J. Alex Halderman

Bredt Family Professor of Computer Science & Engineering
University of Michigan

2260 Hayward Street
Ann Arbor, MI 48109 USA
(*office*) +1 734 647 1806
jhalderm@umich.edu

https://jhalderm.com

August 18, 2023

Research Overview

My research focuses on computer security, with an emphasis on problems that impact society and public policy. My interests include software security, network security, security measurement, privacy and anonymity, election cybersecurity, censorship resistance, computer forensics, and online crime, as well as the interaction of technology with law and policy, politics, and international affairs.

Selected Projects

'23: Robust Logic & Accuracy Testing
'22: Vulnerabilities in Dominion ImageCast X BMD
'21: Antrim County election incident investigation
'20: How human factors limit BMD verifiability
'19: Refraction Networking in ISP-scale production
'19: Leading Michigan Election Security Taskforce
'18: Commercial launch of Censys, Inc.
'17: Testimony to U.S. Senate Russia investigation
'17: Weaknesses in TLS interception middleboxes
'16: U.S. presidential election recounts
'16: Let's Encrypt HTTPS certificate authority
'16: DROWN: Attacking TLS with SSLv2
'15: Weak Diffie-Hellman and the Logjam attack
'14: Understanding Heartbleed's aftermath
'14: Weaknesses of TSA full-body X-ray scanners
'14: Analysis of Estonia's Internet voting system
'13: ZMap Internet-wide network scanner
'12: Widespread weak keys in network devices
'11: Telex, the first Refraction Networking scheme
'10: Hacking Washington D.C.'s Internet voting
'10: Vulnerabilities in India's e-voting machines
'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
  College of Engineering, Computer Science & Engineering Division

  Bredt Family Professor … (2023–present)
  Professor ..... (2016–2023)
  Associate Professor ..... (2015–2016)
  Assistant Professor ..... (2009–2015)

  Director, Center for Computer Security and Society (2014–present)
  Director, CSE Systems Laboratory (2018–present)
- **ISRG** (**Let's Encrypt**); Co-Founder, Board Member, and Corporate Secretary (2013–present)
- **Censys, Inc.**; Co-Founder and Chief Scientist (2017–2020)

Education

- Ph.D. in Computer Science, Princeton University, 2009
  Advisor: Edward Felten Committee: Andrew Appel, Adam Finkelstein, Brian Kernighan, Avi Rubin
  Thesis: *Investigating Security Failures and their Causes: An Analytic Approach to Computer Security*

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

Honors and Awards

– **Internet Defense Prize**, first-place, awarded by the 31st USENIX Security Symposium for "OpenVPN is Open to VPN Fingerprinting" (2022) ($110,000 award "celebrates security research contributions to the protection and defense of the Internet")
– **Best Paper Award** of the 31st USENIX Security Symposium for "The Antrim County 2020 Election Incident: An Independent Forensic Investigation" (2022)
– **Best Paper Award** of the 31st USENIX Security Symposium for "OpenVPN is Open to VPN Fingerprinting" (2022)
– **Test of Time Award** of the 31st USENIX Security Symposium for "Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices" (2022)
– **Levchin Prize** for contributions to real world cryptography, awarded to Let's Encrypt (2022)
– **Best Student Paper Award** of the 41st IEEE Symposium on Security and Privacy for "Can Voters Detect Malicious Manipulation of Ballot Marking Devices?" (2020)
– **President's Award for National and State Leadership**, University of Michigan (2020)
– **Andrew Carnegie Fellowship** (2019)
– Merit Network Eric Aupperle Innovation Award (2017) ("named for Merit's first president, recognizes individuals that enhance their work by using networking and related technologies in exciting ways")
– Pwnie Award in the category of "Best Cryptographic Attack" for "DROWN: Breaking TLS using SSLv2," Black Hat 2016
– Finalist for 2016 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 the College, and a teacher whose scholarly integrity pervades their 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 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
- 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)
- **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] **Logic and Accuracy Testing: A Fifty-State Review**
Josiah Walker, Nakul Bajaj, Braden L. Crimmins, and J. A. Halderman
7th International Joint Conference on Electronic Voting (E-Vote-ID), Oct. 2022.
Acceptance rate: 29%, 10/35

[2] **The Antrim County 2020 Election Incident: An Independent Forensic Investigation**
J. A. Halderman
31st USENIX Security Symposium, Aug. 2022.
Acceptance rate: 18%, 256/1414
Best paper award.

