CSE 6388-001: Special Topics in Information Security – Advance Software Security Analysis
Spring 2019

Instructor Information:

Instructor:	Jiang Ming	GTAs:	
Email:	jiang.ming@uta.edu	Email:	
Office:	ERB 528	Office:	ERB 316
Phone:	(817) 272-0906	Office Phone:	
Office Hours:	Friday 10:30-12:00 PM	Office Hours:	Wed 2:30-4:00 PM
Faculty Profile:	https://www.uta.edu/profiles/jiang-ming	Class Website:	https://elearn.uta.edu

Section Info:	CSE 6388, Section 001
Meeting Times:	Tu/Th 17:30-18:50
Location:	SH 125

Course Description:

This course provides hands-on research training in software security analysis, with a special focus on binary code analysis (e.g., disassembly and data structure reverse engineering), software diversity, symbolic execution, malware unpacking, hardware-assisted malware detection, return-oriented programming: exploitation without code injection, and IoT firmware security. More specifically, the course is structured as a seminar where students jointly present (with the instructor) research papers to their peers. Students will present research papers, write critically about research papers, and conduct a semester-long research project.

In each class, we will discuss 1–2 research papers. Students are expected to read the assigned papers and write a short review (critique) before each class. In addition, one student will do a short presentation about each paper for the day, which will be the starting point for our discussions.

Course Objectives: By the end of the course, students should be able to:

- Identify the elements of good research papers in software security.
- Locate good research papers on a specific topic.
- Identify the contributions, strengths, and limitations of a research paper.
- Generate research ideas based on the relevant literature.
- Develop a plan for exploring a research idea.
- Execute a research plan.
- Write about research findings.
- Present research ideas and findings to an audience.
- Intelligently discuss several of the major research topics in software security.

Prerequisites:

CSE 5380 – Information Security I; CSE 5381 – Information Security II; CSE 5382 – Secure Programming

Required Textbooks and Other Course Materials: None

Note: The instructor reserves the right to modify course policies, the course calendar, and assignment or project point values and due dates.

Course Grades:

Course grades will be based on the following:

Research Paper Presentation: 50%
Class Discussions: 25%
Research Project: 25%

Research Paper Presentations: Each student will be presenting a (set of) research paper(s) to the class, and evaluated based on the following criteria:

1. **Understanding**: Does the presenter understand the material?
2. **Thoughtfulness**: Does the presenter have insights and opinions beyond what was in the paper?
3. **Clarity**: Can the audience understand the presentation? Is the "big picture" clear? Are there useful examples?

4. **Materials**: Do the slides or use of blackboard illustrate and support the talk? Are there diagrams to help convey the technicalities?
5. **Delivery**: Has the presenter practiced?
6. **Non-regurgitation**: Did the presenter do something beyond simply typing sections of the paper as bullet points? Did the presenter motivate the ideas in their own words, or just state ideas from the paper verbatim?
7. **Answering questions**: Can the presenter handle questions from the audience?

Grades for Exams will be curved by the instructor and scaled to a standard A = 90-100, B = 80-89, C = 70-79 scale. Final grades will simply be the weighted average of the scores, based on the percentages shown above. Small amounts of extra credit may be available, but only on a class-wide basis (no individual requests will be granted). **No grade bumps will be offered; 89.99 is a B in this class.**

Make-ups: Make-ups for graded activities may be arranged if your absence is caused by illness or personal emergency. A written explanation (including supporting documentation) must be submitted to your instructor; if the explanation is acceptable, an alternative to the graded activity will be arranged. Make-up arrangements must be arranged prior to the scheduled due date.

Class Attendance Policy: At The University of Texas at Arlington, taking attendance is not required. Rather, each faculty member is free to develop his or her own methods of evaluating students' academic performance, which includes establishing course-specific policies on attendance. As the instructor of this section, I will be grading attendance based on your participation in each lecture. Also, in every class period, you will learn by actively participating in the process of solving problems and working in small groups. Missing class, therefore, means missing out on learning opportunities that cannot be gained from the textbook.

Paper reading assignments with dates:

1. Jan. 17: Binary Code Disassembly
    a. ISSTA'16: Binary Code is Not Easy
    b. USENIX Security'16: An In-Depth Analysis of Disassembly on Full-Scale x86/x64 Binaries

2. Jan. 22: Data Structure Reverse Engineering
    a. NDSS'10: Automatic Reverse Engineering of Data Structures from Binary Execution
    b. NDSS'11: Howard: a Dynamic Excavator for Reverse Engineering Data Structures

3. Jan. 24: Function Recognition (1)
    a. USENIX Security'14: ByteWeight: Learning to Recognize Functions in Binary Code
    b. USENIX Security'15: Recognizing Functions in Binaries with Neural Networks

