TEXAS A&M UNIVERSITY

SYLLABUS

Course title and number	CSCE 489/689: Special Topics in Software Security
Term	Fall 2017
Meeting times and location	MWF 10:20am – 11:10am in HRBB 105

Instructor Information	
Name	Philip Ritchey
Telephone number	(979) 458-1059
Email address	pcr@tamu.edu
Office hours	MWF 8am – 9am, MW 4pm – 6pm, and by appointment
Office location	HRBB 326

Course Description and Prerequisites

Defects in software are sources of vulnerabilities, which in turn are the avenues used by attackers to create and deploy exploits against software. Software defects occur along a continuum between the implementation-level and the design-level. Implementation defects, or bugs, are errors in the source code of software that can result in undefined or incorrect behavior. Design defects, or flaws, are errors in the architecture of software. Software with a flaw will have vulnerabilities even when it is implemented exactly as designed.

This course covers basic principles of design and implementation of defect-free software, code reviews including tool-assisted review by static and dynamic analysis, risk analysis and management, and methods for software security testing.

Prerequisites: CSCE 315 or approval of instructor.

Learning Outcomes

Students will be able to…
list the first principles of security and **explain** why each is important to security and how it enables the development of security mechanisms that can implement desired security policies.
identify specific principles that have been violated in common security failures.
identify appropriate design principles to apply in a given software development scenario.
explain the interaction between security and system usability and importance of human-computer interfaces to system usability.
explain the importance of secure software and the programming practices, development processes, and methodologies that lead to secure software.
explain techniques for specifying program behavior, the classes of well-known defects, and how they manifest themselves in various languages.
perform penetration testing on previously unknown software.
analyze existing source code for functional correctness.
analyze software for defects using industry standard tools.
develop test cases that demonstrate the existence of defects.
develop defect-free software components that satisfy their functional requirements.

Textbooks	
Required:	24 Deadly Sins of Software Security: Programming Flaws and How to Fix Them, Howard, LeBlanc, Viega. ISBN-13: 978-0-07-162675-0.
	Software Security: Building Security In. McGraw. ISBN-13: 978-0-321-35670-3
Recommended:	Secure Coding in C and C++, Seacord, 2nd edition. ISBN-13: 978-0-321-82213-0.

Supplementary Material
All You Ever Wanted to Know About Dynamic Taint Analysis and Forward Symbolic Execution (but might have been afraid to ask). https://edmcman.github.io/papers/oakland10.pdf
Avoiding the Top 10 Software Security Design Flaws. https://www.computer.org/cms/CYBSI/docs/Top-10-Flaws.pdf
Best Kept Secrets of Peer Code Review. http://smartbear.com/SmartBear/media/pdfs/best-kept-secrets-of-peer-code-review.pdf
Build It, Break It, Fix It. https://builditbreakit.org
Burp Suite. https://portswigger.net/burp/
CERT Secure Coding Standards. https://www.securecoding.cert.org
Coverity Scan. https://scan.coverity.com
Crackstation. https://crackstation.net
CWE/SANS Top 25 Most Dangerous Software Errors. https://www.sans.org/top25-software-errors
Damn Vulnerable Web App. http://www.dvwa.co.uk
IEEE Cybersecurity Initiative. http://cybersecurity.ieee.org/
KLEE. https://klee.github.io
List of Static Analysis Tools. https://en.wikipedia.org/wiki/List_of_tools_for_static_code_analysis
Microsoft Security Development Lifecycle. https://www.microsoft.com/sdl
Microsoft Trustworthy Computing Security Development Lifecycle. https://msdn.microsoft.com/en-us/library/ms995349.aspx
NIST Computer Security Resource Center. http://csrc.nist.gov
Offensive Security. https://www.offensive-security.com
Open Web Application Security Project (OWASP). https://www.owasp.org
SANS Secure Coding Reading Room. https://www.sans.org/reading-room/whitepapers/securecode
Secure Programming HOWTO. http://www.dwheeler.com/secure-programs
Security Engineering: A Guide to Building Dependable Distributed Systems. https://www.cl.cam.ac.uk/~rja14/book.html
Smashing the Stack for Fun and Profit. http://phrack.org/issues/49/14.html#article
Symbolic Execution for Finding Bugs. https://www.cs.umd.edu/~mwh/se-tutorial/symbolic-exec.pdf
The Protection of Information in Computer Systems. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1451869&isnumber=31196
US-CERT – Build Security In. https://buildsecurityin.us-cert.gov
Ware Report. http://www.rand.org/pubs/reports/R609-1/index2.html
WebGoat. https://github.com/WebGoat/WebGoat/releases

489 Grading		
Weight	*Component*	*Date*
10%	Participation	Weekly
30%	Homework	Tentative: 22 September, 20 October, 17 November
10%	Presentation	As a group, at least once during the semester
50%	Project	Tentative: 13 October, 27 October, 3 November
Final letter grades will be assigned according to the following cutoffs:		
90+:	A	
80:	B	
70:	C	
60:	D	
Less than 60:	F	

689 Grading		
Weight	*Component*	*Date*
30%	Homework	Tentative: 22 September, 20 October, 17 November
20%	Presentations	Twice during the semester
10%	Annotation Project	8 December
40%	Project	Tentative: 13 October, 27 October, 3 November
Final letter grades will be assigned according to the following ratings:		
Superior	A	
Satisfactory	B	
Needs Improvement	C	
Unsatisfactory	D	
Did Not Participate	F	

Students are expected to read and provide a written summary of an academic article during the course. They are also expected to give a 15-minute presentation on their selected paper to the class. Students enrolled in CSCE 689 are expected to do this twice.

