David Mazières

Professor of Computer Science

Stanford University
353 Serra Mall, Room 290
Stanford, CA 94305

(415) 490-9451
http://www.scs.stanford.edu/~dm/

Education

Massachusetts Institute of Technology ..... Cambridge, MA

Ph.D. in Electrical Engineering and Computer Science ..... September, 2000
Thesis title: *Self-certifying File System.*
Advisor: Prof. M. Frans Kaashoek.

S.M. in Electrical Engineering and Computer Science ..... September, 1997
Thesis title: *Security and Decentralized Control in the SFS Global File System.*

Harvard University ..... Cambridge, MA

A.B. with honors in Computer Science ..... June, 1994
Thesis title: *Abstract Execution in a Multi-Tasking Environment.*

Interests

Computer systems, especially operating systems, security, and privacy.

Teaching

Operating Systems (CS140). An introduction to operating systems, with rigorous programming assignments.

Distributed Systems (CS244B). Covers the principles of distributed systems, including replication, consistency, Byzantine fault tolerance, scalability, naming, and many examples of systems addressing these challenges. Includes one or two short programming assignments followed by a small research project done in teams.

Functional Systems in Haskell (CS240h). Covers an array of practical issues and techniques that arise when building real-world systems in the Haskell programming language.

Advanced Topics in Operating Systems (CS 240). Survey of classic and new papers on operating systems topics, covering virtual memory, synchronization, virtual machines, file systems, scalability, kernel architectures, reliability, and security.

Computer Networking (CS144). An introduction to computer networking, with programming assignments in C.

Computer and Network Security (CS155). Covers principles of computer systems security, including attack techniques and how to defend against them, with programming assignments.

Distributed Storage Systems (CS240D). A detailed examination of a number of topics including RPC programming, disk layout, transactions, and reconciliation in weakly consistent systems.

Advanced Operating Systems Implementation (CS240C). Covers the design and implementation of operating systems.

NYU Classes	**Computer Networks** (undergraduate course).
	Honors Operating Systems (graduate course).
	Computer System Security (graduate course).

Positions

2/15–present	**Professor.** Stanford University, Stanford, CA.
7/14–present	**Founder and Chief Scientist.** GitStar, San Francisco, CA.
7/14–present	**Chief Scientist.** Stellar Development Foundation, San Francisco, CA.
9/07–1/15	**Associate Professor.** Stanford University, Stanford, CA.
10/08–12/08	**Professorial Research Associate.** University College London, London, UK.
9/05–8/07	**Assistant Professor.** Stanford University, Stanford, CA.
9/05–8/07	**Associate Professor** (on leave)**.** New York University, New York, NY.
9/00–8/05	**Assistant Professor.** New York University, New York, NY.
6/99–8/99	**Summer Intern.** Bell Labs, Murray Hill, NJ.
6/95–8/95	**Summer Intern.** DEC Western Research Laboratory, Palo Alto, CA.
6/94–5/95	**Operating Systems Programmer.** Harvard University, Cambridge, MA.
6/93–8/93	**Operating Systems Summer Intern.** Kendall Square Research, Waltham, MA.
2/91–5/95	**Late-night Rock DJ.** WHRB-FM, Cambridge, MA.

Ph.D. Students

Current	David Terei (expected graduation 2018).
	Edward Z. Yang (expected graduation 2017).
	Amit Levy (expected graduation 2017).
	Adam Belay (expected graduation 2016).
	Ali Mashtizadeh (expected graduation 2016).
	Deian Stefan (expected graduation 2015).
Graduated	Vimalkumar Jeyakumar. Thesis: *Millions of Little Minions: Using Packets for Low Latency Network Programming and Visibility*, 2014.
	Steve Rumble. *Thesis: Memory And Object Management In Ramcloud*, 2014.
	Jad Naous. Thesis: *Path-policy compliant networking and a platform for heterogeneous IaaS managemenent*, 2011.
	Nickolai Zeldovich. Thesis: *Securing Untrustworthy Software Using Information Flow Control*, 2007.
	Antonio Nicolosi. Thesis: *Authentication Mechanisms for Open Distributed Systems*, 2007.
	Michael J. Freedman. Thesis: *Democratizing Content Distribution*, 2007.
	Siddhartha Annapureddy. Thesis: *Scaling Data Servers via Cooperative Caching*, 2007.
	Jinyuan Li. Thesis: *Building Trustworthy Storage Services out of Untrusted Infrastructure*, 2006.

