CyberSecurity principles

Prerequisites: Students are expected to have a good understanding of computer architecture, such as memory hierarchy; students are expected to understand operating systems features and functionality. Students are expected to familiar with at least one high level programming language.

Length of Completion:This is a 15 week (one semester) course.

Level of Instruction: This is an upper-division undergraduate level course for computer science or computer engineering majors.

Learning Setting: This course can be taught through in-class lectures or as a hybrid course.

# Course Description

### This course provides fundamental knowledge about cyber security. Software vulnerabilities, threats, attacks, and their mitigation methods will be discussed. The course also focuses on general purpose operating system security and dependability, network security. Secure coding and secure design principles will be introduced as well.

### Learning Outcomes:

* Students will be able to understand basic security concepts, such as availability, confidentiality, integrity, authentication, authorization, and accountability.
* Students will be able to explain fundamental concepts and techniques related to authentication and access control.
* Students will be able to describe the classical cryptography and modern ones that are being used, such as RSA, AES, DES.
* Students will be able to describe the common software vulnerabilities, such as buffer overflow, integer overflow and wrap around, off by one, and to understand the ways to prevent them.
* Students will be able to list fundamentals of secure coding, secure design principles.
* Students will be able to demonstrate how viruses, trojan horses and worms work and the countermeasures for these malwares.
* Students will be able to describe the common web attacks, such as cross-site scripting attack, SQL injection attack.
* Students will be able to understand the issues related to general purpose operating systems for security and dependability and the basics of systems hardening.
* Students will be able to list common network security attacks and explain their mitigations.
* Students will be able to discuss basic concepts of firewalls, IDS, and IPS.
* Students will be able to describe legal and ethical issues in cyber security.
* Students will be able to explain issues related to secure system administration, such as system management, maintenance, patching and upgrading.
* Students will be able to understand security policies and compliance issues related to the implementation of security within organizations.

Materials:List any required materials for the course.

Required Text:

There is no required text for this course.

Suggested Text:

Security in computing (Fifth edition), Prentice Hall, Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies

Computer security principles and practice (Fourth edition), Pearson, William Stallings, Lawrie Brown.

Additional Materials:

Library Resources or Open-Source Materials

SEED Labs, available from: <http://www.cis.syr.edu/~wedu/seed/labs.html>

Technical Specifications:

For the lab experiments, students need a machine with VirtualBox installed and 20GB of free disk space.

Grading:

Homework assignments – 35%

Lab reports – 15%

Mid-term Exam – 25%

Final Exam – 25%

7 Homework assignments (100 points each)

Labs will be using SEED Labs, lab reports will be required (50 points each)

Buffer overflow vulnerability lab (4 hours)

Format string vulnerability lab (2 hours)

Cross-site scripting attack lab (2 hours)

SQL injection attack lab (2 hours)

Exams:

Mid-term exam (2 hours, 100 points)

Final exam (2 hours, 100 points)

Course Schedule:

Module 1: Introduction to Cybersecurity Concepts.

Module 2: Introduction to Cryptography

Module 3: Introduction to Software Security

Module 4: Introduction to Operating System Security

Module 5: Introduction to Web Security

Module 6: Introduction to Network Security

Module 7: Introduction to Secure System Administration

Please attribute Dr. Jim Alves-Foss and Dr. Jia Song, University of Idaho  
  
  
  
Except where otherwise noted, this work is licensed under <https://creativecommons.org/licenses/by-nc-sa/4.0/>  
  
Notwithstanding the non-commercial license terms, non-profit educational institutions are granted a non-exclusive, royalty-free license to adapt and use this material, with attribution.  
  
Creative Commons and the double C in a circle are registered trademarks of Creative commons in the United States and other countries. Third party marks and brands are the property of their respective holders.

Project sponsored by the National Security Agency under grant Number H98230-17-1-0199. The United States Government is authorized to reproduce and distribute reprints notwithstanding any copyright notation herein.