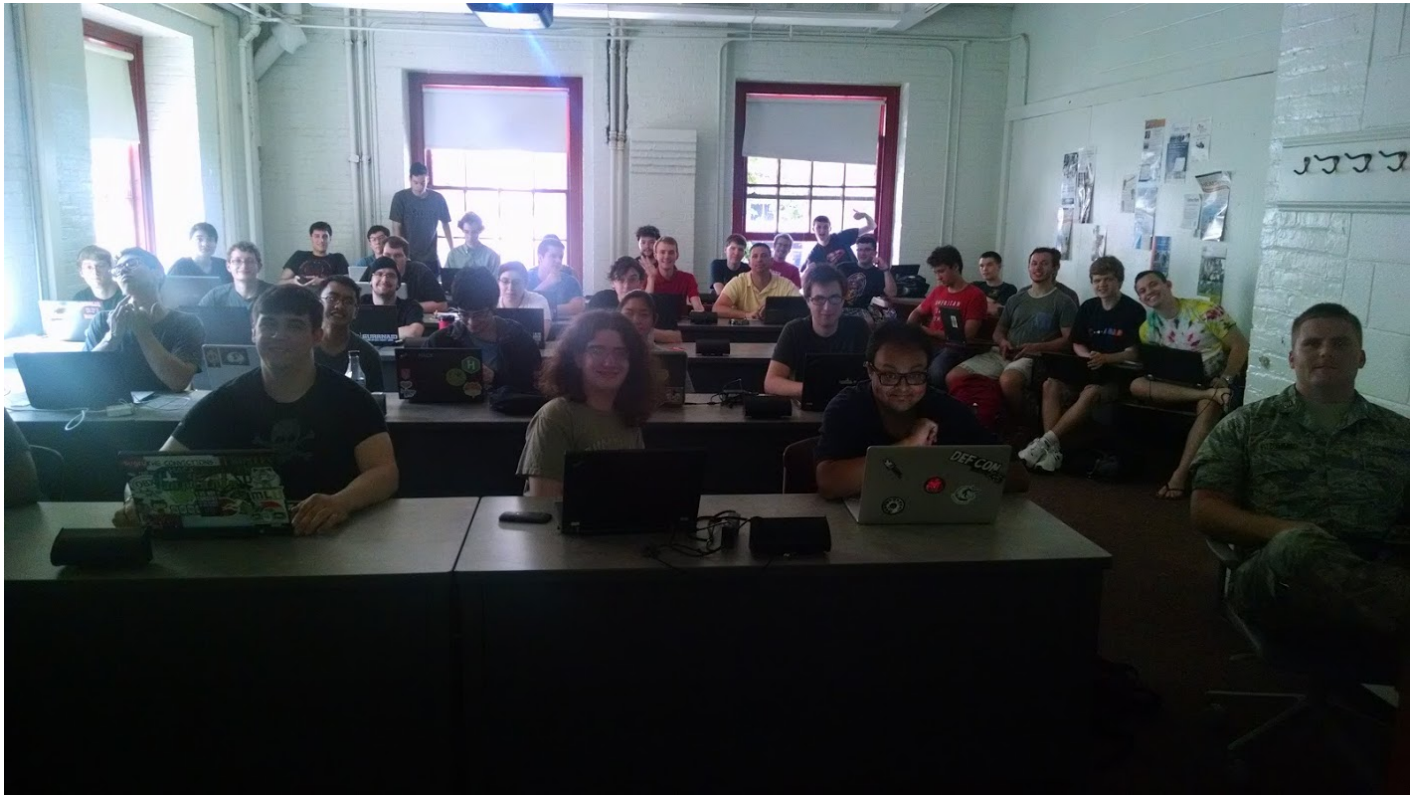
# Malware Analysis - CSCI 4976

This repository contains the materials as developed and used by RPISEC to teach Malware Analysis at Rensselaer Polytechnic Institute in Fall 2015. This was a university course developed and run soley by students, primarily using the Practical Malware Analysis book by Michael Sikorski and Andrew Honig, to teach skills in reverse engineering, malicious behaviour, malware, and anti-analysis techniques.



## About the Course

The Practical Malware Analysis (PMA) book is where many RPISEC members and alumn started. The book reads very well, is full of information, and the lab walkthroughs in the back are invaluable. We didn't want to re-invent the wheel so we structured most of the class around the book. Students were expected to have read the relevant PMA book chapters before class, allowing us to spend much more class time demonstrating skills and techniques and walking through hands-on examples with the students.

**Syllabus:** http://security.cs.rpi.edu/courses/malware-fall2015/Syllabus.pdf

**Note: Most of the samples used in this course are malicious in nature, treat them carefully!**

To help protect people from accidentaly running samples on an important machine, and to prevent anti-malware suites from blocking the course material, **all of the samples are compressed and encrypted with a password of 'infected'.**

## Course Abstract

> *With the increased use of the Internet and prevalence of computing systems in critical infrastructure, technology is undoubtedly a vital part of modern daily life. Unfortunately, the increasingly networked nature of the modern world has also enabled the spread of malicious software, or "malware", ranging from annoying adware to advanced nation-state sponsored cyber-weaponry. As a result, the ability to detect, analyze, understand, control, and eradicate malware is an increasingly important issue of economic and national security.*

> *This course will introduce students to modern malware analysis techniques through readings and hands-on interactive analysis of real-world samples. After taking this course students will be equipped with the skills to analyze advanced contemporary malware using both static and dynamic analysis.*

## Prerequisite Knowledge

This course carried a prereq of Computer Organization - CSCI 2500 at RPI. Computer Organization is RPI's basic computer architecture course that teaches things like C, MIPS assembly, x86 assembly, Datapaths, CPU Pipelining, CPU Caching, Memory Mapping, etc.

