

MAXWELL N. KROHN

MIT Computer Science and AI Lab
The Stata Center, G980
32 Vassar St.
Cambridge, MA 02139

o:617.253.5261
f:617.258.8607
krohn@mit.edu
<http://pdos.csail.mit.edu/~max>

Education

- 2003– **Massachusetts Institute of Technology**, Cambridge, MA
Ph.D. Candidate in Computer Science (degree expected summer 2008)
S.M. in Computer Science, September 2005
Thesis Topic: *Practical Information Flow Control With Flume*
Advisor: Prof. M. Frans Kaashoek
- 1995–1999 **Harvard University**, Cambridge, MA
A.B. *summa cum laude* in Computer Science and Mathematics, June 1999
Thesis title: *On the Definitions of Cryptographic Security*
Advisors: Professors Michael O. Rabin and Michael Mitzenmacher
GPA: 3.9/4.0
- 1991–1995 **Scarsdale High School**, Scarsdale, NY
Graduated first in class, June 1995

Research Interests

Computer systems, with emphasis on operating systems, security and distributed systems.

Research Experience

- 2007– **W5**, or A World Wide Web Without Walls. Conceived of and now prototyping W5, a new architecture for the web. The Facebooks and OpenSocials of the world represent new architectures for application development. W5 argues that they insufficiently protect users and unnecessarily encumber application developers. W5 proposes an alternative architecture, under which users retain control of their data and application developers can justify their existence without hoarding user data. W5 relies on work in decentralized information flow control (DIFC) to be practical [10].
- 2006– **Flume**. Conceived of, designed and implemented the Flume system, which brings DIFC to legacy operating systems like Linux and OpenBSD. Application developers can use Flume to make their applications more robust to attack. My coauthors and I demonstrated how Flume applies to popular open-source software like the MoinMoin wiki. Minimal modifications allow MoinMoin to take advantage of Flume’s security features [2]. Flume also contributes a new, simplified system of labels to track data flow, as well as novel techniques for protecting data integrity on modern web sites.
- 2006– **Tame**. Conceived of, designed and implemented Tame, a new event-based system for managing concurrency in network applications. Code written with Tame abstractions does not suffer from the “stack-ripping” problem associated with other event libraries. Like threaded code, tamed code uses standard control flow, automatically-managed local variables, and modular interfaces between callers and callees. Tame’s implementation consists of C++ libraries and a source-to-source translator; no platform-specific support or compiler modifications are required, and Tame induces little runtime overhead. Experience with Tame in real-world systems, including a popular commercial website, suggests it is easy to adopt and deploy [3].
- 2004–2007 **Asbestos**. Asbestos is a new operating system built to enforce DIFC at the kernel level. Applications built on Asbestos use DIFC to better track their secret data and therefore can be made

- secure by design. Worked to position the research [11], design the label system, design the kernel interface, and build the web server application [1,4].
- 2004–2005 **DOA**, or Delegation-Oriented Architecture, is a proposal for a new Internet architecture that better accommodates “middleboxes,” such as firewalls and NATs, than today’s Internet [5].
- 2003– **OKWS**. Conceived of, designed and implemented OKWS, a secure, high performance extensible web server [7]. This system plugs a number of security holes that plague most popular web servers such as Apache, while delivering significant performance improvements [7]. I actively support OKWS, since the commercial websites OkCupid.com and AddGene.org currently use it.
- 2002–2004 **Multicast Authentication**. The quality of peer-to-peer content distribution can suffer when malicious participants intentionally corrupt content. Content-distribution schemes that use elegant erasure codes for multicast are particularly susceptible to such attacks, since traditional hash-and-sign approaches do not apply. My work in this area presents a novel, practical scheme based on a homomorphic hashing primitive, that enables a downloader to verify received encoded blocks on-the-fly [8].
- 2002–2004 **SUNDR**, the “secure untrusted data repository,” is a network file system I built with researchers at NYU. SUNDR provides strong file system consistency guarantees, even if its central file server behaves maliciously. I worked primarily on the archival block storage server [6].
- 2002–2006 **SFS**. I was a contributor to SFS, the “self-certifying file system.” Implemented a novel two-party proactive authentication scheme called “2-Schnorr.” Integrated 2-Schnorr with SFS, developing key management utilities and server-side support [9]. Assisted in the general release of SFS versions 0.6 and 0.7.
- 1999 **Senior Undergraduate Thesis**. Examined shortcomings in standard definitions of cryptographic security and proposed alternative definitions that rectify these problems. The result was a relaxed definition of security that more accurately models real-world attacks [13]. These ideas later appeared in a Crypto 2003 paper by R. Canetti *et al*.
- 1998 **Evaluation of TDMA Voice Privacy**. Examined a voice privacy system for mobile phones that is still in use. Developed and implemented an algorithm for recovering unencrypted voice data [15].