[3] **OpenVPN is Open to VPN Fingerprinting**
Diwen Xue, Reethika Ramesh, Arham Jain, Michalis Kallitsis, J. A. Halderman, Jedidiah R. Crandall, and Roya Ensafi
31st USENIX Security Symposium, Aug. 2022.
Acceptance rate: 18%, 256/1414
Best paper award.
Internet Defense Prize, first-place winner.

[4] **Improving the Accuracy of Ballot Scanners Using Supervised Learning**
Sameer Barretto, William Chown, David Meyer, Aditya Soni, Atreya Tata, and J. A. Halderman
6th International Joint Conference on Electronic Voting (E-Vote-ID), Oct. 2021.
Acceptance rate: 22%, 11/49.

[5] **Security Analysis of the Democracy Live Online Voting System**
Michael A. Specter and J. A. Halderman
30th USENIX Security Symposium, Aug. 2021.
Acceptance rate: 19%, 246/1295.

[6] **Investigating Large-Scale HTTPS Interception in Kazakhstan**
Ram Sundara Raman, Leonid Evdokimov, Eric Wustrow, J. A. Halderman, and Roya Ensafi
20th ACM Internet Measurement Conference (IMC), Oct. 2020.
Acceptance rate: 25%, 53/216.
Nominated for best paper.

[7] **Running Refraction Networking for Real**
Benjamin VanderSloot, Sergey Frolov, Jack Wampler, Sze Chuen Tan, Irv Simpson, Michalis Kallitsis, J. A. Halderman, Nikita Borisov, and Eric Wustrow
20th Privacy Enhancing Technologies Symposium (PETS), July 2020.
Acceptance rate: 22%, 54/250.

[8] **Characterizing Transnational Internet Performance and the Great Bottleneck of China**
Pengxiong Zhu, Keyu Man, Zhongjie Wang, Zhiyun Qian, Roya Ensafi, J. A. Halderman, and Haixin Duan
ACM SIGMETRICS, June 2020.
Acceptance rate: 20%, 55/280.

[9] **Can Voters Detect Malicious Manipulation of Ballot Marking Devices?**
Matthew Bernhard, Allison McDonald, Henry Meng, Jensen Hwa, Nakul Bajaj, Kevin Chang, and J. A. Halderman
41st IEEE Symposium on Security and Privacy ("Oakland"), May 2020.
Acceptance rate: 12%, 104/841.
Best student paper award.

[10] **Let's Encrypt: An Automated Certificate Authority to Encrypt the Entire Web**
Josh Aas, Richard Barnes, Benton Case, Zakir Durumeric, Peter Eckersley, Alan Flores-López, J. A. Halderman, Jacob Hoffman-Andrews, James Kasten, Eric Rescorla, Seth Schoen, and Brad Warren
26th ACM Conference on Computer and Communications Security (CCS), London, UK, Nov. 2019.
Acceptance rate: 16%, 117/722.

[11] **Conjure: Summoning Proxies from Unused Address Space**
Sergey Frolov, Jack Wampler, Sze Chuen Tan, J. A. Halderman, Nikita Borisov, and Eric Wustrow
26th ACM Conference on Computer and Communications Security (CCS), London, UK, Nov. 2019.
Acceptance rate: 16%, 117/722.

[12] **UnclearBallot: Automated Ballot Image Manipulation**
Matthew Bernhard, Kartikeya Kandula, Jeremy Wink, and J. A. Halderman
4th International Joint Conference on Electronic Voting (E-Vote-ID), Bregenz, Austria, Oct. 2019.
Acceptance rate: 29%, 13/45.

[13] **On the Usability of HTTPS Deployment**
Matthew Bernhard, Jonathan Sharman, Claudia Ziegler Acemyan, Philip Kortum, Dan S. Wallach, and J. A. Halderman
ACM Conference on Human Factors in Computing Systems (CHI), Glasgow, UK, May 2019.
Acceptance rate: 24%, 705/2958.

