

# CS 465

# Computer Security

---

Instructor: Fred Clift

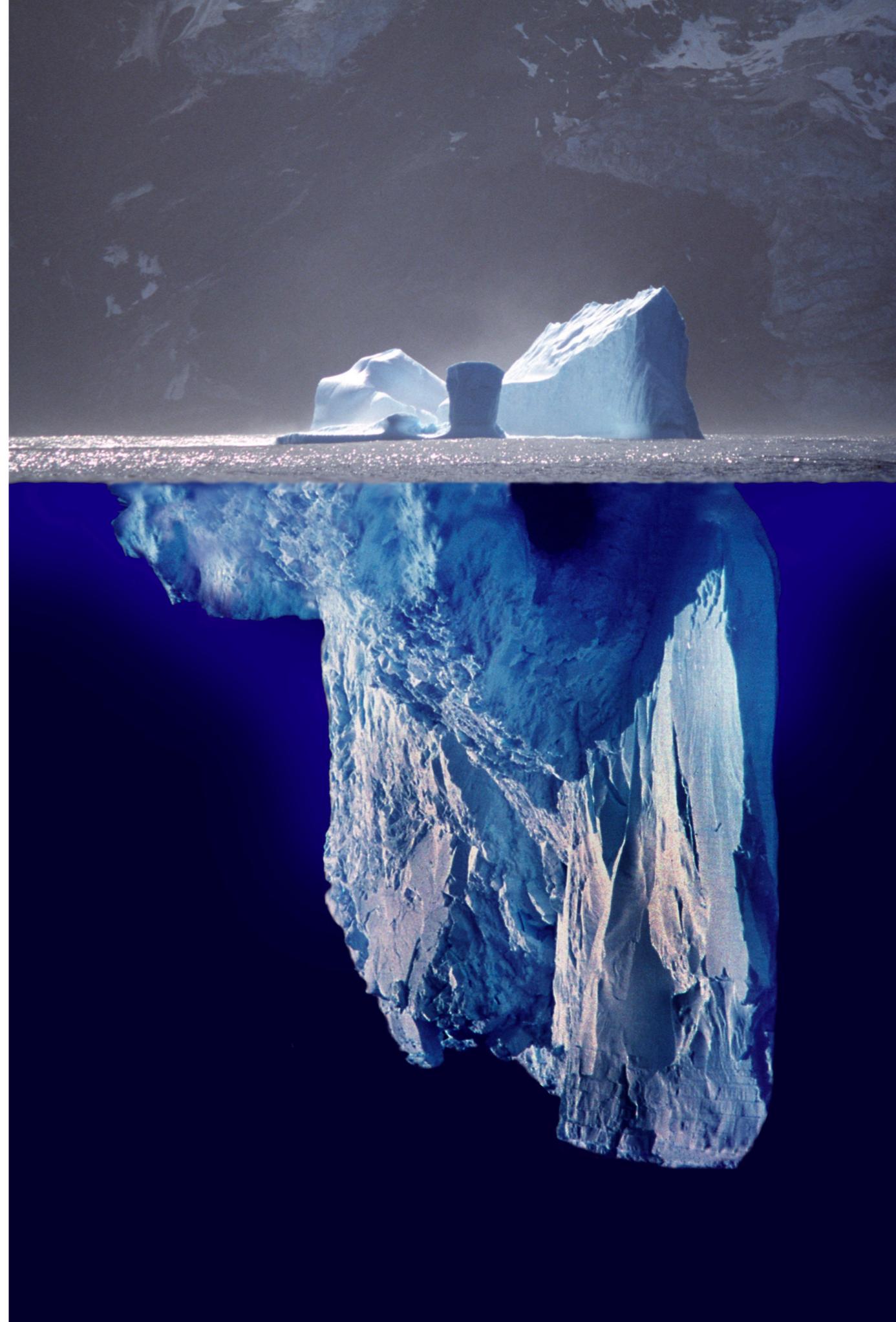
Created with:  
Daniel Zappala  
Kent Seamons

# 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 — whether you are a software developer, data analyst, technology user, security expert



# Learning 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

# Learning Objectives

---

- 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

---

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

# Learning Objectives

---

- Develop leadership skills
  - Be able to make sound technical decisions in the design and acquisition of security technology
  - Develop technical and communication skills needed for leadership roles
  - Be ready to conduct security research in industry or graduate school

# Learning Objectives

---

- Promote a code of ethics that is compliant with the law and in accordance with gospel principles

# Topics of Study

---

- Cryptography
  - symmetric key cryptography
  - public key cryptography
  - cryptographic hash functions
  - MAC

# Topics of Study

---

- Systems
  - SSL/TLS (HTTPS)
  - Secure email
  - Passwords

# Topics of Study

---

- Software Security
  - Buffer overflow
  - Password cracking
  - SQL injection
  - Cross-site scripting
  - Social Engineering

# Logistics

---

- Class web site: [cs465.internet.byu.edu](http://cs465.internet.byu.edu)
- Learning Suite: submit assignments, get grades
- Class discussions: slack (link on class web site)

# Logistics

---

- Reading — occasional reading assigned, please follow along, lectures will assume familiarity with the material
- Homework — due before class most Tuesdays
- Projects — due at midnight, see class schedule
- Exams — 2 midterms + final
- Late Policy — see class website

# Logistics

---

- Study in groups is encouraged — discuss problems, how to solve them, but do your own work
  - Write you own solution
  - Don't view anyone else's code
- Workload — about 6 hours per week
  - First lab is time consuming — start now
  - Workload diminishes during the semester

# Code of Ethics

---

- You commit 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
  - 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

---

- 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

# Code of Ethics

---

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