J. Alex Halderman

Professor, Computer Science and Engineering
University of Michigan

November 4, 2016

2260 Hayward Street
Ann Arbor, MI 48109 USA
(*mobile*) +1 609 558 2312
jhalderm@eecs.umich.edu

J.AlexHalderman.com

Research Overview

My research focuses on computer security and privacy, with an emphasis on problems that broadly impact society and public policy. Topics that interest me include software security, network security, data privacy, anonymity, surveillance, electronic voting, censorship resistance, digital rights management, computer forensics, ethics, and cybercrime. I'm also interested in the interaction of technology with law, regulatory policy, and international affairs.

Selected Projects

'16: Let's Encrypt HTTPS certificate authority
'15: Weak Diffie-Hellman and the Logjam attack
'14: Understanding Heartbleed's aftermath
'14: Security problems in full-body scanners
'14: Analysis of Estonia's Internet voting system
'13: ZMap Internet-wide network scanner
'12: Widespread weak keys in network devices
'11: Anticensorship in the network infrastructure
'10: Hacking Washington D.C.'s Internet voting
'10: Vulnerabilities in India's e-voting machines
'10: Reshaping developers' security incentives
'09: Analysis of China's Green Dam censorware
'09: Fingerprinting paper with desktop scanners
'08: Cold-boot attacks on encryption keys
'07: California's "top-to-bottom" e-voting review
'07: Machine-assisted election auditing
'06: The Sony rootkit: DRM's harmful side effects
'03: Analysis of MediaMax "shift key" DRM

Positions

- **University of Michigan**, Ann Arbor, MI
  Department of Electrical Engineering and Computer Science,
  Computer Science and Engineering Division

  Professor … (2016–present)
  Associate Professor … (2015–2016)
  Assistant Professor … (2009–2015)

  Director, Center for Computer Security and Society (2014–present)

Education

- Ph.D. in Computer Science, Princeton University, June 2009

  Advisor: Ed Felten
  Thesis: *Investigating Security Failures and their Causes: An Analytic Approach to Computer Security*
  Doctoral committee: Andrew Appel, Adam Finkelstein, Brian Kernighan, Avi Rubin

- M.A. in Computer Science, Princeton University, June 2005
- A.B. in Computer Science, *summa cum laude*, Princeton University, June 2003

Honors and Awards

- Pwnie Award in the category of "Best Cryptographic Attack"
  for "DROWN: Breaking TLS using SSLv2," Black Hat 2016
- Finalist for 2016 Facebook Internet Defense Prize
  for "DROWN: Breaking TLS using SSLv2"
- Named one of Popular Science's "Brilliant 10" (2015) ("each year *Popular Science* honors the brightest young minds reshaping science, engineering, and the world")
- **Best Paper Award** of the 22nd ACM Conference on Computer and Communications Security
  for "Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice" (2015)
- Pwnie Award in the category of "Most Innovative Research"
  for "Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice," Black Hat 2015
- IRTF Applied Networking Research Prize for "Neither Snow Nor Rain Nor MITM... An Empirical Analysis of Email Delivery Security" (2015)
- Alfred P. Sloan Research Fellowship (2015)
- University of Michigan College of Engineering 1938 E Award (2015) ("recognizes an outstanding teacher in both elementary and advanced courses, an understanding counselor of students who seek guidance in their choice of a career, a contributor to the educational growth of his/her College, and a teacher whose scholarly integrity pervades his/her service and the profession of Engineering")
- Morris Wellman Faculty Development Assistant Professorship (2015)
  ("awarded to a junior faculty member to recognize outstanding contributions to teaching and research")
- **Best Paper Award** of the 14th ACM Internet Measurement Conference
  for "The Matter of Heartbleed" (2014)
- **Best Paper Award** of the 21st USENIX Security Symposium
  for "Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices" (2012)
- Runner-up for 2012 PET Award for Outstanding Research in Privacy Enhancing Technologies
  for "Telex: Anticensorship in the Network Infrastructure" (2012)
- John Gideon Memorial Award from the Election Verification Network
  for contributions to election verification (2011)
- **Best Student Paper** 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
- Charlotte Elizabeth Procter Honorific Fellowship, Princeton University (2007)
  ("awarded in recognition of outstanding performance and professional promise, and represents high commendation from the Graduate School")
- National Science Foundation Graduate Research Fellowship (2004–2007)

- **Best Paper Award** of the 8th International Conference on 3D Web Technology for “Early Experiences with a 3D Model Search Engine” (2003)
- Princeton Computer Science Department Senior Award (2003)
- Accenture Prize in Computer Science, Princeton University (2002)
- Martin A. Dale Summer Award, Princeton University (2000)
- USA Computing Olympiad National Finalist (1996 and 1997)

Refereed Conference Publications

[1] **The Security Impact of HTTPS Interception**
Zakir Durumeric, Zane Ma, Drew Springall, Richard Barnes, Nick Sullivan, Elie Bursztein, Michael Bailey, J. A. Halderman, and Vern Paxson
To appear in *Proc. 24th Network and Distributed Systems Symposium* (NDSS), February 2017.
Acceptance rate: 16%, 68/423.

[2] **Measuring Small Subgroup Attacks Against Diffie-Hellman**
Luke Valenta, David Adrian, Antonio Sanso, Shaanan Cohney, Joshua Fried, Marcella Hastings, J. A. Halderman, and Nadia Heninger
To appear in *Proc. 24th Network and Distributed Systems Symposium* (NDSS), February 2017.
Acceptance rate: 16%, 68/423.

[3] **An Internet-Wide View of ICS Devices**
Ariana Mirian, Zane Ma, David Adrian, Matthew Tischer, Thasphon Chuenchujit, Tim Yardley, Robin Berthier, Josh Mason, Zakir Durumeric, J. A. Halderman and Michael Bailey
To appear in *Proc. 14th IEEE Conference on Privacy, Security, and Trust* (PST), December 2016.

[4] **Implementing Attestable Kiosks**
Matthew Bernhard, J. A. Halderman, and Gabe Stocco
To appear in *Proc. 14th IEEE Conference on Privacy, Security, and Trust* (PST), December 2016.

[5] **Measuring the Security Harm of TLS Crypto Shortcuts**
Drew Springall, Zakir Durumeric, and J. A. Halderman
To appear in *Proc. 16th ACM Internet Measurement Conference* (IMC), Santa Monica, Nov. 2016.
Acceptance rate: 25%, 46/184.

[6] **Towards a Complete View of the Certificate Ecosystem**
Benjamin VanderSloot, Johanna Amann, Matthew Bernhard, Zakir Durumeric, Michael Bailey, and J. A. Halderman
To appear in *Proc. 16th ACM Internet Measurement Conference* (IMC), Santa Monica, Nov. 2016.
Acceptance rate: 25%, 46/184.