Michael Kaminsky. Thesis: *User Authentication and Remote Execution Across Administrative Domains*, 2004.

Marc Waldman. Thesis: *Secure and Robust Censorship-Resistant Publishing Systems*, 2003.

Awards

Distinguished paper, Oakland 2015 [6].

Alfred P. Sloan Research Fellow, 2002.

Best paper award, USENIX 2001 [41].

NSF Career award, 2001.

MIT George R. Sprowls award for best thesis in computer science, 2000.

Professional activities

Coauthor of several internet drafts for TCP increased security (TCPINC) IETF working group (2013–present).

Program Committees: Oakland 2016, HotOS 2015, ICFP 2014, Haskell Symposium 2013, ASPLOS 2013, NSDI 2011, SIGCOMM 2009, SOSP 2007.

DARPA ISAT 2010–2013. Co-chair, workshop on Fostering adoption of programming languages, February 2013.

Refereed journal publications

(My students are listed in boldface.)

[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):11:1–43, December 2007.

A version of this paper appeared as refereed conference paper [29].

[2] Kevin Fu, M. Frans Kaashoek, and David Mazières. Fast and secure distributed read-only file system. *ACM Transactions on Computer Systems*, 20(1):1–24, February 2002.

A version of this paper appeared as refereed conference paper [42].

[3] J. Bradley Chen, Yasuhiro Endo, Kee Chan, David Mazières, Antonio Dias, Margo Seltzer, and Mike Smith. The measured performance of personal computer operating systems. *ACM Transactions on Computer Systems*, 14(1):3–40, February 1996.

A version of this paper appeared as refereed conference paper [46].

Refereed journal publications in press/accepted

[4] **Deian Stefan**, Alejandro Russo, John C. Mitchell, and David Mazières. Sequential LIO: Flexible dynamic information flow control in the presence of exceptions. *Journal of Functional Programming*, 2015 (estimated).

A version of this paper appeared as refereed conference paper [21].

Refereed conference publications

Conferences:

[5] **Ali José Mashtizadeh**, Andrea Bittau, Dan Boneh, and David Mazières. CCFI: Cryptographically enforced control flow integrity. In *Proceedings of the 22nd ACM Conference on Computer and Communications Security*, Denver, CO, October 2015.

[6] Henry Corrigan-Gibbs, Dan Boneh, and David Mazières. Riposte: An anonymous messaging system handling millions of users. In *Proceedings of the IEEE Symposium on Security and Privacy*, May 2015.

[7] **Deian Stefan**, **Edward Z. Yang**, Petr Marchenko, Alejandro Russo, Dave Herman, Brad Karp, and David Mazières. Protecting users by confining javascript with COWL. In *Proceedings of the 11th Symposium on Operating Systems Design and Implementation*, pages 131–146, 2014.

[8] **Vimalkumar Jeyakumar**, Mohammad Alizadeh, Yilong Geng, Changhoon Kim, and David Mazières. Millions of little minions: Using packets for low latency network programming and visibility. In *Proceedings of the ACM SIGCOMM Conference*, pages 3–14, August 2014.

[9] **Edward Z. Yang** and David Mazières. Dynamic space limits for Haskell. In *Proceedings of the 35th annual conference on Programming Language Design and Implementation*, pages 588–598, June 2014.

[10] Andrea Bittau, **Adam Belay**, **Ali Mashtizadeh**, David Mazières, and Dan Boneh. Hacking blind. In *Proceedings of the 35th Symposium on Security and Privacy (Oakland)*, pages 227–242, May 2014.

