Michael Tran

http://trankmichael.github.io/

tranmichael@protonmail.com
949-207-8743

Education

- **Tufts University School of Engineering** Somerville, MA
  B.S.C.S. Computer Science — B.S. Mathematics *August 2012 - May 2016*
  - **Important Courses:**
    - **Computer Science:** Statistical Pattern Recognition, Programming Languages, Web Development, Probabilistic System Analysis, Algorithms, Computer Security, Machine Structure
    - **Math:** Computational Geometry, Abstract Algebra, Real Analysis, Linear Algebra, Discrete Mathematics

Experience

- **Philips Healthcare (Information Security Innovation)** Andover, MA
  Security Engineer *June 2016 – Current*
  - worked on code evaluations and systems assessments of production applications
  - researched and created machine learning algorithms for analysis of network traffic
  - engaged in third party vendor comparisons and evaluations for enterprise security solutions
- **Tufts University (Computer Science Department)** Medford, MA
  Algorithms - Teaching Assistant *January 2016 – May 2016*
  - Graded student assignments and exams
  - worked with students to understand areas such as sorting, recursion, and dynamic memory
- **Enigma – Tufts Independent Data Journal** Medford, MA
  Editor *January 2015 – December 2015*
  - led workshops for the Tufts community for anyone interested in data science and statistical analysis
- **CoreLogic** Irvine, CA
  Product Development Software Engineering Intern *June 2015 – September 2015*
  - developed a Python application to help automate the development mockup process necessary in a system migration
  - developed a Python application to monitor the performance metrics of different application builds in AppDynamics and QuickBuild
  - improved UX features on Ext JS Web Application

Skills

Technologies: Python, C/C++, Git, Django, Burp, Metasploit, NumPy, Scikit, plot.ly

Projects

Network Alarm: A network alarm implemented in Ruby. the program detects port scanning attacks and leaked plaintext credit card information in a live network stream. Given a web log, the program detects NMAP scans, HTTP error codes, embed shellcode, and leaked credit card information.

Phishing Protection Analytics: A python implementation of phishing detection models for Outlook on both OS X and Windows. The application uses three separate prediction models to classify emails based on semantic content analysis, link/url analysis, and email header analysis.

Data Depth Explorer: Interactive visualizations and descriptions of three different types of multivariate statistical data depth created using Processing.js and Bootstrap. Allows users to input or generate random data to visualize the various statistical centers of point sets.