Teaching Experience

- Fall 2006 **Teaching Assistant** for MIT Course 6.828, Operating System Engineering. Authored and delivered two lectures. Held office hours, authored assignments, assisted students with laboratories.
- Fall 1999 **Teaching Fellow** for the Harvard Extension School’s “Computer Systems and Technology.” This class was an introduction to the concepts and technologies used in modern telecommunication systems, such as digital signal processing. Held office hours, assisting students in the completion of their homework assignments.
- Fall 1997 **Teaching Fellow** for Harvard College’s CS50, “Introduction to Computer Science.” Lectured and led discussion for one hour each week, evaluated 16 undergraduate students, held office hours, authored model assignment solutions, authored and graded problem sets and exams.
- Fall 1996 **Teaching Fellow** for Harvard Extension School’s “Introduction to Computer Science.” Lectured and led discussion for one hour each week, evaluated 25 adult students, held office hours, graded exams and assignments.

Work Experience

- 2003– **OkCupid**, New York, NY
Founder and Chief Scientist. OkCupid.com is an online dating website, built on the OKWS

platform. Launched in early 2004, it currently has a half-million active users, and is growing rapidly. I founded the company with three other partners. I oversee the day-to-day CTO and his staff of ten developers.

- 2002–2003 **New York University**, New York, NY
Junior Research Scientist advised by Prof. David Mazières. Worked on SFS, SUNDR, OKWS and multicast authentication.
- 1999–2002 **SparkNotes, LLC and TheSpark.com**, New York, NY
Founder and CTO. Built a popular family of websites for teens, college students and young adults, which have since ranked in MediaMetrix’s and Nielsen’s top 100 sites. Negotiated venture funding. Assisted in the sale of the company to first *Delia*s* Corporation, and then *Barnes & Noble Booksellers*. Managed transitions between different companies. Reported to the COO of Barnes & Noble and the CEO of Barnes & Noble.com (bn.com). Managed a team of 4 programmers. Developed web-based applications used by millions of users. Developed a custom search engine. Configured and maintained a server cluster.
- 1998–1999 **Lucent Technologies**, Whippany, NJ
Summer Intern in the Secure Communications Group, studying cryptography specialized for digital mobile telephones. Assisted in the development of Third Generation authentication protocols.
- 1997 **Motorola**, Arlington, IL
Summer Intern in the Cellular Infrastructure Group. Developed a graphical testing tool to automate testing of commercial cellular networks.
- 1996 **HotJobs.com**, New York, NY
Summer Intern. Developed and maintained Internet services and applications.

Journal Publications

- [1] Steve VanDeBogart, Petros Efstathopoulos, Eddie Kohler, Maxwell Krohn, Cliff Frey, David Ziegler, Frans Kaashoek, Robert Morris, and David Mazières. Labels and event processes in the Asbestos operating system. *ACM Transactions on Computer Systems*, 25(4):11:1–11:43, 2007.