[7] DROWN: Breaking TLS using SSLv2
Nimrod Aviram, Sebastian Schinzel, Juraj Somorovsky, Nadia Heninger, Maik Dankel, Jens Steube, Luke Valenta, David Adrian, J. A. Halderman, Viktor Dukhovni, Emilia Käsper, Shaanan Cohney, Susanne Engels, Christof Paar, and Yuval Shavitt
Proc. 25th USENIX Security Symposium, Austin, TX, August 2016.
Acceptance rate: 16%, 72/463.
Tied for highest ranked submission.
Pwnie award for best cryptographic attack.
Facebook Internet Defense Prize finalist.

[8] FTP: The Forgotten Cloud
Drew Springall, Zakir Durumeric, and J. A. Halderman
Proc. 46th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Toulouse, June 2016.
Acceptance rate: 22%, 58/259.

[9] Android UI Deception Revisited: Attacks and Defenses
Earlence Fernandes, Qi Alfred Chen, Justin Paupore, Georg Essl, J. A. Halderman, Z. Morley Mao, and Atul Prakash
Proc. 20th International Conference on Financial Cryptography and Data Security (FC), Barbados, February 2016.

[10] Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice
David Adrian, Karthikeyan Bhargavan, Zakir Durumeric, Pierrick Gaudry, Matthew Green, J. A. Halderman, Nadia Heninger, Drew Springall, Emmanuel Thomé, Luke Valenta, Benjamin VanderSloot, Eric Wustrow, Santiago Zanella-Béguelin, and Paul Zimmermann
Proc. 22nd ACM Conference on Computer and Communications Security (CCS), Denver, CO, October 2015.
Acceptance rate: 19%, 128/659.
Best paper award. Perfect review score.
Pwnie award for most innovative research.

[11] Censys: A Search Engine Backed by Internet-Wide Scanning
Zakir Durumeric, David Adrian, Ariana Mirian, Michael Bailey, and J. A. Halderman
Proc. 22nd ACM Conference on Computer and Communications Security (CCS), Denver, CO, October 2015.
Acceptance rate: 19%, 128/659.

[12] Neither Snow Nor Rain Nor MITM... An Empirical Analysis of Email Delivery Security
Zakir Durumeric, David Adrian, Ariana Mirian, James Kasten, Elie Bursztein, Nicholas Lidzborski, Kurt Thomas, Vijay Eranti, Michael Bailey, and J. A. Halderman
Proc. 15th ACM Internet Measurement Conference (IMC), Tokyo, October 2015.
Acceptance rate: 26%, 44/169.
IRTF Applied Networking Research Prize winner.

[13] **The New South Wales iVote System:**
Security Failures and Verification Flaws in a Live Online Election
J. A. Halderman and Vanessa Teague
Proc. 5th International Conference on E-Voting and Identity (VoteID), Bern, Switzerland, September 2015.

[14] **The Matter of Heartbleed**
Zakir Durumeric, Frank Li, James Kasten, Johanna Amann, Jethro Beekman, Mathias Payer, Nicolas Weaver, David Adrian, Vern Paxson, Michael Bailey, and J. A. Halderman
Proc. 14th ACM Internet Measurement Conference (IMC), November 2014.
Acceptance rate: 23%, 43/188
Best paper award.
Honorable mention for Best dataset award.

[15] **Security Analysis of the Estonian Internet Voting System**
Drew Springall, Travis Finkenauer, Zakir Durumeric, Jason Kitcat, Harri Hursti, Margaret MacAlpine, and J. A. Halderman
Proc. 21st ACM Conference on Computer and Communications Security (CCS), Scottsdale, AZ, November 2014.
Acceptance rate: 19%, 114/585.
Highest ranked submission.

[16] **Efficiently Auditing Multi-Level Elections**
Joshua A. Kroll, Edward W. Felten, and J. A. Halderman
Proc. 6th International Conference on Electronic Voting (EVOTE), Lochau, Austria, October 2014.

[17] **Security Analysis of a Full-Body Scanner**
Keaton Mowery, Eric Wustrow, Tom Wypych, Corey Singleton, Chris Comfort, Eric Rescorla, Stephen Checkoway, J. A. Halderman, and Hovav Shacham
Proc. 23rd USENIX Security Symposium, San Diego, CA, August 2014.
Acceptance rate: 19%, 67/350.

[18] **TapDance: End-to-Middle Anticensorship without Flow Blocking**
Eric Wustrow, Colleen Swanson, and J. A. Halderman
Proc. 23rd USENIX Security Symposium, San Diego, CA, August 2014.
Acceptance rate: 19%, 67/350.

[19] **An Internet-Wide View of Internet-Wide Scanning**
Zakir Durumeric, Michael Bailey, and J. A. Halderman
Proc. 23rd USENIX Security Symposium, San Diego, CA, August 2014.
Acceptance rate: 19%, 67/350.

[20] **Elliptic Curve Cryptography in Practice**
Joppe W. Bos, J. A. Halderman, Nadia Heninger, Jonathan Moore, Michael Naehrig, and Eric Wustrow
Proc. 18th Intl. Conference on Financial Cryptography and Data Security (FC), March 2014.
Acceptance rate: 22%, 31/138.

[21] **Outsmarting Proctors with Smartwatches: A Case Study on Wearable Computing Security**
Alex Migicovsky, Zakir Durumeric, Jeff Ringenberg, and J. A. Halderman
Proc. 18th Intl. Conference on Financial Cryptography and Data Security (FC), March 2014.
Acceptance rate: 22%, 31/138.

[22] **Analysis of the HTTPS Certificate Ecosystem**
Zakir Durumeric, James Kasten, Michael Bailey, and J. A. Halderman
Proc. 13th ACM Internet Measurement Conference (IMC), Barcelona, Spain, October 2013.
Acceptance rate: 24%, 42/178.

[23] **ZMap: Fast Internet-Wide Scanning and its Security Applications**
Zakir Durumeric, Eric Wustrow, and J. A. Halderman
Proc. 22nd USENIX Security Symposium, Washington, D.C., August 2013.
Acceptance rate: 16%, 45/277.

[24] **CAge: Taming Certificate Authorities by Inferring Restricted Scopes**
James Kasten, Eric Wustrow, and J. A. Halderman
Proc. 17th Intl. Conference on Financial Cryptography and Data Security (FC), April 2013.

[25] **Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices**
Nadia Heninger, Zakir Durumeric, Eric Wustrow, and J. A. Halderman
Proc. 21st USENIX Security Symposium, pages 205–220, Bellevue, WA, August 2012.
Acceptance rate: 19%, 43/222.
Best paper award.
Named one of *Computing Reviews'* Notable Computing Books and Articles of 2012.

