10340 Swift Stream Pl #412
Columbia, MD 21044
☎ 646-402-5075
✉ mb@ivybells.com

Matthew Burnside

Education

2011 **Ph.D. (in progress)**, *Columbia University*, New York, NY, *4.0/4.0*.
Advisor: Angelos Keromytis

2005 **M.Phil.**, *Columbia University*, New York, NY, *3.9/4.0*.
Advisor: Angelos Keromytis

2002 **M.Eng.**, *Massachusetts Institute of Technology*, Cambridge, MA, *4.5/5.0*.
Thesis: An Architecture for Secure Resource Discovery
Advisor: Srinivas Devadas

2000 **B.S.**, *Massachusetts Institute of Technology*, Cambridge, MA, *4.3/5.0*.

Work experience

2009–now **Computer systems researcher**, *Department of Defense*, Washington, DC.
Performing cutting edge research in network security.

2002–2009 **Graduate research assistant**, *Columbia University*, New York, NY.
Performed cutting edge research in network and systems security.

2007–2009 **Technical consultant**, New York, NY.
Provided expert consulting services in multiple networking-related patent litigations.

2005 **Technical consultant**, *Revive Systems, Inc.*, New York, NY.
Introduced and exploited security flaws to test a software self-healing environment.

2000 **Intern**, *MIT Project Oxygen*, Cambridge, MA.
Designed and implemented a peer-to-peer network for secure resource discovery.

1999 **Intern**, *Netegrity, Inc*, Waltham, MA.
Designed and implemented a caching system for certificate revocation lists in a Verisign public key infrastructure.

1998 **Intern**, *MIT Media Laboratory*, Cambridge, MA.
Software Agents Group. Designed and implemented a regular expression and template parser for a vector database.

1997 **Intern**, *MIT Laboratory for Computer Science*, Cambridge, MA.
Clinical Decision Making Group. Implemented a mechanical ventilator controller.

Teaching

2006 **Instructor**, *Columbia University*.
W1003: Introduction to Programming, (summer), 15 students

2006 **Instructor**, *Columbia University*.
W1003: Introduction to Programming, (summer), 34 students

2006 **Instructor**, *Columbia University*.
W3827: Fundamentals of Computer Systems, (spring), 45 students

2005 **Teaching assistant**, *Columbia University*.
W4118: Operating Systems, (fall), 61 students

2005 **Teaching assistant**, *Columbia University*.
W3827: Fundamentals of Computer Logic, (summer), 4 students

2005 **Teaching assistant**, *Columbia University*.
W4180: Network Security, (spring), 46 students

2004 **Teaching assistant**, *Columbia University*.
W3824: Computer Organization, (summer), 10 students

2004 **Teaching assistant**, *Columbia University*.
W4118: Operating Systems, (spring), 36 students

2003 **Teaching assistant**, *Columbia University*.
W3824: Computer Organization, (summer), 12 students

2002 **Teaching assistant**, *Massachusetts Institute of Technology*.
6.170: Software Engineering, (fall), 20 students

Service

Program committee.
Workshop on Privacy in the Electronic Society (WPES '05)

External reviewer.
USENIX Security '08, IEEE S&P '08, TISSEC '07, ACSAC '07, CCS '07, ISC '07, DIMVA '07, AsiaCrypt '07, NDSS '07, IEEE S&P '07, ICDCS '07, NDSS '06, CCS '05, USENIX Security '05, ICDCS '05, WISA '04, LCN '04, NDSS '04

Supervised research projects

2008 *Public Key Sudo*, Mack Lu.

2008 *Applied Asynchronous Policy Enforcement*, Hyuksoo Seo.

2006 *Automatic Repair Validation Library*, Mack Lu. (with Mike Locasto)

2005 *Network topologies for MIXnets*, Miguel Maldonado.

Technical

Proficient in BSD, Linux, Windows, Mac OS X environments.

Languages: C, Python, Java

Programming experience with OpenBSD kernel, TCP/IP stack internals, SSH and SSL protocol stacks.

Publications

Journal publications

[1] Angelos D. Keromytis, Theo de Raadt, Jason Wright, and Matthew Burnside. Cryptography as an operating system service: A case study. *ACM Transactions on Computer Systems (ToCS)*, 24(1):1–38, 2006.

[2] Matthew Burnside and Angelos D. Keromytis. The case for crypto protocol awareness inside the OS kernel. *ACM SIGARCH Computer Architecture News*, 33(1):58–64, March 2005.

