Instructor

Fred Clift
Office: 2258 TMCB
Office Hours: by appointment
Email: fred AT clift.org
Phone: (text preferred) 801-376-0305

TAs

Location: 1160 TMCB

Please check our hours for any changes before coming in.

	Monday	Tuesday	Wednesday	Thursday	Friday
8AM	Tyler	Tyler	Tyler	Tyler	Tyler
9AM	Max	Matt starting at 9:30AM	Max	Matt starting at 9:30AM	Max
10AM	Max	Matt	Max	Matt	Max
11AM	Tyler	Matt	Tyler	Matt	Tyler
12PM	Tyler	Matt	Tyler	Matt	Tyler
1PM	Matt	Matt to 1:30PM	Matt	Matt to 1:30PM	Matt
2PM	Matt		Matt		Matt, Tyler
3PM					Matt, Tyler
4PM		Max starting at 4:15PM		Max, Tyler starting at 4:15PM	Tyler
5PM		Max to 5:15PM		Max, Tyler to 5:15PM	

Email: cs465ta@cs.byu.edu

Discussion Group

https://groups.google.com/d/forum/byu-cs-465-fall-2015 [https://groups.google.com/d/forum/byu-cs-465-fall-2015]

Apply for membership to this google group, and we'll add you. Please include your name in your request.

Lecture

NOTE: Room Changed!

Section 001: TTh 3:00 ~ 4:15 pm, B092 JFSB

Description

This course will cover fundamental principles of computer security. The course consists of two parts:

- Part 1: **Applied Cryptography** - We will study and experiment with basic cryptographic primitives (symmetric encryption, asymmetric encryption, MAC, and cryptographic hash functions). We will learn how these primitives are used to achieve certain security properties. We will then study real-world protocols like HTTPS and secure email to see how these primitives are used in real systems.
- Part 2: **Software Security** - We will learn about some of the most common errors that software developers make that attackers then exploit. We will learn how to avoid or prevent these mistakes.

Prerequisites

CS 360 (concurrent) or Instructor Consent

Classroom Procedures

Student learning activities consist of exams, homework, and hands-on programming projects.

Projects:

Each week that a project is assigned, it is due at 5 PM on Friday. Students are encouraged to meet project deadlines. I want to see all students complete every lab by the end of the semester. As an incentive to help you stay current, late days and early days (maximum of 5) for each project will be recorded (weekends and university holidays excluded). A total of **five (5)** free early days for the semester will be given. At the end of the semester, you will receive a penalty if your late day balance exceeds your early day balance. Your overall project points may be penalized up to 2% for each late day on your final balance. If all projects are completed, the penalty for late days will be capped at 20% so that your grade is reduced by a maximum of one letter grade.

Project Pass-off Policies

- Projects may be written in the language of your choice unless instructed otherwise.
- Projects must be passed off by the TA in person, unless instructed otherwise.
- You may pass off a project after the deadline for full credit, and without using late days, provided you email a SHA-1 checksum of all files associated with your project to the TA before the deadline. You can generate the checksum again at passoff to convince the TA that your assignment was completed on time. You can generate a checksum on linux using openssl (e.g., >openssl dgst -sha1 <filename>). Search online for how to do this on other systems.

Homework:

Homework is due on Tuesday at the beginning of class. Please submit it online in LearningSuite before it is due.
Grading: Each homework is worth 25 points

Late Homework Policy:

- Submitted by the following class period after it is due: max 15 pts
- Submitted by the next exam: max 10 pts

Study Habits

Successful students attend class regularly and complete assignments on time. Students are encouraged to work together in groups to discuss topics and assignments. A good rule of thumb is that only your hands should be on the keyboard when you are entering your solution. Do not share your work with any other students in the class or with a student in a future classes.

Learning Outcomes

1) Build a system: Implement a cryptographic algorithm from a standards specification.
2) Break and fix a system: Demonstrate how attackers compromise real-world systems, and then show how to prevent these attacks.

Grading Scale

A 93-100	B- 80-82	D+ 67-69
A- 90-92	C+ 77-79	D 63-66
B+ 87-89	C 73-76	D- 60-62
B 83-86	C- 70-72	E 59 and lower