

MICAH SHERR

ADDRESS

3330 Walnut Street
Room 302
Philadelphia, PA 19104
E-mail: msherr@cis.upenn.edu
Homepage: <http://www.cis.upenn.edu/~msherr>

RESEARCH INTERESTS

Anonymity, electronic voting system security, network security, protocol design and analysis, network intrusion detection and prevention, data confidentiality, human-scale security, and privacy.

EDUCATION

- University of Pennsylvania* Ph.D. in Computer and Information Science, September 2003 - August 2008 (expected).
Advisor: Matt Blaze
- University of Pennsylvania* M.S.E. in Computer and Information Science. September 2003 - May 2005.
- University of Pennsylvania* B.S.E. in Computer Science and Engineering, *cum laude*. September 1996 - May 2000.
-

PUBLICATIONS

Refereed Publications

- Adam Aviv, Pavol Černý, Sandy Clark, Eric Cronin, Gaurav Shah, Micah Sherr, and Matt Blaze. Security Evaluation of the ES&S Voting Machines and Election Management System. In Third USENIX/ACCURATE Electronic Voting Technology Workshop (EVT '08), August 2008. *To appear*.
- Micah Sherr, Boon Thau Loo, and Matt Blaze. Veracity: A Fully Decentralized Service for Securing Network Coordinate Systems. In 7th International Workshop on Peer-to-Peer Systems (IPTPS 2008), February 2008.
- Eric Cronin, Micah Sherr, and Matt Blaze. On the (un)reliability of eavesdropping. *International Journal of Security and Networks (IJSN)*. 3(2):103-113, 2008.
- Micah Sherr, Boon Thau Loo, and Matt Blaze. Towards Application-Aware Anonymous Routing. In Second Workshop on Hot Topics in Security (HotSec07), August 2007.
- Micah Sherr, Eric Cronin, and Matt Blaze. Measurable Security through Isotropic Channels. In Fifteenth Annual Security Protocols Workshop, April 2007.
- Madhukar Anand, Eric Cronin, Micah Sherr, Matt Blaze, Zachary Ives, and Insup Lee. Sensor network security: more interesting than you think. In First Workshop on Hot Topics in Security (HotSec06), April 2006.
- Eric Cronin, Micah Sherr, and Matt Blaze. On the reliability of current generation network eavesdropping tools. In Second Annual IFIP WG 11.9 International Conference on Digital Forensics, January 2006.
- Micah Sherr, Eric Cronin, Sandy Clark, and Matt Blaze. Signaling vulnerabilities in wiretapping systems. *IEEE Security & Privacy*, 3(6):13-25, November 2005.

- Eric Cronin, Micah Sherr, and Matt Blaze. Listen too closely and you may be confused. In Thirteenth International Workshop on Security Protocols, April 2005.
- Micah Sherr, Michael Greenwald, Carl A. Gunter, Sanjeev Khanna, and Santosh S. Venkatesh. Mitigating DoS attacks through selective bin verification. In First Workshop on Secure Network Protocols (NPsec), November 2005.
- Mark Weiner, Micah Sherr, and Abigail Cohen. Metadata tables to enable dynamic data modeling and web interface design. *International Journal of Medical Informatics*, 65(1):51-58, April 2002.

Non-refereed Publications

- Patrick McDaniel, Matt Blaze, and Giovanni Vigna (Team Leads) *et al.*. EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing. December 2007.
- Matt Blaze, Arel Cordero, Sophie Engle, Chris Karlof, Naveen Sastry, Micah Sherr, Till Stegers, and Ka-Ping Yee. Source Code Review of the Sequoia Voting System. Part of the California Secretary of State Top-to-Bottom Review of electronic voting machines. July 2007.
- Micah Sherr. Approaches to Anonymity on the Internet: Measurements and Limitations. WPE-II Written Report. Department of Computer and Information Science, University of Pennsylvania. March 2007.
- Madhukar Anand, Eric Cronin, Micah Sherr, Matt Blaze, and Sampath Kannan. Security protocols with isotropic channels. University of Pennsylvania Technical Report, number TR-CIS-06-18, Nov 2006.
- Eric Cronin, Micah Sherr, and Matt Blaze. The eavesdropper's dilemma. University of Pennsylvania Technical Report, number MS-CIS-05-24. Aug 2005.

RESEARCH EXPERIENCE

Application-Aware Anonymity (A³)

Developed A³, a flexible architecture for deploying anonymity-based services on the Internet. A³ allows applications to tailor their anonymity properties and performance characteristics according to specific requirements. Using A³, hosts can establish anonymous routes with specific anonymity and network properties (topology, diversity, end-to-end latency, etc.), making practical the anonymization of next-generation Internet services previously considered unfit for anonymity.

