

CS-166

Information Security

Course Introduction

Instructor: Dr. Chao-Li Tarng

chaoli.tarng@sjsu.edu

Computer Science Department, SJSU

Fall 2025

CS-166 Class Information

- Class Lectures: Mon/Wed 3:00 pm – 4:15 pm
 - Classroom: DH 415
- Office Hour:
 - ENG 187 (In-person or online Zoom meetings)
 - Priority given to in-person visits
 - Time: Tuesday 2:30pm – 3:30pm, or by appointment
 - Zoom link information available on Canvas

Prerequisite for CS-166

- CS-146 Data Structure and Algorithm and
- One of the following courses
 - CS 47 Introduction to Computer Science
 - CMPE 102 Assembly Language Programming
 - CMPE 120 Computer Organization and Architecture
- Need to submit proof (unofficial transcript) to Canvas assignment
 - Due by the third lecture

About the Instructor

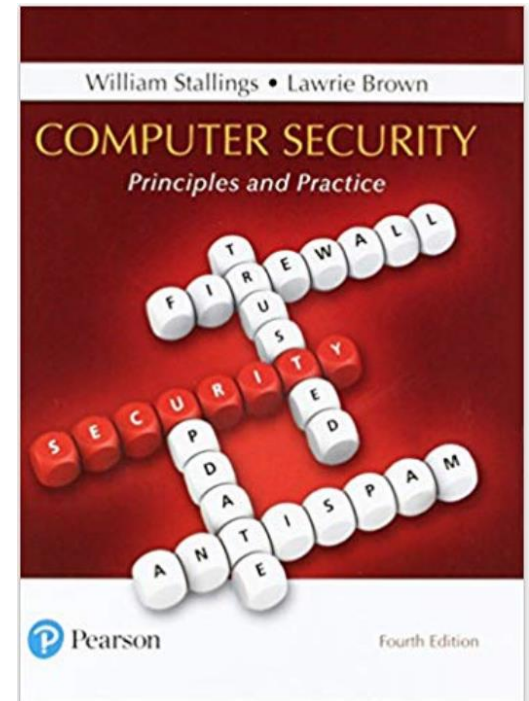
- Dr. Chao-Li Tarng
 - University of Washington, Ph.D. of ECE
 - Previously worked at Cisco as Director of Engineering
 - Networking and security
 - Teach CS-166, CMPE-50, CMPE-130, CMPE-132, CMPE-209, EE-30, EE-281, EE-286

ISA

- Aniket Ramesh Mali
 - aniketramesh.mali@sjsu.edu

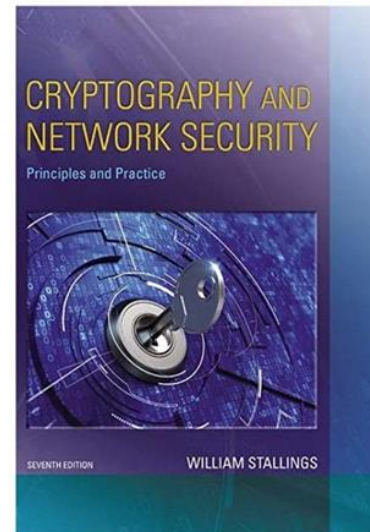
Course Materials

- Textbook (required)
 - William Stallings, Lawrie Brown, *Computer Security: Principles and Practice* (4th Edition), Prentice Hall, 2018, ISBN-13: 978-0134794105 (eText ISBN: 9780134794181)
 - *E-book is available through our library. See the syllabus to get the link.*
 - Slides and additional handouts
 - Require regular checking Canvas before each class



Course Materials (cont'd)

- Reference Books
 - Wenliang Du, *Computer Security: A Hands-on Approach* <https://www.handsonsecurity.net>
 - W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th Ed., Pearson 2017. ISBN 10: 0134444280, ISBN 13: 978-0134444284



Course Description/Goals

- **This course consists of three components:**
 1. Theoretical study of security models, cryptography methodologies, and algorithms
 - Threats, vulnerabilities, DES/AES/RC4/RSA/DH, SHA hash, virus/worms, network security, etc.
 2. Hands-on experiences on security, attacks and defenses (i.e. ethical hacking/penetration testing)
 - Linux, encryption/decryption, password cracking, SQL injection, XSS, DoS/DDoS, buffer overflow attacks, etc.
 3. Team-based project – your choice of topics in security

