Course Title: Engineering runtime Malware Detection

Term: Summer 2016

Week 01: Introduction

- Course Overview
- Semester Project Overview
- Overview of malware
- Static and dynamic analysis
- Signature based and behavior based malware detection
- Overview of real time malware detection & current state of the art

Week 02: Fundamental Suspicion Assessment

- Key broad suspicion assessment areas
- Malware behavior categories
- Definitions of “not suspicious”, “low suspicious”, “medium suspicious”, and “highly suspicious”
- When to escalate suspicion
- Detecting a highly suspicious object as early as possible in real time

Week 03: Passive Monitoring

- The importance of determining where and what to monitor
- Background Monitoring
- Windows File System
- Windows Processes and Memory
- Windows Registry
- Windows Networking

Week 04: Data Collection

- Deciding where in OS to place data collectors
- How to store collected data
- Collection granularity

Week 05: Data Correlation

- Linking data to its owner
- Creating parent-child relationships
- Malware infection trees

Week 06: Data Analysis

- Filtering collected data
• Frequency vs. Occurrence

Week 07: Determining a Process is Highly Suspicous
• Setting the threshold for highly suspicious
• Identifying highly suspicious objects in the early stages
• Handling highly suspicious objects

Week 08: Real Time Detection System Design
• Enumerating threats of interest for target system
• Requirements gathering
• Defining highly suspicious
• Determine needed data to collect

Week 09: Real Time Detection System Implementation
• Assessing data collection capability of target system
• Building and running data collectors
• Running real time analysis logic to assess suspicion
• Testing for False Positives and False Negatives

Week 10: Handling Suspicious Objects
• Eradication
• Quarantine
• Suspension
• System disinfection and restoration

Week 11:

Week 12:

Week 13: Semester Project Presentations

In-Class Exercises
Class sessions will include computer exercises/experiments to learn and explore the tools and techniques related to runtime monitoring and analysis. These exercises are not graded. The students will be advised of when these exercises will occur and students may bring their personal laptops if desired.

Course Grading Policy
There will be a total of 5 homework assignments, and a semester project. The homework serve as mini-projects based on class lecture. The homework will also help students develop their semester projects. Students are required to complete a group semester project building a runtime monitoring and malware analysis system for the Windows
operating system. Each group will present their project to the class during the last weeks of the semester.

**Evaluation:**
Semester Project - 80 points
Reading Assignment Quizzes - 20 points

### Final Grade

<table>
<thead>
<tr>
<th>Grade</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>90 points and above</td>
</tr>
<tr>
<td>B</td>
<td>between 80 and 89 points</td>
</tr>
<tr>
<td>C</td>
<td>between 70 and 79 points</td>
</tr>
<tr>
<td>D</td>
<td>between 60 and 69 points</td>
</tr>
<tr>
<td>F</td>
<td>below 60 points</td>
</tr>
</tbody>
</table>

**Grade disputes**
You have up to 7 days after receiving your grade to raise any issues regarding the grading of your weekly assignments or semester project. After that 7-day window your grade is final and you cannot appeal it.

**Students with Disabilities**
Individuals with documented disabilities may be eligible to receive services/accommodations from CMU's Equal Opportunity Services (EOS) office. For more information, please contact Larry Powell (lpowell@andrew.cmu.edu).

**Copyright Notice**
Please do not post or otherwise redistribute materials distributed in class.

**Academic Integrity Policy**
Students at Carnegie Mellon are engaged in preparation for professional activity of the highest standards. Each profession constrains its members with both ethical responsibilities and disciplinary limits. To assure the validity of the learning experience a university establishes clear standards for student work.

In any presentation, creative, artistic, or research, it is the ethical responsibility of each student to identify the conceptual sources of the work submitted. Failure to do so is dishonest and is the basis for a charge of cheating or plagiarism, which is subject to disciplinary action.

*Cheating* includes but is not necessarily limited to:

1. Plagiarism, explained below.
2. Submission of work that is not the student's own for papers, assignments or exams.
3. Submission or use of falsified data.
4. Theft of or unauthorized access to an exam.
5. Use of an alternate, stand-in or proxy during an examination.
6. Use of unauthorized material including textbooks, notes or computer programs in the preparation of an assignment or during an examination.
7. Supplying or communicating in any way unauthorized information to another student for the preparation of an assignment or during an examination.
8. Collaboration in the preparation of an assignment. Unless specifically permitted or required by the instructor, collaboration will usually be viewed by the university as cheating. Each student, therefore, is responsible for understanding the policies of the department offering any course as they refer to the amount of help and collaboration permitted in preparation of assignments.
9. Submission of the same work for credit in two courses without obtaining the permission of the instructors beforehand.

Plagiarism includes, but is not limited to, failure to indicate the source with quotation marks or footnotes where appropriate if any of the following are reproduced in the work submitted by a student:
1. A phrase, written or musical.
2. A graphic element.
3. A proof.
4. Specific language.
5. An idea derived from the work, published or unpublished, of another person.