[26] **Attacking the Washington, D.C. Internet Voting System**
Scott Wolchok, Eric Wustrow, Dawn Isabel, and J. A. Halderman
In Angelos D. Keromytis, editor, *Financial Cryptography and Data Security (FC)*, volume 7397 of *Lecture Notes in Computer Science*, pages 114–128. Springer, 2012.
Acceptance rate: 26%, 23/88.
Election Verification Network John Gideon Memorial Award.

[27] **Telex: Anticensorship in the Network Infrastructure**
Eric Wustrow, Scott Wolchok, Ian Goldberg, and J. A. Halderman
Proc. 20th USENIX Security Symposium, pages 459–474, San Francisco, CA, August 2011.
Acceptance rate: 17%, 35/204.
Runner-up for 2012 PET Award for Outstanding Research in Privacy Enhancing Technologies.

[28] **Internet Censorship in China: Where Does the Filtering Occur?**
Xueyang Xu, Z. Morley Mao, and J. A. Halderman
In Neil Spring and George F. Riley, editors, *Passive and Active Measurement*, volume 6579 of *Lecture Notes in Computer Science*, pages 133–142. Springer, 2011.
Acceptance rate: 29%, 23/79.

[29] **Absolute Pwnage: Security Risks of Remote Administration Tools**
Jay Novak, Jonathan Stribley, Kenneth Meagher, and J. A. Halderman
In George Danezis, editor, *Financial Cryptography and Data Security (FC)*, volume 7035 of *Lecture Notes in Computer Science*, pages 77–84. Springer, 2011.
Acceptance rate: 20%, 15/74.

[30] **Security Analysis of India's Electronic Voting Machines**
Scott Wolchok, Eric Wustrow, J. A. Halderman, Hari K. Prasad, Arun Kankipati, Sai Krishna Sakhamuri, Vasavya Yagati, and Rop Gonggrijp
Proc. 17th ACM Conference on Computer and Communications Security (CCS), pages 1–14. ACM, Chicago, IL, October 2010.
Acceptance rate: 17%, 55/320.
Highest ranked submission.

[31] **Sketcha: A Captcha Based on Line Drawings of 3D Models**
Steve Ross, J. A. Halderman, and Adam Finkelstein
Proc. 19th International World Wide Web Conference (WWW), pages 821–830. ACM, Raleigh, NC, April 2010.
Acceptance rate: 12%, 91/754.

[32] **Defeating Vanish with Low-Cost Sybil Attacks Against Large DHTs**
Scott Wolchok, Owen S. Hofmann, Nadia Heninger, Edward W. Felten, J. A. Halderman, Christopher J. Rossbach, Brent Waters, and Emmett Witchel
In *Proc. 17th Network and Distributed System Security Symposium (NDSS)*. Internet Society, San Diego, CA, February–March 2010.
Acceptance rate: 15%, 24/156.

[33] **Fingerprinting Blank Paper Using Commodity Scanners**
William Clarkson, Tim Weyrich, Adam Finkelstein, Nadia Heninger, J. A. Halderman, and Edward W. Felten
IEEE Symposium on Security and Privacy (Oakland), pages 301–314. IEEE, May 2009.
Acceptance rate: 10%, 26/254.

[34] **Lest We Remember: Cold-Boot Attacks on Encryption Keys**
J. A. Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten
Proc. 17th USENIX Security Symposium, pages 45–60, San Jose, CA, July 2008.
Acceptance rate: 16%, 27/170.
Best student paper award.
Pwnie award for most innovative research.

[35] **Harvesting Verifiable Challenges from Oblivious Online Sources**
J. A. Halderman and Brent Waters
Proc. 14th ACM Conference on Computer and Communications Security (CCS), pages 330–341. ACM, Washington, D.C., October 2007.
Acceptance rate: 18%, 55/302.

[36] **Lessons from the Sony CD DRM Episode**
J. A. Halderman and Edward W. Felten
Proc. 15th USENIX Security Symposium, pages 77–92, Vancouver, BC, August 2006.
Acceptance rate: 12%, 22/179.

[37] **A Convenient Method for Securely Managing Passwords**
J. A. Halderman, Brent Waters, and Edward W. Felten
Proc. 14th International World Wide Web Conference (WWW), pages 471–479. ACM, Chiba, Japan, May 2005.
Acceptance rate: 14%, 77/550.

[38] **New Client Puzzle Outsourcing Techniques for DoS Resistance**
Brent Waters, Ari Juels, J. A. Halderman, and Edward W. Felten
Proc. 11th ACM Conference on Computer and Communications Security (CCS), pages 246–256. ACM, Washington, D.C., October 2004.
Acceptance rate: 14%, 35/251.

[39] **Early Experiences with a 3D Model Search Engine**
Patrick Min, J. A. Halderman, Michael Kazhdan, and Thomas Funkhouser
Proc. 8th International Conference on 3D Web Technology (Web3D), pages 7–18. ACM, Saint Malo, France, March 2003.
Best paper award.

Book Chapters

[40] **Practical Attacks on Real-world E-voting**
J. A. Halderman
In Feng Hao and Peter Y. A. Ryan (Eds.), *Real-World Electronic Voting: Design, Analysis and Deployment*, pages 145–171, CRC Press, 2016.

Journal Publications

[41] **Lest We Remember: Cold-Boot Attacks on Encryption Keys**
J. A. Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten
Communications of the ACM, 52(5):91–98, 2009.

[42] **A Search Engine for 3D Models**
Thomas Funkhouser, Patrick Min, Michael Kazhdan, Joyce Chen, J. A. Halderman, David P. Dobkin, and David Jacobs
ACM Transactions on Graphics (TOG), 22(1):83–105, 2003.

Refereed Workshop Publications

[43] **Content-Based Security for the Web**
Alexander Afanasyev, J. A. Halderman, Scott Ruoti, Kent Seamons, Yingdi Yu, Daniel Zappala, and Lixia Zhang
Proc. 2016 New Security Paradigms Workshop (NSPW), September 2016.

[44] **Umbra: Embedded Web Security through Application-Layer Firewalls**
Travis Finkenauer and J. A. Halderman
Proc. 1st Workshop on the Security of Cyberphysical Systems (WOS-CPS), Vienna, Austria, September 2015.

[45] **Replication Prohibited: Attacking Restricted Keyways with 3D Printing**
Ben Burgess, Eric Wustrow, and J. A. Halderman
Proc. 9th USENIX Workshop on Offensive Technologies (WOOT), Washington, DC, August 2015.