[14] **403 Forbidden: A Global View of Geoblocking**
Allison McDonald, Matthew Bernhard, Benjamin VanderSloot, Will Scott, J. A. Halderman, and Roya Ensafi
18th ACM Internet Measurement Conference (IMC), Boston, MA, Oct. 2018.
Acceptance rate: 24%, 43/174.

[15] **Quack: Scalable Remote Measurement of Application-Layer Censorship**
Benjamin VanderSloot, Allison McDonald, Will Scott, J. A. Halderman, and Roya Ensafi
27th USENIX Security Symposium, Baltimore, MD, Aug. 2018.
Acceptance rate: 19%, 100/524.

[16] **Tracking Certificate Misissuance in the Wild**
Deepak Kumar, Zhengping Wang, Matthew Hyder, Joseph Dickinson, Gabrielle Beck, David Adrian, Joshua Mason, Zakir Durumeric, J. A. Halderman, and Michael Bailey
39th IEEE Symposium on Security and Privacy ("Oakland"), San Francisco, CA, May 2018.
Acceptance rate: 11%, 63/549.

[17] **Initial Measurements of the Cuban Street Network**
Eduardo Pujol, Will Scott, Eric Wustrow, and J. A. Halderman
17th ACM Internet Measurement Conference (IMC), London, UK, Nov. 2017.
Acceptance rate: 23%, 42/179.

[18] **Public Evidence from Secret Ballots**
Matthew Bernhard, Josh Benaloh, J. A. Halderman, Ronald L. Rivest, Peter Y. A. Ryan, Philip B. Stark, Vanessa Teague, Poorvi L. Vora, and Dan S. Wallach
2nd International Joint Conference on Electronic Voting (E-Vote-ID), Bregenz, Austria, Oct. 2017.

[19] **Understanding the Mirai Botnet**
Manos Antonakakis, Tim April, Michael Bailey, Matt Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J. A. Halderman, Luca Invernizzi, Michalis Kallitsis, Deepak Kumar, Chaz Lever, Zane Ma, Joshua Mason, Damian Menscher, Chad Seaman, Nick Sullivan, Kurt Thomas, and Yi Zhou
26th USENIX Security Symposium, Vancouver, BC, Aug. 2017.
Acceptance rate: 16%, 85/522.

[20] **Security Challenges in an Increasingly Tangled Web**
Deepak Kumar, Zane Ma, Zakir Durumeric, Ariana Mirian, Joshua Mason, J. A. Halderman, and Michael Bailey
26th World Wide Web Conference (WWW), Banff, AB, Apr. 2017.
Acceptance rate: 17%, 164/966.

[21] **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
24th Network and Distributed Systems Symposium (NDSS), San Diego, CA, Feb. 2017.
Acceptance rate: 16%, 68/423.

[22] **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
24th Network and Distributed Systems Symposium (NDSS), San Diego, CA, Feb. 2017.
Acceptance rate: 16%, 68/423.

[23] **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
14th IEEE Conference on Privacy, Security, and Trust (PST), Auckland, NZ, Dec. 2016.

[24] **Implementing Attestable Kiosks**
Matthew Bernhard, J. A. Halderman, and Gabe Stocco
14th IEEE Conference on Privacy, Security, and Trust (PST), Auckland, NZ, Dec. 2016.

[25] **A Security Analysis of Police Computer Systems**
Benjamin VanderSloot, Stuart Wheaton, and J. A. Halderman
14th IEEE Conference on Privacy, Security, and Trust (PST), Auckland, NZ, Dec. 2016.

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

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

[28] **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
25th USENIX Security Symposium, Austin, TX, Aug. 2016.
Acceptance rate: 16%, 72/463.
Pwnie award for best cryptographic attack.

Highest ranked submission.
Internet Defense Prize finalist.

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

[30] **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
20th Intl. Conference on Financial Cryptography and Data Security (FC), Barbados, Feb. 2016.

[31] **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
22nd ACM Conference on Computer and Communications Security (CCS), Denver, CO, Oct. 2015.
Acceptance rate: 19%, 128/659.
Best paper award.
Pwnie award for most innovative research.
Perfect review score.
CACM Research Highlight.

