

Curriculum Vitae: Michael Bailey

Michael D. Bailey
Department of Electrical Engineering and Computer Science
University of Michigan
Ann Arbor, MI 48109, USA
Email: mibailey@umich.edu
URL: <http://www.eecs.umich.edu/~mibailey>

Professional Preparation

2006 Ph.D. in Computer Science, University of Michigan, Ann Arbor, MI.
1995 M.S. in Computer Science, DePaul University, Chicago, IL.
1992 B.S. in Computer Science, University of Illinois, Urbana, IL.

Appointments

UNIVERSITY OF MICHIGAN, ANN ARBOR, MICHIGAN Assistant Research Scientist (2007-Present), Adjunct Lecturer (Winter 2008), Research Project Manager (2004 - 2007)

In this role I perform basic and applied research in the area of networking and computer security. I am responsible for identifying and selecting the problems to be studied, the approach to them, and the organization and presentation of results obtained. In particular, I oversee research related activities for a variety of research grants awarded to Farnam Jahanian, Z. Morley Mao, and other faculty in the Software Systems Research Lab (SSRL). I participate in writing at new research proposals, lead in writing technical articles for publication, and conduct research related outreach and community service through presentation of published results in conferences and workshops, and by participating in program committees and panels. In addition, I teach classes in core computer science, and in my specific subfields (i.e., Distributed Systems, Networking, and Security).

ARBOR NETWORKS, INC., ANN ARBOR, MICHIGAN Director of Engineering (2001 - 2004)

As Director of Engineering I coordinated the actions of engineering managers, architects, engineers, and release engineering for all of Arbor's products. I oversaw design, implementation, documentation, and QA activities. I was responsible for all evaluations, hiring and budget activities (3M+) for a department of 30 people. As a director, routinely interfaced with product marketing, sales, HR, legal and finance as well as performed deployment, operations, and sales engineering tasks for marquee customers. Major milestones included developing software engineering processes, building the QA team, growing the engineering team from 10-30, and the delivery (on-time) of 3 new software products and associated follow on releases.

UNIVERSITY OF MICHIGAN, ANN ARBOR, MICHIGAN Graduate Student Research Assistant (1995-2001, 2004)

As a student I performed research in a variety of areas including artificial intelligence, learner center design, computer games, dynamic web caching, networking, and computer security. My thesis (completed in 2006), entitled "A Scalable Hybrid Architecture for Measuring, Tracking, and Characterizing Internet Threat Dynamics", proposed and evaluated an architecture consisting of lightweight and heavyweight honeypots for measuring Internet threats such as denial of service attacks, worms, and botnets.

DEPAUL UNIVERSITY, CHICAGO, ILLINOIS Instructor (1994 - 1995)

Worked as an instructor for DePaul University, teaching undergraduate programming classes. Responsibilities included preparing and delivering lectures, coordinating GSI activities, developing and administering exams, and assigning student grades.

AMOCO CORPORATION, CHICAGO, ILLINOIS Programmer/Analyst (1992 - 1994)

Completed individual and team projects to meet client specifications for a variety of new software systems. Each project consisted of defining client needs, producing program specifications, developing test plans, coding and documentation.

Conference Publications

- Xu Chen, Jon Andersen, Z. Morley Mao, Michael D. Bailey, and Jose Nazario. Towards an Understanding of Anti-Virtualization and Anti-Debugging Behavior in Modern Malware. In Proceedings of the 38th Annual IEEE International Conference on Dependable Systems and Networks (DSN '08), pages 177-186, Anchorage, Alaska, USA, June 2008. 260 submissions, 63 accepted (24%)
- Michael D. Bailey, Jon Oberheide, Jon Andersen, Zhuoqing Morley Mao, Farnam Jahanian, and Jose Nazario. Automated Classification and Analysis of Internet Malware. In Proceedings of the 10th International Symposium on Recent Advances in Intrusion Detection (RAID '07), pages 178-197, Gold Coast, Australia, September 2007. 101 submissions, 16 accepted (16%)
- Sushant Sinha, Michael D. Bailey, and Farnam Jahanian. Shedding Light on the Configuration of Dark Addresses. In Proceedings of the 14th Annual Network & Distributed System Security Symposium (NDSS '07), pages 125-139, San Diego, California, USA, February-March 2007. (15%)
- Evan Cooke, Michael D. Bailey, Farnam Jahanian, and Richard Mortier. The Dark Oracle: Perspective-Aware Unused and Unreachable Address Discovery. In Proceedings of the 3rd Symposium on Networked Systems Design & Implementation (NSDI '06), pages 101-114, San Jose, California, USA, May 2006. 110 submissions, 28 accepted (25%)
- Michael D. Bailey, Evan Cooke, Farnam Jahanian, Niels Provos, Karl Rosaen, and David Watson. Data Reduction for the Scalable Automated Analysis of Distributed Darknet Traffic. In Proceedings of the 5th ACM SIGCOMM Conference on Internet Measurement (IMC '05), pages 239-252, Berkeley, California, USA, October 2005. 148 submissions, 36 accepted (24%)
- Michael D. Bailey, Evan Cooke, Farnam Jahanian, and Jose Nazario. The Internet Motion Sensor - A Distributed Blackhole Monitoring System. In Proceedings of the 12th Annual Network & Distributed System Security Symposium (NDSS '05), pages 167-179, San Diego, California, USA, February 2005. 124 submissions, 16 accepted (13%)

