TEXAS A&M UNIVERSITY

Course Syllabus

Course Information

Course Number:	CSCE 451
Course Title:	**Software Reverse Engineering (REEN)**
Section:	TBD
Time:	TBD
Location:	HRBB 113
Credit Hours:	3

Instructor Details

Instructor:	Jyh-Charn Liu
Office:	PETR 435
Phone:	979-845-8739
E-Mail:	liu@cse.tamu.edu
Office Hours:	By appointment, on-line

TEACHING ASSISTANT

Office:	EABA 108B
Email:	hdwang@tamu.edu
Office hour	By appointment, on-line

Course Description

This course aims to introduce the art of inferring, and/or reproducing of partial or complete high-level computing logics from a binary executable code without the original source codes. The course starts with introduction of the relationship among high level programming languages and X86 ASM statements. It will then expand to the X86 instruction set architecture (ISA) and its computing models, and the compiler generated binary executables. Through extensive hands-on exercises, assignments and tests, students will be guided to learn to develop the reserving strategy, starting from scope of reversing goal, hypothesis formation, iterative validation, selection of tool chains for static and dynamic analysis, disassembling, up to validation of reversing outcomes. The class also introduces basics of exploits, and defensive design against static and dynamic analysis.

Students are required to learn about the basics of legality and ethics of software reversing. The 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 consequences. RE related laws differ greatly in different countries, regions, 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 RE cases.

Course Prerequisites

- Minimal requirement: CSCE 313, or instructor’s approval. Students must be proficient in common HLL languages, programming, and common microprocessor architecture(s).
- 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.

Special Course Designation

N/A

Course Learning Outcomes

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

- Identify common copyrights and other related laws governing software rights and their reverse engineering activities.
- Gain knowledge on the relationship between HLL and Assembly statements.
- Identify and utilize the knowledge on the compilation process to identify high level language programs and their machine code interpretations.
- Extract the needed binary code structure information from the portable executable file formats.
- Formulation and optimization of reversing strategies (such as brute force based, or math logic based) to perform static & dynamic analysis of binary codes.
- Survey of RE resources
- Validation of disassembler outcomes.
- Gain knowledge on anti-analysis techniques to protect binaries.

Textbook and/or Resource Materials

- None required
- Reference books (not exclusive)
  - Assembly language for Intel based computers, by Irvine
  - 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)
- A laptop computer with sufficient performance to run a designated Linux virtual machine, compilers and RE tools. The laptop should also have large HDD space and main memory. Past experience suggests that common laptops would be usable for class activities, but lack of computing resources can significantly affect the productivity or even classwork outcomes.
- Major tools
  IDA Pro, Ghidra, Godbolt.org, Linux and compilers, various utility tools

Grading Policy

• *Labs, exercises, assignments*	*40%*
• *Tests*	*40%*

- *Final Project 20%*
- *The grading scale: By numerical ranking of total scores.*

Special rules for graded 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.

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.
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.

Graded Attendance –

- All absences from graded activities – tests, quizzes and some timed lab exercises require prior approval of the instructor. Students without prior absence approval may be allowed to make up the missing activity with 25% or more grade penalty.
- Students are responsible for any missed materials.
- University excused absence are defined by student rule 7; see http://student-rules.tamu.edu/rule07.
- 3-strike rule: a final grade of D/F for missing 3 graded activities.
- If advance notification is not possible (e.g. unexpected illness, family emergency) for the absence, contact the instructor at the earliest time with some supporting evidence/document.

Late Work Policy

- *Late work will be accepted up to one day late with a 25% penalty.*

Course Schedule

Week (15)	***Topic***	***Assignments***
1	*High level languages (HLL) constructs (I)*	*In class exercises/lab*
2	*HLL constructs & ASM (II)*	*In class exercises/lab*
3	*Stack, accumulator-based processor, function call*	*In class exercises/lab*
	Mixed HLL & ASM programming (Godbolt) (I)	*Quiz 1*
4	*HLL & ASM programming & DBG (Godbolt) (II)*	*In class exercises/lab*
5	*Binary reversing (I)*	*In class exercises/lab*
6	*Ethics & legality*	*Reading and report*
7	Binary reversing (II)	*In class exercises/lab*
8	Binary reversing (III)*, Tool: binary code visualization Rigi, CcNav*	*In class demo, take home assignment*
9	Binary reversing (IV), *Tool: Ghidra or IDA Pro*	*In class follow along/lab, take home assignment*
10	Binary reversing (V), *Tool: Ghidra or IDA Pro, De-compiler validation, semantic labeling*	