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

[33] **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
15th ACM Internet Measurement Conference (IMC), Tokyo, Japan, Oct. 2015.
Acceptance rate: 26%, 44/169.
IRTF Applied Networking Research Prize winner.

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

[35] **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
14th ACM Internet Measurement Conference (IMC), Vancouver, BC, Nov. 2014.
Acceptance rate: 23%, 43/188
Best paper award.
Honorable mention for Best dataset award.

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

[37] **Efficiently Auditing Multi-Level Elections**
Joshua A. Kroll, Edward W. Felten, and J. A. Halderman
6th International Conference on Electronic Voting (E-Vote), Bregenz, Austria, Oct. 2014.

[38] **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
23rd USENIX Security Symposium, San Diego, CA, Aug. 2014.
Acceptance rate: 19%, 67/350.

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

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

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

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

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

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

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

[46] **Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices**
Nadia Heninger, Zakir Durumeric, Eric Wustrow, and J. A. Halderman
21st USENIX Security Symposium, pages 205–220, Bellevue, WA, Aug. 2012.
Acceptance rate: 19%, 43/222.
Best paper award.
Named one of *Computing Reviews'* Notable Computing Books and Articles of 2012.
Test of Time award (2022).

[47] **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.

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

[49] **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, eds., *Passive and Active Measurement*, volume 6579 of *Lecture Notes in Computer Science*, pages 133–142. Springer, 2011.
Acceptance rate: 29%, 23/79.

[50] **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.

[51] **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
17th ACM Conference on Computer and Communications Security (CCS), Chicago, IL, Oct. 2010.
Acceptance rate: 17%, 55/320.
Highest ranked submission.

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

[53] **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
17th Network and Distributed System Security Symposium (NDSS). San Diego, CA, Feb. 2010.
Acceptance rate: 15%, 24/156.

[54] **Fingerprinting Blank Paper Using Commodity Scanners**
William Clarkson, Tim Weyrich, Adam Finkelstein, Nadia Heninger, J. A. Halderman, and Edward W. Felten
30th IEEE Symposium on Security and Privacy, pages 301–314, Oakland, CA, May 2009.
Acceptance rate: 10%, 26/254.

[55] **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
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.
CACM Research Highlight.

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

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

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

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

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

Book Chapters

[61] **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, Dec. 2016.

Journal Publications

[62] **Challenges in Cybersecurity: Lessons from Biological Defense Systems**
Edward Schrom, Ann Kinzig, Stephanie Forrest, Andrea L. Graham, Simon A. Levin, Carl T. Bergstromg, Carlos Castillo-Chavez, James P. Collins, Rob J. de Boeri, Adam Doupée, Roya Ensafi, Stuart Feldman, Bryan T. Grenfell, J. A. Halderman, Silvie Huijben, Carlo Maley, Melanie Mosesr, Alan S. Perelson, Charles Perrings, Joshua Plotkin, Jennifer Rexford, and Mohit Tiwari
Mathematical Biosciences, 362, 2023.

[63] **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
Communications of the ACM, 61(1):106–114, 2019.

[64] **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.

[65] **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

[66] **RemoteVote and SAFE Vote: Towards Usable End-to-End Verification for Vote-by-Mail**
Braden L. Crimmins, Marshall Rhea, and J. A. Halderman
7th Workshop on Advances in Secure Electronic Voting, May 2022.

[67] **Bernoulli Ballot-Polling: A Manifest Improvement for Risk-Limiting Audits**
Kellie Ottoboni, Matthew Bernhard, J. A. Halderman, Ronald L. Rivest, and Philip B. Stark
4th Workshop on Advances in Secure Electronic Voting, St. Kitts, Feb. 2019.

[68] **An ISP-Scale Deployment of TapDance**
Sergey Frolov, Fred Douglas, Will Scott, Allison McDonald, Benjamin VanderSloot, Rod Hynes, Adam Kruger, Michalis Kallitsis, David Robinson, Nikita Borisov, J. A. Halderman, and Eric Wustrow
7th USENIX Workshop on Free and Open Communications on the Internet (FOCI), Vancouver, BC, Aug. 2017.

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

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

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

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

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

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

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

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

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

[78] **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
2009 USENIX Electronic Voting Technology Workshop / Workshop on Trustworthy Elections (EVT/WOTE), Montreal, QC, Aug. 2009.

