CS 465

Course Introduction
Course Objectives

• Prepare students with the technical and communication skills so that they can assume leadership roles in their chosen area

• 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 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
Course Goals (I)

• Gain a broad knowledge of computer and network 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 Goals (II)

• 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

• Understand the basic principles of secure software design
  • Avoid common design and development errors
  • Understand the correct usage of standard cryptographic primitives
Course Goals (III)

• Gain hands-on experience with course concepts
  • Programming projects

• Improve written and verbal communication skills
  • Rigorous written exams
  • Written homework
  • Lab writeups
  • Class/Group discussions – teach one another

• Gain a healthy skepticism about the security of real-world systems
Topics

• Applied Cryptography
• Real-world Systems
  • TLS (HTTPS)
  • Secure email
  • Passwords
• Software Security
  • Buffer overflow
  • Password cracking
  • SQL injection
  • Cross-site scripting
  • Social Engineering
Logistics

- Course grades and assignment submission in LearningSuite
- Course website https://wiki.cs.byu.edu/cs-465/
- Class discussions in a Google Group
  - byu-cs-465-fall-2014
- Homework
  - Regularly assigned, due at the start of class each Tuesday
- Programming projects
  - Due Friday at 5 PM during most weeks during the semester
- Exams
  - 2 exams during the semester + final exam
- Study in groups!
  - Discuss all aspects of the course
  - Do your own work (i.e., write your own homework, program your own code, acknowledge all outside sources)
- Workload – average 6 hours/week plus class time
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
• Failure to comply could result in:
  • Suspension of my computer privileges in the CS Department
  • Expulsion from BYU
  • Possible criminal prosecution