Workshop Publications

- Jon Oberheide, Michael D. Bailey, and Farnam Jahanian. PolyPack: An Automated Online Packing Service for Optimal Antivirus Evasion. In 3rd USENIX Workshop on Offensive Technologies (WOOT '09), Montreal, Canada, August 2009.
- Sushant Sinha, Michael D. Bailey, and Farnam Jahanian. One Size Does Not Fit All: 10 Years of Applying Context Aware Security. In Proceedings of the 2009 IEEE International Conference on Technologies for Homeland Security (HST '09), Waltham, Massachusetts, USA, May 2009.

- Michael D. Bailey, Evan Cooke, Farnam Jahanian, Yunjing Xu, and Manish Karir. A Survey of Botnet Technology and Defenses. In Proceedings of the Cybersecurity Applications & Technology Conference For Homeland Security (CATCH '09), pages 299-304, Washington, District of Columbia, USA, March 2009.
- Scott E. Coull, Fabian Monrose, Michael K. Reiter, and Michael D. Bailey. The Challenges of Effectively Anonymizing Network Data. In Proceedings of the Cybersecurity Applications & Technology Conference For Homeland Security (CATCH '09), pages 230-236, Washington, District of Columbia, USA, March 2009.
- Sushant Sinha, Michael Bailey, and Farnam Jahanian. Shades of Grey: On the effectiveness of reputation based 'blacklists'. In 3rd International Conference on Malicious and Unwanted Software (Malware 2008), October 7-8, 2008, Alexandria, VA, USA.
- Evan Cooke, Michael D. Bailey, Z. Morley Mao, David Watson, Farnam Jahanian, and Danny McPherson. Toward Understanding Distributed Blackhole Placement. In Proceedings of the 2nd Workshop on Rapid Malcode (WORM '04), pages 54-64, Washington, District of Columbia, USA, October 2004.

Books, Chapters, Magazine Articles

- Michael D. Bailey, Evan Cooke, Farnam Jahanian, David Watson, and Jose Nazario. The Blaster Worm: Then and Now. IEEE Security and Privacy, 3(4):26-31, 2005.

Other Manuscripts

- David Dittrich, Michael D. Bailey, and Sven Dietrich. Have we Crossed the Line? The Growing Ethical Debate in Modern Computer Security Research. In (Poster at) Proceedings of the 16th ACM Conference on Computer and Communication Security (CCS '09), Chicago, IL, USA, November 2009. A longer version appears as:
 - David Dittrich, Michael D. Bailey, and Sven Dietrich. Towards community standards for ethical behavior in computer security research. Technical Report 2009-01, Stevens Institute of Technology, Hoboken, NJ, USA, April 2009.
- Michael D. Bailey, Evan Cooke, Farnam Jahanian, Andrew Myrick, and Sushant Sinha. Practical Darknet Measurement. In Proceedings of the 40th Annual Conference on Information Sciences and Systems (CISS '06), pages 1496-1501, Princeton, New Jersey, USA, March 2006. (Invited paper)
- Michael D. Bailey, Evan Cooke, David Watson, Farnam Jahanian, and Niels Provos. A Hybrid Honeypot Architecture for Scalable Network Monitoring. Technical Report CSE-TR-499-04, University of Michigan, Ann Arbor, Michigan, USA, October 2004.
- Michael D. Bailey, Farnam Jahanian, G. Robert Malan, Jose Nazario, Dug Song, and Robert Stone. Measuring, Characterizing, and Tracking Internet Threat Dynamics. In Proceedings of the OpenSig 2003 Workshop (OpenSig '03), New York, New York, USA, October 2003. (Invited paper)

In Submission

- Erin Kenneally, Michael D. Bailey, and Douglas Maughan. A Tool for Understanding and Applying Ethical Principles in Network and Security Research. In submission, October 2009.
- Sushant Sinha, Michael Bailey, and Farnam Jahanian. Improving SPAM blacklisting through dynamic thresholding and speculative aggregation. In submission, September 2009.

