

Matthew Burnside

490 Computer Science Building
1214 Amsterdam Ave. M.C. 0401
New York, NY 10027-7003
(212) 939-7156
<http://www.cs.columbia.edu/~mb>

Education

- Ph.D. (Computer Science), Columbia University, in progress.
Advisor: Angelos Keromytis.
- M.Eng. (Computer Science and Engineering), Massachusetts Institute of Technology, 2002.
Thesis: An Architecture for Secure Resource Discovery.
Advisor: Srinivas Devadas.
- B.S. (Computer Science and Engineering), Massachusetts Institute of Technology, 2000.

Teaching

- Instructor, w1003, Introduction to Programming, Columbia University, Summer 2007.
- Instructor, w3827, Fundamentals of Computer Systems, Columbia University, Spring 2006.
- Instructor, w1003, Introduction to Programming, Columbia University, Summer 2006.
- TA, w3827, Fundamentals of Computer Systems, Columbia University, Summer 2005.
- TA, w4180, Network Security, Columbia University, Spring 2005.
- TA, w4180, Operating Systems, Columbia University, Fall 2005.
- TA, w3824, Computer Organization, Columbia University, Summer 2004.
- TA, w4118, Operating Systems, Columbia University, Spring 2004.
- TA, w3824, Computer Organization, Columbia University, Summer 2003.
- TA, 6.170, Software Engineering, MIT, Fall 2002.

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 proceedings

- [1] 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. To appear.
- [2] Matthew Burnside and Angelos Keromytis. Path-based access control for enterprise networks. In *11th Information Security Conference (ISC2008)*, September 2008. To appear.
- [3] 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.
- [4] Matthew Burnside and Angelos D. Keromytis. Arachne: Integrated enterprise security management. In *8th Annual IEEE SMC Information Assurance Workshop*, pages 214–220, June 2007.
- [5] 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.
- [6] 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.
- [7] 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.
- [8] Matthew Burnside and Angelos D. Keromytis. High-speed I/O: The operating system as a signalling mechanism. In *Proceedings of ACM SIGCOMM Workshop on Network-I/O Convergence: Experience, Lessons, Implications (NICELI)*, pages 220–227, November 2003.
- [9] 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 (SAC2003)*, March 2003.
- [10] 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.
- [11] 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.

Service

- Program Committee
 - Workshop on Privacy in the Electronic Society (WPES 2005).
- External Reviewer
 - USENIX Security 2008, IEEE S&P 2008, TISSEC 2007, ACSAC 2007, CCS 2007, ISC 2007, DIMVA 2007, AsiaCrypt 2007, NDSS 2007, IEEE S&P 2007, ICDCS 2007, NDSS 2006, CCS 2005, USENIX Security 2005, ICDCS 2005, WISA 2004, LCN 2004, NDSS 2004.

Supervised research projects

- *Public Key Sudo*, Mack Lu (2008)
- *Applied Asynchronous Policy Enforcement*, Hyuksoo Seo (2008)
- *Automatic Repair Validation Library*, Mack Lu (2006, with Mike Locasto)
- *Network topologies for MIXnets*, Miguel Maldonado (2005)

Work experience

March 2007 - present Expert consultant in multiple networking-related patent litigations.

June 2005 - August 2005 Columbia University STV (for Revive Systems, Inc., now StackSafe, Inc.)

August 2002 - present Graduate research assistant, Columbia University.

June 2000 - September 2000 Intern, MIT Project Oxygen.

June 1999 - September 1999 Intern, Netegrity, Inc.

June 1998 - September 1998 Intern, MIT Media Laboratory, Software Agents group.

June 1997 - September 1997 Intern, MIT Laboratory for Computer Science, Clinical Decision-Making group.

Talks

[1] Matthew Burnside. Methods for network anonymity. New York, NY, November 2004.

[2] Matthew Burnside. The case for crypto protocol awareness inside the OS kernel. Boston, MA, October 2004.