EVEREST: Evaluation and Validation of Election-Related Equipment, Standards, and Testing

Evaluated source code of Election Systems & Software electronic voting system. Analyzed security properties of DRE (touchscreen) system and central optical ballot counter.

California Secretary of State's Top-to-Bottom Review of Electronic Voting Systems

Evaluated source code of Sequoia voting systems, including direct-recording electronic (DRE) voter-facing machines and backend tabulation software. Analyzed source code to determine the security and reliability properties of the electronic voting system.

Isotropism

Co-developed communication theory and analytical model of *Isotropic channels*, special broadcast communication media in which no party can reliably determine the source of an intercepted message and no party can reliably direct a message towards a particular receiver. Designed protocols for achieving near-perfectly secure confidentiality in Isotropic channels, as well as logical overlay networks for constructing Isotropic channels using the Internet infrastructure.

Distributed Detection and Inference

The Distributed Detection and Inference (DDI) program at Intel Research, Santa Clara proposes a collaborative and distributed system for detecting stealthy and emerging worms. Research concentrated on investigating the efficacy of DDI in enterprise networks. Developed worm models and containment strategies, and implemented an ns2-based simulator to measure the effectiveness of the DDI approach.

Trustworthy Eavesdropping and Countermeasures (TNEC) Project

Investigated the reliability of Internet and telephone interception systems. Co-developed *confusion* technique, a unilateral information theoretic approach to confidentiality in which the sender or a third-party injects noise to mask plaintext messages. Co-discovered confusion-related vulnerabilities in telephone wiretap systems.

PROFESSIONAL EXPERIENCE

University of Pennsylvania, PhD Candidate, September 2003 – Present

Conducted research towards PhD degree.

University of California, Berkeley, Source Code Reviewer, June 2007 – July 2007

Analyzed source code of Sequoia electronic voting systems as part of the California Secretary of State's Top-to-Bottom review of California's electronic voting systems.

Intel Research, Intel Corporation, Intern, June 2006 – March 2007

Investigated the efficacy of Distributed Detection and Inference (DDI), a collaborate worm detection system, on enterprise networks. Developed worm models and worm containment strategies. Implemented an ns2-based simulator to analyze the performance of DDI against various worm models.

Columbia University, Programmer / Analyst, August 2001 – June 2003

Designed and implemented web based applications for Student Information Systems department. Conducted research and proof-of-concept designs. Built, maintained, and administered software-based clustering (OpenMOSIX clustering) of Linux servers.

Independent Security Consultant, July 2001

Secured production environment for a major financial institution's online banking website. Enumerated various potential security vulnerabilities in the proposed system's infrastructure and implementation.

Scient, Inc., Consultant, Technology Innovation Center, July 2000 – June 2001

Oversaw installation and configuration of Oracle, WebLogic, Netscape iPlanet, SiteMinder, and NCipher software on Sun servers. Created server monitoring tools for MIS reporting. Engaged in research for Scient's Any-to-Any initiative, a program for designing commercial "write once, run everywhere" programming packages. Authored series of internal papers that focused on creating programming and testbed environments for wireless applications compatible with the Palm VII device.

Netegrity, Inc., Intern, May 1999 – August 1999

Netegrity, Inc. is a security company whose flagship product, SiteMinder, is used by major financial and corporate institutions to manage authentication and authorization across disparate systems within a company's intranet. Designed and engineered Managed Self Registration (MSR) software. Developed specialized and proprietary programming language and interpreter. The MSR language allowed developers to create custom applications for assigning and retracting access privileges, as well as registering new identities with the SiteMinder user repository.

TEACHING EXPERIENCE

Co-instructor, Operating Systems Laboratory (CSE381). Fall 2005, Fall 2006, and Fall 2007

Prepared and presented weekly lectures. Developed and evaluated class projects. Oversaw teaching assistants.

Mentor, Undergraduate Senior Project (CSE400/401). Fall 2005 – Spring 2006

Mentored undergraduate student conducting senior project on *confusion* eavesdropping countermeasures.

Teaching Assistant, Software Systems (CIS505). Spring 2005

Prepared assignments, evaluated semester projects, and guest lectured on security and cryptography.

Teaching Assistant, Operating Systems (CSE380). Fall 2004

Evaluated projects and assignments.

Member, University of Pennsylvania CIS Dept. Alumni Advisory Board. Spring 2007 – Present

PROFESSIONAL ACTIVITIES

Program Committee, 17th USENIX Security Symposium (Security 2008)

External reviewer, 3rd International Conference on Very Large Databases (VLDB 2007)

External reviewer, 26th International Conference on Distributed Computing Systems (ICDCS 2006)

External reviewer, 47th Symposium on Foundations of Computer Science (FOCS 2006)

External reviewer, 3rd Applied Cryptography and Network Security (ACNS 2005)

Student Member, Usenix Advanced Computing Systems Association