

J. Alex Halderman

Assistant Professor of Electrical Engineering and
Computer Science, The University of Michigan

2260 Hayward St., Ann Arbor, MI 48109
jhalderm@eecs.umich.edu · 609 558 2312

<http://J.AlexHalderman.com>

November 13, 2009

Education

Princeton University Princeton, NJ

- Ph.D. in Computer Science, June 2009
Thesis: *Investigating Security Failures and their Causes:
An Analytic Approach to Computer Security*
Adviser: Ed Felten
- M.A. in Computer Science, June 2005
- B.A. in Computer Science, *summa cum laude*, June 2003
Thesis: *Digital Privacy-Rights Management for Ubiquitous Recording*
Advisers: Andrew Appel, Ed Felten, and Tom Funkhouser

Honors

- Pwnie Award nomination in the category of [Mass ownage](#) for “Green Dam Youth Escort Long URL Stack Buffer Overflow,” Black Hat 2009
- Best Student Paper Award of the 17th USENIX Security Symposium for “Lest We Remember: Cold Boot Attacks on Encryption Keys,” 2008
- Pwnie Award in the category of [Most Innovative Research](#) for “Lest We Remember: Cold Boot Attacks on Encryption Keys,” Black Hat 2008
- Princeton University Charlotte Elizabeth Procter Honorific Fellowship, 2007
(“awarded in recognition of outstanding performance and professional promise, and represents high commendation from the Graduate School”)

- National Science Foundation Graduate Fellowship, Princeton, 2004–2007
- Best Paper Award of the 8th International Conference on 3D Web Technology for “Early Experiences with a 3D Model Search Engine,” 2003
- Phi Beta Kappa, 2003; Sigma Xi, 2003
- Princeton Computer Science Department Senior Award, 2003
- Accenture Prize in Computer Science, 2002
- Martin A. Dale Summer Award, 2000
- USA Computing Olympiad National Finalist, 1996 and 1997

Publications

- Scott Wolchok, Owen S. Hofmann, Nadia Heninger, Edward W. Felten, J. Alex Halderman, Christopher J. Rossbach, Brent Waters, and Emmett Witchel. **Defeating Vanish with Low-Cost Sybil Attacks Against Large DHTs**. To appear in *Proc. 17th Network and Distributed System Security Symposium (NDSS '10)*, February-March 2010.
- Steve Checkoway, Ariel J. Feldman, Brian Kantor, J. Alex Halderman, Edward W. Felten, and Hovav Shacham. **Can DREs Provide Long-Lasting Security? The Case of Return-Oriented Programming and the AVC Advantage**. In *Proc. 2009 USENIX/ACCURATE/IAVoSS Electronic Voting Technology Workshop (EVT '09)*, Montreal, QC, August 2009.
- Scott Wolchok, Randy Yao, and J. Alex Halderman. **Analysis of the Green Dam Censorware System**. Technical report, June 2009.
- William Clarkson, Tim Weyrich, Adam Finkelstein, Nadia Heninger, J. Alex Halderman, and Edward W. Felten. **Fingerprinting Blank Paper Using Commodity Scanners**. In *Proc. IEEE Symposium on Security and Privacy*, Oakland, CA, May 2009.
- J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten. **Lest We Remember: Cold Boot Attacks on Encryption Keys**. In *Proc. 17th USENIX Security Symposium*, San Jose, CA, July 2008. **Best student paper award**. Reprinted in *Communications of the ACM*, May 2009.
- J. Alex Halderman, Eric Rescorla, Hovav Shacham, and David Wagner. **You Go to Elections with the Voting System You Have: Stop-Gap Mitigations for Deployed Voting Systems**. In *Proc. 2008 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT '08)*, San Jose, CA, July 2008.

