CSCE 465: Computer and Network Security
Section 500
Spring 2017

Last Modified January 25, 2017

1 Class Time and Location

Lecture: MW 4:10pm – 5:25pm in HRBB 113

2 Course Description and Prerequisites

CSCE 465. Computer and Network Security. (3-0). Credit 3.
Fundamental concepts and principles of computer security, operating system and network security, secret key and public key cryptographic algorithms, hash functions, authentication, firewalls and intrusion detection systems, IPSec and VPN, wireless and web security.
Prerequisite: CSCE 313 and CSCE 315; junior or senior classification; or approval of instructor.

3 Instructor Information

Instructor
Dr. Philip Ritchey AGGIE ALLY QPR Green Dot[1]
Office: 326 HRBB
Phone: 979-862-6476
Email: pcr@tamu.edu, PGP Public Key
Office hours: Tuesday 3pm – 4pm, Friday 10am – 11am, and by appointment.

Teaching Assistant
Kevin Hong
Office: HRBB 502A
Phone: 614-558-6767
Email: ghitsh@tamu.edu
Office hours: MW 1pm – 2pm, and by appointment

[1] I am willing to provide a safe haven, a listening ear, and support for lesbian, gay, bisexual, and transgender people or anyone dealing with sexual orientation issues. I am a QPR gatekeeper for suicide prevention. I support violence prevention efforts across campus.

4 Course Websites

`http://faculty.cse.tamu.edu/ritchey/courses/csce465/spring17`
`https://ecampus.tamu.edu`
`https://piazza.com/tamu/spring2017/csce465/home`

5 Textbook

Required
Michael T. Goodrich and Roberto Tamassia, Introduction to Computer Security, 1st ed., Addison-Wesley, 2011.

Reference
Ross Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd ed., Wiley, 2008. `https://www.cl.cam.ac.uk/~rja14/book.html`

6 Grading

Weight	Component	Date
50%	Homework	≈Bi-Weekly
10%	Exam I	22 February
20%	Exam II	3 April
20%	Final Exam	5 May, 3:30pm – 5:30pm
10%	Class Participation	Everyday

Final letter grades will be assigned according to the following cutoffs:

90+:	A
80:	B
70:	C
60:	D
less than 60:	F

This space unintentionally left blank.

7 Learning Outcomes

The objective of this course is to provide students with a general practical and theoretical understanding of fundamental concepts and principles of computer and network security. Specifically, through this course, student are expected to be able to:

- Describe different types of attacks, their characteristics, and the actors that might perform them
- Identify significant vulnerabilities, risks, and points at which specific security technologies/methods should be employed in the architecture of a typical, complex system
- List the principles of security and describe why each principle is important to security and how it enables the development of security mechanisms that can implement desired security policies
- Analyze common security failures and identify specific design principles that have been violated
- Identify the needed design principle when given a specific scenario
- Use a programming language to solve complex problems in a secure and robust manner
- Identify the elements of a cryptographic system
- Describe how various cryptographic algorithms and protocols function
- Describe the differences between symmetric and asymmetric algorithms
- Identify appropriate cryptographic protocols, tools and techniques for a given situation
- Identify strengths and weaknesses, different modes of operation, and issues that have to be addressed in an implementation of a cryptosystem.
- List and describe the major components of applicable laws and policies related to cyber defense pertaining to the storage and transmission of data