Goals

- Deep understanding on security algorithms and standards
- Learn how security attacks work and how to defend against them through hands-on approaches

Required Knowledge

- We will be using Linux to conduct the hands-on exercises. It is mandatory that you know the basics of Linux commands
 - A Linux tutorial lecture will be offered
- Networking
 - IP/TCP/UDP, packet formats, ports, ARP, DNS
 - Packet sniffer (Wireshark and tcpdump)
 - A short introductory networking lecture will be offered
- Programming skills using C/C++/Java/**Python**
 - You need to pick up the knowledge
- Familiarity with either Windows or Mac OSX
 - Need to learn how to configure and install software of your own PC/Mac

Virtual Labs

- We will be using Linux and install them on virtual machines using Oracle VirtualBox
 - VirtualBox is free
 - VMware is also free and can be used as well
- Benefit of virtual machines vs real machines
 - Can run multiple machines (guest OS) concurrently on a single PC (host)
 - Can create roll-back points in case of VM getting messed up
 - Can create a “sandbox” for attacks so it will not affect the real network
 - VMs running in a segregated private network
- We will learn how to ~~install OS from scratch and~~ import existing VMs.

Evaluation

- Individual HW and lab assignments and quizzes (20%)
 - For HW/labs, you can discuss with others but must be working and submitting individually
 - No sharing of writing, figures, pictures, programs, etc.
 - Zero points for plagiarism. Multiple offenses will be reported to the department chair.
 - Three quizzes (in-person on Canvas)
- Exams
 - Two midterms ($2 \times 20\% = 40\%$)
 - Final exam (25%)
 - Online exams using Canvas in the classroom
- Course project (group) (15%)
 - Team based (two persons per team)
 - Peer review within the team
 - Team to propose the topic. Potential topics will be discussed.
 - Reports and final presentation (in person)

Project: Team, Topic, and Process

- Team Formation:
 - A team of 2 – 3 people
- Team proposes the topic and gets approval from the instructor
- Recommended Topics:
 - Theoretical study of some crypto algorithm(s) and
 - Hands-on implementation of some crypto algorithm(s)
 - Performming (ethically) security attacks, detections or defenses
 - Security applications, such as blockchains, IoT, etc.
 - Internet security: Honey pots, social networking, etc.
 - Propose your own topic in security
 - A list of topics will be discussed later
- Learn lifetime skills
 - Research and define the topics of your study
 - Analyze and solve the study/problem you defined
 - Document your finding
 - Present and demo in the class

Project Deliverables

- **Project Abstract**
 - project title
 - group members: names and student ID's
 - abstract of the project and schedule
- **Interim Progress Report**
 - Report the progress and challenges with mitigation plans
- **Final Reports :**
 - Include the following sections:
 - Problem statement (why the problem is important)
 - The chosen algorithm(s) and how it is related to security
 - Programming and execution
 - Your findings and analysis
 - Future extension
 - A report template will be provided
- **Presentation - in class**
 - 10 - 15 minute (TBD) presentation in Powerpoint/PDF and demo (live or video)

Department Policy

- Submit a photocopy of an unofficial transcript showing the prerequisite to Canvas assignment.
 - Highlight your name and the prerequisite.
 - Due: in a week
- Permission number
 - Show prerequisite before getting a permission number

Course Schedule

- See syllabus

Serious Extenuating Circumstances And Proof Required

- Only the following items count as a serious extenuating circumstance
 - Hospitalization or being treated in the emergency room at the time of the quiz/exam
 - Death in the IMMEDIATE family (spouse, child, father, mother, grandparent who lives with you)
 - A governmentally dictated appointment that cannot/should not be re-scheduled (this has to be cleared ahead of time)
- Proof required for these
 - Original or certified copy of admission document showing the date/s
 - Death certificate and proof of relationship
 - Original appointment letter

Excuses NOT Approved (borrowed mostly from Dr Black)

- Incarceration, being kidnapped, being locked out of house
- Traffic congestion, blown tires, parking problems, traffic school, jury duty (full time students are excused)
- Going on vacation, getting married, being a wedding attendant, death of non-immediate family member in or out of the US.
- Working overtime, oversleeping, being hung over
- Taking multiple exams on the same day
- Showing up at the wrong time, day or place
- Just not adequately prepared to take an exam
- These are some examples of illegitimate excuses which will **NOT** be approved. And, yes, students have tried in the past.