AARON SEGAL

51 Prospect Street
New Haven, CT 06511
(914) 500-7976
aaron.segal@yale.edu

EDUCATION

Ph.D., Computer Science
Yale University, New Haven, CT
Began September 2011

M.S., Computer Science
Brown University, Providence, RI
December 2010

B.A., Economics & Mathematics, minor in Computer Science
Boston University, Boston, MA
Magna Cum Laude, May 2009

PUBLICATIONS

Aaron Segal, Bryan Ford, Joan Feigenbaum. "Catching Bandits and *Only* Bandits: Privacy-Preserving Intersection Warrants for Lawful Surveillance." In Proceedings of the 4th USENIX Workshop on Free and Open Communications on the Internet (FOCI 14). August 2014

Debayan Gupta, Aaron Segal, Aurojit Panday, Gil Segev, Michael Schapirax, Joan Feigenbaum, Jenifer Rexford, Scott Shenker. "A New Approach to Interdomain Routing Based on Secure Multi-Party Computation." In Proceedings of the 2012 ACM Workshop on Hot Topics in Networks. October 2012

Master's Thesis: "Rational Secret Sharing with Side Information in Point-to-Point Networks via Time -Delayed Encryption." December 2010.

RECENT PROFESSIONAL EXPERIENCE

U.S. Naval Research Laboratory
NREIP Intern — May – August 2014
Determine vulnerabilities and potential attacks against live Tor software, build simulator of measurement tool in testbed onion-routing network as part of Naval Research Enterprise Internship Program

Yale University
Teaching Assistant — January 2012 – May 2014
Mentor students, hold office hours, grade homework and exam problems for undergraduate- and graduate-level computer science courses

Factset Research Systems
Software Engineer — March – August 2011
Enhance functionality of financial analysis software by integrating machine learning algorithms into existing code, spend time on-call handling critical errors and outages for the FactSet live application

SELECTED PROGRAMMING PROJECTS

Integrated an existing machine-learning algorithm into live code being used for the FactSet application news pipeline, making major changes to object-oriented base class code without affected inherited classes **(Implemented using C++ and Python, on Red Hat Linux)**

Programmed a vacuum-like robot to play soccer in structured environments, using techniques in computer vision, localization, subsumption architecture and path planning **(Implemented using C++ and Player, on Debian Linux)**

For undergraduate research, implemented a new cryptographic key agreement protocol for two parties across a network **(Implemented using C++ on Windows)**