[46] **Green Lights Forever: Analyzing the Security of Traffic Infrastructure**
Branden Ghena, William Beyer, Allen Hillaker, Jonathan Pevarnek, and J. A. Halderman
Proc. 8th USENIX Workshop on Offensive Technologies (WOOT), San Diego, CA, August 2014.

[47] **Zippier ZMap: Internet-Wide Scanning at 10Gbps**
David Adrian, Zakir Durumeric, Gulshan Singh, and J. A. Halderman
Proc. 8th USENIX Workshop on Offensive Technologies (WOOT), San Diego, CA, August 2014.

[48] **Internet Censorship in Iran: A First Look**
Simurgh Aryan, Homa Aryan, and J. A. Halderman
Proc. 3rd USENIX Workshop on Free and Open Communications on the Internet (FOCI), Washington, D.C., August 2013.

[49] **Illuminating the Security Issues Surrounding Lights-Out Server Management**
Anthony Bonkoski, Russ Bielawski, and J. A. Halderman
Proc. 7th USENIX Workshop on Offensive Technologies (WOOT), Washington, D.C., August 2013.

[50] **Crawling BitTorrent DHTs for Fun and Profit**
Scott Wolchok and J. A. Halderman
Proc. 4th USENIX Workshop on Offensive Technologies (WOOT), Washington, D.C., August 2010.

[51] **Can DREs Provide Long-Lasting Security?**
The Case of Return-Oriented Programming and the AVC Advantage
Steve Checkoway, Ariel J. Feldman, Brian Kantor, J. A. Halderman, Edward W. Felten, and Hovav Shacham
Proc. 2009 USENIX/ACCURATE/IAVoSS Electronic Voting Technology Workshop / Workshop on Trustworthy Elections (EVT/WOTE), Montreal, QC, August 2009.

[52] **You Go to Elections with the Voting System You Have:**
Stop-Gap Mitigations for Deployed Voting Systems
J. A. Halderman, Eric Rescorla, Hovav Shacham, and David Wagner
In *Proc. 2008 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT)*, San Jose, CA, July 2008.

[53] **In Defense of Pseudorandom Sample Selection**
Joseph A. Calandrino, J. A. Halderman, and Edward W. Felten
Proc. 2008 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT), San Jose, CA, July 2008.

[54] **Security Analysis of the Diebold AccuVote-TS Voting Machine**
Ariel J. Feldman, J. A. Halderman, and Edward W. Felten
Proc. 2007 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT), Washington, D.C., August 2007.

[55] **Machine-Assisted Election Auditing**
Joseph A. Calandrino, J. A. Halderman, and Edward W. Felten
Proc. USENIX/ACCURATE Electronic Voting Technology Workshop (EVT), Washington, D.C., August 2007.

[56] **Privacy Management for Portable Recording Devices**
J. A. Halderman, Brent Waters, and Edward W. Felten
Proc. 2004 ACM Workshop on Privacy in the Electronic Society (WPES), pages 16–24, ACM, Washington, D.C., October 2004.
Acceptance rate: 22%, 10/45.

[57] **Evaluating New Copy-Prevention Techniques for Audio CDs**
J. A. Halderman
In Joan Feigenbaum, editor, *Digital Rights Management*, volume 2696 of *Lecture Notes in Computer Science*, pages 101–117. Springer, 2003.

Selected Other Publications

[58] **The Security Challenges of Online Voting Have Not Gone Away**
Robert Cunningham, Matthew Bernhard, and J. A. Halderman
IEEE Spectrum, November 3, 2016.

[59] **TIVOS: Trusted Visual I/O Paths for Android**
Earlence Fernandes, Qi Alfred Chen, Georg Essl, J. A. Halderman, Z. Morley Mao, and Atul Prakash
Technical report, Computer Science and Engineering Division, University of Michigan, Ann Arbor, MI, May 2014.

[60] **Tales from the Crypto Community:**
The NSA Hurt Cybersecurity. Now It Should Come Clean
Nadia Heninger and J. A. Halderman
Foreign Affairs, October 23, 2013.

[61] **Ethical Issues in E-Voting Security Analysis**
David G. Robinson and J. A. Halderman
In George Danezis, Sven Dietrich, and Kazue Sako, editors, *Financial Cryptography and Data Security*, volume 7126 of *Lecture Notes in Computer Science*, pages 119–130. Springer, 2011. Invited paper.

[62] **To Strengthen Security, Change Developers' Incentives**
J. A. Halderman
IEEE Security & Privacy, 8(2):79–82, March/April 2010.

[63] **Analysis of the Green Dam Censorware System**
Scott Wolchok, Randy Yao, and J. A. Halderman
Technical report, Computer Science and Engineering Division, University of Michigan, Ann Arbor, MI, June 2009.

[64] **AVC Advantage: Hardware Functional Specifications**
J. A. Halderman and Ariel J. Feldman
Technical report, TR-816-08, Princeton University Computer Science Department, Princeton, New Jersey, March 2008.

[65] **Source Code Review of the Diebold Voting System**
J. A. Calandrino, A. J. Feldman, J. A. Halderman, D. Wagner, H. Yu, and W. Zeller
Technical report, California Secretary of State's "Top-to-Bottom" Voting Systems Review (TTBR), July 2007.

[66] **Digital Rights Management, Spyware, and Security**
Edward W. Felten and J. A. Halderman
IEEE Security & Privacy, 4(1):18–23, January/February 2006.

[67] **Analysis of the MediaMax CD3 Copy-Prevention System**
J. A. Halderman
Technical report, TR-679-03, Princeton University Computer Science Department, Princeton, New Jersey, October 2003.

Selected Legal and Regulatory Filings

[68] **Request for DMCA Exemption: Games with Insecure DRM and Insecure DRM Generally**
Comment to the Librarian of Congress of J. A. Halderman, represented by B. Reid, P. Ohm, H. Surden, and J. B. Bernthal, regarding the U.S. Copyright Office 2008–2010 DMCA Anticircumvention Rulemaking, Dec. 2008.
(*Outcome:* Requested exemption granted in part.)

[69] **Request for DMCA Exemption for Audio CDs with Insecure DRM**
Comment to the Librarian of Congress of E. Felten and J. A. Halderman, represented by D. Mulligan and A. Perzanowski, regarding the U.S. Copyright Office 2005–2006 DMCA Anticircumvention Rulemaking, Dec. 2005.
(*Outcome:* Requested exemption granted in part.)

Patents

[70] Controlling Download and Playback of Media Content
Wai Fun Lee, Marius P. Schilder, Jason D. Waddle, and J. A. Halderman
U.S. Patent No. 8,074,083, issued Dec. 2011.

[71] System and Method for Machine-Assisted Election Auditing
Edward W. Felten, Joseph A. Calandrino, and J. A. Halderman
U.S. Patent No. 8,033,463, issued Oct. 2011.

