CS 465 Computer Security

Kent Seamons
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 (1)

- Gain a broad knowledge of computer and network security
- Understand basic security terminology and use it accurately in technical discussions
- Understand the various threats facing digital systems and the technology to ameliorate those threats
- Understand the limitations of technology to creating a secure system
- Understand the basic principles of cryptography and how cryptographic building blocks can be assembled to provide basic 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
Course Goals (2)

- Understand the basic principles of secure software design
  - Avoid common design and development errors
  - Understand the correct usage of standard cryptographic primitives
- Gain hands-on experience with course concepts
  - Programming labs
- Improve writing skills
  - Rigorous written exams
  - Written homework
- Improve verbal presentation skills
  - Class/Group discussions
Topics

- Cryptography
- Access Control
  - Kerberos
  - TLS
  - Secure email
  - Password authentication
- Network and Software Security
  - Software security
  - Malicious software
  - Defenses
  - Social Engineering
  - Privacy
Class Organization

- Review course web pages
  - Study policies page, schedule
- Homework – regularly assigned, due in class
- Programming labs
- Exams
- Study in groups!
  - Discuss all aspects of the course
  - But do your own work (i.e., write your own homework, program your own code, acknowledge all outside sources)
- Workload – average 10 hours per week outside of class
Pre-requisites

- Required
  - CS 240

- Suggested
  - CS 330
  - CS 312
Textbooks

- Secrets and Lies – Schneier
- Network Security Essentials – Stallings
- Outside sources occasionally
Code of Ethics

- Each student is expected to be committed to the following:
  I commit to the ethical study of computer security for educational purposes. I will refrain from using the knowledge I gain to knowingly probe and attack computer security systems, unless I have first been given explicit permission from the owners or operators of those systems. Examples of unethical practices include cracking passwords to gain unauthorized access, deliberately spreading viruses or Trojan horses, conducting a denial of service attack, and attempting buffer overflow attacks. I understand that failure to comply could result in suspension of my computer privileges in the CS Department and possibly subject me to criminal prosecution. I will carefully consider ethical issues as my knowledge of computer security increases. I will strive to formulate a personal code of ethics of the highest integrity.
Word of Honor

I have been asked what I mean by my word of honor. I will tell you. Place me behind prison walls -- walls of stone ever so high, ever so thick, reaching ever so far into the ground -- there is the possibility that in some way or another I may escape; but stand me on the floor and draw a chalk line around me and have me give my word of honor never to cross it. Can I get out of the circle? No, Never! I'd die first!"

-- Karl G. Maeser