[11] Nikhil Handigol, Brandon Heller, **Vimalkumar Jeyakumar**, David Mazières, and Nick McKeown. I know what your packet did last hop: Using packet histories to troubleshoot networks. In *Proceedings of the 11th Symposium on Networked Systems Design and Implementation*, pages 71–85, Seattle, WA, April 2014.

[12] **Ali José Mashtizadeh**, Andrea Bittau, Yifeng Frank Huang, and David Mazières. Replication, history, and grafting in the Ori file system. In *Proceedings of the 24th Symposium on Operating Systems Principles*, pages 151–166, November 2013.

[13] **Deian Stefan**, Pablo Buiras, **Edward Z. Yang**, **Amit Levy**, **David Terei**, Alejandro Russo, and David Mazières. Eliminating cache-based timing attacks with instruction-based scheduling. In *Proceedings of the 18th European Symposium on Research in Computer Security*, September 2013.

[14] Pablo Buiras, **Amit Levy**, **Deian Stefan**, Alejandro Russo, and David Mazières. A library for removing cache-based attacks in concurrent information flow systems. In *Proceedings of the 8th International Symposium on Trustworthy Global Computing*, August 2013.

[15] **Vimalkumar Jeyakumar**, Mohammad Alizadeh, David Mazières, Balaji Prabhakar, Changhoon Kim, and Albert Greenberg. EyeQ: Practical network performance isolation at the edge. In *Proceedings of the Symposium on Networked Systems Design and Implementation*, April 2013.

[16] **Adam Belay**, Andrea Bittau, **Ali Mashtizadeh**, **David Terei**, David Mazières, and Christos Kozyrakis. Dune: Safe user-level access to privileged CPU features. In *Proceedings of the 10th Symposium on Operating Systems Design and Implementation*, October 2012.

[17] Daniel B. Giffin, **Amit Levy**, **Deian Stefan**, **David Terei**, David Mazières, John Mitchell, and Alejandro Russo. Hails: Protecting data privacy in untrusted web applications. In

Proceedings of the 10th Symposium on Operating Systems Design and Implementation, October 2012.

[18] **David Terei**, Simon Marlow, Simon Peyton Jones, and David Mazières. Safe Haskell. In *Proceedings of the 5th ACM symposium on Haskell*, September 2012.

[19] **Deian Stefan**, Alejandro Russo, Pablo Buiras, **Amit Levy**, John C. Mitchell, and David Mazières. Addressing covert termination and timing channels in concurrent information flow systems. In *Proceedings of the 17th ACM SIGPLAN International Conference on Functional Programming (ICFP)*, September 2012.

[20] **Jad Naous**, Michael Walfish, **Antonio Nicolosi**, David Mazières, Michael Miller, and Arun Seehra. Verifying and enforcing network paths with ICING. In *Proceedings of the 7th ACM International Conference on emerging Networking EXperiments and Technologies (CoNEXT)*, December 2011.

[21] **Deian Stefan**, Alejandro Russo, John C. Mitchell, and David Mazières. Flexible dynamic information flow control in haskell. In *Proceedings of the 4th Symposium on Haskell*, pages 95–106, September 2011.

[22] Arjun Roy, **Stephen M. Rumble**, **Ryan Stutsman**, Philip Levis, David Mazières, and **Nickolai Zeldovich**. Energy management in mobile devices with the cinder operating system. In *Proceedings of the EuroSys*, pages 139–152, April 2011.

[23] Andrea Bittau, Michael Hamburg, Mark Handley, David Mazières, and Dan Boneh. The case for ubiquitous transport-level encryption. In *Proceedings of the 19th USENIX Security Symposium*, August 2010.

[24] **Nickolai Zeldovich**, Silas Boyd-Wickizer, and David Mazières. Securing distributed systems with information flow control. In *Proceedings of the 6th Symposium on Networked Systems Design and Implementation*, pages 293–308, San Francisco, CA, April 2008.

[25] **Jinyuan Li** and David Mazières. Beyond one-third faulty replicas in Byzantine fault tolerant systems. In *Proceedings of the 4th Symposium on Networked Systems Design and Implementation*, pages 131–144, Cambridge, MA, April 2007.

