John J. Seymour, III

seymour1@umbc.edu sites.google.com/site/jjseymour3
https://github.com/seymour1/ https://www.kaggle.com/seymour1

Research Interests	Machine Learning, Malware Analysis, Quantum Computing
Proficiencies	bash, python, git, sklearn, nltk, tweepy, boto, matplotlib
Comfortable with	xgboost, seaborn, docker, spacy, gcloud, apache spark, mysql

Work Experience

ZeroFOX, Inc

Senior Data Scientist, September 2016 - Present

- Piloted ZeroFOX FoxThreats program for threat hunting on social media
- Added LIME, an explainer for black box machine learning classifiers, to ZeroFOX machine learning capabilities
- Co-created classifier to find spammers and off-platform redirects for a social networking site

Data Scientist, September 2015 - September 2016

- Drove development and sales through internal data science and information security research
- Demonstrated thought leadership at top tier information security conferences (Black Hat USA, DEF CON, BSidesLV, SecTor)
- Led development of SNAP_R, a pen-testing tool using machine learning to automate generation of individually tailored phishing messages on social media
- Developed solution to detect money-flipping scam posts on Instagram
- Created datasets for future product offerings using Mechanical Turk/Amazon S3
- Research covered by Forbes, The Atlantic, BBC Technology, among others

CyberPoint International, LLC

Student Intern, Summer 2015

- Recreated top Kaggle Malware Competition models and compared to models in the CyberPoint Machine Learning Model Training Pipeline.
- Added the Python xgboost library and the t-SNE dimensionality reduction algorithm to the Model Training Pipeline.
- Created multiple Java programs with various algorithms and data structures for use in the DARPA Space/Time Analysis for Cybersecurity project.

Army Research Lab

Student Intern, Summer 2014

- Transformed satisfiability problems into problems the D-Wave SR10V6 could solve using ToQ, a D-Wave proprietary software.
- Demonstrated and reduced bias in D-Wave chips using Python, error correcting codes, and statistical techniques.

University of Maryland, Baltimore County

Graduate Research Assistant, UMBC DREAM Lab, January 2014 - May 2015

- Created Bash Scripts and Cron jobs to scrape urlquery.net for links to websites redirecting to exploit kits.
- Integrated VirtualBox, Wireshark, Bash and Python scripts, and Suricata to intercept and record all traffic to exploit kit landing pages.
- Published multiple papers on Exploit Kit classification and overgeneralization in malware classification.

Graduate Teaching Assistant, August 2012 - December 2013

- Teaching Assistant for Network Security, Computer Security, Cryptography, Automata Theory, and Introduction to Object-Oriented Programming.
- Introduced students to Metasploit/Kali Linux and theoretical aspects of cybersecurity.

Graduate Research Assistant, UMBC Cyber Defense Lab, January 2012 - August 2013

- Designed, tested, deployed, and maintained the SecurityEmpire website and game.
- Administered Mercurial repository, managed Red Hat server with Apache HTTPD to host project, and developed server-side code using PHP and MySQL.

Pyxis Engineering/Applied Signals Technology

Associate Engineer, June 2009 - January 2010

- Designed, tested, and deployed a Training Request Management System using Java, Spring, HTML, CSS, Javascript, JUnit, MySQL, Apache Maven, and Apache Tomcat.

Education

University of Maryland, Baltimore County (UMBC)

Ph.D. in Computer Science (Expected Fall 2017)

For list of publications, see https://sites.google.com/site/jjseymour3/publications

Graduate GPA: 4.0/4.0

M.S. in Computer Science (Fall 2014)

Thesis Title: Quantum Classification of Malware

Presented at DEFCON23, Summer 2015

B.S. *cum laude* in Computer Science (Fall 2011)

B.S. *cum laude* in Mathematics (Fall 2011)

B.A. *cum laude* in Philosophy (Fall 2011)

Certificate of General Honors

Undergraduate GPA: 3.70/4.00