CS 465 Fall 2017 Introduction

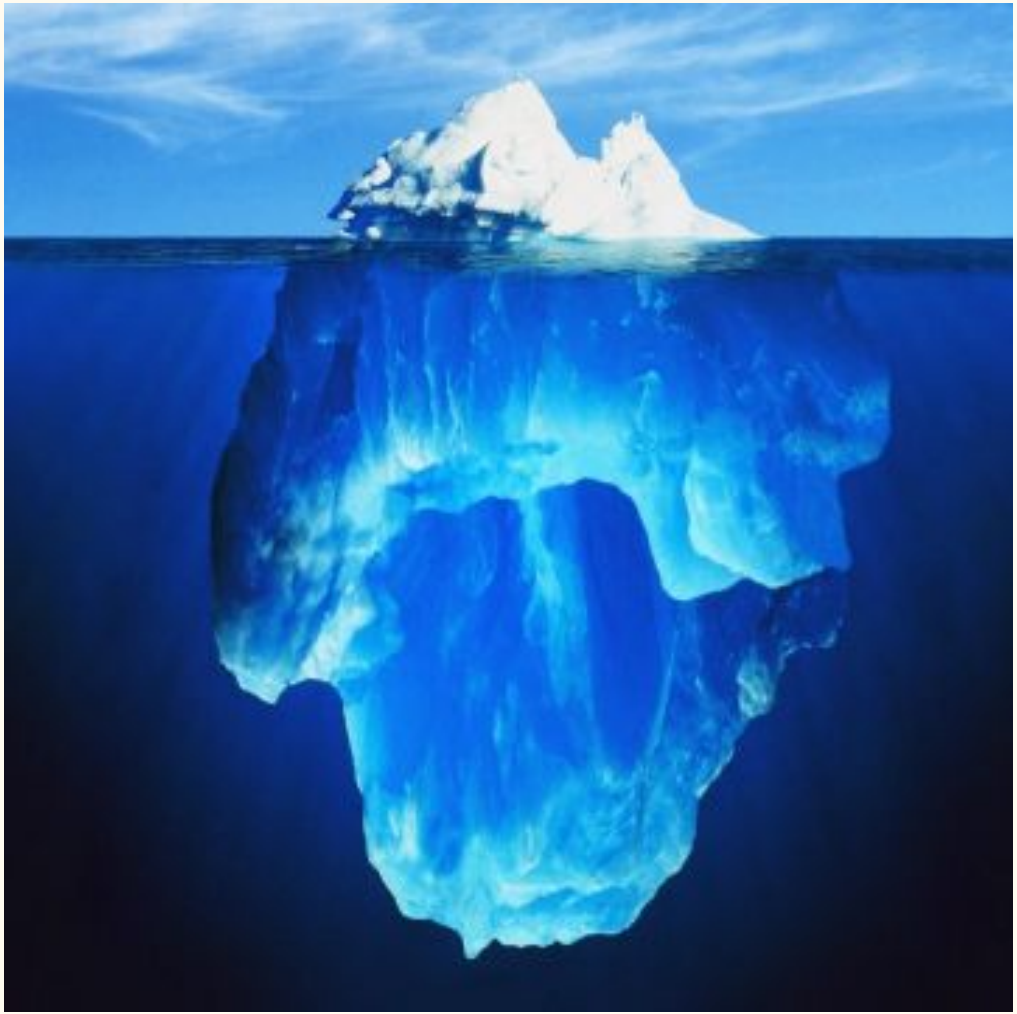
—

Instructor: Kent Seamons

Tip of the Iceberg

This class will introduce you to the important field of computer security.

- Principles and patterns
- Way of thinking
- Lifelong learning
- Relevant to you both personally and professionally
- Software developer, manage data, technology user, security expert



Course Objectives

- Gain a breadth of knowledge in computer security
- Understand basic security terminology and use it accurately in technical discussions
- Understand the kinds of threats facing people and systems and the technology to address those threats
- Understand the limitations of technology in creating a secure system

Course Objectives

- Prepare students to make sound technical decisions in the design and acquisition of security technology
- Provide students with a basic understanding of the principles of secure software design
- Prepare students with the technical and communication skills so that they can assume leadership roles in their chosen area
- Prepare students to conduct security research in industry or graduate school
- Promote a code of ethics that is compliant with the law and in accordance with gospel principles

Learning Objectives - Applied Cryptography

- Understand the basic principles of cryptography and how cryptographic building blocks can be assembled to provide security services
  - Remove the ***mystery*** of cryptography and replace it with knowledge of basic principles
  - Understand the use of cryptography in existing security protocols
  - Be able to explain how a protocol meets a given set of security requirements

Learning Objectives - Secure Software

- Understand the basic principles of secure software design
  - Avoid common design and development errors
  - Understand basic usage of standard cryptographic primitives

Learning Activities

- Hands-on experience
  - Programming projects
- Teach - Improve written and verbal communication skills
  - Rigorous written exams
  - Written homework
  - Lab reports
  - Class/Group discussions – teach one another
- Gain a healthy skepticism about the security of real-world systems

Topics of Study

- Applied Cryptography
  - Encryption, one-way hash, MAC
- Real-world Systems
  - SSL/TLS (HTTPS)
  - Secure email
  - Passwords
- Software Security
  - Buffer overflow
  - Password cracking
  - SQL injection
  - Cross-site scripting
  - Social Engineering

Logistics

- All assignments submitted to LearningSuite
- Grade information available in LearningSuite
- Course website
  - https://wiki.cs.byu.edu/cs-465/
- Class discussions in a Google Group - please join
  - byu-cs-465-fall-2017

Logistics

- Homework (25 pts each)
  - Regularly assigned, due before the start of class almost every Tuesday
  - HW 1
  - See late policy - complete by next class period (15), by next exam (10)
- Programming projects (100 pts each)
  - Due Friday before midnight during most weeks during the semester
  - Project #1 due Friday Sep 15
  - See late policy: Start with 5 early days, goal is to end with a positive balance
- Exams
  - 2 exams during the semester + final exam

Logistics

- Study in groups!
  - Discuss all aspects of the course
  - Do your own work
    (i.e., write your own homework, develop your own code,
    acknowledge all outside sources)
- Workload – average 6 hours/week plus class time
  - First lab is time consuming for many students, start now
  - Workload starts high and tapers off as the semester progresses

Code of Ethics

- Each student is expected to be committed to:
  - Ethically study computer security for educational purposes
  - Refrain from using the knowledge gained to knowingly probe and attack computer security systems, unless having first received written permission from the owners or operators of those systems
  - Unethical practices include: cracking passwords to gain unauthorized access, deliberately spreading viruses or Trojan horses, conducting a denial of service attack, attempting buffer overflow attacks, impersonating another person on a computer system you do not own
  - Carefully consider ethical issues as knowledge of computer security increases
  - Strive to formulate a personal code of ethics of the highest integrity

Code of Ethics

- Failure to comply could result in:
  - Suspension of my computer privileges in the CS Department
  - Expulsion from BYU
  - Possible criminal prosecution