11	Binary reversing (VI)*: Password cracking*	*In class exercises/lab/timed test*
12	Binary reversing (VII), *Tool: Symbolic computing Z3/ANGR*	
13	*Term projects – assigned binary images*	
14	*Term project*	
15	*Term project*	

Optional Course Information Items

N/A

University Policies

Attendance Policy

The university views class attendance and participation as an individual student responsibility. Students are expected to attend class and to complete all assignments.

Please refer to Student Rule 7 in its entirety for information about excused absences, including definitions, and related documentation and timelines.

Makeup Work Policy

Students will be excused from attending class on the day of a graded activity or when attendance contributes to a student’s grade, for the reasons stated in Student Rule 7, or other reason deemed appropriate by the instructor.

Please refer to Student Rule 7 in its entirety for information about makeup work, including definitions, and related documentation and timelines.

Absences related to Title IX of the Education Amendments of 1972 may necessitate a period of more than 30 days for make-up work, and the timeframe for make-up work should be agreed upon by the student and instructor” (Student Rule 7, Section 7.4.1).

“The instructor is under no obligation to provide an opportunity for the student to make up work missed because of an unexcused absence” (Student Rule 7, Section 7.4.2).

Students who request an excused absence are expected to uphold the Aggie Honor Code and Student Conduct Code. (See Student Rule 24.)

Academic Integrity Statement and Policy

"An Aggie does not lie, cheat or steal, or tolerate those who do."

"Texas A&M University students are responsible for authenticating all work submitted to an instructor. If asked, students must be able to produce proof that the item submitted is indeed the work of that student. Students must keep appropriate records at all times. The inability to authenticate one's work, should the instructor request it, may be sufficient grounds to initiate an academic misconduct case" (Section 20.1.2.3, Student Rule 20).

Texas A&M at College Station
You can learn more about the Aggie Honor System Office Rules and Procedures, academic integrity, and your rights and responsibilities at aggiehonor.tamu.edu.

Texas A&M at Galveston
You can learn more about the Honor Council Rules and Procedures as well as your rights and responsibilities at tamug.edu/HonorSystem.

Texas A&M at Qatar
You can learn more about academic integrity and your rights and responsibilities at Texas A&M University at Qatar by visiting the Aggie Honor System website.

Americans with Disabilities Act (ADA) Policy

Texas A&M University is committed to providing equitable access to learning opportunities for all students. If you experience barriers to your education due to a disability or think you may have a disability, please contact the Disability Resources office on your campus (resources listed below) Disabilities may include, but are not limited to attentional, learning, mental health, sensory, physical, or chronic health conditions. All students are encouraged to discuss their disability related needs with Disability Resources and their instructors as soon as possible.

Texas A&M at College Station
Disability Resources is located in the Student Services Building or at (979) 845-1637 or visit disability.tamu.edu.

Texas A&M at Galveston
Disability Resources is located in the Student Services Building or at (409) 740-4587 or visit tamug.edu/counsel/Disabilities.

Texas A&M at Qatar
Disability Services is located in the Engineering Building, room 318C or at +974.4423.0316 or visit https://www.qatar.tamu.edu/students/student-affairs/disability-services.

Title IX and Statement on Limits to Confidentiality

Texas A&M University is committed to fostering a learning environment that is safe and productive for all. University policies and federal and state laws prohibit gender-based discrimination and sexual harassment, including sexual assault, sexual exploitation, domestic violence, dating violence, and stalking.

With the exception of some medical and mental health providers, all university employees (including full and part-time faculty, staff, paid graduate assistants, student workers, etc.) are Mandatory Reporters and must report to the Title IX Office if the employee experiences, observes, or becomes aware of an incident that meets the following conditions (see University Rule 08.01.01.M1):

- The incident is reasonably believed to be discrimination or harassment.
- The incident is alleged to have been committed by or against a person who, at the time of the incident, was (1) a student enrolled at the University or (2) an employee of the University.