[26] **Nickolai Zeldovich**, Silas Boyd-Wickizer, Eddie Kohler, and David Mazières. Making information flow explicit in HiStar. In *Proceedings of the 7th Symposium on Operating Systems Design and Implementation*, pages 263–278, Seattle, WA, November 2006.

[27] **Michael J. Freedman**, Karthik Laskhminarayanan, and David Mazières. OASIS: Anycast for any service. In *Proceedings of the 3rd Symposium on Networked Systems Design and Implementation*, pages 129–142, San Jose, CA, May 2006.

[28] Scott Garriss, **Michael Kaminsky**, **Michael J. Freedman**, Brad Karp, David Mazières, and Haifeng Yu. Re: Reliable email. In *Proceedings of the 3rd Symposium on Networked Systems Design and Implementation*, pages 297–310, San Jose, CA, May 2006.

[29] Petros Efstathopoulos, Maxwell Krohn, Steve VanDeBogart, Cliff Frey, David Ziegler, Eddie Kohler, David Mazières, Frans Kaashoek, and Robert Morris. Labels and event processes in the Asbestos operating system. In *Proceedings of the 20th ACM Symposium on Operating Systems Principles*, pages 17–30, Brighton, UK, October 2005. ACM.

[30] **Siddhartha Annapureddy**, **Michael J. Freedman**, and David Mazières. Shark: Scaling file servers via cooperative caching. In *Proceedings of the 2nd Symposium on Networked Systems Design and Implementation*, pages 129–142, Boston, MA, May 2005.

[31] **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*, pages 91–106, San Francisco, CA, December 2004.

[32] **Michael Kaminsky**, Eric Peterson, Daniel B. Giffin, Kevin Fu, David Mazières, and M. Frans Kaashoek. REX: Secure, extensible remote execution. In *Proceedings of the 2004 USENIX*, pages 199–212, Boston, MA, June–July 2004. USENIX.

[33] Maxwell N. 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*, pages 226–240, Oakland, CA, May 2004.

[34] **Michael J. Freedman**, Eric Freudenthal, and David Mazières. Democratizing content publication with Coral. In *Proceedings of the 1st Symposium on Networked Systems Design and Implementation*, pages 239–252, San Francisco, CA, March 2004.

[35] **Michael Kaminsky**, George Savvides, David Mazières, and M. Frans Kaashoek. Decentralized user authentication in a global file system. In *Proceedings of the 19th ACM Symposium on Operating Systems Principles*, pages 60–73, Bolton Landing, NY, October 2003. ACM.

[36] **Nickolai Zeldovich**, Alexander Yip, Frank Dabek, Robert T. Morris, David Mazières, and M. Frans Kaashoek. Multiprocessor support for event-driven programs. In *Proceedings of the 2003 USENIX*, pages 239–252, San Antonio, TX, June 2003. USENIX.

[37] **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*, pages 233–248, February 2003.

[38] David Mazières and Dennis Shasha. Building secure file systems out of Byzantine storage. In *Proceedings of the 21st Annual ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing*, pages 108–117, July 2002. The full version is available as NYU computer science department technical report TR2002-826, May 2002.

[39] **Marc Waldman** and David Mazières. Tangler – a censorship-resistant publishing system based on document entanglements. In *Proceedings of the 8th ACM Conference on Computer and Communications Security*, pages 126–135, November 2001.

[40] Athicha Muthitacharoen, Benjie Chen, and David Mazières. A low-bandwidth network file system. In *Proceedings of the 18th ACM Symposium on Operating Systems Principles*, pages 174–187, Chateau Lake Louise, Banff, Canada, October 2001. ACM.

[41] David Mazières. A toolkit for user-level file systems. In *Proceedings of the 2001 USENIX*, pages 261–274. USENIX, June 2001.

[42] Kevin Fu, M. Frans Kaashoek, and David Mazières. Fast and secure distributed read-only file system. In *Proceedings of the 4th Symposium on Operating Systems Design and Implementation*, 2000.