[79] **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 *USENIX Electronic Voting Technology Workshop (EVT)*, San Jose, CA, July 2008.

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

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

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

[83] **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., Oct. 2004.

[84] **Evaluating New Copy-Prevention Techniques for Audio CDs**
J. A. Halderman
ACM Workshop on Digital Rights Management, Nov. 2002. In Joan Feigenbaum, ed., *Digital Rights Management*, volume 2696 of *Lecture Notes in Computer Science*, pages 101–117.

Selected Other Publications

[85] **Improving the Security of United States Elections with Robust Optimization**
Braden Crimmins, J. A. Halderman, and Bradley Sturt
In submission, Aug. 2023.

[86] **Testimony in Opposition to Internet Voting in Michigan**
J. A. Halderman
Testimony to the Michigan House Committee on Elections regarding H.B. 4210, May 9, 2023.

[87] **Remembering Peter Eckersley**
J. A. Halderman
Remarks delivered at his memorial service, March 4, 2023

[88] **ICS Advisory: Vulnerabilities Affecting Dominion Voting Systems ImageCast X**
Findings credited to J. A. Halderman and Drew Springall
CISA/ICS-CERT (ICSA-22-154-01), June 3, 2022

[89] **Election Security Problems Still Must Be Addressed**
Susan Greenhalgh and J. A. Halderman
Newsweek, Sept. 27, 2021.

[90] **Security Analysis of Georgia's ImageCast X Ballot Marking Devices**
J. A. Halderman and Drew Springall
Expert report submitted on behalf of plaintiffs Donna Curling, et al. in *Curling v. Raffensperger*, Civil Action No. 1:17-CV-2989-AT, U.S. District Court for the Northern District of Georgia, Atlanta Division, July 1, 2021

[91] **Analysis of the Antrim County, Michigan November 2020 Election Incident**
J. A. Halderman
Expert report prepared for the Michigan Secretary of State and Department of Attorney General, Mar. 26, 2021.

[92] **Elections Should be Grounded in Evidence, Not Blind Trust**
Philip B. Stark, Edward Perez, and J. A. Halderman
Barrons, Jan. 4, 2021.

[93] **Scientists say no credible evidence of computer fraud in the 2020 election outcome, but policymakers must work with experts to improve confidence**
Matt Blaze, J. A. Halderman, Joseph Lorenzo Hall, Harri Hursti, *et al.*
Public statement from election security experts, Nov. 16, 2020.

[94] **Michigan Election Security Advisory Commission Report and Recommendations**
J. A. Halderman *et al.*
Report prepared for the State of Michigan, Oct. 2020.

[95] **Internet Voting Is Happening Now—And it could destroy our elections**
Rachel Goodman and J. A. Halderman
Slate, Jan. 15, 2020.

[96] **Beyond Acceptable Advertisement: Better Understanding Blocking Extensions**
Benjamin VanderSloot, Steven Sprecher, and J. A. Halderman
Technical report, Computer Science and Engineering Division, University of Michigan, Ann Arbor, MI, May 2019.

[97] **U.S. House Testimony Regarding Federal Funding for Election Cybersecurity**
J. A. Halderman
Testimony before the U.S. House Appropriations Subcommittee on Financial Service and General Government, "Election Security: Ensuring the Integrity of U.S. Election Systems," Feb. 27, 2019.

[98] **I Hacked an Election. So Can the Russians.**
J. A. Halderman
Video op/ed in collaboration with *The New York Times*, Apr. 5, 2018.

[99] **U.S. Senate Testimony Regarding Russian Interference in the 2016 U.S. Elections**
J. A. Halderman
Testimony before the U.S. Senate Select Committee on Intelligence, June 21, 2017.

[100] **Here's How to Keep Russian Hackers from Attacking the 2018 Elections**
J. A. Halderman and J. Talbot-Zorn
The Washington Post, June 21, 2017.

[101] **Want to Know if the Election was Hacked? Look at the Ballots**
J. A. Halderman
Posted on Medium, Nov. 23, 2016. (Read by over a million people.)

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

[103] **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.

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

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

[106] **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.

[107] **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, Mar. 2008.

[108] **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.