Conference and workshop proceedings

[1] Michael E. Locasto, Matthew Burnside, and Darrell Bethea. Pushing boulders uphill: The difficulty of network intrusion recovery. In *Proceedings of the 23rd Large Installation System Administration Conference (LISA '09)*, November 2009.

[2] Matthew Burnside and Angelos D. Keromytis. F3ildcrypt: End-to-end protection of sensitive information in web services. In *Proceedings of the 12th Information Security Conference (ISC '09)*, September 2009. (Acceptance rate: 27.6%).

[3] Michael E. Locasto, Matthew Burnside, and Angelos D. Keromytis. Online network forensics for automatic repair validation. In *Proceedings of the 3rd International Workshop on Security (IWSEC '08)*, November 2008. (Acceptance rate: 19.1%).

[4] Matthew Burnside, Mack Lu, and Angelos Keromytis. Authentication on untrusted remote hosts with public-key Sudo. In *22nd Large Installation System Administration Conference (LISA '08)*, November 2008.

[5] Matthew Burnside and Angelos D. Keromytis. Asynchronous policy evaluation and enforcement. In *Proceedings of the 2nd Computer Security Architecture Workshop (CSAW 2)*, October 2008.

[6] Matthew Burnside and Angelos Keromytis. Path-based access control for enterprise networks. In *11th Information Security Conference (ISC2008)*, September 2008. (Acceptance rate: 23.9%).

[7] Michael E. Locasto, Matthew Burnside, and Darrell Bethea. Research directions for network intrusion recovery. In *SOUPS Workshop on Usable IT Security Management (USM)*, July 2008. Invited paper.

[8] Matthew Burnside and Angelos D. Keromytis. Arachne: Integrated enterprise security management. In *8th Annual IEEE SMC Information Assurance Workshop*, pages 214–220, June 2007.

[9] Matthew Burnside and Angelos D. Keromytis. Low latency anonymity with mix rings. In *Proceedings of the 9th Information Security Conference (ISC)*, pages 32–45, 2006. (Acceptance rate: 20.2%).

[10] Matthew Burnside and Angelos D. Keromytis. The case for crypto protocol awareness inside the OS kernel. In *Proceedings of the Workshop on Architectural Support for Security and Anti-Virus (WASSA), held in conjunction with the 11th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS-XI)*, pages 54–60, October 2004.

[11] Matthew Burnside and Angelos D. Keromytis. Accelerating application-level security protocols. In *Proceedings of the 11th IEEE International Conference on Networks (ICON)*, pages 313–318, September/October 2003.

[12] Matthew Burnside and Angelos D. Keromytis. High-speed I/O: The operating system as a signaling mechanism. In *Proceedings of ACM SIGCOMM Workshop on Network-I/O Convergence: Experience, Lessons, Implications (NICELI)*, pages 220–227, November 2003.

[13] Sanjay Raman, Dwaine Clarke, Matthew Burnside, Srinivas Devadas, and Ronald Rivest. Access-controlled resource discovery for pervasive networks. In *Proceedings of ACM Symposium on Applied Computing (SAC '03)*, March 2003.

[14] Dwaine E. Clarke, Blaise Gassend, Thomas Kotwal, Matt Burnside, Marten van Dijk, Srinivas Devadas, and Ronald L. Rivest. The untrusted computer problem and camera-based authentication. In *Proceedings of First International Conference, Pervasive 2002*, pages 114–124, August 2002.

[15] Matthew Burnside, Dwaine Clarke, Todd Mills, Andrew Maywah, Srinivas Devadas, and Ronald Rivest. Proxy-based security protocols in networked mobile devices. In *Proceedings of ACM Symposium on Applied Computing (SAC2002)*, March 2002.

Technical reports

[1] Michael Locasto, Matthew Burnside, and Angelos D. Keromytis. Bloodhound: Searching out malicious input in network flows for automatic repair validation. Technical Report CUCS-016-06, Columbia University, April 2006.

[2] Matthew Burnside, Dwaine Clarke, Srinivas Devadas, and Ronald Rivest. Distributed SPKI/SDSI-based security for networks of devices. Technical report, MIT Laboratory for Computer Science, December 2002.

[3] Todd Mills, Matthew Burnside, John Ankcorn, and Srinivas Devadas. A proxy-based architecture for secure networked wearable devices. Technical report, MIT Laboratory for Computer Science, May 2001.