UTD	**Course**	**CS/SE 6332**
	Professor	Dr. Zhiqiang Lin
	Term	Fall 2016
	Meetings	**ECSS 2.201**

Professor's Contact Information

Web page	http://www.utdallas.edu/~zhiqiang.lin
Office Location	ECSS 3.226
Email Address	zhiqiang.lin@utdallas.edu (Please type 6332 on the subject)
Office Hours	Friday 4PM – 6PM

TA's Contact Information

TA	TBA
TA Office Location	TBA
TA Email Address	TBA (Please type 6332 on the subject)
TA Office Hours	TBA

General Course Information

Pre-requisites, Co-requisites, & other restrictions	**Prerequisite:** CS 3340; CS 3376; CS 4348
Course Description	CS 6332 is a graduate level, research oriented, systems and software security class. The goal of this course is to understand the low-level details of the real system software implementations such as OS kernels by using techniques such as virtual machine introspection; examine the state of the art attacks, such as memory exploits (e.g., ROP); design practical systems defense (e.g., using the recent advances such as hardware support for trusted computing); design program analysis to reverse engineer the binary code.
Learning Outcomes	The learning outcome is students shall be able to understand and know • **Automated program analysis for the reverse engineering of the binary code**. Static binary code analysis. Dynamic Binary code instrumentation. Data flow analysis, pointer analysis, and control flow analysis. Program slicing. • **Vulnerability Discovery, Memory Exploits, and system defense**. Understand the common software vulnerabilities such as buffer overflow, format string, integer overflows. Understand how to develop exploits against each vulnerability, and understand how to bypass the state-of-the-art defense • **Virtual Machine Introspection**. Understand how to use hypervisor level monitoring to introspect kernel events, to design intrusion detection systems, as well as control the guest OS execution. • **Hardware supported for trusted computing**. Learn the recent hardware advances in trusted computing, e.g., SGX, and understand how to design

	security applications by using SGX.
Required Texts & Materials	• [CHR] Ed Skoudis; Tom Liston. ``Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses", Second Edition [Available Online http://proquest.safaribooksonline.com/9780131481046] • [AOE] Erickson, Jon. ``Hacking: The Art of Exploitation", 2nd Edition [Available Online at http://proquest.safaribooksonline.com/book/networking/security/9781593271442] • [SRE] Eldad Eilam. ``Reversing: Secrets of Reverse Engineering" [Available Online at http://proquest.safaribooksonline.com/book/software-engineering-and-development/9780764574818]
Suggested Texts, Readings, & Materials	• [CSAPP] Randal E. Bryant and David R. O'Hallaron. ``Computer Systems: A Programmer's Perspective, 2/E" • [TSH] Kozoil, Jack. ``The Shellcoder's Handbook: Discovering and Exploiting Security Holes" • [PPA] Principles in Program Analysis. Springer. • [SGX] Intel Software Guard Extension References •

Assignments & Academic Calendar

Week	Course Content
	Binary Code Analysis
1	x86 assembly
2	Static analysis w/ IDA, BinNav
3	Dynamic analysis w/ PIN, QEMU
4	Program analysis (Point-to, Heap)
5	Program analysis (Slicing, Taint analysis)
	Vulnerability, Exploits, and Defense
6	Buffer overflow, format string, integer overflow
7	Control flow hijack, code injection,
8	Return into libc, return oriented programming.
9	Defense against memory exploits, ASLR, CFI, DEP
	Trusted computing
10	Introduction to Intel SGX
11	Anti-reverse engineering with SGX
12	Securing outsource computing with SGX
	Virtualization based systems security
13	Virtual machine introspection (VMI)
14	Techniques and applications of VMI
15	Using VMI for memory forensics

Course Policies

Grading (credit) Criteria	**Course Projects: 60%** **Course Participation : 10%** **Final Exam : 30%** **Letter grades will be assigned as follows:** 98-100 A+ 92-97 A 90-91 A-

88-89 B+
82-87 B
80-81 B-
78-79 C+
72-77 C
70-71 C-
68-69 D+
62-67 D
60-61 D
Below 60 F

All programming assignments are to be individual efforts. Please do not collaborate with other students. Copying of programming assignments or exams, in whole or in part, from other sources will be considered an act of scholastic dishonesty. This policy includes copying from other students, from assignments from previous semesters or from the Internet.

