Course: ENPM 808O – Intrusion Detection: From Theory to Practice
Semester: Spring 2016
Day(s): TBD
Time: ONLINE
Location: ONLINE
Instructor: Assane Gueye
Phone: 301-975-5456
Email: agueye@umd.edu

Course Description

Intrusion detection systems (IDSs) constitute an essential component of any network security solution package. Underlying IDSs is a great deal of fascinating mathematics mostly taken from various fields such as Probability Theory, Statistic, and Detection Theory. A good understanding of this mathematical background will enable Security Officers to better appreciate the benefits and limitations of IDSs and prepare them to become better practitioners.

The goal of this course is two-fold. First, it will provide to students a hands-on exposure to the mathematical principles and techniques used in intrusion detection. Second, students will experiment with the real-life process of going from a theoretical intrusion detection solution to its implementation. The course will proceed by introducing mathematical concepts on an "as needed" basis, motivated by their direct applications to intrusion detection.

The class consists of lectures, homework assignments, labs, and a class project. Topics covered include: overview of intrusion detection (host and network-based IDSs, techniques of intrusion detection—anomaly and signature-based), a brief review of the mathematical background of IDSs, and case studies of mathematical solutions for IDSs and the issues related to their applications in the real-world.

Disclaimer: there are many ad hoc approaches to IDS. In this course we only focus on approaches that build on some mathematical ground.

Textbook(s)

Book Recommendation: We will be pooling from several sources for the materials of this class. As a consequence, there will be no required book. For reading, articles and book chapters will be provided. We will also suggested additional documentation for each particular topic that we cover.

Course Outline

- Part 1 (Setting the stage)
  - Overview of intrusion detection
    - Host-based, Network-based, and distributed IDS
    - Real-time vs. Post-facto
Techniques of intrusion detection
  ✓ Signature-based detection techniques
  ✓ Anomaly-based detection techniques
  ✓ Specification-Based
  ✓ Behavioral Techniques

- **Part 2 (Mathematics of IDSs)**
  - Mathematical background
    ✓ Quick introduction to probability and statistics
    ✓ Quick Introduction to detection and estimation theory
  - Case Studies
    ✓ ROC (receiver operating characteristic) and the false positive & missed detection tradeoff
    ✓ Bayesian Detection Techniques (Spam filtering)
    ✓ (Sequential) Hypothesis Testing for Attack Detection
    ✓ Sequential Probability Ratio Testing for scan classification, data classification techniques and algorithms
    ✓ Base Rate Fallacy and the false alarm dilemma
    ✓ Distributed IDSs and data fusion (sufficient statistics)
    ✓ McHugh’s critique
    ✓ Change point detection for finding stealthy distributed activity
    ✓ Characterizing “(ab)normal” behavior: Machine learning and pattern matching algorithms
    ✓ Audit data selection and the theory of sampling.

- **Part 3 (Experimental tools)—TBD**
  - Bro: A System for Detecting Network Intruders in Real-Time
  - Snort and Network Intrusion Analysis
  - Suricata

- **Part 4 (Other topics we might cover)**
  - Graph theory and virus propagation
  - Characterizing audit data: Information theory entropy
  - Neural networks
  - Audit data analysis and mining
  - Attack graphs for incidents analysis and attack correlation
  - Response and counter-response: a game theoretical approach
  - Policy and legal issues surrounding the use of IDS
  - Response: What to do with detection once it occurs

---

**Code of Academic Integrity**

The University of Maryland, College Park has a nationally recognized Code of Academic Integrity, administered by the Student Honor Council. This Code sets standards for academic integrity at Maryland.
for all undergraduate and graduate students. As a student you are responsible for upholding these standards for this course. It is very important for you to be aware of the consequences of cheating, fabrication, facilitation, and plagiarism. For more information on the Code of Academic Integrity of the Student Honor Council, please visit http://shc.umd.edu/SHC/HonorPledgeInformation.aspx.