CS 4379/5375

Software Reverse Engineering

This course focuses on incorporating security technologies and methods into new and existing systems; learning how attackers expose vulnerabilities; analyzing threats; applying methods to prevent and defeat attacks; and understanding the ethical responsibilities and obligations associated with developing, acquiring, and operating software systems.

Course URL:

http://cs5375.cs.utep.edu/

Office Hours:

M, W, 10:00am-11:30am @ ~~CCSB, G.0512~~ Prospect Hall, 122

Instructor:

- Dr. Jaime C. Acosta
  Office: Chemistry and Computer Science Building 3.1018
  Email: jcacosta@utep.edu

TA:

- Alberto Morales
  Office: Prospect Hall, SFS Laboratory
  Email: admorales3@miners.utep.edu

Class location and time:

The course codes are CRN 16204/16205 for CS4379/CS5375 respectively. Class will be held in the Chemistry and Computer Science Building, Room CCSB G.0208 on Thursdays from 6:00pm to 8:50pm.

Course materials:

This course does not require the purchase of a textbook; all resource material will be posted on the course website. Much of the material from this course will derive from the following books:

- Eldad Eilam, *Reversing: Secrets of Reverse Engineering*. Wiley, 2005.
- Stuart McClure, Joel Scambray, George Kurtz, *Hacking Exposed 7: Network Security Secrets and Solutions, Seventh Edition*. McGraw-Hill Osborne Media, 2012
- Michael Sikorski and Andrew Honig, *Practical Malware Analysis*. No Starch Press, 2012.

Students should have access to a personal computer with administrative privileges.

Learning Outcomes:

Level 3: Synthesis and Evaluation (Level 3 outcomes are those in which the students can apply the material in new situations. This is the highest level of mastery.) Upon successful completion of this course, students will be able to:

- Explain the variety of methods by which attackers can damage software or data associated with software via weaknesses in the design or coding of the system at the assembly level.
- Analyze threats to software systems.
- Analyze threats to operational environments.
- Design and plan for effective countermeasures such as access control, authentication, intrusion detection, encryption, and coding checklists.

Level 2: Application and Analysis (Level 2 outcomes are those in which the student can apply the material in familiar situations, e.g., can work a problem of familiar structure with minor changes in the details.) Upon successful completion of this course, students will be able to:

- Deploy appropriate countermeasures, such as layers, access controls, privileges, intrusion detection, encryption, and coding checklists.
- Explain how adversaries are able to identify vulnerabilities and generate exploits for public and private software systems.
- Detect data exfiltration activities and conduct detailed analysis to describe the malignant logic and potential impacts.

Level 1: Knowledge and Comprehension (Level 1 outcomes are those in which the student has been exposed to the terms and concepts at a basic level and can supply basic definitions.) The material has been presented only at a superficial level. Upon successful completion of this course, students will be able to:

- Describe the types of safety and security risks associated with network infrastructures.

Course Policies:

- Homework assignments are due at the beginning of the class, unless specified otherwise.
- Assignments may be discussed with others, but solutions must be designed, written, and tested by you or, in the case of group assignments, by your group.
- No make-up exams or assignments will be given except under extreme conditions.
- It is the student's responsibility to independently cover any material missed.

Grades:

Assignments	40%
Tests	25%
Final Exam	30%
Participation	5%

Final letter grades will be assigned as follows:

A = 90% through 100%
B = 80% through 89%
C = 70% through 79%
D = 60% through 69%
F = Less than 60%

Submission of late work:

All assignments are due at the beginning of class. Late work will be accepted at most two days late, unless specified by the instructor, and will be marked down two letter grades. After two days the assignment will not be accepted.

Standards of Conduct and Academic Dishonesty

You are expected to conduct yourself in a professional and courteous manner, as prescribed by the UTEP Standards of Conduct: http://admin.utep.edu/Default.aspx?PageContentID=2237&tabid=30295
Academic dishonesty includes but is not limited to cheating, plagiarism and collusion. Cheating may involve copying from or providing information to another student, possessing unauthorized materials during a test, or falsifying data (for example program outputs) in laboratory reports. Plagiarism occurs when someone represents the work or ideas of another person as his/her own. Collusion involves collaborating with another person to commit an academically dishonest act. Professors are required to - and will - report academic dishonesty and any other violation of the Standards of Conduct to the Dean of Students.

When in doubt, please ask. On exams you must submit your own work and you may not give or receive help. On assignments you must submit your own work. Submissions that are "identical" will be considered as a clear evidence of cheating.

Students with Disabilities

In accordance with the UTEP procedure, if you need accommodations for equal access in this course, please do the followings:

- Contact Disabled Student Service Office (DSSO) (915) 747-5148 to verify your eligibility.
- Contact me before or at the beginning of the first class to discuss your individual needs for accommodations, with an official letter of accommodation or other documents.

Ethics and Security Vulnerabilities:

During this course, you will learn skills used by professional security evaluators to identify and remediate vulnerabilities. Tampering with systems and exploiting vulnerabilities without written consent has severe consequences including academic suspension and legal prosecution and could prevent you from ever working in your field of study.

In two words: **act responsibly!**

Tentative Schedule:

	Topics Covered	Assignments
Week 1	Course Introduction/Legal	
Week 2	Reverse Engineering IA-32 and Common Tools	A. Reversing Introduction B. Low-level analysis C. IA-32 Stack D. Static Disassembly
Week 3		
Week 4	Application-level Vulnerabilities	E. Stack Vulnerabilities F. IA-32 Heap G. Dynamic Debugging H. Heap Vulnerabilities
Week 5		
Week 6	OS-level Vulnerabilities	I. DLL Injection J. Process Injection Theory K. Process Injection Implementation L. Authentication/Authorization M. Credentials Management
Week 7	Test	
Week 8	Malware	N. Malware Categories O. Malware Obfuscation
Week 9		
Week 10	Secure Software Development	P. Secure Coding
Week 11	Test	
Week 12	Networking and Attacks	Q. Telecommunications Intro R. Routing S. Remote Exploitation
Week 13	Cyber Defense	T. Network Defenses
Week 14	Malware Forensics	U. Advanced Persistent Threat
Week 15		
Week 16	Graduate Student Presentations	
Week 17	Final Exam	

Graduate Students

Students in the CS5375 section will have an additional class project that entails reading a recent and relevant research paper, writing a synopsis, and presenting it to the class in the form of a 20 minute presentation. In addition, these students will also present a demonstration of a technology, methodology, or approach that comes directly from research paper or from a related source. This will also be presented to the class.