

CSE5636 – Network Security Syllabus for Spring 2009

Course Goal: The goal of this course is to introduce students to network security including cryptography mechanisms, intrusion detection, and network perimeter security. The course includes three major components. First we consider mechanisms used to provide confidentiality, authentication, and integrity. This will include an introduction to cryptography and crypto-analysis. Second, we consider traffic monitoring including basic tools (Ethereal and TCPDUMP) used to analyze captured traffic streams. After a brief review of the traffic generated by basic TCP/IP protocols, a number of well-known attack streams are analyzed. Third we consider statistical anomaly detection and its role in detecting previously unseen attacks. Along the way we will introduce methods and some of the many tools used by hackers. We will also consider SNORT (perhaps the most commonly used freeware for intrusion detection) and learn to use TCPDUMP filters. Practical methods will be complemented with an introduction to some of the research in related areas.

Course Prerequisites: Students will need to have some knowledge of networking, such as that obtained in CSE5231 or equivalent. For the material on statistical anomaly detection, basic knowledge of Calculus I and II will be required as well as a course in Probability and Statistics. We will review some material from Probability and Statistics. Some knowledge of Linear Algebra will be helpful but can be acquired during the course (with additional work from the student).

Instructor/Office Hours: Dr. G. Marin. Email: gmarin@fit.edu. Phone: 321-674-7559.
Office hours: Tuesday 12:30pm to 2pm and Thursday 10:30am to noon in Olin 259 E/C - other times by appointment.

Course Content (Subject to change)

Introduction and Overview

- What is network security?
- Principles of cryptography
- Authentication
- Integrity
- Key Distribution and certification
- Access control: firewalls
- Attacks and counter measures

Traffic Analysis and Filtering

- Using Ethereal and TCPDUMP
- Examining IP Header Fields
- Recognizing Attacks
- Examining Embedded Protocol Header Fields
- Real-world Analysis
- Writing TCPDUMP Filters

Intrusion Detection Systems

- Overview
- The False Alarm Problem
- Introduction to SNORT
- SNORT Filtering Rules
- Real-world Analysis

Statistical Anomaly Detection

Characterizing "Normal" Traffic
Classical Statistical Distributions
Self-Similarity and Fractal Dimension
Pattern Recognition
 Protocol distributions
 Address distributions
 Port distributions
 Protocol State Violation

Mid-Term Test: Thursday, February 19

Final Exam (comprehensive): Monday, May 4, 3:30pm – 5:30pm

Test Policy: Every effort will be made to hold the two tests and final as scheduled. Students must take all tests (and the exam) at the appointed time or receive a grade of 0 for the test/exam. Only verifiable emergencies will be considered as exceptions to this policy. In case of such an emergency, you must contact the Dr. Marin as soon as humanly possible to avoid receiving a 0 grade. You must speak with him BEFORE any test or exam that you must miss unless the absence was completely unpredictable (such as a car accident on the way to the exam!).

Project: Each student will complete a project and present it at an assigned time, which will likely be during the last two weeks of class. This may involve the implementation of a security mechanism, for example, or may involve a detailed descriptive presentation on something related to the topics covered in class. Both a written report and classroom presentation are required. Presentation of the **proposed** project is due on Thursday, February 26.

Grade

Your grade in the course will be determined as follows:

Mid-Term Test: 30%
Homework: 20%
Project and Class Participation: 20%
Final Exam: 30%

A: 90 – 100; B: 80 - 89; C: 70 – 79; D: 60 – 69; F: Below 60. (I may choose to vary this for borderline grades.)

Class Policy: You must work alone during the tests. Any talking during a test or the exam will be assumed to be an attempt for an unfair advantage and will result in a 0 grade for that test/exam and may be referred elsewhere in the University for further action (as will any appearance of cheating such as looking at a neighbors test, passing papers or other materials, or using books or notes or calculator during a test unless approved before the test.) A second incident will result in an F for the final course grade. Any disruptive behavior in class (talking, etc.) may also result in a lower final grade.

Security Ethics: It is anticipated that the course will enable students to help defend their own systems and perhaps their employers' networks and systems from the ever increasing threat posed by hackers, viruses, worms, spam, and similar problems. In learning this material, however, students must be aware that it is unethical and may well be **illegal** to target any machines unless they own them or they have specific permission from the owner in advance.

Nothing said in class should be interpreted to imply that students should test or attack machines or networks that they do not own, and students must assume full responsibility for any such actions.

Lecture Materials: Will be available via the web typically in pdf format. Presentation slides will usually be available within a day or so after the material for that section is complete. Any such material is provided for educational purposes only and cannot be further reproduced or distributed without possible violation of copyright laws.

G. Marin