- Joseph A. Calandrino, J. Alex Halderman, and Edward W. Felten. **In Defense of Pseudo-random Sample Selection**. In *Proc. 2008 USENIX/ACCURATE Electronic Voting Technology Workshop* (EVT '08), San Jose, CA, July 2008.
- J. Alex Halderman and Ariel J. Feldman. **AVC Advantage: Hardware Functional Specifications**. Princeton University Computer Science Tech Report TR-816-08, March 2008.
- J. Alex Halderman and Brent Waters. **Harvesting Verifiable Challenges from Oblivious Online Sources**. In *Proc. 14th ACM Conference on Computer and Communications Security* (CCS '07), pages 330–341, Washington, DC, October 2007.
- Ariel Feldman, J. Alex Halderman, and Edward W. Felten. **Security Analysis of the Diebold AccuVote-TS Voting Machine**. In *Proc. 2007 USENIX/ACCURATE Electronic Voting Technology Workshop* (EVT '07), Boston, MA, August 2007.
- Joseph A. Calandrino, J. Alex Halderman, and Edward W. Felten. **Machine-Assisted Election Auditing**. In *Proc. 2007 USENIX/ACCURATE Electronic Voting Technology Workshop* (EVT '07), Boston, MA, August 2007.
- Joseph A. Calandrino, Ariel Feldman, J. Alex Halderman, David Wagner, Harlan Yu, and William Zeller. **Source Code Review of the Diebold Voting System**. Part of the California Secretary of State's "Top-to-Bottom" Voting Systems Review, August 2007.
- J. Alex Halderman and Edward W. Felten. **Lessons from the Sony CD DRM Episode**. In *Proc. 15th USENIX Security Symposium*, pages 77–92, Vancouver, BC, August 2006.
- Edward W. Felten and J. Alex Halderman. **Digital Rights Management, Spyware, and Security**. *IEEE Security and Privacy* 4(1):18–23, January/February 2006.
- J. Alex Halderman, Brent Waters, and Edward W. Felten. **A Convenient Method for Securely Managing Passwords**. In *Proc. 14th International World Wide Web Conference* (WWW '05), pages 471–479, Chiba, Japan, May 2005.
- J. Alex Halderman, Brent Waters, and Edward W. Felten. **Privacy Management for Portable Recording Devices**. In *Proc. 2004 ACM Workshop on Privacy in the Electronic Society* (WPES '04), pages 16–24, Washington, DC, October 2004.
- Brent Waters, Ari Juels, J. Alex Halderman, and Edward W. Felten. **New Client Puzzle Outsourcing Techniques for DoS Protection**. In *Proc. 11th ACM Conference on Computer and Communications Security* (CCS '04), pages 246–256, Washington, DC, October 2004.
- J. Alex Halderman. **Analysis of the MediaMax CD-3 Copy-Prevention System**. Princeton University Computer Science Technical Report TR-679-03, October 2003.

- Patrick Min, J. Alex Halderman, Michael Kazhdan, and Thomas Funkhouser. **Early Experiences with a 3D Model Search Engine**. In *Proc. 8th International Conference on 3D Web Technology (Web3D '03)*, pages 7–18, Saint Malo, France, March 2003. **Best paper award**.
- Thomas Funkhouser, Patrick Min, Michael Kazhdan, Joyce Chen, J. Alex Halderman, David Dobkin, and David Jacobs. **A Search Engine for 3D Models**. *ACM Trans. Graph.* 22(1):83–105, January 2003.
- J. Alex Halderman. **Evaluating New Copy-Prevention Techniques for Audio CDs**. In *Proc. 2002 ACM Workshop on Digital Rights Management (DRM '02)*, Washington, DC, November 2002.