Speaking

Major Invited Talks and Keynotes

- **Let's Encrypt**
  Invited speaker, TTI/Vanguard conference on Cybersecurity, Washington, D.C., Sept. 28, 2016.
- **Elections and Cybersecurity: What Could Go Wrong?**
  Keynote speaker, 19th Information Security Conference (ISC), Honolulu, September 9, 2016.
- **Internet Voting: What Could Go Wrong?**
  Invited speaker, USENIX Enigma, San Francisco, January 27, 2016.
- **Logjam: Diffie-Hellman, Discrete Logs, the NSA, and You**
  32c3, Hamburg, December 29, 2015.
- **The Network Inside Out: New Vantage Points for Internet Security**
  Invited talk, China Internet Security Conference (ISC), Beijing, September 30, 2015.
- **The Network Inside Out: New Vantage Points for Internet Security**
  Keynote speaker, ESCAR USA (Embedded Security in Cars), Ypsilanti, Michigan, May 27, 2015.
- **Security Analysis of the Estonian Internet Voting System.**
  31c3, Hamburg, December 28, 2014.
- **The Network Inside Out: New Vantage Points for Internet Security**
  Keynote speaker, 14th Brazilian Symposium on Information Security and Computer Systems (SBSeg), Belo Horizonte, Brazil, November 4, 2014.
- **Empirical Cryptography: Measuring How Crypto is Used and Misused Online**
  Keynote speaker, 3rd International Conference on Cryptography and Information Security in Latin America (Latincrypt), Florianópolis, Brazil, September 2014.
- **Healing Heartbleed: Vulnerability Mitigation with Internet-wide Scanning**
  Keynote speaker, 11th Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA), London, July 10, 2014.
- **Fast Internet-wide Scanning and its Security Applications.**
  30c3, Hamburg, December 28, 2013.
- **Challenging Security Assumptions**. Three-part tutorial. 2nd TCE Summer School on Computer Security, Technion (Haifa, Israel), July 23, 2013.

- **Verifiably Insecure: Perils and Prospects of Electronic Voting**
  Invited talk, Computer Aided Verification (CAV) 2012 (Berkeley, CA), July 13, 2012.
- **Deport on Arrival: Adventures in Technology, Politics, and Power**
  Invited talk, 20th USENIX Security Symposium (San Francisco, CA), Aug. 11, 2011.
- **Electronic Voting: Danger and Opportunity**
  Keynote speaker, ShmooCon 2008 (Washington, D.C.), Feb. 15, 2008.

Selected Talks (2009–present)

- **The Legacy of Export-grade Cryptography in the 21st Century.** Invited talk, Summer school on real-world crypto and privacy, Croatia, June 9, 2016.
- **Let's Encrypt: A Certificate Authority to Encrypt the Entire Web.** Invited talk, Cubaconf, Havana, April 25, 2016.
- **Logjam: Diffie-Hellman, Discrete Logs, the NSA, and You.** Invited talk, NYU Tandon School of Engineering, April 8, 2016 [host: Damon McCoy]; Invited talk, UIUC Science of Security seminar, February 9, 2016 [host: Michael Bailey].
- **The Network Inside Out: New Vantage Points for Internet Security.** Invited talk, Qatar Computing Research Institute, Doha, May 24, 2015; Invited talk, University of Chile, Santiago, April 8, 2015; Invited talk, Princeton University, October 15, 2014; Invited talk, U.T. Austin, March 9, 2014.
- **Decoy Routing: Internet Freedom in the Network's Core.** Invited speaker, Internet Freedom Technology Showcase: The Future of Human Rights Online, New York, Sep. 26, 2015.
- **The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election.** 5th International Conference on E-Voting and Identity (VoteID), Bern, Switzerland, Sep. 3, 2015; Invited talk, IT Univ. of Copenhagen, Sep. 1, 2015; Invited talk (with Vanessa Teague), USENIX Journal of Election Technologies and Systems Workshop (JETS), Washington, D.C., Aug. 11, 2015.
- **Security Analysis of the Estonian Internet Voting System.** Invited talk, 5th International Conference on E-Voting and Identity (VoteID), Bern, Switzerland, Sep. 3, 2015; Invited talk, Google, Mountain View, CA, June 3, 2014; Invited talk, Copenhagen University, June 12, 2014.
- **Indiscreet Tweets.** Rump session talk; 24th USENIX Security Symposium, Washington, D.C., August 12, 2015.
- **How Diffie-Hellman Fails in Practice.** Invited talk, IT Univ. of Copenhagen, May 22, 2015.
- **Influence on Democracy of Computers, Internet, and Social Media.** Invited speaker, Osher Lifelong Learning Institute at the University of Michigan, March 26, 2015.
- **E-Voting: Danger and Opportunity.** Invited talk, University of Chile, Santiago, April 7, 2015; Keynote speaker, 14th Brazilian Symposium on Information Security and Computer Systems (SBSeg), Belo Horizonte, Brazil, November 3, 2014; Crypto seminar, University of Tartu, Estonia, October 10, 2013; Invited speaker, US–Egypt Cyber Security Workshop, Cairo, May 28, 2013; Invited speaker, First DemTech Workshop on Voting Technology for Egypt, Copenhagen, May

1, 2013; Invited keynote, 8th CyberWatch Mid-Atlantic CCDC, Baltimore, MD, Apr. 10, 2013; Invited speaker, Verifiable Voting Schemes Workshop, University of Luxembourg, Mar. 21, 2013; Invited speaker, MHacks hackathon, Ann Arbor, MI, Feb. 2, 2013; Public lecture, U. Michigan, Nov. 6, 2012.

– **Internet Censorship in Iran: A First Look.** 3rd USENIX Workshop on Free and Open Communications on the Internet (FOCI), Aug. 13, 2013.

– **Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices.** Invited talk, NSA, Aug. 8, 2013; Invited talk, Taiwan Information Security Center Workshop, National Chung-Hsing University (Taichung, Taiwan), Nov. 16, .2012

– **Securing Digital Democracy**. U. Maryland, Apr. 8, 2013 [host: Jonathan Katz]; CMU, Apr. 1, 2013 [host: Virgil Gligor]; Cornell, Feb. 28, 2013 [host: Andrew Myers].

– **Telex: Anticensorship in the Network Infrastructure**. Invited speaker, Academia Sinica (Taipei), Nov. 14, 2012 [host: Bo-Yin Yang]; TRUST Seminar, U.C., Berkeley, Dec. 1, 2011 [host: Galina Schwartz]; Think Conference, Nov. 5, 2011; Ideas Lunch, Information Society Project at Yale Law School, Oct. 26, 2011; Invited speaker, Committee to Protect Journalists Online Press Freedom Summit (San Francisco), Sept. 27, 2011.

