Curriculum Vitae — Blaine Nelson

Department of Computer Science	Phone:	+49 (0)331 977 3067
University of Potsdam	Email:	bnelson@cs.uni-potsdam.de
Building 4, Office 0.20		blaine.nelson@gmail.com
August-Bebel-Str. 89	Homepage:	https://www.cs.uni-potsdam.de/∼bnelson/
14482 Potsdam, Germany	Research page:	http://blaine-nelson.com/research/index.html

Career & Research Interests

My current career focus is on the application and theory of secure learning—a field addressing the consequences of machine learning algorithms in security-sensitive systems. Topics of interest include machine learning, computer security & privacy, secure/adversarial learning, robust learning, intrusion/spam detection, online learning, large-scale learning, and game theory.

List of publications available at http://www.blaine-nelson.com/research/blaine-nelson-pubs.pdf

Education

▷ University of California, Berkeley, CA
- Ph.D Computer Science, December 2010.
  - *Dissertation Title*: Behavior of Machine Learning Algorithms in Adversarial Environments.
  - *Committee*: Anthony D. Joseph, Peter L. Bartlett, Terry Speed, and J. D. Tygar.
- M.S. Computer Science, December 2005.
  - *Thesis Topic*: Designing, Implementing and Analyzing a System for Virus Detection.
  - *Adviser*: Anthony D. Joseph

▷ University of South Carolina, Columbia, SC
- B.S. Computer Science with a minor in Mathematics, May 2003.
  - *Magna Cum Laude* with Honors from South Carolina Honors College.

Research Experience

▷ Postdoctoral Researcher (*Supervisor*: Tobias Scheffer). *University of Potsdam, Germany*, 2013–present.
- Investigating robust learning methods for secure learning.
- Co-teaching a class on machine learning and a seminar on game theory in machine learning.

▷ Humboldt Postdoctoral Research Fellow (*Supervisors*: Pavel Laskov & Andreas Zell). *University of Tübingen, Germany*, 2011–2013.
- Member of Reactive Security (RSec) group studying machine learning for security applications.
- Published 4 peer-reviewed/workshop papers analyzing machine learning in adversarial settings.
- Organized 3 lectures on techniques for English technical writing.
- Co-taught a class on advanced methods for machine learning.

▷ Graduate Researcher (*Adviser*: Anthony Joseph). *University of California, Berkeley.* 2003–2010.
- Co-led the SecML research group under the advisement of Anthony Joseph, Doug Tygar, & Satish Rao; set research directions; organized students; and lead two research projects.
- Published 7 peer-reviewed/workshop papers, 2 journal articles, and 1 book chapter analyzing machine learning in adversarial settings.
- Developed an experimental framework for parallelizing large experiments on clusters / Amazon EC2.
- Lead a reading group studying Robust Statistics.

▷ Summer Research Intern (*Mentor*: Ira Cohen). *Hewlett-Packard Labs, Palo Alto.* June–August 2006.
- Studied algorithms for clustering with pairwise constraints and developed a new clustering approach leading to a publication at ICML in 2007 and a patent (US Patent No: 7,870,136).

▷ Research Experience for Undergrads Fellow (*Adviser*: Leslie Collins). *Duke University.* Summer 2002.
- Undertook a research project using neural networks to identify electromagnetic signatures from low-metal-content landmines resulting in one publication.

Teaching and Mentor Experience

- ▷ Co-lecturer with Prof. Dr. Tobias Scheffer, Dr. Niels Landwehr, Dr. Christoph Sawade, & Uwe Dick. *University of Potsdam*, Summer 2013.
  - *Course*: Maschinelles Lernen (Machine Learning) 2
  - Preparing and presenting 2 lectures, homeworks, & final exam
- ▷ Seminar co-organizer with Prof. Dr. Tobias Scheffer & Michael Großhans. *University of Potsdam*, 2013.
  - *Seminar*: Seminar Spieltheorie im maschinellen Lernen (Game Theory in Machine Learning)
- ▷ Co-lecturer with Dr. Pavel Laskov. *University of Tübingen*, Summer 2012.
  - *Course*: Advanced Topics in Machine Learning.
  - Prepared and presented 6 lectures; designed and corrected exercises and final exam.
- ▷ Teaching Assistant for Prof. Dr. Andreas Zell. *University of Tübingen*, Winter 2011/2012.
  - *Course*: Künstliche Intelligenz (Artificial Intelligence)
  - Co-taught weekly exercise sections and designed and corrected weekly exercises.
- ▷ Mentor for summer research interns. *University of California, Berkeley*. Summer 2010.
  - Co-mentored 10 Research Experience for Undergraduates (REU) students.
  - Directed & organized 3 student groups to undertake a large-scale modeling/simulation project.
- ▷ Undergraduate Student Mentor. *University of California, Berkeley*. 2006–2010.
  - Mentored senior students with research projects designed to give them research experience.
  - 7 students graduated: 2 are pursuing graduate degrees.
- ▷ Volunteer Teacher with *San Quentin's Prison University Project*. 2004–2010.
  - Taught and tutored preparatory mathematics (Math 50) once per week.
  - Co-taught College Algebra (MTH 115). Summer/Fall 2008 and Spring 2009.
- ▷ Teaching Assistant for Dr. Stuart Russell. *University of California, Berkeley* Fall 2005.
  - *Course*: Artificial Intelligence (CS 188).
  - Taught 2 exercise sections; designed & corrected homework, programming projects, & exam

Scientific Community Activities

Organizational Activities

- ▷ Co-chair for the 2013 Workshop on Artificial Intelligence and Security (AISec) with Christos Dimitrakakis and Elaine Shi, to be held in October, 2013.
- ▷ Co-chair for the 2012 Workshop on Artificial Intelligence and Security (AISec) with Benjamin Rubinstein and Alvaro Càrdenas, October, 2012.
- ▷ Coordinator for the Dagstuhl Perspectives Workshop: Machine Learning Methods for Computer Security, September 9–14, 2012.

Participation as a Reviewer

- ▷ Member of Workshop Program Committees: PSDML 2010 and AISec 2011, 2012, and 2013.
- ▷ Reviewer for the conferences ICML 2013, NIPS 2011, 2012 and 2013, and for journals JMLR, Neurocomputing, TDSC, Computers & Security, and EURASIP Journal on Information Security.

Honors and Awards

- ▷ Humboldt Postdoc Fellowship from the Alexander von Humboldt Foundation, 2011.
- ▷ Outstanding Student in Computer Science at University of South Carolina, 2003.
- ▷ Honorable Mention in Computer Research Association's Outstanding Undergraduate, 2002.
- ▷ Bausch and Lomb Science Award, 1999.
- ▷ University of S. Carolina Alumni Association Scholarship and Math & Science Dean's Scholarship, 1999.
- ▷ Attained rank of Eagle Scout in Boy Scouts of America, 1997.

Miscellaneous

- ▷ *Programming languages*: Java (primary), Python, Perl, R, Matlab
- ▷ Proficient with Ubuntu Linux, Windows and MacOS platforms
- ▷ *Spoken Languages*: English and conversational German