

John Bethencourt

Email bethenco@cs.berkeley.edu
Web <http://www.cs.berkeley.edu/~bethenco/>
Address 2021 Blake St Apt A, Berkeley, CA 94704
Mobile 510 508 5807

EDUCATION

- **University of California, Berkeley.**
Ph.D. in Computer Science expected December 2010. Advised by Dawn Song.
- **Carnegie Mellon University.**
Spent two years as a Ph.D. student in Computer Science before transferring to Berkeley when advisor (Dawn Song) moved there.
- **University of Wisconsin, Madison.**
B.S. received in May 2005 with majors in Computer Science, Mathematics, and Computer Engineering. GPA of 3.96 in Computer Science and 3.64 overall.

PUBLICATIONS

- New Techniques for Private Stream Searching. John Bethencourt, Dawn Song, and Brent Waters. *ACM Transactions on Information and System Security (TISSEC) 12 (3), January 2009.*
- Analysis-Resistant Malware. John Bethencourt, Dawn Song, and Brent Waters. *15th Network and Distributed System Security Symposium (NDSS), February 2008.*
- Ciphertext-Policy Attribute-Based Encryption. John Bethencourt, Amit Sahai, and Brent Waters. *28th IEEE Symposium on Security and Privacy (Oakland), May 2007.*
- Multi-Dimensional Range Query over Encrypted Data. Elaine Shi, John Bethencourt, Hubert Chan, Dawn Song, and Adrian Perrig. *28th IEEE Symposium on Security and Privacy (Oakland), May 2007.*
- Cryptographic Methods for Storing Ballots on a Voting Machine. John Bethencourt, Dan Boneh, and Brent Waters. *14th Network and Distributed System Security Symposium (NDSS), February 2007.*
- New Constructions and Practical Applications for Private Stream Searching (Extended Abstract). John Bethencourt, Dawn Song, and Brent Waters. *27th IEEE Symposium on Security and Privacy (Oakland), May 2006.*
- Mapping Internet Sensors with Probe Response Attacks. John Bethencourt, Jason Franklin, and Mary Vernon. *14th USENIX Security Symposium, August 2005.* Received the conference's Best Paper award.
- Running Quake II on a Grid. Glenn Deen, Matthew Hammer, John Bethencourt, Iris Eiron, John Thomas, and James Kaufman. *IBM Systems Journal 45, No. 1, pp. 21-44, January 2006.*

HONORS AND AWARDS

(graduate)

- NSF Graduate Research Fellowship, 2006
- NDSEG Fellowship, 2006

(undergraduate)

- Best Paper, USENIX Security 2005
- Dowling Prize, 2005 (UW Math Dept.)
- Fred W. and Josephine Colbeck Scholarship, 2004 (UW ECE Dept.)
- Robert Mensel Scholarship, 2003 (UW ECE Dept.)
- Richard H. Thomas Family Distinguished Scholarship, 2002 (UW ECE Dept.)
- Henry Vilas Scholarship, 2000 (UW)
- Kemper K. Knapp Scholarship, 2000 (UW)
- Freshman Engineering Scholarship, 2000 (UW College of Engr.)

EXPERIENCE

- **SRI International.** May 2006 - August 2006
Research Intern
Collaborated with Brent Waters of SRI and Dan Boneh of Stanford on several cryptography and systems security projects. Developed new cryptographic techniques for secure ballot storage on DRE voting machines and wrote paper appearing in NDSS 2007 on this topic. Also developed and released GPL implementations of recent cryptographic techniques.
- **IBM, Almaden Research Center.** May 200{4, 5} - August 200{4, 5}
Research Intern
In 2004, investigated trade-offs between communication and computation encountered when distributing a parallel problem with nearest neighbor connectivity in a grid computing environment with a shared whiteboard for communication. The following summer, developed a distributed, agent-based simulator which allows the modeling of the spread of infectious disease at the national level.
- **CS Dept. of UW Madison, CIPART Project.** January 2004 - May 2005
Research Assistant
Worked on a research project investigating the potential utility of exchanging security log data between network administration sites and conducted an investigation of an attack on networks for log sharing. Gave talks on this work at the Army Research Office workshops on critical infrastructure protection in May 2004 and June 2005. Presented a paper on the discovered attack at the USENIX Security 2005, where it won the best paper award.
- **IBM, Extreme Blue Program.** June 2003 - August 2003
Computer Science Intern
Participated in Extreme Blue internship program at the Almaden Research Center. Designed and implemented system which applied grid computing to massively multiplayer online games with two other students. Presented results to CEO Sam Palmissano. Project was featured at the 2003 Linux-World conference and in Technology Review, eWeek, and Slashdot. Coauthored a paper on this work which appeared in the IBM Systems Journal.
- **CS Dept. of UW Madison, Condor Project.** January 2002 - March 2003
Project Assistant
Implemented research work in the field of high throughput distributed computing using C, C++, and Perl. Partially designed a sub-system for running parallel programs on distributed resources.

PROFESSIONAL ACTIVITIES

- External paper reviewer for CCSW 2009, PETS 2009, Pairing 2009, AISec 2008, CCS 2008, SIGCOMM 2008, CSFS 2008, Oakland 2008, WORM 2007, EVT 2007, RAID 2007, EuroSys 2007, CCS 2006, MINENET 2006, NSDI 2006, ISPEC 2006, Financial Cryptography 2006, AsiaCCS 2006, NDSS 2006, the Journal of Computer Security, IEEE Transactions on Dependable and Secure Computing, and ACM Computing Surveys.

COMMUNITY ACTIVITIES

- **Dec/5.** September 2005 - May 2006
Member
Helped to organize and run social events for the faculty and students of the CMU School of Computer Science.
- **Undergraduate Projects Laboratory.** January 2001 - May 2005
Coordinator
Helped to organize and run a computer club for undergraduates at the University of Wisconsin. Responsible along with the other coordinators for planning projects, giving tutorials, helping direct the operation of the UPL, and systems administration of a network of about a dozen machines, several hundred user accounts, and a variety of servers (NFS, web, mail, DNS, etc.).