Our expected demographic for Malware Analysis was students with zero reverse engineering experience. That said, to be able to take this course you will probably need at least the following skills.

- Working knowledge of C/C++
- Any assembly level experience

## Lecture Breakdown

| Lecture | Title | Topics |
|---|---|---|
| 01 | Introduction | Syllabus, Basic Static Analysis, Basic Dynamic Analysis |
| 02 | Advanced Static Analysis | x86, IDA, Code Constructs |
| 03 | Analyzing Windows Programs | WinAPI, Handles, Windows Internals, Networking, COM |
| 04 | Advanced Dynamic Analysis | Debugging Concepts and Tools |
| 05 | Malware Behavior | Malicious Activities and Techniques |
| 06 | Data Encoding and Malware Countermeasures | Hiding Data, Malware Countermeasures |
| 07 | Covert Malware Launching | Covert Launching and Execution |
| 08 | Anti-Analysis | Anti-Disassembly, Anti-VM, Anti-Debugging, Anti-AV |
| 09 | Packing and Unpacking | Packers, Packing, and Unpacking |
| 10 | Intro to Windows Kernel | Kernel Basics, Windows Kernel API, Windows Drivers, Kernel Debugging |
| 11 | Rootkit Techniques | Hooking, Patching, Direct Kernel Object Manipulation |
| 12 | Rootkit Anti-Forensics and Covert Channels | Anti-forensics, Covert Channels |

## Lab Breakdown

| Lab | Topic |
|---|---|

| Lab | Topic |
| --- | --- |
| 01 | Basic Analysis |
| 02 | Advanced Static Analysis |
| 03 | Analyzing Windows Programs |
| 04 | Advanced Dynamic Analysis |
| 05 | Malware Behavior |
| 06 | Data Encoding and Malware Countermeasures |
| 07 | Covert Malware Launching |
| 08 | Anti Analysis |
| 09 | Packing and Unpacking |
| 10 | Windows Kernel |

## Project Breakdown

| Project | Topic |
| --- | --- |
| 01 | Malware Behavior |
| 02 | Runtime Process Manipulation |
| 03 | Unpacking and Automation |
| 04 | APT Sample Analysis |

Links for additional exercises:

- Practical Malware Analysis Labs
- Practical Reverse Engineering Labs

## Analysis Environment

Setting up a "safe" and usable analysis environment can range from easy to impossible, depending on how far you want to go. The PMA book devotes an entire chapter (Chapter 2) to this problem. For the purposes of this class, we decided to set up a Windows 7 32-bit virtual machine. Unfortunately, while all the software we used for the class is free, Windows is not, thus we cannot distribute this VM like we distributed the Warzone for MBE. We have, however, included a comprehensive list, and a collection of installers, of all the tools we used throughout the course. There are a few "essentials" that we haven't listed but are still included in the installer package (python, cygwin, etc).

Visit the releases page for the latest package.

### Tools

- Dependency Walker
- Fakenet
- FileAlyzer 2.0
- HxD
- IDA Free
- ImpREC
- LordPE
- Malcode Analyst Pack
- OllyDbg

- PEiD
- PEview
- Regshot
- Resource Hacker
- Sysinternals Suite
- UPX
- Visual Studio
- Windbg
- Wireshark

## Frequently Asked Questions

If you are ever stuck on a problem or have any questions, you're more than welcome to ask on IRC.

**What is the password to the zip files?**

'infected', no quotes.

**Are these files malicious/dangerous?**

Yes. Not all of them are malicious in nature, but most are. Always keep them inside a proper analysis environment.

**Why are the lecture slides for XYZ so sparse?**

Much of lecture time was spent in hands on examples, with the expectation that students had read the material in the PMA book ahead of time. Thus the slide content referring to material from the PMA book is meant as more of an outline. Read the chapters and then go through the lab walkthroughs in the back of the PMA book, they are a great resource.

**Do you have videos of the lectures?**

Sadly we did not record any of the lectures, maybe next time.

**Where can I learn more?**

Play more wargames:

- IO Wargame
- Pwnable KR
- Pwnable TW
- OverTheWire
- Reversing KR
- W3Challs
- crackmes.de

Reverse more samples:

- Contagio
- Kernelmode.info
- Malware.lu
- malwr
- Hybrid Analysis

The following books are excellent resources for expanding your knowledge of malware analysis and reverse engineering. We recommend working through them in the following order:

- Practical Malware Analysis
- Practical Reverse Engineering

- Rootkits: Subverting the Windows Kernel
- The Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System
- Rootkits and Bootkits: Reversing Modern Malware and Next Generation Threats

These three books are also excellent:

- The Antivirus Hacker's Handbook
- The Art of Memory Forensics
- Windows Internals

And when they're happening, play CTFs!

**I have a question, how can I get in touch with you?**

Our club keeps a pretty active IRC presence. Someone there can probably answer your question.

**Server:** `irc.rpis.ec` **Port:** `6667`, or `6697` (SSL)

If you would like a more formal means of communication, you can reach us at `contact [at] rpis.ec`

# Licensing

This course was explicitly designed for academic & educational use only. Please keep this in mind when sharing and distributing our course material. The specific licenses involved can be found below.

**Lecture Slides**

The lectures are covered by the Creative Commons Attribution-NonCommercial 4.0 International license CC BY-NC 4.0.

# Acknowledgements

Hundreds of hours and countless all nighters went into the production and execution of this course. This section serves to recognize those who made all of this possible.

## Original Authors


- Branden Clark
- Austin Ralls
- Aaron Sedlacek


## Special Thanks


- The RPI CS Department for giving us this opportunity and letting us run with it
- Professor Bülent Yener for sponsoring such a course
- Our students who put up with us all semester