Presentations and Invited Talks

- Enterprise Testbeds. EU/US Summit Series on Cyber Trust: System Dependability & Security, Dublin, Ireland, November 15-16, 2006
- Using Hybrid Honeypots to Monitor Internet Threats .The Joint Information Security Workshop on Internet Monitor and Analysis (ISWIMA), Tokyo, Japan, August 8th, 2006.
- The Internet Motion Sensor: A Distributed Blackhole Monitoring System, Lockdown 2005, Madison, Wisconsin, July 15, 2005
- Tracking Global Threats with the Internet Motion Sensor, NANOG 32, Reston, Virginia, October 17-19, 2004
- The Internet Motion Sensor, ISP Security and NSP-SEC BOF VI at NANOG 31, San Francisco, California, May 23-25, 2004
- Measuring Global Worm Activity, ISP Security and NSP-SEC BOF V at NANOG 30, Miami, Florida, February 8-10, 2004
- Shining Light on Dark Address Space, Craig Labovitz, Abha Ahuja and Michael Bailey, NANOG 23, Oakland, California, October 21-23, 2001

Synergistic Activities

As a research scientist I perform a variety of activities focused on researching the security and availability of complex distributed systems. In my role as an active member of IEEE, ACM, and Usenix, I routinely serve the community as a part of the program committee for conferences in my domain area. While not required by my position, I teach classes, give guest lectures in other's classes, and give invited talks to a broad community of network and security practitioners. In addition to traditional research products (i.e., publications), my research attempts to provide tools and data that make a substantive impact on the operations of today's networks. For example:

- As part of the DHS PREDICT project, our Virtual Center for Network and Security Data provides network and security researchers with valuable datasets for evaluation of new techniques and methods. We have made over 2.5TB of netflow data and 17 TB of network telescope data available in an anonymized form to security researchers.
- The Internet Motion Sensor (IMS) project is a network of distributed sensors that provides the capability to quickly and accurately characterize emerging threats like bots and worms. In addition to the numerous external networks, this software is actively deployed and used by the administrative staff of the College of Engineering (CAEN), the Information Technology Division (ITD), and our upstream service provider (Merit Network, Inc.).
- In our project entitled Detecting and Dismantling Botnet Command and Control Infrastructure using Behavioral Profilers and Bot Informants we are developing and deploying a system to detect and dismantle botnets. This software is deployed at the United States Computer Emergency Response Team (US-CERT) where this software helps protect 14 government agencies and networks. Furthermore, we are currently engaged in a technology transfer of this work to state and local governments through a pilot at the city of Seattle, WA.

Professional Activities

- Senior Member of IEEE
- Member of ACM, USENIX
- Chair for several conferences and workshops including:

- Third USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET '10)
- 40th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN '10) (finance chair)
- Program Committee for numerous conferences and workshops including:
 - 40th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN '20)
 - Workshop on Ethics in Computer Security Research (WECSR 2010)
 - 17th Annual Network and Distributed System Security Conference (NDSS '10)
 - 12th International Symposium on Recent Advances in Intrusion Detection (RAID '09)
 - Second USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET '09)
 - 11th International Symposium on Recent Advances in Intrusion Detection (RAID '08)
 - First USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET '08)
 - Proceedings of the 5th ACM workshop on Rapid Malcode (WORM '07)
 - First Workshop on Hot Topics in Understanding Botnets (HotBots '07)
 - Proceedings of the 4th ACM workshop on Rapid Malcode (WORM '06)
- External reviewer for numerous journals, conferences, and workshops including:
 - 16th ACM Conference on Computer and Communications Security (CCS 2009)
 - ACM Transactions on Information and System Security (TISSEC)
 - 30th IEEE Symposium on Security & Privacy (Oakland 2009)
 - 6th USENIX Symposium on Networked Systems Design and Implementation (NSDI '09)
 - Workshop: Research on Enterprise Networking (WREN 2009)
 - 18th USENIX Security Symposium (Usenix Security '09)
 - 15th Annual Network and Distributed System Security Symposium (NDSS 2008)
 - 15th Annual ACM Computer and Communications Security Conference (CCS 2008)
 - 38th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN '08)
 - 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN '07)
 - 10th International Symposium on Recent Advances in Intrusion Detection (RAID '07)
 - 9th International Symposium on Recent Advances in Intrusion Detection (RAID '06)
 - Second Workshop on Hot Topics in System Dependability (HotDep '06)
 - 2006 Internet Measurement Conference (IMC '06)

