8.Analyze malware the determine obfuscation techniques and identification.

b. Explicitly indicate which of the student outcomes listed in Criterion 3 or any other outcomes are addressed by the course.

In this course the student will have to show

(a) an ability to apply knowledge of mathematics, science, and engineering (N/A)

(b) an ability to design and conduct experiments (simulations), as well as to analyze, interpret data (N/A)

(c) an ability to design a system, component, or process to meet desired needs (N/A)

(d) an ability to function in multi-disciplinary teams (N/A)

(e) an ability to identify, formulate, and solve engineering problems (homework) (N/A)

(f) an understanding of professional and ethical responsibility (N/A)

(g) an ability to communicate effectively (through project reports) (N/A)

(h) the broad education necessary to understand the impact of engineering solutions in a global and societal context (N/A)

(i) a recognition of the need, and an ability to engage in life-long learning (N/A)

(j) a knowledge of contemporary issues (N/A)

(k) an ability to use the techniques, skills, and modern engineering tools necessary for engineering practice (N/A)

(l) a knowledge of probability and statistics (N/A)

Brief list of the topics to be covered

1.Malware Analysis and Reverse Engineering Basic Static Techniques

2.Malware Analysis in Virtual Machines Basic Dynamic Analysis

3.A Crash Course in x86 Disassembly IDA Pro

4.Recognizing C Code Construction Assembly Analyzing Malicious Windows Programs

5.Debugging OLLYDbg

6.Malware Behavior Covert Malware Launching

GRADING:

Course Requirements	Weight
Quizzes	6%
Assignments	30%
Midterm Exams	14%
Final Project	20%
Final Exam	30%
Overall Grade	100%

Conversion of Numerical Grade to Letter Grade

95<=A<=100	82<=B<85	70<=C<73
90<=A-<94	78<=B-<81	60<=D<69
86<=B+<89	74<=C+<77	F: Below 60