[43] David Mazières, **Michael Kaminsky**, M. Frans Kaashoek, and Emmett Witchel. Separating key management from file system security. In *Proceedings of the 17th ACM Symposium on Operating Systems Principles*, pages 124–139, Kiawa Island, SC, December 1999. ACM.

[44] David Mazières and M. Frans Kaashoek. The design, implementation and operation of an email pseudonym server. In *Proceedings of the 5th ACM Conference on Computer and Communications Security*, pages 27–36, 1998.

[45] M. Frans Kaashoek, Dawson R. Engler, Gregory R. Ganger, Héctor M. Briceño, Russell Hunt, David Mazières, Thomas Pinckney, Robert Grimm, John Jannotti, and Kenneth Mackenzie. Application performance and flexibility on exokernel systems. In *Proceedings of the 16th ACM Symposium on Operating Systems Principles*, pages 52–65, Saint-Malo, France, October 1997. ACM.

[46] J. Bradley Chen, Yasuhiro Endo, Kee Chan, David Mazières, Antonio Dias, Margo Seltzer, and Mike Smith. The measured performance of personal computer operating systems. In *Proceedings of the 15th Symposium on Operating Systems Principles*, pages 299–313, December 1995.

Workshops:

[47] **Vimalkumar Jeyakumar**, Mohammad Alizadeh, Changhoon Kim, and David Mazières. Tiny packet programs for low-latency network control and monitoring. In *Proceedings of the 12th ACM Workshop on Hot Topics in Networks*, College Park, MD, November 2013.

[48] **Edward Z. Yang**, **Deian Stefan**, John Mitchell, David Mazières, Petr Marchenko, and Brad Karp. Toward principled browser security. In *Proceedings of the 14th Workshop on Hot Topics in Operating Systems*, May 2013.

[49] Nikhil Handigol, Brandon Heller, **Vimalkumar Jeyakumar**, David Mazières, and Nick McKeown. Where is the debugger for my software-defined network? In *Proceedings of the Workshop on Hot Topics in Software Defined Networking*, August 2012.

[50] **Vimalkumar Jeyakumar**, Mohammad Alizadeh, David Mazières, Balaji Prabhakar, and Changhoon Kim. EyeQ: Practical network performance isolation for the multi-tenant cloud. In *Proceedings of the 4th USENIX Workshop on Hot Topics in Cloud Computing*, June 2012.

[51] **Deian Stefan**, Alejandro Russo, David Mazières, and John C. Mitchell. Disjunction category labels. In *Proceedings of the NordSec 2011 Conference*, October 2011.

[52] Arun Seehra, **Jad Naous**, Michael Walfish, David Mazières, **Antonio Nicolosi**, and Scott Shenker. A policy framework for the future internet. In *Proceedings of the 8th Workshop on Hot Topics in Networks*, October 2009.

[53] **Jad Naous**, **Ryan Stutsman**, David Mazières, Nick McKeown, and **Nickolai Zeldovich**. Delegating network security through more information. In *Proceedings of the Workshop on Research on Enterprise Networking*, August 2009.

[54] **Stephen M. Rumble**, **Ryan Stutsman**, Philip Levis, David Mazières, and **Nickolai Zeldovich**. Apprehending joule thieves with cinder. In *Proceedings of the First ACM Workshop on Networking, Systems, Applications on Mobile Handhelds*, August 2009.

[55] **Michael J. Freedman**, Ion Stoica, David Mazières, and Scott Shenker. Group therapy for systems: Using link attestations to manage failures. In *Proceedings of the 5th International Workshop on Peer-to-Peer Systems*, Santa Barbara, CA, February 2006.

[56] Maxwell Krohn, Petros Efstathopoulos, Cliff Frey, 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*, Santa Fe, NM, June 2005.

[57] **Antonio Nicolosi** and David Mazières. Secure acknowledgment of multicast messages in open peer-to-peer networks. In *Proceedings of the 3rd International Workshop on Peer-to-Peer Systems (IPTPS '04)*, pages 259–268, San Diego, CA, February 2004.

[58] **Petar Maymounkov** and David Mazières. Rateless codes and big downloads. In *Proceedings of the 2nd International Workshop on Peer-to-Peer Systems (IPTPS '03)*, pages 247–255, Berkeley, CA, February 2003.