Assignments

There will be **6** programming assignments during the semester. Assignments will be posted in eLearning and should be turned in via **eLearning** ONLY. **No e-mail submissions are accepted**. **No late submissions are accepted.**
Submissions should contain:
1.) A pseudocode or algorithm of your solution plan with explanatory documentation where you think necessary.
2.) A class diagram for your solution drawn **using a UML tool**. Manual solutions are not acceptable. A list of URLs to such tools are provided under elearning -> Web links for your convenience. If you want, you can use a UML tool that is not listed in eLearning.
3.) A text copy of all source code(s) (.java). PLEASE INCLUDE A COMMENT SECTION AT THE BEGINNING OF YOUR CODE WITH YOUR NAME, LASTNAME, SECTION NUMBER, AND DESCRIBE HOW TO RUN YOUR PROGRAM.
4.) A text copy of your input(s) and displayed outputs of your code (.txt or .doc)
5.) Copies of all executable (.class) files.

Assignments will be graded on a 100 point basis, utilizing the following criteria:

Criteria	**Sub Criteria**		**Maximum Score**
Source Code	Program Design	Partitioning	5%
		Organization	5%
		Efficiency	5%
		Coupling	5%
	Comments		10%
	Coding Style	Formatting	5%
		Naming	5%
		Capitalization	5%
Execution	Program Execution	No crashes	5%
		Error Recovery	5%
		Efficiency	5%
	Specification	Nominal cases	25%
		Special cases	5%
Documentation			10%
		Total	***100%***

	Try to write code that is easy to understand and maintain. **1. Source Code: (45%)** **1.1. Program Design: 20%** Many times you can write code that fulfills the requirements by just writing a single main() method. But most times, the problem is complicated enough to require several steps, which may be repeated one or more times. Please design your programs so that the functionality is spread across multiple methods that each accomplish a particular task, and name the method according to the task it performs. *Points Criteria* **1.1.1. Partitioning:** Is the required functionality spread logically across multiple methods (or classes)? **1.1.2. Organization:** Is the overall program flow easy to follow? Is it easy for an outsider to figure out how your software works? **1.1.3. Efficiency:** Do the individual methods accomplish their given tasks as efficiently as possible? Are unnecessary variables, loops, methods, and classes eliminated? **1.1.4. Coupling:** Are methods (and classes) "loosely coupled"? Does each method only receive the data it needs in order to accomplish its task? Are the "public" methods and variables appropriately so? Is information as hidden as possible? **1.2. Comments: 10%** · Every file should have a header that includes your name, CS2336.nnn, & the homework number. · Every class should have an extensive header comment explaining the purpose of the class. · Every method should have comments explaining what it does, what its parameters are, and what values it returns. · Significant variables and sections of code should have comments explaining their purpose. Avoid meaningless comments like "Declare the variables" or "This code adds one to the variable". **1.3. Coding Style: 15%** You should try to follow most of the coding standards for Java (see http://java.sun.com/docs/codeconv/), but these three are especially important: *Points Criteria* **1.3.1. Formatting:** Is code properly indented to indicate blocks? **1.3.2. Naming: I**s everything (significant variables, classes, methods) named logically and descriptively? (Not required for looping variables and throwaway variables.) **1.3.3. Capitalization:** · Package names are lowercase: java.io, java.net, etc. · Class (and interface) names should be nouns, with the first letter of each internal word capitalized: Loan, AmortizationTable, Person, HashMap · Method names should be verbs, with the first letter lowercase & the first letter of each internal word capitalized: run(), runFaster(), runForYourLife() · Constants should be in all upper-case, with words separated by an underscore, e.g.: `final int THIS_IS_A_CONSTANT = 1;` **2. Execution: (45%)** This section has to do with how well your program runs. If your program does not compile, please be aware that you may get no credit in this section.

	2.1. Program Execution: 15% *Points Criteria* **2.1.1. No crashes:** Does the program actually run all the way through the simplest possible test case without crashing? **2.1.2. Error Detection & Recovery:** Does the program react well (does not crash) to unexpected or inconsistent events or input? Are exceptions handled appropriately? **2.1.3. Efficiency:** Does the program finish executing in a reasonable amount of time? **2.2. Specification: 30%** This is really the most important part: does your program do what it is supposed to do? *Points Criteria* **2.2.1. Nominal case:** Does the software correctly fulfill the requirements of the assignment for the "expected" test cases? **2.2.2. Special cases:** Does the software correctly handle unusual but legal test cases? Example: square root of a negative number, interest payment higher than loan payment For assignments that seem arbitrarily restricted ("your program must save 4 runs", "your program must accept up to 10 names"), points will be not taken off as long as your program meets at least those requirements. You may exceed them without penalty. **3. Documentation (10%)** All assignments must be submitted with supporting documentation. At a minimum, this should include an algorithm report and a UML class diagram if you have more than a few classes. You should describe the overall flow of your program at least at a high level. If there are any parts of the program that are unusually complex, you should specify those parts in detail, using pseudocode or a flowchart.
Project	There will be **three** projects that will be posted in eLearning and should be turned in via **eLearning** ONLY. **No e-mail submissions are accepted**. **No late submissions are accepted.** Students can form groups of max. 3 students for the project. Group work is strongly encouraged. Please choose your own team mates. Each group should clearly indicate the firstname and lastname of students in the group. Each group should designate a group member to submit its project via eLearning. ONE SUBMISSION PER GROUP IS SUFFICIENT. **Ideally, members of each group should receive the same grade.** To ensure fairness, peer evaluations will be collected to reflect good/poor performance within each group. So, the members of the same group MAY NOT get the same grade due to peer evaluations. Students should form their groups by the end of week 2. Each group should hand in a **one page document** describing the group members and the delegated tasks for each member to the professor. The same grading policy that is used for the assignments applies to projects. Please see the "Assignments" category above to see the detailed grading policy. Each project due date is **specified in the syllabus**. Please note that the due date for the project cannot be extended.
Make-up Exams	