4. Jan. 29: Function Recognition (2)
    a. EuroS&P'17: Compiler-Agnostic Function Detection in Binaries
    b. ACSAC'18: Now You See Me: Real-time Dynamic Function Call Detection

5. Jan. 31: Data Type Detection
    a. NDSS'11: TIE: Principled Reverse Engineering of Types in Binary Programs
    b. USENIX Security'17: Neural Nets Can Learn Function Type Signatures from Binaries

6. Feb. 5: Static Binary Rewriting
    a. USENIX Security'15: Reassembleable Disassembling
    b. NDSS'17: Ramblr: Making Reassembly Great Again

7. Feb. 7: Software Diversity (1)
    a. S&P'14: SoK: Automated Software Diversity
    b. Layered Assurance Workshop 2016: Composition Challenges for Automated Software Diversity

8. Feb.12: Software Diversity (2)
    a. New Security Paradigms Workshop 2016: Searching for Software Diversity - Attaining Artificial Diversity through Program Synthesis
    b. ACM Workshop on Moving Target Defense 2018: Quantifying the Effectiveness of Software Diversity using Near-Duplicate Detection Algorithms

9. Feb.14: Symbolic Execution (1)
    a. OSDI'08: KLEE: Unassisted and Automatic Generation of High-Coverage Tests for Complex Systems Programs
    b. NDSS'08: Automated Whitebox Fuzz Testing

10. Feb. 19: Symbolic Execution (2)
    a. ASPLOS'11: S2E: A Platform for In-Vivo Multi-Path Analysis of Software Systems
    b. ICSE'13: Billions and Billions of Constraints: Whitebox Fuzz Testing in Production

11. Feb. 21: Return-oriented Programming: Exploitation without Code Injection (1)
    a. CCS'07: The Geometry of Innocent Flesh on the Bone: Return-into-libc without Function Calls (on the x86)
    b. USENIX Security'11: Q: Exploit Hardening Made Easy

12. Feb. 26: Return-oriented Programming (2)
    a. S&P'13: SoK: Eternal War in Memory
    b. S&P'13: Just-In-Time Code Reuse: On the Effectiveness of Fine-Grained Address Space Layout Randomization

13. Feb. 28: Return-oriented Programming (3)
    a. NDSS'15: Isomeron: Code Randomization Resilient to (Just-In- Time) Return-Oriented Programming
    b. S&P'16: Return to the Zombie Gadgets: Undermining Destructive Code Reads via Code Inference Attacks

14. Mar. 5: Return-oriented Programming (4)
    a. Euro S&P'17: CodeArmor: Virtualizing the Code Space to Counter Disclosure Attacks.
    b. CCS'17: The Dynamics of Innocent Flesh on the Bone: Code Reuse Ten Years Later

15. Mar. 7: Software Debloating
    a. USENIX Security'18: Debloating Software through Piece-Wise Compilation and Loading
    b. CCS'18: Effective Program Debloating via Reinforcement Learning

16. Mar. 19: Malware Unpacking
    a. S&P'15: SoK: Deep Packer Inspection: A Longitudinal Study of the Complexity of Run-Time Packers
    b. CCS'18: Towards Paving the Way for Large-Scale Windows Malware Analysis: Generic Binary Unpacking with Orders-of-Magnitude Performance Boost

17. Mar. 21: Using Hardware Performance Counters for Security (1): Malware Detection
    a. ISCA'13: On the Feasibility of Online Malware Detection with Performance Counters
    b. RAID'14: Unsupervised Anomaly-Based Malware Detection Using Hardware Features Erika Leal

18. Mar. 26: Using Hardware Performance Counters for Security (2): ROP Mitigation
    a. USENIX Security'13: Transparent ROP Exploit Mitigation Using Indirect Branch Tracing
    b. SIGDROP: Signature-based ROP Detection using Hardware Performance Counters

19. Mar. 28: Using Hardware Performance Counters for Security (3): Rootkits Detection
    a. DAC'13: NumChecker: Detecting Kernel Control-Flow Modifying Rootkits by Using Hardware Performance Counters.
    b. AsiaCCS'17: On the Detection of Kernel-Level Rootkits Using Hardware Performance Counters

20. Apr. 2: Using Hardware Performance Counters for Security (4): Myth or Fact?
    a. AsiaCCS'18: Hardware Performance Counters Can Detect Malware: Myth or Fact?
    b. S&P'19: SoK: The Challenges, Pitfalls, and Perils of Using Hardware Performance Counters for Security

21. Apr. 4: IoT Security (1): Towards Automated Firmware Dynamic Analysis
    a. Workshop on Binary Analysis Research 2018: Avatar^2: A Multi-Target Orchestration Platform
    b. NDSS'16: Towards Automated Dynamic Analysis for Linux-based Embedded Firmware