Refereed Conference Publications

- [2] Maxwell Krohn, Alexander Yip, Micah Brodsky, Natan Cliffer, M. Frans Kaashoek, Eddie Kohler, and Robert Morris. Information flow control for standard OS abstractions. In *Proceedings of the 21st Symposium on Operating Systems Principles (SOSP)*, Stevenson, WA, October 2007.
- [3] Maxwell Krohn, Eddie Kohler, and M. Frans Kaashoek. Events can make sense. In *Proceedings of the 2007 USENIX Annual Technical Conference*, June 2007.
- [4] Petros Efstathopoulos, Maxwell Krohn, Steve VanDeBogart, Cliff Frey, David Ziegler, Eddie Kohler, David Mazières, M. Frans Kaashoek, and Robert Morris. Labels and event processes in the Asbestos operating system. In *Proceedings of the 20th Symposium on Operating Systems Principles (SOSP)*, Brighton, UK, October 2005. (Best paper award).
- [5] Michael Walfish, Jeremy Stribling, Maxwell Krohn, Hari Balakrishnan, Robert Morris, and Scott Shenker. Middleboxes no longer considered harmful. In *Proceedings of the 6th Symposium on Operating Systems Design and Implementation (OSDI)*, December 2004.
- [6] Jinyuan Li, Maxwell Krohn, David Mazières, and Dennis Shasha. Secure untrusted data repository (SUNDR). In *Proceedings of the 6th Symposium on Operating Systems Design and Implementation (OSDI)*, December 2004.
- [7] Maxwell Krohn. Building secure high-performance web services with OKWS. In *Proceedings of the 2004 USENIX Annual Technical Conference*, Boston, MA, June 2004.

- [8] Maxwell Krohn, Michael J. Freedman, and David Mazières. On-the-fly verification of rateless erasure codes for efficient content distribution. In *Proceedings of the IEEE Symposium on Security and Privacy*, Oakland, CA, May 2004.
- [9] Antonio Nicolosi, Maxwell Krohn, Yevgeniy Dodis, and David Mazières. Proactive two-party signatures for user authentication. In *Proceedings of the 10th Annual Network and Distributed System Security Symposium (NDSS)*, San Diego, CA, February 2003.

Refereed Workshop Publications

- [10] Maxwell Krohn, Alexander Yip, Micah Brodsky, Robert Morris, and Michael Walfish. A World Wide Web Without Walls. In *Proceedings of the 6th ACM Workshop on Hot Topics in Networks (HotNets)*, Atlanta, GA, November 2007.
- [11] Maxwell Krohn, Petros Efstathopoulos, Cliff Frey, M. Frans Kaashoek, Eddie Kohler, David Mazières, Robert Morris, Michelle Osborne, Steve VanDeBogart, and David Ziegler. Make least privilege a right (not a privilege). In *Proceedings of the 10th Workshop on Hot Topics in Operating Systems (HotOS)*, Santa Fe, NM, June 2005.

Theses

- [12] Maxwell Krohn. Building fast and secure web services with OKWS. Master's thesis, Massachusetts Institute of Technology, 2005. Advised by M. Frans Kaashoek.
- [13] Maxwell Krohn. On the definitions of cryptographic security. Senior undergraduate thesis, Harvard University, 1999. Advised by Michael O. Rabin and Michael Mitzenmacher.

Technical Reports

- [14] Micah Brodsky, Petros Efstathopoulos, M. Frans Kaashoek, Eddie Kohler, Maxwell Krohn, David Mazières, Robert Morris, Steve VanDeBogart, and Alexander Yip. Toward secure services from untrusted developers. Technical Report TR-2007-041, MIT CSAIL, August 2007.
- [15] Maxwell Krohn. Evaluation of TDMA voice privacy. Report for Lucent Technologies. <http://pdos.lcs.mit.edu/~max/docs/tdma2.ps.gz>, August 1998.

