Network Security

Prerequisites: Students are expected to have a solid understanding of binary data representations, including endianness; students are expected to have a familiarity with different types of networks and network devices; students are expected to have a knowledge of cyber security consistent with a one semester introductory level course discussing cyber security principles, threats, vulnerabilities and mitigations. Students should come with an innate curiosity, a willingness to complete out-of-class readings on schedule and a willingness to participate in active discussions in class.

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

Level of Instruction: This is an upper-division/graduate 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

### Practical topics in network security; policy and mechanism, malicious code; intrusion detection, prevention, response; cryptographic techniques for privacy and integrity; emphasis on trade-offs between risk of misuse, cost of prevention, and societal issues; concepts implemented in programming assignments and hands-on labs.

### Learning Outcomes:

* Students will be able to describe the fundamental concepts, technologies, components and issues related to communications and data networks.
* Students will be able to describe a basic network architecture given a specific need and set of hosts/clients.
* Students will be able to describe and discuss data network architectures and protocols.
* Students will be able to track and identify the packets involved in a simple TCP connection (or a trace of such a connection).
* Students will be able to use a network monitoring tools (e.g., WireShark).
* Students will be able to use a network mapping tool (e.g., Nmap).
* Students will be able to describe the various concepts in network defense.
* Students will be able to apply their knowledge to implement network defense measures.
* Students will be able to identify the elements of a cryptographic system.
* Students will be able to describe the differences between symmetric and asymmetric cryptographic algorithms.
* Students will be able to describe which cryptographic protocols, tools and techniques are appropriate for a given situation.
* Students will be able to describe how crypto can be used, strengths and weaknesses, modes, and issues that have to be addressed in an implementation (e.g., key management), etc.

Materials:

Required Text:

There is no required text for this course.

Additional Materials:

Links to reference materials will be made available on the course website.

Library Resources or Open-Source Materials

Links to reference materials will be made available on the course website. Such as:

* Internet Protocol Specifications ([IETF RFCs](https://www.ietf.org/rfc.html))
* [OpenSSL List of Relevant Standards](https://www.openssl.org/docs/standards.html)

Technical Specifications:

Students need a machine with [VirtualBox](https://www.virtualbox.org/wiki/Downloads) installed and 20GB of free diskspace, or access to laboratory servers with the installed VMs.

Grading:

Written Homework (20pts):

* Posted in Homework folder of BbLearn
  + Each student will be required to prepare a set of literature reviews. These are 1-page summaries of relevant articles.
    - Assignment overview: homework/lit-review.docx
    - Grading Rubric: homework/lit-review-rubric.pdf
  + Students will be assigned sets of questions to answer.
  + Students will also be required to complete some surveys

Labs (20pts): (all will be posted in the Labs folder of BbLearn)

* Throughout this course, students will be working on labs to develop the hands-on skills needed by cybersecurity professionals.

In Class Participation (10pts):

* This class will involve several discussion sessions. Students are expected to participate in these.
* This means attendance is very important.

Exams (50pts) :

* Midterm 20pts (Oct 9)
* Final 30pts (10 am-12 noon Pacific time -- Dec 12)

CS 538 only (20pts):

* Term paper/project

Course Schedule:

Module 0: Introduction, Course Overview and Discussion of Prerequisite

Material

Module 1: Networking and Network Security Fundamentals

Module 2: Understanding Cryptography and Cryptographic Protocols

Module 3: Network Defense

Module 4: Network Security Administration

Module 5: Advanced Networking (if time permits)

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.