22. Apr. 9: IoT Security (2): Fuzzing in IoT Devices
    a. NDSS'18: IOTFUZZER: Discovering Memory Corruptions in IoT Through App-based Fuzzing
    b. NDSS'18: What You Corrupt Is Not What You Crash:Challenges in Fuzzing Embedded Devices

23. Apr. 11: IoT Security (3): Vulnerability Detection
    a. NDSS'15: Firmalice - Automatic Detection of Authentication Bypass Vulnerabilities in Binary Firmware
    b. CCS'17: FirmUSB: Vetting USB Device Firmware using Domain Informed Symbolic Execution

24. Apr. 16: IoT Security (4): Vulnerability Search
    a. ASPLOS'18: FirmUp: Precise Static Detection of Common Vulnerabilities in Firmware
    b. CCS'17: Neural Network-based Graph Embedding for Cross-Platform Binary Code Similarity Detection

25. Apr. 18: IoT Security (5): Device Drivers and Security Testing
    a. USENIX Security'18: Charm: Facilitating Dynamic Analysis of Device Drivers of Mobile Systems
    b. USENIX Security'18: Inception: System-Wide Security Testing of Real-World Embedded Systems Software

26. Apr. 23: IoT Security (6): ZigBee Protocol
    a. S&P'17: IoT Goes Nuclear: Creating a ZigBee Chain Reaction
    b. WiSec '17: Insecure to the touch: attacking ZigBee 3.0 via touchlink commissioning

27. Apr. 25: IoT Security (7): Smart Home
    a. CCS'18: HoMonit: Monitoring Smart Home Apps from Encrypted Traffic
    b. S&P'19: SoK: Security Evaluation of Home-Based IoT Deployments

Course Schedule (Subject to Change):

Week	*Class Dates*	*Topic*
1.	Jan. 15 & 17	Class Intro + Binary Code Disassembly
2.	Jan. 22 & 24	Data Structure Reverse Engineering + Function Recognition (1)
3.	Jan. 29 & 31	Function Recognition (2) + Data Type Detection
4.	Feb. 5 & 7	Static Binary Rewriting + Software Diversity (1)
5.	Feb. 12 & 14	Software Diversity (2) + Symbolic Execution (1)
6.	Feb. 19 & 21	Symbolic Execution (2) + Return-oriented Programming (1)
7.	Feb. 26 & 28	Return-oriented Programming (2,3)
8.	Mar. 5 & 7	Return-oriented Programming (4) + Software Debloating
9.	Mar.12 & 14	**Spring Break**
10.	Mar.19 & 21	Malware Unpacking + HPC for Security (1)
11.	Mar.26 & 28	HPC for Security (2, 3)
12.	Apr. 2 & 4	HPC for Security (4) + Automated Firmware Dynamic Analysis
13.	Apr. 9 & 11	Fuzzing in IoT Devices + Vulnerability Detection
14.	Apr. 16 & 18	Firmware Vulnerability Search + Security Testing
15.	Apr. 23 & 25	ZigBee Protocol + Smart Home

As the instructor for this course, I reserve the right to adjust this schedule in any way that serves the educational needs of the students enrolled in this course. –Jiang Ming

Drop Policy: Students may drop or swap (adding and dropping a class concurrently) classes through self-service in MyMav from the beginning of the registration period through the late registration period. After the late registration period, students must see their academic advisor to drop a class or withdraw. Undeclared students must see an advisor in the University Advising Center. Drops can continue through a point two-thirds of the way through the term or session. It is the student's responsibility to officially withdraw if they do not plan to attend after registering. **Students will not be automatically dropped for non-attendance.** Repayment of certain types of financial aid administered through the University may be required as the result of dropping classes or withdrawing. For more information, contact the Office of Financial Aid and Scholarships (http://wweb.uta.edu/aao/fao/).

Disability Accommodations: UT Arlington is on record as being committed to both the spirit and letter of all federal equal opportunity legislation, including *The Americans with Disabilities Act (ADA), The Americans with Disabilities Amendments Act (ADAAA), and Section 504 of the Rehabilitation Act*. All instructors at UT Arlington are required by law to provide "reasonable accommodations" to students with disabilities, so as not to discriminate on the basis of disability. Students are responsible for providing the instructor with official notification in the form of a letter certified by the **Office for Students with Disabilities (OSD)**.

Students experiencing a range of conditions (Physical, Learning, Chronic Health, Mental Health, and Sensory) that may cause diminished academic performance or other barriers to learning may seek services and/or accommodations by contacting:

The Office for Students with Disabilities, (OSD) www.uta.edu/disability or calling 817-272-3364.
Counseling and Psychological Services, (CAPS) www.uta.edu/caps/ or calling 817-272-3671.