	A student can ONLY get a make up exam if it was missed due to an extreme emergency (proved by official documents), and arrangements are made BEFORE the exam date.
Extra Credit	No extra credit is offered.
Late Work	No late submission is accepted.
Class Attendance	Attendance will not be taken, but students are responsible for everything done and said in the class, such as detailed explanation of course slides, extra examples, etc. So, regular attendance will be beneficial to students.
Field Trip Policies	*Off-campus, out-of-state, and foreign instruction and activities are subject to state law and University policies and procedures regarding travel and risk-related activities. Information regarding these rules and regulations may be found at the website address http://www.utdallas.edu/BusinessAffairs/Travel_Risk_Activities.htm. Additional information is available from the office of the school Dean. Below is a description of any travel and/or risk related activity associated with this course.* No off-campus activities are scheduled.
Student Conduct and Discipline	The University of Texas System and The University of Texas at Dallas have rules and regulations for the orderly and efficient conduct of their business. It is the responsibility of each student and each student organization to be knowledgeable about the rules and regulations which govern student conduct and activities. General information on student conduct and discipline is contained in the UTD publication, *A to Z Guide*, which is provided to all registered students each academic year. The University of Texas at Dallas administers student discipline within the procedures of recognized and established due process. Procedures are defined and described in the *Rules and Regulations, Board of Regents, The University of Texas System, Part 1, Chapter VI, Section 3*, and in Title V, Rules on Student Services and Activities of the university's *Handbook of Operating Procedures*. Copies of these rules and regulations are available to students in the Office of the Dean of Students, where staff members are available to assist students in interpreting the rules and regulations (SU 1.602, 972/883-6391). A student at the university neither loses the rights nor escapes the responsibilities of citizenship. He or she is expected to obey federal, state, and local laws as well as the Regents' Rules, university regulations, and administrative rules. Students are subject to discipline for violating the standards of conduct whether such conduct takes place on or off campus, or whether civil or criminal penalties are also imposed for such conduct.
Academic Integrity	The faculty expects from its students a high level of responsibility and academic honesty. Because the value of an academic degree depends upon the absolute integrity of the work done by the student for that degree, it is imperative that a student demonstrate a high standard of individual honor in his or her scholastic work. Scholastic dishonesty includes, but is not limited to, statements, acts or omissions related to applications for enrollment or the award of a degree, and/or the submission

	as one's own work or material that is not one's own. As a general rule, scholastic dishonesty involves one of the following acts: cheating, plagiarism, collusion and/or falsifying academic records. Students suspected of academic dishonesty are subject to disciplinary proceedings. Plagiarism, especially from the web, from portions of papers for other classes, and from any other source is unacceptable and will be dealt with under the university's policy on plagiarism (see general catalog for details). This course will use the resources of turnitin.com, which searches the web for possible plagiarism and is over 90% effective. **Any student plagiarizing will fail the class with an "F" grade and WILL HAVE TO BE REPORTED TO the University of Texas at Dallas Dean of Students to initiate the academic dishonesty procedures as explained in "Student Discipline and Conduct - UTDSP5003" at** http://policy.utdallas.edu/utdsp5003**.**
Email Use	**To protect privacy of students, e-mail communication will not involve discussions of specific grade information. If you would like to discuss your grades, you can do so either in class, or during office hours.** The University of Texas at Dallas recognizes the value and efficiency of communication between faculty/staff and students through electronic mail. At the same time, email raises some issues concerning security and the identity of each individual in an email exchange. The university encourages all official student email correspondence be sent only to a student's U.T. Dallas email address and that faculty and staff consider email from students official only if it originates from a UTD student account. This allows the university to maintain a high degree of confidence in the identity of all individual corresponding and the security of the transmitted information. UTD furnishes each student with a free email account that is to be used in all communication with university personnel. The Department of Information Resources at U.T. Dallas provides a method for students to have their U.T. Dallas mail forwarded to other accounts.
Withdrawal from Class	The administration of this institution has set deadlines for withdrawal of any college-level courses. These dates and times are published in that semester's course catalog. Administration procedures must be followed. It is the student's responsibility to handle withdrawal requirements from any class. In other words, I cannot drop or withdraw any student. You must do the proper paperwork to ensure that you will not receive a final grade of "F" in a course if you choose not to attend the class once you are enrolled.
Student Grievance Procedures	Procedures for student grievances are found in Title V, Rules on Student Services and Activities, of the university's *Handbook of Operating Procedures*. In attempting to resolve any student grievance regarding grades, evaluations, or other fulfillments of academic responsibility, it is the obligation of the student first to make a serious effort to resolve the matter with the instructor, supervisor, administrator, or committee with whom the grievance originates (hereafter called "the respondent"). Individual faculty members retain primary responsibility for assigning grades and evaluations. If the matter cannot be resolved at that level, the grievance must be submitted in writing to the respondent with a copy of the respondent's School Dean. If the matter is not resolved by the written response provided by the respondent, the

