Practical Malware Analysis

Dan Bruce, David Clark and Héctor D. Menéndez

Department of Computer Science
University College London

Malware Analysis Labs

Understanding Reverse Engineering.

Understanding Static Analysis.

Understanding Dynamic Analysis.

Labs Structure

Lab 1: Introduction to Computer Architecture.

Lab 2: Introduction to Assembly

Lab 3: Assembly and C.

Labs 4 and 5: Reverse Engineering.

Lab 6: Packing.

Lab 7: Debugging.

Lab 8: Network Analysis and Emulators.

Lab 9: Machine Learning.

The Architecture

Malware will interact with different elements of the system and the computer.

It is important to have a basic knowledge about these elements to understand different attacks.

Assembly

Reverse Engineering of Binary Files is a frequent practice in Malware Analysis.

This requires a good understanding of Assembly code.

This part is going to focus on understanding assembly.

C to Assembly

This part is focused on understanding how high level programs are translated to assembly.

This will help to have a high level look of assembly code.

Reverse Engineering

These labs aim to show how to apply reverse engineering to a specific program.

We will use an open-source program named Radare.

We will analyse high level programs and we will have a look to their assembly code in order to extract information about how they work.

Packing Analysis

This lab aim to show different packing detection tools in order to help during the analysis process.

We will use different open tools for this task.

Debugging

This lab continues with the idea of reverse engineering and show other methodologies which belong to static analysis.

These methodologies complement the information provided by the RE process.

Network Analysis and Emulation

This lab shows different tools to perform dynamic analysis as a complement to static analysis.

We will not run Malware but we will try to understand Malware behaviour.

Machine Learning

This lab aims to show some machine learning concepts in malware detection.

We will also focus on the limitations on machine learning algorithms in front of adversaries.

Coursework

The coursework will be published between session 7 and 8.

It will cover the reverse engineering part.

The List

Here, you can find a good list of Malware analysis tools and databases:
`https://github.com/rshipp/awesome-malware-analysis`

Have a look to the tools.