Funding Activities

Author of and PI, CO-PI, or Key personnel for numerous awarded grants:

- “Multi-Tiered Distributed Indication, Warning and Defense System” (ARDA, Key personnel)
- “The Internet Motion Sensor Project” (Intel, Key personnel)
- “The Internet Motion Sensor Project” (Cisco, Key personnel)
- “Detecting and Dismantling Botnet Command and Control Infrastructure using Behavioral Profilers and Bot Informants” (DHS, co-PI)

- “Virtual Center for Network and Security Data (Phase I)” (DHS, co-PI)
- “Virtual Center for Network and Security Data (Phase II)” (DHS, co-PI)
- “Virtual Center for Network and Security Data (Phase III)” (DHS, co-PI)
- “Topology-Aware Internet Threat Detection Using Pervasive Darknets.” (NSF, co-PI)
- “Collaborative Research: Enabling Security and Network Management Research for Future Networks” (NSF, co-PI)
- “New Frameworks for Detecting and Minimizing Information Leakage in Anonymized Network Data” (DHS, co-PI)
- “Collaborative Research: CT-L: CLEANSE: Cross-Layer Large-Scale Efficient Analysis of Network Activities to Secure the Internet” (NSF, PI)
- “CRI-IAD: Collaborative Research: Enabling Security and Network Management Research for Future Networks” (NSF, co-PI)
- “Botnet Attribution and Removal: From Axioms to Theories to Practice” (ONR, co-PI)
- “TC; Small: In-Cloud Security Services for Mobile Devices” (NSF, co-PI)

Teaching Experience

- EECS 591, Distributed Systems, Winter 2008, 19 Students (Q1 - 3.93, Q2 - 4.00)
- Various “guest lectures” including: EECS 591 - Distributed Systems (Winter 2003), EECS 489 - Computer Networks (Fall 2004, Winter 2005), EECS 496 - Professionalism and Ethics (Fall 2006), EECS 589 - Advanced Computer Networks (Fall 2006)

Department, College, and University Service Assignments

- DCO Faculty Liaison, 2007-2008

Students Supervised

Xu (Simon) Chen, Ph.D. in CS (currently enrolled), member of the Ph.D. committee; Kelsey M. Harris, BS in CS (currently enrolled, Dartmouth); Vaibhav Mallya, BS in CS (currently enrolled); Eric Vander Weele, MS in CS (currently enrolled); Junjing Xu, Ph.D. in CS (currently enrolled); Sushant Sinha, Ph.D. in CS in 2009 (Yahoo, India); Mark Griffen, BS in CS in 2009 (USAF); Stephen Hufnagel, MS in CS in 2007 (Microsoft); Kayle Hinkle, MS in CS in 2007 (Microsoft); Gabriele Giaquinto, MS in CS in 2007 (Microsoft); Andrew Myrick, MS in CS in 2007 (Apple); Jon Andersen, MS in CS in 2007 (Citrix); Rushi Desai, MS in CS in 2005 (Microsoft); Karl Rosaen, MS in CS in 2005 (Google)

Collaborators in Last 48 Months

Morley Mao, Farnam Jahanian, Kang Shin (University of Michigan); Jose Nazario (Arbor Network); Niels Provos (Google); Paul Barford, Jignesh Patel (University of Wisconsin); David Dittrich (University of Washington); Manish Karir (Merit Network); Nick Feamster, Wenke Lee, Alex Gray, David Dagon, Jon Giffin, Mustaque Ahamad, Xiaoming Huo (Georgia Tech); Fabian Monrose, Mike Reiter (University of North Carolina); John Mitchell (Stanford)

University); Giovanni Vigna, Chris Kruegel (University of California at Santa Barbara); Paul Vixie (Internet Systems Consortium); Phillip A. Porras, Vinod Yegneswaran (SRI International)

Graduate Advisor

Farnam Jahanian (University of Michigan)