COSC 7370 Network Intrusion Detection

Fall 2016

Title: Network Intrusion Detection

Course Number: COSC 7370

Section Number: 29422

Instructor: Stephen Huang, 594-PGH, Email: shuang@cs.uh.edu, 713-743-3338

Office Hours: Monday 4-5pm, Thursday 11-12am, and by appointment

Class Room: M-120

Course Website: http://www.cs.uh.edu/~acl/cs7370/, *Coming Soon*

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, User Authentication.

Major topics:

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

Textbooks and References: Instructor's notes and papers. A list of reference books is given below.

(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.
(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.

Grading: Homework, presentations, project, test and class participation.