COSC 6397 Network Intrusion Detection

Fall 2019

Title: Network Intrusion Detection

Course Number: COSC 6397

Section Number: 28246

Instructor: Stephen Huang, 209-PGH, Email: shuang@cs.uh.edu, 713-743-3338

Office Hours: Monday & Tuesday 1-2 pm, Wednesday 4-5 pm, and by appointment

Class Room: AH-301

Course Website: http://www.cs.uh.edu/~acl/cs6397/, *in progress.*

Prerequisites: Graduate standing with the following courses: data structures and algorithms, operating systems. Courses in Network, Security, AI, machine learning, and statistics may be helpful.

Description: Introduction to Computer Security, Concepts of intrusion detection, anomaly detection, signature-based detection, automated response to attacks, tracing intruders, network tools for intrusion detection, Machine learning techniques. This course was previously taught as COSC 7397. It has been moved to the 6000 level and the content has been adjusted somewhat.

Major topics:

- Stepping Stone Detection
- Correlation
- Modeling
- Anomaly Detection
- Logging
- Incident Response
- Tools

Textbooks and References: Instructor's notes and papers. A list of popular Cyber Security textbooks are given below. There is no need to purchase any of them.

(1) William Stallings and Laurie Brown, *Computer Security: Principle and Practice*, Pearson Prentice-Hall, 2008.
(2) Matt Bishop, *Introduction to Computer Security*, Addison Wesley, 2005, new edition 2018.
(3) Edward Amoroso, *Intrusion Detection: An Introduction to Internet Surveillance, Correlation, Trace Back, Traps, and Responses*, Intrusion.Net Books, Sparta, New Jersey, 1999.
(4) Stephen Northcutt and Judy Novak, *Network Intrusion Detection*, 3rd Ed., New Riders, 2003.
(5) Carl Endorf, Eugene Schultz, and Jim Mellander, *Intrusion Detection and Prevention*, McGraw Hill, 2004.
(6) Jack Koziol, *Intrusion Detection with Snort*, Sams Publishing, 2003.
(7) Edward Amoroso, *Fundamentals of Computer Security Technology*, Prentice-Hall, 1994.
(8) Wenliang Du, Computer Security, Amazon.

Grading:

- This is a graduate course and students are expected to actively participate in the discussion during class. Attendance and participation in class will count about 10-20% of the course grade.

- There will be some assignments which may requires programming, using tools, and data analysis. This part will count about 40% of the course grade.
- Students are expected to read a recent security paper and present the paper in class. This will count about 20% of the grade.
- It is not likely that we are going to have final exam. If no final is given, there may be additional presentation, reading, report, or assignments.