The annotation project is an opportunity for students in CSCE 689 to explore a topic in software security in greater depth. Students will read a *classic* paper related to software security, and annotate that paper to make it accessible to a broader audience. More specifically, the annotation will give an in-depth account of the historical context of the work along with biographical accounts into the private lives of the author (or authors). The annotation should also help the reader understand the magnitude of the paper's impact on the field of security. Finally, where appropriate, the annotation should include personal thoughts.

Tentative Schedule of Topics

Day	*Topic*
8/28/2017	Introduction and Course Overview
8/30/2017	Foundational Concepts in Security
9/1/2017	Paper Presentation - Ritchey
9/4/2017	Principles of Secure Design I
9/6/2017	Principles of Secure Design II
9/8/2017	Paper Presentation - Ritchey
9/11/2017	A Risk Management Framework
9/13/2017	Input Validation and Data Sanitization
9/15/2017	Paper Presentations - Students
9/18/2017	Overruns and Overflows
9/20/2017	Exceptions and Error Handling
9/22/2017	Paper Presentations - Students
9/25/2017	Leakage
9/27/2017	Race Conditions
9/29/2017	Paper Presentations - Students
10/2/2017	A Taxonomy of Coding Errors
10/4/2017	Common Bugs and Flaws
10/6/2017	Project Workday
10/9/2017	Software Security Touchpoints
10/11/2017	Code Review I: Peer
10/13/2017	Project Workday
10/16/2017	Code Review II: Static Analysis
10/18/2017	Code Review III: Dynamic Analysis
10/20/2017	Project Workday
10/23/2017	Architectural Risk Analysis
10/25/2017	Penetration Testing I
10/27/2017	Project Workday
10/30/2017	Penetration Testing II
11/1/2017	Fuzzing
11/3/2017	Project Workday
11/6/2017	Risk-Based Security Testing
11/8/2017	Cryptographic Sins
11/10/2017	Paper Presentations - Students
11/13/2017	Abuse Cases
11/15/2017	Networking Sins
11/17/2017	Paper Presentations - Students
11/20/2017	Security Requirements and Operations
11/22/2017	No Class (Thanksgiving Break)
11/24/2017	No Class (Thanksgiving Break)
11/27/2017	Special Topic: TBD
11/29/2017	Special Topic: TBD
12/1/2017	Paper Presentations - Students
12/4/2017	Special Topic: TBD
12/6/2017	Special Topic: TBD
12/12/2017	8:00am – 10:00am Final Exam Time Reserved

Policies

Attendance Policy
You are strongly encouraged to attend every class, arrive on time, and stay the whole time. You are responsible for learning the material covered in class regardless of your attendance.

Typesetting
All written (i.e. non-coding) homework must be typed.
You are strongly encouraged to typeset your work using LaTeX.
Resources for LaTeX can be found on the course website and on the Internet.
Microsoft Word and OpenOffice Write are acceptable, yet vastly inferior, alternatives.

Late and Missed Work
Late submissions of homework and projects are not accepted.
Exams and other in-class work can be made up in the event of a documented University Excused Absence. See rule 07 of the student rules: https://student-rules.tamu.edu/rule07.

Version Control
You are strongly encouraged to use a version control system to track changes and back up your work. Texas A&M has an institutional GitHub account (https://github.tamu.edu) that you can use. Aside from Git, other free options for version control include SVN, CVS, Mercurial, and Perforce.

Submission to eCampus
All homework and projects will be submitted to eCampus (https://ecampus.tamu.edu). Written assignments must be submitted as PDFs. Submission of source code must follow the instructions in the homework or project specifications.

Piazza
All questions and comments about the course should be posted on Piazza (https://piazza.com). Piazza is designed and managed so that you can get help quickly and efficiently from classmates, the PTs, the graders, the TAs, and me. If you email a question or comment about the course to me or a TA, you will very likely be redirected to Piazza. You may post questions or comments to the instructors on Piazza privately, however this privilege will be revoked if it is misused.

Email Formatting
When you send email to me or a TA, the subject must be prefixed with [CSCE 489/689] and you must sign your name to the email. Putting [CSCE 489/689] in the subject will let us know in which course of ours you are enrolled. Signing your name will let us know who you are. If you do not sign your name, we may assign you one at random in our reply. You are encouraged to encrypt and sign all emails to me. My PGP public key is on my home page and the MIT key server (https://pgp.mit.edu).

Discussion of Grades
Federal law prohibits the instructor, TAs, and graders from discussing grades over email or phone. If you have a question about your grade, you must discuss it with us in-person, such as during office hours.

Harassment and Discrimination
Texas A&M is committed to the fundamental principles of academic freedom, equality of opportunity and human dignity. To fulfill its multiple missions as an institution of higher learning, Texas A&M encourages a climate that values and nurtures collegiality, diversity, pluralism and the uniqueness of the individual within our state, nation and world. All decisions and actions involving students and employees should be based on applicable law and individual merit.

Texas A&M University prohibits harassment and discrimination against any member of the University community on the basis of race, religion, color, sex, age, national origin or ancestry, genetic information, marital status, parental status, sexual orientation, gender identity and expression, disability, or status as a veteran.

Students who believe they have experienced harassment or discrimination prohibited by this statement are encouraged to contact the Office of the Dean of Student Life at 979-845-3113.

Americans with Disabilities Act (ADA) Policy Statement
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, currently located in the Disability Services building at the Student Services at White Creek complex on west campus or call 979-845-1637. For additional information, visit http://disability.tamu.edu.

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

For all academic work in this and every course, it is expected of you that you shall neither give nor receive any unauthorized aid.

All violations of the Aggie code of Honor will be reported to the Aggie Honor System Office.

For more information, see https://aggiehonor.tamu.edu/RulesAndProcedures/.