– **Deport on Arrival: Adventures in Technology, Politics, and Power**. Guest lecture, U-M School of Art and Design, Nov 5, 2012 [host: Osman Khan]; Invited speaker, CS4HS Workshop, U. Michigan, Aug. 21, 2012; Invited speaker, U. Michigan IEEE, Feb. 15, 2012.

– **Attacking the Washington, D.C. Internet Voting System**. Invited speaker, International Foundation for Election Systems (IFES), Nov. 2, 2012 [host: Michael Yard]; Invited speaker, IT University of Copenhagen, May 11, 2012 [host: Carsten Schürmann].

– **Voter I*Don't***. Rump session talk; 21st USENIX Security Symposium (Bellevue, WA), Aug. 8, 2012; Rump session talk; EVT/WOTE '12 (Bellevue, WA), Aug. 6, 2012 [with Josh Benaloh].

– **Reed Smith's Evening with a Hacker**. Keynote speaker (New Brunswick, NJ), Oct. 20, 2011.

– **Are DREs Toxic Waste?** Rump session talk, 20th USENIX Security Symposium (San Francisco), Aug. 10, 2011; Rump session talk, EVT/WOTE '11 (San Francisco), Aug. 8, 2011.

– **Security Problems in India's Electronic Voting Machines**. Dagstuhl seminar on Verifiable Elections and the Public (Wadern, Germany), July 12, 2011; Harvard University, Center for Research on Computation and Society (CRCS) seminar, Jan. 24, 2011 [host: Ariel Procaccia]; U. Michigan, CSE seminar, Nov. 18, 2010 [with Hari Prasad]; MIT, CSAIL CIS Seminar, Nov. 12, 2010 [with Hari Prasad; host: Ron Rivest]; Distinguished lecture, U.C. San Diego, Department of Computer Science, Nov. 9, 2010 [with Hari Prasad; host: Hovav Shacham]; U.C. Berkeley, Center for Information Technology Research in the Interest of Society (CITRIS), Nov. 8, 2010 [with Hari Prasad; host: Eric Brewer]; Google, Inc., Tech Talk (Mountain View, CA), Nov. 5, 2010 [with Hari Prasad; host: Marius Schilder]; U.C., Berkeley TRUST Security Seminar, Nov. 4, 2010 [with Hari Prasad; host: Shankar Sastry]; Stanford University, CS Department, Nov. 3, 2010 [with Hari Prasad; host: David Dill]; Princeton University, Center for Information Technology Policy, Oct. 28, 2010 [with Hari Prasad, host: Ed Felten]; University of Texas at Austin, Department of Computer Science, Aug. 27, 2010 [host: Brent Waters].

- **Ethical Issues in E-Voting Security Analysis.** Invited talk, Workshop on Ethics in Computer Security Research (WECSR) (Castries, St. Lucia), Mar. 4, 2011 [with David Robinson].
- **Electronic Voting: Danger and Opportunity.** Invited speaker, "Interfaces 10: Technology, Society and Innovation," Center for Technology and Society (CTS/FGV) (Rio de Janeiro), Dec. 2, 2010 [host: Ronaldo Lemos]; Invited speaker, Conference on "EVMs: How Trustworthy?," Centre for National Renaissance (Chennai, India), Feb. 13, 2010; Google, Inc., Tech Talk (Mountain View, CA), Jan. 10, 2008; Star Camp (Cape Town, South Africa), Dec. 8, 2007; Lehigh University, Nov. 27, 2007; Princeton OiT Lunch-'n-Learn, Oct. 24, 2007; University of Waterloo (Canada), Feb. 28, 2007.
- **A New Approach to Censorship Resistance.** Think Conference, Nov. 7, 2010.
- **Practical AVC-Edge CompactFlash Modifications can Amuse Nerds [PACMAN].** Rump session, 19th USENIX Security Symposium (Washington, D.C.), Aug. 11, 2010; Rump session, EVT/WOTE '10 (Washington, D.C.), Aug. 9, 2010.
- **Legal Challenges to Security Research.** Guest lecture, Law 633: Copyright, U. Michigan Law School, Apr. 7, 2010; Invited talk, University of Florida Law School, Oct. 12, 2006.
- **Adventures in Computer Security.** Invited talk, Greenhills School, grades 6–12 (Ann Arbor, MI), Mar. 8, 2010.
- **The Role of Designers' Incentives in Computer Security Failures.** STIET Seminar, U. Michigan, Oct. 8, 2009.
- **Cold-Boot Attacks Against Disk Encryption.** Invited speaker, SUMIT 09 Security Symposium, U. Michigan, Oct. 20, 2009.
- **On the Attack.** Distinguished lecture, U.C. Berkeley EECS, Nov. 18, 2009.

Selected Other Speaking (2010–present)

- Moderator: **Apple & the FBI: Encryption, Security, and Civil Liberties.** Panelists: Nate Cardozo and Barbara McQuade. U-M Dissonance Speaker Series, April 12, 2016.
- Moderator: **Privacy, IT Security and Politics.** Panelists: Ari Schwartz and David Sobel. U-M ITS SUMIT_2015, Oct. 22, 2015.
- Panelist: **The Future of E-Voting Research.** 5th International Conference on E-Voting and Identity (VoteID), Bern, Switzerland, Sep. 4, 2015.
- Moderator: **Panel on Research Ethics.** 24th USENIX Security Symposium, Washington, D.C., August 13, 2015.
- Panelist: **Theories of Privacy in Light of "Big Data."** Michigan Telecommunications and Technology Law Review Symposium on Privacy, Technology, and the Law, University of Michigan Law School, Feb. 21, 2015.
- Panelist: **Measuring Privacy.** Big Privacy symposium, Princeton University CITP, Apr. 26, 2013 [moderator: Ed Felten].