Mandatory Reporters must file a report regardless of how the information comes to their attention – including but not limited to face-to-face conversations, a written class assignment or paper, class discussion, email, text, or social media post. Although Mandatory Reporters must file a report, in most instances, a person who is subjected to the alleged conduct will be able to control how the report is handled, including whether or not to pursue a formal investigation. The University's goal is to make sure you are aware of the range of options available to you and to ensure access to the resources you need.

Texas A&M at College Station

Students wishing to discuss concerns in a confidential setting are encouraged to make an appointment with Counseling and Psychological Services (CAPS).

Students can learn more about filing a report, accessing supportive resources, and navigating the Title IX investigation and resolution process on the University's Title IX webpage.

Texas A&M at Galveston

Students wishing to discuss concerns in a confidential setting are encouraged to make an appointment with the Counseling Office in the Seibel Student Center, or call (409)740-4587. For additional information, visit tamug.edu/counsel.

Students can learn more about filing a report, accessing supportive resources, and navigating the Title IX investigation and resolution process on the Galveston Campus' Title IX webpage.

Texas A&M at Qatar

Texas A&M University at Qatar students wishing to discuss concerns in a confidential setting are encouraged to visit the Health and Wellness website for more information.

Students can learn more about filing a report, accessing supportive resources, and navigating the Title IX investigation and resolution process on the University's Title IX webpage.

Statement on Mental Health and Wellness

Texas A&M University recognizes that mental health and wellness are critical factors that influence a student's academic success and overall wellbeing. Students are encouraged to engage in healthy self-care by utilizing available resources and services on your campus

Texas A&M College Station
Students who need someone to talk to can contact Counseling & Psychological Services (CAPS) or call the TAMU Helpline (979-845-2700) from 4:00 p.m. to 8:00 a.m. weekdays and 24 hours on weekends. 24-hour emergency help is also available through the National Suicide Prevention Hotline (800-273-8255) or at suicidepreventionlifeline.org.

Texas A&M at Galveston
Students who need someone to talk to can call (409) 740-4736 from 8:00 a.m. to 5:00 p.m. weekdays or visit tamug.edu/counsel for more information. For 24-hour emergency assistance during nights and weekends, contact the TAMUG Police Dept at (409) 740-4545. 24-hour emergency help is also available through the National Suicide Prevention Hotline (800-273-8255) or at suicidepreventionlifeline.org.

Texas A&M at Qatar
Texas A&M University at Qatar students wishing to discuss concerns in a confidential setting are encouraged to visit the Health and Wellness website for more information.

Campus-Specific Policies

Texas A&M at Galveston

Classroom Access and Inclusion Statement

Texas A&M University is committed to engaged student participation in all of its programs and courses and provides an accessible academic environment for all students. This means that our classrooms, our virtual spaces, our practices and our interactions are as inclusive as possible and we work to provide a welcoming instructional climate and equal learning opportunities for everyone. If you have an instructional need, please notify me as soon as possible.

The Aggie Core values of respect, excellence, leadership, loyalty, integrity and selfless service in addition to civility, and the ability to listen and to observe others are the foundation of a welcoming instructional climate. Active, thoughtful and respectful participation in all aspects of the course supports a more inclusive classroom environment as well as our mutual responsibilities to the campus community.

Statement on the Family Educational Rights and Privacy Act (FERPA)

FERPA is a federal law designed to protect the privacy of educational records by limiting access to these records, to establish the right of students to inspect and review their educational records and to provide guidelines for the correction of inaccurate and misleading data through informal and formal hearings. Currently enrolled students wishing to withhold any or all directory information items may do so by going to howdy.tamu.edu and clicking on the "Directory Hold Information" link in the Student

Records channel on the MyRecord tab. The complete FERPA Notice to Students and the student records policy is available on the Office of the Registrar webpage.

Items that can never be identified as public information are a student's social security number, citizenship, gender, grades, GPR or class schedule. All efforts will be made in this class to protect your privacy and to ensure confidential treatment of information associated with or generated by your participation in the class.

Directory items include name, UIN, local address, permanent address, email address, local telephone number, permanent telephone number, dates of attendance, program of study (college, major, campus), classification, previous institutions attended, degrees honors and awards received, participation in officially recognized activities and sports, medical residence location and medical residence specialization.