[59] **Michael Freedman** and David Mazières. Sloppy hashing and self-organizing clusters. In *Proceedings of the 2nd International Workshop on Peer-to-Peer Systems (IPTPS '03)*, pages 45–55, Berkeley, CA, February 2003.

[60] Frank Dabek, **Nickolai Zeldovich**, M. Frans Kaashoek, David Mazières, and Robert Morris. Event-driven programming for robust software. In *Proceedings of the 10th ACM SIGOPS European Workshop*, pages 186–189, September 2002.

[61] **Petar Maymounkov** and David Mazières. Kademlia: A peer-to-peer information system based on the XOR metric. In *Proceedings of the 1st International Workshop on Peer-to-Peer Systems (IPTPS '02)*, pages 53–65, Cambridge, MA, March 2002.

[62] David Mazières and Dennis Shasha. Don't trust your file server. In *Proceedings of the 8th Workshop on Hot Topics in Operating Systems*, pages 113–118, May 2001.

[63] David Mazières and M. Frans Kaashoek. Escaping the evils of centralized control with self-certifying pathnames. In *Proceedings of the 8th ACM SIGOPS European Workshop*, pages 118–125, 1998.

[64] David Mazières and M. Frans Kaashoek. Secure applications need flexible operating systems. In *Proceedings of the 6th Workshop on Hot Topics in Operating Systems*, pages 56–61, May 1997.

Non-refereed publications

[65] David Mazières. The Stellar consensus protocol: A federated model for internet-level consensus. `https://www.stellar.org/papers/stellar-consensus-protocol.pdf`, April 2015.

[66] **Nickolai Zeldovich**, Silas Boyd-Wickizer, Eddie Kohler, and David Mazières. Making information flow explicit in HiStar. *Communications of the ACM*, 54(11):93–101, November 2011.

[67] Dan Boneh, David Mazières, and Raluca Ada Popa. Remote oblivious storage: Making oblivious RAM practical. Technical Report MIT-CSAIL-TR-2011-018, MIT, March 2011.

[68] John Ousterhout, Parag Agrawal, David Erickson, Christos Kozyrakis, Jacob Leverich, David Mazières, Subhasish Mitra, Aravind Narayanan, Diego Ongaro, Guru Parulkar, Mendel Rosenblum, **Stephen M. Rumble**, Eric Stratmann, and **Ryan Stutsman**. The case for RAMCloud. *Communications of the ACM*, 54(7):121–130, July 2011. A version appeared in SIGOPS OSR 43(4):92ŋ105, January 2009.

[69] David Mazières. Blocking unwanted mail with mail avenger. *Virus Bulletin*, pages S2–S4, July 2005.

[70] Kevin Fu, **Michael Kaminsky**, and David Mazières. Using SFS for a secure network file system. *;login: The Magazine of Usenix & Sage*, 27(6):6–16, December 2002.

[71] David Mazières and Michael D. Smith. Abstract execution in a multi-tasking environment. Technical Report TR-31-94, Harvard University, November 1994.

Non-refereed conference/symposium publications

[72] Daniel Giffin, Stefan Heule, **Amit Levy**, David Mazières, John Mitchell, Alejandro Russo, Amy Shen, **Deian Stefan**, **David Terei**, and **Edward Z. Yang**. Security and the average programmer. In *Proceedings of the 3rd Conference on Principles of Security and Trust*, April 2014. (invited).

[73] Niels Provos and David Mazières. A future-adaptable password scheme. In *Proceedings of the 1999 USENIX, Freenix track (the on-line version)*, Monterey, CA, June 1999. USENIX. from `http://www.usenix.org/events/usenix99/provos.html`.

Statement of customary practices

In computer systems, paper authors are typically ordered from the greatest to the least amount of effort invested in a paper. Among coauthors who invested comparable effort, authors are listed from most junior to most senior. Ties are broken alphabetically (or very occasionally reverse alphabetically).

Patents

None.

Stanford, CA, October 13, 2015