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

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

Selected Legal and Regulatory Filings

[111] **Voter Privacy and VVSG 2.0**
Braden Crimmins, Dhanya Narayanan, J. A. Halderman, and Drew Springall
Public comments in response to U.S. EAC VVSG 2.0 annual review, June 6, 2023.

[112] **Request for DMCA Exemption: Security Research**
Petition to the U.S. Copyright Office of J. Alex Halderman
represented by Cara Groseth, Lucas Knudsen, Wilson Scarbeary, and Blake Reid
Eighth Triennial Section 1201 Proceeding, 2020–2021
(*Outcome:* Requested exemption granted in part.)

[113] **Request for DMCA Exemption: Security Research**
Petition to the U.S. Copyright Office of Edward W. Felten and J. Alex Halderman
represented by Elizabeth Field, Justin Manusov, Brett Hildebrand, Alex Kimata, and Blake Reid
Seventh Triennial Section 1201 Proceeding, 2017–2018
(*Outcome:* Requested exemption granted in part.)

[114] **Request for DMCA Exemption: Security Research**
Petition to the Librarian of Congress of Steve Bellovin, Matt Blaze, Edward Felten, J. Alex Halderman, and Nadia Heninger, represented by Andrea Matwyshyn
Sixth Triennial Section 1201 Proceedings, 2014–2015
(*Outcome:* Requested exemption granted in part.)

[115] **Request for DMCA Exemption: Games with Insecure DRM and Insecure DRM Generally**
Petition to the Librarian of Congress of J. Alex Halderman
represented by Blake Reid, Paul K. Ohm, Harry A. Surden, and J. Brad Bernthal
Fourth Triennial Section 1201 Proceedings, 2008–2010
(*Outcome:* Requested exemption granted in part.)

[116] **Request for DMCA Exemption for Audio CDs with Insecure DRM**
Petition to the Librarian of Congress of Edward Felten and J. Alex Halderman
represented by Deirdre Mulligan and Aaron Perzanowski
Third Triennial Section 1201 Proceedings, 2005–2006
(*Outcome:* Requested exemption granted in part.)

Patents

[117] **Scanning Engine with Multiple Perspectives**
Jeff Cody, David Adrian, J. A. Halderman, and Paul A. Parkanzky
Patent pending.

[118] **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.

[119] **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 Talks and Keynotes

- **Election Security in the Disinformation Age**
  Distinguished lecture, Harvard, Oct. 13, 2022.
- **Election Cybersecurity Progress Report: Will the U.S. be Ready for 2020?**
  35c3, Leipzig, Dec. 27, 2018.
- **Cyberattacks on Election Infrastructure**
  Keynote speaker, DIMVA 2018, Paris, June 29, 2018.

– **Recount 2016: A Security Audit of the U.S. Presidential Election**
Keynote speaker, NDSS, Feb. 27, 2017.

– **Recount 2016: An Uninvited Security Audit of the U.S. Presidential Election**
33c3, Hamburg, Dec. 28, 2016.

– **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, Sept. 9, 2016.

– **Internet Voting: What Could Go Wrong?**
Invited speaker, USENIX Enigma, San Francisco, Jan. 27, 2016.

– **Logjam: Diffie-Hellman, Discrete Logs, the NSA, and You**
32c3, Hamburg, Dec. 29, 2015.

– **The Network Inside Out: New Vantage Points for Internet Security**
Invited speaker, China Internet Security Conference (ISC), Beijing, Sept. 30, 2015.

– **The Network Inside Out: New Vantage Points for Internet Security**
Keynote speaker, ESCAR USA (Embedded Security in Cars), Ypsilanti, MI, May 27, 2015.

– **Security Analysis of the Estonian Internet Voting System**
31c3, Hamburg, Dec. 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, Nov. 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, Sept. 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, Dec. 28, 2013.

– **Verifiably Insecure: Perils and Prospects of Electronic Voting**
Invited speaker, Computer Aided Verification (CAV) 2012, Berkeley, July 13, 2012.

– **Deport on Arrival: Adventures in Technology, Politics, and Power**
Invited speaker, 20th USENIX Security Symposium, San Francisco, Aug. 11, 2011.

– **Electronic Voting: Danger and Opportunity**
Keynote speaker, ShmooCon 2008, Washington, D.C., Feb. 15, 2008.

