SYLLABUS

Department of Computer Science and Engineering

CSCE 451/652, Software Reverse Engineering (REEN)

Spring 2021

3 credit hours, elective
Updated Jan. 19, 2021

INSTRUCTOR

Jyh-Charn (Steve) Liu
HRBB 502B Tel: 845-8739, Email: liu@cs.tamu.edu
Office Hours: by appointments

TEACHING ASSISTANT

Mr. Donald J. (DJ) Beyette Email: thunder4780@tamu.edu

LEARNING OBJECTIVES: Develop and apply skills for static and dynamic analysis of x86 binaries. Learn about ELF data structures and how they are used during the execution of applications.

OUTCOMES:

At end of the class, students should be proficient in the following aspects.

(1) Identify common copyrights and other related laws governing software rights and their reverse engineering activities.
(2) Identify the connection from high level language programs to their machine code representations.
(3) Extract the program execution flows from the portable binary executable files.
(4) Formulation and optimization of reversing strategies (such as brute force based, or math logic based) to perform static analysis of binary codes. Hypothesize the necessity of further dynamic analysis of binary codes.
(5) Basics of anti-analysis techniques to protect binaries.

COURSE PREREQUISITES AND WORKLOAD:

- Minimal requirement: CSCE 313, or instructor's approval. Students are expected to be proficient in programming, computer architecture, and self-learning of program analysis tools.
- JR/SR classification, but exception can be made per instructor's approval.
- This class has extensive hands-on work. Students are advised to weigh their overall workload in taking this course.

TECHNICAL THEMES

Architecture & Assembly language

- Basics of low level software and their relationship with hardware resources. (Instruction set architectures, privileges, interrupt, address space)

Design

- Programming in Assembly, exploits (virus, drivers)

Binary Analysis

- From HLL statements to binary idioms.
- Executable header, symbols,
- Disassembly tools such as Ghidra, IDA Pro, Radare2, and debuggers
- Anti-analysis techniques: Virtual ISA, Address space layout randomization (ASLR), code packing

GRADING POLICY:
Curved.
Rules for missing assignments: D or worse for 3 missing assignments. C or worse for 2 missing assignments.
Submitted Assignments: Programming. Note: All projects will be archived for future classes as teaching and learning references.

- Quiz and Test:
    - ISA instruction set, HLL structures (week 4) (15 points)
    - Basics of reversing of binary (Week 8) (15 points)
- Programming/Analysis Assignments: 6 (40 points)
    - Tuesday lab: self-learning and group working on assignments, and make summary of major questions
    - Thursday lab: response to top *x* questions from Tuesday work
    - Topics
        - Tool Installation
        - X86 instruction set
        - Running examples
        - How to reverse binary
        - Code breaker level 1
        - Code breaker level 2
- Topical Term Project: 1 (20 points) 3 persons/team
    - Check point 1 - one pager (week 3)
    - Check point 2 – proposal (5 pages) (week 6)
    - Final check – video recorded code demo, project final report

REVERSE ENGINEERING AND HACKING

The common term hacking refers to the process of exploiting vulnerability of software systems by manual or automated processes. Learning about hacking practices is essential to build defensive software systems, but misuse of the skills in the real world environment can have serious legal implications. RE related laws differ with the country, region, and types of activities. Students are advised to take great cautions in their conducts. A “gut feeling, common sense” based mentality can lead to regrettable situations. In this class students will learn about selective legal cases related to real world hacking.

TEXTBOOKS

- None required
- Reference books (not exclusive)
    - Assembly language for Intel based computers, by Irvine

- Reverse Engineering for Beginner
- The IDA Pro Book, by Chris Eagle
- Reverse Engineering, secret of reverse engineering, by Eldad Eilam
- Practical Malware analysis, by M. Sikorski and A. Honig
- Open literature, vendors technical information (Intel, Microsoft)

LECTURE, DISCUSSION AND BYOD (BRING YOUR OWN DEVICES)

The class follows a staged development process as follows: (1) Getting to know with the instruction sets, (2) making connections between instruction flows with high level language statements, (3) Executable file format, (4) tools for dynamic and static analysis, (5) code patterns, flow analysis, (6) reversing high level logic.

Lectures will be posted on the web site: Software Reverse Engineering – Real Time Distributed Systems Lab (tamu.edu)

Students should bring their own laptops with installed VM during all class hours.

Copy and paste is not allowed for composition of all reports and programs.

ATTENDANCE POLICY:

- Except for University excused absence, students are responsible for any missed materials. Attendance policies are defined by student rule 7; see http://student-rules.tamu.edu/rule07.
- Tests
  - Test 1:
  - Test 2:
  - Due to the electronic, real time nature of on-line tests, accommodation will be granted only to extraordinary situations, such as illness or family emergency. (Job interview is not on the list.)
- Missing assignments
  - For excused absences: an opportunity will be provided to make up any graded work.
  - For unexcused absences: a grade of zero will be assigned to the missed work/test. At discretion of the instructor, a missed test is subject to a 25% penalty even if retaking of the test is granted.
- To request approval of an absence, send me an e-mail explaining the reason for the absence.   If advance notification is not possible (e.g. unexpected illness) send the e-mail within 48 hours to justify the absence. For illness, a note from a doctor or clinic is required.

Special rules for team projects

- Every student is required to contribute technical and documentation work.
- If there is a project partner dispute, it is critical to report the issue quickly to the instructor or TA. Otherwise, you share grade consequences if the issues contribute to a poor grade.

COMMUNICATIONS: Emails and the Canvas system will be used extensively. All emails related to this class should be sent to liu@cse.tamu.edu. Please add a subject heading “RE21 your subject”

SCHOLASTIC DISHONESTY will not be tolerated. Plagiarism is the presentation of the work of someone else without giving him or her due credit. Any such incidents will be dealt with in accordance with the procedures outlined in the University Student Rules. Some specific rules:

1. In most cases, you are encouraged to discuss assignments, but the final product submitted for grade **must be the individual work of the person turning it in.**

2. If code from two or more students is essentially identical, and it is determined **to the satisfaction of the instructor** that the code is the product of a group effort, **the assignment may be rejected with no credit for any of the students involved.**
3. Always be prepared to answer the questions: “What is your contribution?” “Where did you get this design?” “What is your responsibility and contribution in the team?”
4. **Using third party codes and tools** to solve challenging computing problems is critical to most software reverse engineering, and therefore is allowed. When doing so, it is a must to have full disclosure prior reporting results. Claiming credit without such disclosure will be considered cheating.

“*An Aggie does not lie, cheat or steal, or tolerate those who do.*” For additional information, please visit: http://aggiehonor.tamu.edu.

STUDENTS WITH DISABILITIES: The Americans with Disabilities Act (ADA) is a federal anti-discrimination statute that provides comprehensive civil rights protection for persons with disabilities. Among other things, this legislation requires that all students with disabilities be guaranteed a learning environment that provides for reasonable accommodation of their disabilities. If you believe you have a disability requiring an accommodation, please contact Disability Services, 701 West Campus Blvd
1224 TAMU, or call 845-1637. For additional information visit http://disability.tamu.edu

COPYRIGHT NOTICE: The handouts used in this course are copyrighted and cannot be copied without permission. By “handouts,” this means all materials generated for this class, which includes but is not limited to, syllabi, quizzes, exams, lab and homework problems, lab handbook, lab manuals, in-class materials, review sheets, and Web site materials. You must obtain the instructor’s explicit permission to video/record the class contents.