8 Schedule of Topics

Schedule is *tentative and subject to change.*

Day	Topic	Reading	Lab
18-Jan	Introduction	Ch. 1	
23-Jan	Guest Speaker: Brian from NSA		
25-Jan	Introduction	Ch. 1	
30-Jan	Cryptography	Ch. 8	Secret Key Encryption
1-Feb	Cryptography	Ch. 8	Secret Key Encryption
6-Feb	Cryptography (PSO)	Ch. 8	
8-Feb	Operating Systems Security	Ch. 3	Buffer Overflow
13-Feb	Operating Systems Security	Ch. 3	Buffer Overflow
15-Feb	Operating Systems Security (PSO)	Ch. 3	
20-Feb	Malware	Ch. 4	
22-Feb	**Exam 1**	**Ch. 1, 8, 3, 4**	
27-Feb	Network Security I	Ch. 5	TCP/IP Attack
1-Mar	Network Security I	Ch. 5	TCP/IP Attack
6-Mar	Network Security I	Ch. 5	TCP/IP Attack
8-Mar	Network Security (DNS Attack Demo)		TCP/IP Attack
13-Mar	Spring Break: No Class		
15-Mar	Spring Break: No Class		
20-Mar	Network Security II	Ch. 6	
22-Mar	Network Security II	Ch. 6	
27-Mar	Network Security II	Ch. 6	
29-Mar	Malware	Ch. 4	
3-Apr	**Exam 2**	**Ch. 5, 6, 4**	
5-Apr	Web Security	Ch. 7	SQL Injection
10-Apr	Web Security	Ch. 7	SQL Injection
12-Apr	Web Security (PSO)	Ch. 7	
17-Apr	Security Models and Practice	Ch. 9	Android Device Rooting
19-Apr	Security Models and Practice	Ch. 9	Android Device Rooting
24-Apr	Security Models and Practice	Ch. 9	
26-Apr	Physical Security	Ch. 2	
1-May	Distributed Applications Security	Ch. 10	
3-May	Reading Day: No Class		
5-May	**Final Exam 3:30pm – 5:30pm**	**Comprehensive**	

9 Policies

9.1 Attendance

It is strongly recommended that you 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.

9.2 Late and Missed Work

Late homework is not accepted without a University excused absence.
Missed exams cannot be made up without a University excused absence.
See rule 07 of the student rules: `https://student-rules.tamu.edu/rule07`.

9.3 Typesetting

All homework must be typeset in LaTeX or typed in Microsoft Word or OpenOffice Write. You must submit a PDF file. Resources for LaTeX can be found on the course website and on the Internet.

9.4 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, Perforce.

9.5 Collaboration

You are explicitly permitted and encouraged to work together on homeworks with the condition that all work you submit is your own. If you work with others to solve a homework problem, you must present the solution on your own. You are explicitly forbidden to use the work of others in your homework solutions. Copypasta[2] will result in an automatic grade of zero on the assignment for all parties involved.

9.6 Regrading

We work very hard to ensure that all work is graded correctly and completely. If you believe that your work has been graded incorrectly or incompletely, you must **meet with the instructor to request a regrade within one week of the date the work is returned**. Warning: Your work will be completely regraded and you may end up losing points.

9.7 Return of Graded Work

We will make an effort to return your graded work to you within one week of the date of submission. You may pick up your graded work from the instructor during office hours.

9.8 Extra Credit

There are 10 extra points built in to the final grade rubric. This is the only extra credit that is available in the course. Do not waste your time asking for more or different extra credit.

[2] Copypasta (n): A derogatory term for content which contains a direct or nearly direct copy-and-paste of material belonging to someone else, often accompanied by an attempt to pass off the content as new or original.

9.9 Curving

This class is not curved.

9.10 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 and myself. If you email a question or comment about the course to me, you will very likely be redirected to Piazza. You may post questions or comments to the instructor on Piazza privately, however this privilege will be revoked if it is misused. Course materials may be posted on Piazza.

9.11 eCampus

Course materials may be posted on eCampus (`https://ecampus.tamu.edu`). This include lecture slides and homework problem sets. Grades on assignments and exams will be reported on eCampus.

9.12 Email Formatting and Security

The subject of emails must be prefixed with [CSCE 465] and you must include your name in the email. Putting [CSCE 465] in the subject will let me know the course about which you are emailing. Signing your name will let me know who you are. If you do not sign your name, I might assign you one at random in my 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`).

9.13 Discussion of Grades

Federal law prohibits the instructor, TA, 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.

9.14 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 `https://disability.tamu.edu`.

9.15 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 845-3113.

9.16 Academic Integrity Statement and Policy – Aggie Code of Honor

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 recieve 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/`.