Only those students who have officially documented a need for an accommodation will have their request honored. Information regarding diagnostic criteria and policies for obtaining disability-based academic accommodations can be found at www.uta.edu/disability or by calling the Office for Students with Disabilities at (817) 272-3364.

Title IX: *The University of Texas at Arlington does not discriminate on the basis of race, color, national origin, religion, age, gender, sexual orientation, disabilities, genetic information, and/or veteran status in its educational programs or activities it operates. For more information, visit www.uta.edu/eos. or information regarding Title IX, visit www.uta.edu/titleIX.*

Academic Integrity: Students enrolled all UT Arlington courses are expected to adhere to the UT Arlington Honor Code:

I pledge, on my honor, to uphold UT Arlington's tradition of academic integrity, a tradition that values hard work and honest effort in the pursuit of academic excellence.

I promise that I will submit only work that I personally create or contribute to group collaborations, and I will appropriately reference any work from other sources. I will follow the highest standards of integrity and uphold the spirit of the Honor Code.

UT Arlington faculty members may employ the Honor Code as they see fit in their courses, including (but not limited to) having students acknowledge the honor code as part of an examination or requiring students to incorporate the honor code into any work submitted. Per UT System Regents' Rule 50101, §2.2, suspected violations of university's standards for academic integrity (including the Honor Code) will be referred to the Office of Student Conduct. Violators will be disciplined in accordance with University policy, which may result in the student's suspension or expulsion from the University.

Additionally, there is a special ethics form for this course about malicious hacking that you must sign and uphold.

Student Support Services Available: The University of Texas at Arlington provides a variety of resources and programs designed to help students develop academic skills, deal with personal situations, and better understand concepts and information related to their courses. These resources include tutoring, major-based learning centers, developmental education, advising and mentoring, personal counseling, and federally funded programs. For individualized referrals to resources for any reason, students may contact the Maverick Resource Hotline at 817-272-6107 or visit http://www.uta.edu/resources for more information.

Electronic Communication: UT Arlington has adopted MavMail as its official means to communicate with students about important deadlines and events, as well as to transact university-related business regarding financial aid, tuition, grades, graduation, etc. All students are assigned a MavMail account and are responsible for checking the inbox regularly. There is no additional charge to students for using this account, which remains active even after graduation. Information about activating and using MavMail is available at: http://www.uta.edu/oit/cs/email/mavmail.php.

Students will be given accounts for the ASCENT security-teaching lab. All students are expected to be responsible users of the computer systems used for this course. In particular, students are expected to abide by the code of ethics associated with this course.

Student Feedback Survey: At the end of each term, students enrolled in classes categorized as "lecture," "seminar," or "laboratory" shall be directed to complete an online Student Feedback Survey (SFS). Instructions on how to access the SFS for this course will be sent directly to each student through MavMail approximately 10 days before the end of the term. Each student's feedback enters the SFS database anonymously and is aggregated with that of other students enrolled in the course. UT Arlington's effort to solicit, gather, tabulate, and publish student feedback is required by state law; students are strongly urged to participate. For more information, visit http://www.uta.edu/sfs.

Final Review Week: A period of five class days prior to the first day of final examinations in the long sessions shall be designated as Final Review Week. The purpose of this week is to allow students sufficient time to prepare for final examinations. During this week, there shall be no scheduled activities such as required field trips or performances; and no instructor shall assign any themes, research problems or exercises of similar scope that have a completion date during or following this week *unless specified in the class syllabus*. During Final Review Week, an instructor shall not give any examinations constituting 10% or more of the final grade,

except makeup tests and laboratory examinations. In addition, no instructor shall give any portion of the final examination during Final Review Week. During this week, classes are held as scheduled. In addition, instructors are not required to limit content to topics that have been previously covered; they may introduce new concepts as appropriate.

Emergency Exit Procedures: Should we experience an emergency event that requires us to vacate the building, students should exit the room and move toward the nearest exit, which is right in front of you when you exit the classroom. When exiting the building during an emergency, one should never take an elevator but should use the stairwells. Faculty members and instructional staff will assist students in selecting the safest route for evacuation and will make arrangements to assist individuals with disabilities.

Student Support Services: UT Arlington provides a variety of resources and programs designed to help students develop academic skills, deal with personal situations, and better understand concepts and information related to their courses. Resources include tutoring, major-based learning centers, developmental education, advising and mentoring, personal counseling, and federally funded programs. For individualized referrals, students may visit the reception desk at University College (Ransom Hall), call the Maverick Resource Hotline at 817-272-6107, send a message to resources@uta.edu, or view the information at: http://www.uta.edu/universitycollege/resources/index.php

Emergency Phone Numbers: In case of an on-campus emergency, call the UT Arlington Police Department at **817-272-3003** (non-campus phone), **2-3003** (campus phone). You may also dial **911**. Non-emergency number 817-272-3381.