Positions

- Assistant Professor, Department of Electrical Engineering and Computer Science, Computer Science and Engineering Division, University of Michigan, 2008–present
- Visiting Research Collaborator, Center for Information Technology Policy, Princeton University, 2008–present
- Consulting Computer Scientist, Elysium Digital (Cambridge, MA), 2007–present
- Research Assistant, University of California, Berkeley, Summer 2007; helped lead state-sponsored electronic voting security review
- Intern, Google (Mountain View, CA), Summer 2005 and Summer 2006; worked with Video and Application Security teams
- Research Assistant, Princeton, Shape Retrieval and Analysis group, Summer 2002
- Founder, Web Immersion (Newtown, PA), 2000–2001

Teaching

- **Introduction to Computer Security**, EECS 398, University of Michigan, Fall 2009.
- **Computer and Network Security**, EECS 588, University of Michigan, Winter 2009.
- **The Computational Universe**, COS 116, Princeton, Spring 2006. Helped develop the course, an introduction to computer science for liberal arts majors (with Sanjeev Arora).
- **Information Technology and the Law**, COS 491, Princeton, Spring 2006. Assisted in instruction for this interdisciplinary seminar (with Ed Felten).
- **Digital Photography**, VIS 452, Princeton, 2003–2005. Assisted in instruction (with Andrew Moore).

- **CourseBlog** system, Princeton, 2005–2008. Developed and maintained instructional blogging software used by classes in several departments.

Service

- **Research and Education**

- Participated in the founding of Princeton’s **Center for Information Technology Policy**, a joint venture between the School of Engineering and Applied Science and the Woodrow Wilson School for Public and International Affairs; helped chart the organization’s direction, recruit students and staff, and establish research priorities; 2005–present.
- Have been a frequent contributor to **Freedom-to-Tinker** (a blog organized by Ed Felten that is widely read in law, policy, and computer security communities), posting essays on topics such as privacy, DRM, and electronic voting security; 2003–present.
- Co-founded **The Art of Science**, an interdisciplinary art competition that showcases images and videos produced in the course of scientific research as well as creative works that incorporate tools and ideas from science; 2004–2006.

- **Law and Policy**

- Helped lead the California Secretary of State’s “Top-to-Bottom” voting systems security review, 2007.
- Served on a New Jersey citizens’ task force to improve election security; filed expert testimony on voting security at the behest of the N.J. Public Advocate; 2007.
- Successfully petitioned the U.S. Copyright Office for an exemption to the DMCA to facilitate the investigation and repair of security problems caused by audio CD DRM, 2006.
- Served as a technical expert for the U.S. Federal Trade Commission on DRM’s harm to consumers; filed expert testimony on this subject for the Electronic Frontier Foundation; 2005–2006.

- **Program Committees**

- 2010 ACM Conference on Computer and Communications Security (CCS 10)
- 2010 USENIX Security Symposium
- 2010 IEEE Symposium on Security and Privacy (Oakland ‘10)
- 2010 International World Wide Web Conference (WWW ‘10), security track
- 2010 USENIX/ACCURATE/IAVOSS Electronic Voting Technology Workshop (EVT ‘10)

- 2009 ACM Conference on Computer and Communications Security (CCS 09)
- 2009 ACM Workshop on Digital Rights Management (DRM 09)
- 2009 ACM Workshop on Multimedia Security (MMS 09)
- 2009 USENIX Workshop on Offensive Technologies (WOOT 09)
- 2009 International World Wide Web Conference (WWW 09), security track
- 2008 ACM Conference on Computer and Communications Security (CCS 08)
- 2008 International World Wide Web Conference (WWW 08), security track
- 2008 ACM Workshop on Privacy in the Electronic Society (WPES 08)
- 2008 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT 08)

Selected Press Coverage

- **E-Voting**

Fox News and CNN (live demos), CBS Evening News, New York Times, LA Times, USA Today, Wall Street Journal, Washington Post, Newark Star-Ledger, Time, Fortune, MIT Tech Review, Harper's Index, NPR Science Friday, BBC World Service, Slashdot, hundreds more.

- **DRM**

MSNBC, CNBC, and MTV, USA Today (front page profile), New York Times, Washington Post, Boston Globe, Reuters (Yahoo and CNN home pages), San Jose Mercury News, Newark Star-Ledger, New Scientist, Wired, NPR, CNET, Slashdot, BoingBoing, hundreds more.