Talks

- October 2007 "Information Flow Control for Standard OS Abstractions," conference talk at SOSP 2007.
- June 2007 "Events Can Make Sense," conference talk at the USENIX Annual Technical Conference 2007.
- June 2005 "Make the Principle of Least Privilege a Right (Not a Privilege)," workshop talk at HotOS X
- June 2004 "Building Fast and Secure Web Services With OKWS," conference talk at the USENIX Annual Technical Conference 2004
- May 2004 "On-The-Fly Verification of Rateless Erasure Codes," conference talk at the IEEE Symposium on Security and Privacy (Oakland 2004)

Awards

- 2005 SOSP best paper
- 2003 MIT EECS Fellowship
- 2003 NSF Graduate Research Fellowship
- 1999 *Phi Beta Kappa*
- 1999 Thomas Temple Hoopes Prize for outstanding senior thesis

| | |
|-----------|--|
| 1999 | Kirkland House Masters Award |
| 1999 | Henry Russell Shaw Traveling Fellowship (Declined) |
| 1996 | Detur Book Prize for high first-year GPA. |
| 1995–1999 | John Harvard Scholarship (Honorary) |
| 1995 | National Merit Scholar |

Professional Service

Reviewed papers for SOSP 2003, 2005 and 2007.

Academic Software Projects

| | |
|-----------|--|
| 2007– | A new secret project: please ask in person! |
| 2006– | The Flume project: code for the user-space reference monitor, Linux kernel modules, kernel patches, and a <code>glibc</code> interposition layer. Released under GPL. |
| 2005 | The SCIGen random paper generator. Released under GPL. |
| 2004–2006 | Python support for <code>sfslite</code> and OKWS. Released under GPL. |
| 2004–2005 | Prototypes of DOA servers and middleboxes. Released under GPL. |
| 2003– | <code>sfslite</code> , a stripped-down version of the SFS libraries, packaged with the Tame preprocessor and libraries. Actively maintained, in use in several academic projects at MIT and CMU, released under GPL. |
| 2003–2004 | A package for deploying commercial-grade load-balancers on commodity hardware, built with the Click modular router, and a new configuration language. |
| 2003–2004 | An implementation of homomorphic hashing and Maymounkov’s “Online Codes” [8]. |
| 2003–2004 | High-performance archival block store for SUNDR [6]. |
| 2002– | OKWS. Actively-maintained, released under GPL. Has support for XML-RPC, SSL, server-side compression, etc. The Coral CDN is built on OKWS’s foundation classes. |
| 2002– | Self-certifying file system (SFS). Contributor; redesigned key management system. |

Other Activities

| | |
|-----------|--|
| 2007 | MIT Festival Jazz Ensemble , Lead Alto Saxophone. |
| 2007 | Harvard Boston-Area Alumni Jazz Ensemble , Alto Saxophone II. |
| 1996–1999 | The Harvard Advocate (the University’s literary magazine) Publisher . Managed staff, finances, operations and editorial procedures. |
| 1996–1999 | Harvard Habitat For Humanity Chair . Managed a pool of 50 volunteers, leading work trips during the semester and over spring break. Raised funds. |
| 1996–1999 | Harvard University Jazz Band , Tenor and Alto Saxophone. |

Hobbies

Cycling, ice-hockey, skiing (racing in High School), softball (3-year captain of CSAIL’s team).

References

Prof. M. Frans Kaashoek
MIT Computer Science & AI Lab
32 Vassar Street, 32-G992
Cambridge, MA 02139
(617) 253-7149
kaashoek@csail.mit.edu

Prof. Eddie Kohler
UCLA Computer Science Department
4531C Boelter Hall
Los Angeles, CA 90095
(310) 267-5450
kohler@cs.ucla.edu

Prof. Robert Morris
MIT Computer Science & AI Lab
32 Vassar Street, 32-G972
Cambridge, MA 02139
(617) 253-5983
rtm@csail.mit.edu

Prof. David Mazières
Stanford University Computer Science Dept.
353 Serra Mall, #290
Stanford, CA 94305
(650) 723-8777
<http://www.scs.stanford.edu/~dm>

Cambridge, MA, October 2, 2008