	student may submit a written appeal to the School Dean. If the grievance is not resolved by the School Dean's decision, the student may make a written appeal to the Dean of Graduate or Undergraduate Education, and the deal will appoint and convene an Academic Appeals Panel. The decision of the Academic Appeals Panel is final. The results of the academic appeals process will be distributed to all involved parties. Copies of these rules and regulations are available to students in the Office of the Dean of Students, where staff members are available to assist students in interpreting the rules and regulations.
Incomplete Grades	As per university policy, incomplete grades will be granted only for work unavoidably missed at the semester's end and only if 70% of the course work has been completed. An incomplete grade must be resolved within eight (8) weeks from the first day of the subsequent long semester. If the required work to complete the course and to remove the incomplete grade is not submitted by the specified deadline, the incomplete grade is changed automatically to a grade of **F**.
Disability Services	The goal of Disability Services is to provide students with disabilities educational opportunities equal to those of their non-disabled peers. Disability Services is located in room 1.610 in the Student Union. Office hours are Monday and Thursday, 8:30 a.m. to 6:30 p.m.; Tuesday and Wednesday, 8:30 a.m. to 7:30 p.m.; and Friday, 8:30 a.m. to 5:30 p.m. The contact information for the Office of Disability Services is: The University of Texas at Dallas, SU 22 PO Box 830688 Richardson, Texas 75083-0688 (972) 883-2098 (voice or TTY) Essentially, the law requires that colleges and universities make those reasonable adjustments necessary to eliminate discrimination on the basis of disability. For example, it may be necessary to remove classroom prohibitions against tape recorders or animals (in the case of dog guides) for students who are blind. Occasionally an assignment requirement may be substituted (for example, a research paper versus an oral presentation for a student who is hearing impaired). Classes enrolled students with mobility impairments may have to be rescheduled in accessible facilities. The college or university may need to provide special services such as registration, note-taking, or mobility assistance. It is the student's responsibility to notify his or her professors of the need for such an accommodation. Disability Services provides students with letters to present to faculty members to verify that the student has a disability and needs accommodations. Individuals requiring special accommodation should contact the professor after class or during office hours.
Religious Holy Days	The University of Texas at Dallas will excuse a student from class or other required activities for the travel to and observance of a religious holy day for a religion whose places of worship are exempt from property tax under Section 11.20, Tax Code, Texas Code Annotated. The student is encouraged to notify the instructor or activity sponsor as soon as

	possible regarding the absence, preferably in advance of the assignment. The student, so excused, will be allowed to take the exam or complete the assignment within a reasonable time after the absence: a period equal to the length of the absence, up to a maximum of one week. A student who notifies the instructor and completes any missed exam or assignment may not be penalized for the absence. A student who fails to complete the exam or assignment within the prescribed period may receive a failing grade for that exam or assignment. If a student or an instructor disagrees about the nature of the absence [i.e., for the purpose of observing a religious holy day] or if there is similar disagreement about whether the student has been given a reasonable time to complete any missed assignments or examinations, either the student or the instructor may request a ruling from the chief executive officer of the institution, or his or her designee. The chief executive officer or designee must take into account the legislative intent of TEC 51.911(b), and the student and instructor will abide by the decision of the chief executive officer or designee.
Off-Campus Instruction and Course Activities	Off-campus, out-of-state, and foreign instruction and activities are subject to state law and University policies and procedures regarding travel and risk-related activities. Information regarding these rules and regulations may be found at http://www.utdallas.edu/BusinessAffairs/Travel_Risk_Activities.htm. Additional information is available from the office of the school dean.

These descriptions and timelines are subject to change at the discretion of the Professor.