Sam Houston State University

Department of Computer Science

COSC 5330: Malware
Syllabus
Fall 2017

General Information

Instructor: Dr. Peter A. Cooper
Office: AB1 214
Phone: 294 1569
Email: cooper@shsu.edu

Course Title: Malware
Course Code: CS 5325
Couse Day/Time ONLINE

Course Description

This course provides exposure to the important associated with the organization, identification, isolation and neutralization of malicious software. The course examines the history and classification of malware, and the forensic analysis of systems to identify malware issues. Credit: 3 hrs.

Course Texts

Honig, A & Sikorski, M. *Practical Malware Analysis*. ISBN13: 978-1593272906

Course goals

At the end of this course the ideal student should be able to

- Understand the internal structures functions of the most common forms of malware
- Develop a Virtual Malware Lab
- Forensically examine systems for malware
- Apply appropriate commercial and open source tools for the defense of systems and networks against malware
- Develop skill in producing professional reports on analysis and the protocols used,

Teaching Strategy

You are all graduate students, and, as such, will be experiencing a very different approach to instruction in this class. I do not intent to use lectures as the primary instructional method. Instead, I will direct you to address **grand challenges**, where you are provided with an end goal, and you need to map your own path to achieving that goal.

We will have synchronous evening sessions every other week, providing you an opportunity to

- Ask questions if you are experiencing a problem or need clarification
- Provide information to classmates to support their development of solutions to the grand challenges
-

Grading Criteria

This course is a primarily hands-on course with practical activities taking place as a group and individually. As such the grading is done in relation to responses to:

- 8 Synchronous evening sessions
    - In general I expect everyone to participate in these session to the best of your ability. We will be using Zoom as the AV resource to get everyone together. I will be posting a request for a suitable day/time. The sessions will not be exclusively lecture format but

include a significant Q&A component to ensure that you are all on task and keeping up with the readings/workload.
    - **Grading:** Are you there? Are you participating? Are you contributing?
- 4 Grand Challenges
    - The grand challenges are designed to test a wide range of concepts and skills presented in the prior course material. Students will be expected to collaborate on conceptual, theoretical, and practical issues. However, final solutions and implementation evidence are submitted individually. In other words, you can get help from your classmates on **how** to do things, but you have to actually do them yourself and demonstrate that you have.
    - **Grading** To what extent did you meet the goal of the challenge? To what extent did you report results in a coherent and professional manner? Did you meet the deadline?
- 1 Semester Portfolio
    - The semester portfolio consists of responses to lab exercises in the course text. Those responses will follow a standard professional format, as defined in the first class session. The portfolios will be in electronic format, submitted to blackboard and updated on a weekly basis.
    - **Grading:** Is the portfolio complete? Are the reports provided in a coherent and professional manner? Did you meet the deadline?

There are no exams, quizzes or tests in this class.

Course Topics

1. Techniques for the Lay Person. The Virtual Malware Lab
2. Static Analysis Techniques I. Grand Challenge #1
3. X86 Architecture. Code Disassembly.
4. IDA Pro. Assembly ⇔ C.
5. Dynamic Analysis Techniques I. Grand Challenge #2
6. Windows API. The Registry. Tracking Active Malware.
7. Advanced Static Analysis. Grand Challenge #3.
8. Debugging. OLLYDBG
9. Kernel Debugging. WINDBG
10. Malware Behavior.
11. Data Encoding. Grand Challenge #4.
12. Anti-Debugging. Anti-VM Techniques
13. Packing

Attendance Requirements

In accordance with University Policy, regular attendance is required. However, no points will be awarded or subtracted based on your attendance. You are responsible for all material covered in every class, regardless of whether you attended or not. It is your responsibility to obtain notes, assignments, etc., from fellow class members if you miss a class. This course has one face-to-face section and one online section. Students in the online section are permitted to attend in person or online during the live feed from the face-to-face sessions. All sessions are recorded and will be available via blackboard within 24 hours of each session.

Academic Dishonesty

All students are expected to engage in all academic pursuits in a manner that is above reproach. Students are expected to maintain complete honesty and integrity in the academic experiences both in and out of the classroom. Any student found guilty of dishonesty in any phase of academic work will be subject to disciplinary action. The University and its official representatives may initiate disciplinary proceedings against a student accused of any form of academic dishonesty including, but not limited to, cheating on an examination or other academic work which is to be submitted, plagiarism, collusion and the abuse of resource materials.

Classroom Conduct
Students will refrain from behavior in the classroom that intentionally or unintentionally disrupts the learning process and, thus, impedes the mission of the university. Please turn off or mute your cellular phone and/or pager before class begins. Students are prohibited from eating in class, using tobacco products, making offensive remarks, reading newspapers, sleeping, talking among each other at inappropriate times, wearing inappropriate clothing, or engaging in any other form of distraction. Inappropriate behavior in the classroom shall result in a, minimally, a directive to leave class or being reported to the Dean of Students for disciplinary action in accordance with university policy.

Visitors in the Classroom
Occasion visiting of classes by responsible persons is allowed with prior arrangement with the instructor, as long as it does not interfere with the registered members of the class or the educational process.

Americans with Disabilities Act
Students with disabilities covered by the Americans with disabilities Act should go to the Counseling Center and Services for Students with Disabilities (SSD) in a timely manner to obtain the documentation required. Students are responsible for initiating the process of documenting the need for an accommodation under the ADA act.

Religious Observance
University policy allows for student to observe religious holy days without penalty. If you intend to miss class as a result of the observance of a religious holy day or as a result of the necessary traveling time required for religious observance, such an absence will not be penalized. As a courtesy, it would be appreciated if you notify the instructor in advance in writing, of the dates and times of class sessions that are to be missed. Students absent from class as a result of religious observance are required to submit any due assignments immediately on their return to the classroom. Makeup tests and quizzes will also be provided on return to the class.

Office Hours
- TTH 10:00 – 11:30, 2:00 – 3:00
- MW 10:30 – 11:30, 2:00 – 3:00

The most effective way of contacting me is by email: **cooper@shsu.edu**