Selected Testimony and Legislative Briefings

– **Testimony in Opposition to Internet Voting in Michigan**
Michigan House Committee on Elections, May 9, 2023.

– **Election Technology: Achieving Security and Trust**
Louisiana Voting System Commission, Baton Rouge, Dec. 15, 2021.

– **Cybersecurity and U.S. Election Infrastructure**
Democratic Senate Caucus Policy Lunch, U.S. Capitol, Sept. 26, 2019.

– **U.S. House Testimony Regarding Federal Funding for Election Cybersecurity**
Testimony before the U.S. House Appropriations Subcommittee on Financial Service and General Government, Feb. 27, 2019.

– **Congressional Briefing on Election Cybersecurity**
Hosted by Rep. Mike Quigley and Rep. John Katko. Sep. 26, 2018.

– **Congressional Briefing on Election Cybersecurity**
Co-panelists: Harri Hursti, Tony Schaffer, Liz Howard, Shantiel Soeder, Dan Savickas; moderator: Trey Greyson. July 10, 2018.

– **Congressional Briefing: Hacked Voting Machine Demonstration**
Hosted by Senators Kamala Harris and James Lankford. Apr. 12, 2018.

– **Congressional Briefing: Strengthening Election Cybersecurity**
Co-panelists: Nicole Austin-Hillery, Tony Shaffer, Bruce Fein, Susan Greenhalgh, Shane Schoeller. Oct. 19, 2017.

– **Congressional Briefing: Free, Automated, and Open Web Encryption**
Hosted by Congressional Cybersecurity Caucus. Aug. 8, 2017.

– **U.S. Senate Testimony Regarding Russian Interference in the 2016 U.S. Elections**
Testimony before the U.S. Senate Select Committee on Intelligence, June 21, 2017.

– **Congressional Briefing: Strengthening Election Cybersecurity**
Co-panelists: James Woolsey, Tony Shaffer, Lawrence Norden, Susan Greenhalgh, James Scott; moderator: Karen Greenberg. May 15, 2017.

– **Testimony on Vulnerabilities in the Washington, D.C. Internet Voting System**
D.C. Board of Elections and Ethics Hearing re Readiness for the Nov. 2010 General Election, Oct. 8, 2010.

Selected Talks

– **Robust Logic & Accuracy Testing (RLAT).** State Certification Testing of Election Systems National Conference (SCTESNC), June 13, 2023.

– **DVSOrder and Election CVD Issues.** EVN Conference, Washington, D.C., Mar. 17, 2023; State Certification Testing of Election Systems National Conference (SCTESNC), June 12, 2023.

– **Remembering Peter Eckersley.** Internet Archive, San Francisco, Mar. 4, 2023.

– **Election Security in the Age of Disinformation**
Invited speaker, IT University Copenhagen, Sep. 23, 2022; Keynote speaker, Merit Member Conference, Dearborn, MI, May 10, 2022; Nathan Krasnopoler Memorial Lecture, Johns Hopkins, Oct. 26, 2021; Invited speaker, Doug Jones Festschrift, U. Iowa, Oct. 8, 2021; Invited speaker, Washtenaw County League of Women Voters, Apr. 14, 2021.

– **Securing Democracy's Critical Infrastructure.** UIUC, Mar. 24, 2022.

– **Running Refraction Networking at ISP Scale.** Merit Research Summit, Nov. 16, 2021.