- Panelist: **Civil Society's Challenge in Preserving Civic Participation**. The Public Voice workshop: Privacy Rights are a Global Challenge, held in conjunction with the 34th International Conference of Data Protection and Privacy Commissioners, Punta del Este, Uruguay, Oct. 22, 2012 [moderator: Lillie Coney].
- Panelist: **Election Technologies: Today and Tomorrow**. Microsoft Faculty Summit (Redmond), July 17, 2012 [moderator: Josh Benaloh].
- Panelist: **Is America Ready to Vote on the Internet?** CSPRI Seminar, George Washington University (Washington, D.C.), May 16, 2012 [moderator: Lance Hoffman].
- Panelist: **Technical Methods of Circumventing Censorship**. Global Censorship Conference, Yale Law School, Mar. 31, 2012.
- Panelist: **Internet Voting**. RSA Conference (San Francisco), Mar. 1, 2012 [moderator: Ron Rivest].
- Panelist: **The Law and Science of Trustworthy Elections**. Association of American Law Schools (AALS) Annual Meeting, Jan. 5, 2012 [moderator: Ron Rivest].
- Panelist: **Connecticut Secretary of State's Online Voting Symposium** (New Britain, CT), Oct. 27, 2011 [moderator: John Dankosky].
- Panelist: **CS Saves the World**. Michigan CSE Mini-symposium, Mar. 19, 2011 [moderator: Prabal Dutta].
- Panelist: **Cyber Security / Election Technology**. Overseas Voting Foundation Summit, Feb. 10, 2011 [moderator: Candice Hoke].
- ~~Tutorial speaker/organizer: **Security Issues in Electronic Voting**, ICISS (Gandhinagar, India), Dec. 15, 2010~~ [canceled under threat of deportation].
- Invited testimony: On **D.C. Board of Elections and Ethics Readiness for the Nov. 2010 General Election**. D.C. Council Hearing, Oct. 8, 2010.
- Panelist and organizer: **India's Electronic Voting Machines**. EVT/WOTE (Washington, D.C.), Aug. 9, 2010.
- Panelist: **Ethics in Networking and Security Research**. ISOC Network and Distributed System Security Symposium (San Diego, CA), Mar. 2, 2010 [moderator: Michael Bailey].

Advising and Mentoring

Graduate Students

- Allison McDonald (Ph.D. in progress)
- Matthew Bernhard (Ph.D. in progress)
- Benjamin VanderSloot (Ph.D. in progress)
- David Adrian (Ph.D. in progress)
- Andrew Springall (Ph.D. in progress; NSF Graduate Research Fellowship)
- Zakir Durumeric (Ph.D. in progress; Google Ph.D. Fellowship in Computer Security)
- Travis Finkenauer (M.S. 2016; went on to security position at Juniper Networks)
- Eric Wustrow (Ph.D. 2016; went on to tenure track faculty position at U. Colorado, Boulder)
- James Kasten (Ph.D. 2015; went on to software engineering position at Google)
- Scott Wolchok (M.S. 2011; went on to software engineering position at Facebook)

Post Docs

- Colleen Swanson (2014–15)

Doctoral Committees

- Denis Bueno (C.S. P.D. expected 2016, Michigan)
- Eric Crockett (C.S. Ph.D expected 2016, Georgia Tech)
- Jakub Czyz (C.S. Ph.D. 2016, Michigan)
- Eric Wustrow (C.S. Ph.D. 2016, Michigan; chair)
- James Kasten (C.S. Ph.D. 2015, Michigan; chair)
- Jing Zhang (C.S. Ph.D. 2015, Michigan)
- Katharine Cheng (C.S. Ph.D. 2012, Michigan)
- Matt Knysz (C.S. Ph.D. 2012, Michigan)
- Zhiyun Qian (C.S. Ph.D. 2012, Michigan)
- Xin Hu (C.S. Ph.D. 2011, Michigan)
- Ellick Chan (C.S. Ph.D. 2011, UIUC)

Undergraduate Independent Work

- 2016: Ben Burgess, Noah Duncan
- 2015: Ben Burgess, Rose Howell, Vikas Kumar, Ariana Mirian, Zhi Qian Seah
- 2014: Christopher Jeakle, Andrew Modell, Kollin Purcell
- 2013: David Adrian, Anthony Bonkoski, Alex Migicovsky, Andrew Modell, Jennifer O'Neil
- 2011: Yilun Cui, Alexander Motalleb
- 2010: Arun Ganesan, Neha Gupta, Kenneth Meagher, Jay Novak, Dhritiman Sagar, Samantha Schumacher, Jonathan Stribley
- 2009: Mark Griffin, Randy Yao

Teaching

- **Introduction to Computer Security**, EECS 388, University of Michigan
  Terms: Fall 2017, Fall 2016, Fall 2015, Fall 2014, Fall 2013, Fall 2011, Fall 2010, Fall 2009
  Created new undergrad security elective that has grown to reach >750 students/year. An accessible intro, teaches the security mindset and practical skills for building and analyzing security-critical systems.
- **Computer and Network Security**, EECS 588, University of Michigan
  Terms: Winter 2016, Winter 2015, Winter 2014, Winter 2013, Winter 2012, Winter 2011, Winter 2010, Winter 2009
  Redesigned core grad-level security course. Based around discussing classic and current research papers and performing novel independent work. Provides an intro. to systems research for many students.
- **Securing Digital Democracy**, Coursera (MOOC)
  Designed and taught a massive, open online course that explored the security risks—and future potential—of electronic voting and Internet voting technologies; over 20,000 enrolled students.

Professional Service

Program Committees

- 2017 ISOC Network and Distributed Systems Security Symposium (NDSS '17)
- 2016 ACM Internet Measurement Conference (IMC '16)
- 2016 USENIX Security Symposium (Sec '16)
- 2016 International Joint Conference on Electronic Voting (E-VOTE-ID '16)
- 2016 Workshop on Advances in Secure Electronic Voting (Voting '16)
- 2015 ACM Conference on Computer and Communications Security (CCS '15)
- 2015 ACM Internet Measurement Conference (IMC '15)
- 2015 USENIX Security Symposium (Sec '15)
- 2014 ACM Conference on Computer and Communications Security (CCS '14)
- 2014 USENIX Security Symposium (Sec '14)
- 2013 ACM Conference on Computer and Communications Security (CCS '13)
- **Program co-chair**, 2012 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE '12)
- 2012 Workshop on Free and Open Communications on the Internet (FOCI '12)
- 2012 IEEE Symposium on Security and Privacy ("Oakland" '12)
- 2012 International Conference on Financial Cryptography and Data Security (FC '12)
- 2011 Workshop on Free and Open Communications on the Internet (FOCI '11)
- 2011 Electronic Voting Technology Workshop (EVT/WOTE '11)
- 2010 ACM Conference on Computer and Communications Security (CCS '10)
- 2010 USENIX/ACCURATE/IAVOSS Electronic Voting Technology Workshop (EVT '10)
- 2010 USENIX Security Symposium (Sec '10)
- 2010 IEEE Symposium on Security and Privacy (Oakland '10)
- 2010 International World Wide Web Conference (WWW '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)
- 2008 ACM Conference on Computer and Communications Security (CCS '08)
- 2008 ACM Workshop on Privacy in the Electronic Society (WPES '08)
- 2008 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT '08)
- 2008 International World Wide Web Conference (WWW '08)

Boards

- Board of Directors for the Internet Security Research Group (2014–present)
- Board of Advisors for the Verified Voting Foundation (2012–present)

