Special Topics I Syllabus Summer 2019

Tathagata Mukherjee

March 2019

Introduction to Malware Analysis

The goal of this course is to introduce the students to the basics of malware reverse engineering. Malware (called variously as spyware, virus, Trojan etc.) are nothing but computer programs which when loaded on to a computer causes the computer to behave in ways so as to compromise the safety and security of the user. Malwares are used for data theft, surveillance and a host of other malicious purposes. With the preponderance of hand held computers (like cell phones and tablets) in our lives, the threat of malware infections and and the consequences there of are ever more potent. Thus it behooves us to understand how malwares work. One of the major bottlenecks in this endeavor is the fact that the source code of malwares are generally not available. Thus security researchers are left with the task of understanding a malware using only the distributable file (the executable). The only way to tackle this is to use reverse engineering in order to get a peek into how the malware was designed and to learn how it works. Standard techniques of software reverse engineering though useful, needs to be used with extreme caution and care, more so because any mistake can have serious consequences. Moreover, malware writers almost always use advanced obfuscation techniques in order to thwart the efforts of the security researchers. Thus malware analysis involves a mix of advanced reverse engineering (usually called static analysis) and dynamic analysis. Any one of them alone may not be enough to reveal the inner workings of the malware. This course intends to expose the students to malware analysis using reverse engineering and dynamic analysis. After completing the course a student should be able to statically analyze a malware even if advanced obfuscation techniques are used. Further he/she should be able to setup a sandboxed environment for dynamic analysis and use the same to dynamically analyze the malware and draw conclusions about the purpose, nature and exploit used by the malware. The course will cover the following topics:

1. Introduction to the x86 assembly language
2. Introduction to Ghidra: The NSA Reversing framework
3. Introduction to malware static analysis

4. Introduction to malware dynamic analysis

5. Introduction to obfuscation

6. Introduction to exploitation (Memory corruption, ASLR, Heap exploits etc.)

7. Setting up of malware analysis lab

Credits

This will be a 3 credit course with letter grade.

Prerequisites

The student should have some familiarity with Unix, Windows and any one programming language.

Materials & Books

We will primarily use Ghidra a high end reverse engineering framework as the tool for all out work. Its free and has been released very recently by NSA. One of the objectives of the course would be to make the students expert on Ghidra. The instructor will also be learning the tool as the it has been released in the last two weeks at the time of this writing. We will use the following books on a need basis:

1. The Shellcoder's Handbook: Discovering and Exploiting Security Holes.

2. Reverse Engineering for Beginners: Online eBook.

3. Practical Malware Analysis: A bit dated but still relevant. This is the book we will use for learning about the wonderful OS called Windows - I am kidding of course :) Linux is the wonderful OS.

4. My notes. I will hand over notes from time to time.

Assessment

The performance of the students will be assessed based on performance on hands on projects. The class will meet once a week in an informal setting and will consist mainly of presentations both from the instructor and the students. The projects will be assigned by the instructor and will be done in groups, with the instructor playing an active role. There will be no tests.

Statement from Instructor

In this course you will learn the “darkest art” of computer science and at the end of it you will know how to invoke demons (pun intended) that cause havoc in the digital world. This will be more potent than any cybersecurity course that you have taken. You will gain access to live weapons grade malware. However please do remember that with great power comes great responsibility. I am imparting the knowledge to you to use for GOOD. Never use these skills for personal gain or to show off. I or UAH will not be responsible in any way if you put these skills to the wrong use.