The Application of Machine Learning to Cybersecurity
“Cyber Analytics”
Lecture 1

John Cavazos

Dept of Computer & Information Sciences

University of Delaware

CISC 849 : CyberAnalytics

Bio of Instructor

- John Cavazos <cavazos@cis.udel.edu>
- Associate Professor, CIS
- Founder and CTO, Cyber 20/20 Inc.
- Previously: JP Morgan Faculty Fellow, Institute for Financial Services Analytics
- Research
  - Application of Machine Learning to Real-World Problems
    - Compilation (e.g., Automatic Tuning of Programs)
    - High-performance Computing (e.g., Accelerators)
    - Cybersecurity (e.g., Malware Detection)

Lecture 1: Overview

- Structure of Course
- Administrivia

Topics of Interest

- Anything of interest at the cross-section of Advanced Analytics and Cybersecurity
- E.g., any of these applied to cybersecurity:
  - High-performance computing
  - Machine Learning and Predictive Analytics
  - Visualization
  - Big Data and the Cloud
  - Chat bots

Structure of the Course

- First few lectures done by myself and my research group
- Next N lectures are done by:
    - Guest Lectures
    - Students
        - Research paper presentations (20 mins.)
        - Project status updates

Structure of the Course

- Projects
- Two projects (next slide)
  - Team projects (2 or 3 per team)
  - Project reports will be due for both projects
    - Amount of work proportional to size of team
  - Presentation due for Project 1 and 2

Project 1: Topic Review

- Choose a topic of interest (from list instructor specifies)
- Implement some discrete piece identified in first day
- Extensive programming and/or analysis
- Deliverable: Project Report
  - ~2 pages per team member
  - Template available online (font size, margins,etc.)
- Project hand out available soon

Project 2: Implementation

- Extension of Project 1 (recommended)
  - Potential to perform a new project
- Extensive programming and/or analysis
- Deliverable: Report (~2 pgs per team member)
  - Conference paper format
  - Project presentation (~10 mins)
- Project handout available in a couple weeks

Basis for Grading

- Your individual paper presentations (20%)\
- Class Quizzes (5%)
- Team Projects (75%)
  - Project 1 (30%)
    - Presentation and Project Report
  - Project 2 (45%)
    - Status Reports
    - Presentation and Project report

No Midterm or Final!

Lecture 1: Overview

- Structure of Course
- Administrivia

Background/References

- Should be familiar with a programming language for projects
  - For example, Python, R, C++, Java, etc.

- No textbook required
  - There are several references, see course website

Project Guidelines

- Papers should be
  - Well-written and formatted correctly
  - Properly referenced
  - Results should be presented with graphs
  - Intellectual merit most important factor
- Negative result is fine
  - However, must demonstrate something interesting

Think of this as writing a conference paper!

Expectations

- Class participation
- Ask questions
- Challenge all speakers.
- NOT a lecture class or a passive experience. ACTIVE learning.
- Most common project problem: Not getting started
- *Ask for help if you need it!*
  - I will hold office hours Saxby's on Amstel Ave.
    - Email *first* me whenever you want an appointment.
  - Require checkpoints to show me status!