- External Advisory Board for the DemTech Project, IT University of Copenhagen (2011–present)
- Advisory Council for the Princeton University Department of Computer Science (2012–2014)

Department and University Service

- Faculty Advisor for Michigan Hackers student group (2012–present)
- CSE Graduate Affairs Committee (member, 2014–present)
- CSE Undergraduate Program Advising (CS/ENG) (2011–present)
- Faculty Senate, Rules Committee of the Senate Assembly (member, 2011–12)
- CSE Graduate Admissions Committee (member, 2010–11)
- CSE Graduate Committee (member, 2009–10)

Broader Impact of Selected Projects

- **Let's Encrypt: A Certificate Authority to Encrypt the Entire Web** (2016)
  Co-founded a new HTTPS certificate authority to provide free, browser-trusted, automatically validated certificates for all domains. Developed in partnership with EFF and Mozilla, Let's Encrypt has helped secure millions of websites and is now issuing certificates at a greater rate than all other CAs combined.
- **The Logjam Attack and Weak Practical Use of Diffie-Hellman** (2015)
  Introduced Logjam, a practical attack on TLS that affected nearly 10% of popular HTTPS websites. Our results suggest that state-level attackers can break 1024-bit Diffie-Hellman, providing the first parsimonious explanation for how NSA is decrypting widespread VPN traffic, as revealed by Snowden.
- **Security Analysis of the Estonian Internet Voting System** (2014)
  Led the first rigorous security review of world's most significant Internet voting system. Based on code review, laboratory testing, and in-person observation, our study revealed significant shortcomings that could allow state-level attackers to upset national elections.
- **ZMap Internet-Wide Scanner Open-Source Project** (2013)
  Created ZMap, a network probing tool designed for Internet-wide measurement research that achieves up to 10,000× better performance than earlier tools. Now a thriving open-source project, ZMap is available in major Linux distros. We also maintain Scans.io, a public scan data repository.
- **Detection of Widespread Weak Keys in Network Devices** (2012)
  After conducting the largest Internet-wide survey of HTTPS and SSH hosts, we uncovered serious flaws in cryptographic public key generation affecting millions of users. We disclosed vulnerabilities to more than 60 network device makers and spawned major changes to the Linux random number generator.
- **The Telex Anticensorship System** (2011)
  Invented a fundamentally new approach to circumventing state-level Internet censorship, based on placing anticensorship technology into core network infrastructure outside the censoring country. Prototype attracted over 100,000 users, mainly in China. Now testing next-gen. schemes at partner ISP.
- **Attacking Washington, D.C.'s Internet Voting System** (2010)
  Participated in the first public security trial of an Internet voting system set to be deployed in a real election. We found serious flaws that allowed us to change all votes without detection. This led to the system being scrapped, and the widespread media coverage has altered the debate on Internet voting.

- **Analysis of India's E-Voting System** (2010)
  Participated in the first independent security review of the electronic voting machines used by half a billion voters in India. The flaws uncovered in our work were front-page news. After arresting my coauthor and threatening to deport me, officials eventually moved to adopt a paper trail nationwide.
- **Green Dam Youth Escort Censorware** (2009)
  Uncovered security problems and copyright infringement in client-side censorship software mandated by the Chinese government. Findings helped catalyze popular protest against the program, leading China to reverse its policy requiring installation on new PCs.
- **Cold-Boot Attacks** (2008)
  Developed the "cold boot" attack against software disk encryption systems, which altered widespread thinking on security assumptions about the behavior of RAM, influenced computer forensics practice, and inspired the creation of a new subfield of theoretical cryptography.
- **California "Top-to-Bottom" Review** (2007)
  Helped lead the California Secretary of State's "top-to-bottom" review of electronic voting machines, the first public review of this technology by any state. Our reports led California to discontinue use of highly vulnerable touch-screen voting systems and altered the course of election technology in the U.S.
- **DMCA Exemptions for Security** (2006 and 2010)
  Worked with legal teams to successfully petition the U.S. Copyright Office to create exemptions to the Digital Millennium Copyright Act (which prohibits circumventing DRM) in order to allow the public to investigate and repair security problems caused by certain DRM. One of only six exemptions granted.
- **Sony DRM Rootkit** (2005)
  Discovered dangerous security side-effects in the design of copy protection software used for music CDs. Resulted in the recall of millions of discs, class action lawsuits, and an investigation by the U.S. Federal Trade Commission in which I served as a technical expert on DRM's harm to consumers' security.
- **The Art of Science** (2004)
  Co-founded an interdisciplinary art competition at Princeton University that showcases images and videos produced in the course of scientific research as well as creative works that incorporate tools and ideas from science. Following international attention, the concept has spread to many other campuses.

Outreach and Press Coverage

I'm a regular contributor to Freedom-to-Tinker, a blog hosted by Princeton's CITP. My posts discuss current issues in security and public policy or announce new research results, aiming to communicate findings to nonspecialists.

I'm happy to speak to the press when I believe the topic is important for the public to understand. Much of my research has received significant media attention.

Selected media outlets *Television:* CNN, Fox News, CBS Evening News, NBC Nightly News, MSNBC, CNBC, MTV, Al Jazeera, C-SPAN. *Radio:* NPR News, NPR Science Friday, BBC World Service, The Diane Rehms Show. *Print*: The New York Times, LA Times, USA Today (front page profile), The Wall Street Journal, Washington Post, Boston Globe, Times of India, Time, Fortune, Harpers (incl. Harpers Index), The Atlantic; The Economist, New Scientist, MIT Tech Review, Businessweek, Redbook, PC Magazine, Playboy (long-form profile). *Online*: Hacker News (dozens of top stories), Slashdot (>40 stories), Reddit (top of front page), BoingBoing, CNET News, Wired News, TechNewsDaily, Science Daily, Gizmodo, TechDirt, Ars Technica, The Register, Huffington Post, Politico, The Drudge Report, and hundreds more.

References

Edward W. Felten
Professor
Princeton University
ACM Fellow, NAE Member
felten@cs.princeton.edu

Farnam Jahanian
Provost
Carnegie Mellon University
AAAS, ACM, & IEEE Fellow
farnam@andrew.cmu.edu

Ronald L. Rivest
Professor
MIT
A.M. Turing Award Winner
rivest@mit.edu

Michael Bailey
Associate Professor
UIUC
mdbailey@illinois.edu

Matt Blaze
Professor
University of Pennsylvania
mab@crypto.com

Avi Rubin
Professor
Johns Hopkins University
rubin@jhu.edu

Doug Tygar
Professor
U. C. Berkeley
doug.tygar@gmail.com

Dan Wallach
Professor
Rice University
dwallach@cs.rice.edu

David Wagner
Professor
U. C. Berkeley
daw@cs.berkeley.edu