– **Cybersecurity and U.S. Elections**
Invited speaker, Microsoft Election Law Security Roundtable, Sept. 25, 2020; Invited speaker, U-M Florida Seminars, Feb. 4, 2020; Invited speaker, CyberSec & AI Prague, Oct. 25, 2019; Invited speaker, Indiana University Research, Feb. 7, 2019; Invited speaker, Arizona State, Jan. 16, 2019; Invited speaker, University of San Diego, Nov. 16, 2018; Invited speaker, UMass Amherst, Oct. 31, 2018; Invited speaker, U-M Alumni Association, Oct. 18, 2018; Invited speaker, MIT EmTech, Aug. 13, 2018; Invited speaker, DEFCON Voting Village, Aug. 10, 2018; Invited speaker, U.C. Irvine Election Security Summit, Irvine, Mar. 13, 2018; Invited speaker, Global Election Summit, San Francisco, May 17, 2017; Invited speaker, Wolverine Caucus Forum, Lansing, Feb. 21, 2017; Invited speaker, CSE Science on Screen at Michigan Theater, Ann Arbor, Jan. 25, 2017.
– **Let's Encrypt: An Automated Certificate Authority to Encrypt the Entire Web**
ACM CCS, Nov. 19, 2019; Invited speaker, OWASP Copenhagen, Nov. 25, 2019;
Invited talk, Summer school on real-world crypto and privacy, Croatia, June 9, 2017;
Invited talk, Cubaconf, Havana, Apr. 25, 2016.
– **The Security Impact of HTTPS Interception**. Invited talk, GOTO Copenhagen, Oct. 2, 2017.
– **Elections and Cybersecurity: What Could Go Wrong?**
Keynote speaker, Merit Security Summit, Ypsilanti, MI, Nov. 7, 2016.
– **The Legacy of Export-grade Cryptography in the 21st Century**
Invited talk, Summer school on real-world crypto and privacy, Croatia, June 9, 2016.
– **Logjam: Diffie-Hellman, Discrete Logs, the NSA, and You**
Invited talk, NYU Tandon School of Engineering, Apr. 8, 2016; Invited talk, UIUC Science of Security seminar, February 9, 2016.
– **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, Apr. 8, 2015; Invited talk, Princeton University, Oct. 15, 2014; Invited talk, U.T. Austin, Mar. 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, Sept. 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, Sept. 3, 2015; Invited talk, IT Univ. of Copenhagen, Sept. 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, Sept. 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., Aug. 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, Mar. 26, 2015.

– **E-Voting: Danger and Opportunity**
Invited talk, University of Chile, Santiago, Apr. 7, 2015; Keynote speaker, 14th Brazilian Symposium on Information Security and Computer Systems (SBSeg), Belo Horizonte, Brazil, Nov. 3, 2014; Crypto seminar, University of Tartu, Estonia, Oct. 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.

– **Fast Internet-wide Scanning and its Security Applications**. Think Conference, Nov. 9, 2013.

– **Internet Censorship in Iran: A First Look**
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

– **Challenging Security Assumptions**
Three-part tutorial. 2nd TCE Summer School on Computer Security, Technion, Haifa, July 2013.

– **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; TRUST Seminar, U.C., Berkeley, Dec. 1, 2011; Think Conference, Nov. 5, 2011; 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; 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; Invited speaker, IT University of Copenhagen, May 11, 2012.

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

– **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].
– ~~**Tutorial speaker/organizer: Security Issues in Electronic Voting,** ICISS (Gandhinagar, India), Dec. 15, 2010~~ [canceled under threat of deportation].
– **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.
– **AACS, BD+, and the Limits of DRM**
DIMACS/DyDAn Workshop on Internet Privacy, Rutgers University, Sept. 18, 2008.

– **Security Through the Lens of Failure**. UCSD, Apr. 2, 2008; U. Michigan, Mar. 25, 2008,

– **Harvesting Verifiable Challenges from Oblivious Online Sources**. ACM Conference on Computer and Communications Security (Washington, D.C.), Oct. 31, 2007.

– **Dangerous Tunes: Lessons from the Sony CD DRM Episode**
SRI International (Palo Alto, CA), July 14, 2006; University of Waterloo (Canada), Mar. 9, 2006.

– **A Convenient Method for Securely Managing Passwords**
International World Wide Web Conference (Chiba, Japan), May 12, 2005.

– **Privacy Management for Portable Recording Devices**
ACM Workshop on Privacy in the Electronic Society (Washington, D.C.), Oct. 18, 2004.

– **Evaluating New Copy-Prevention Techniques for Audio CDs**
ACM Workshop on Digital Rights Management (Washington, D.C.), Nov. 18, 2002.

Selected Panels

– Fireside chat: **Internet Voting.** Moderator: Charles Clancy. (Opposite Bradley Tusk.) Exploring Secure and Accessible Elections for the Next Generation workshop, MITRE, Dec. 9, 2021.

– Panelist: **Cybersecurity.** Co-panelists: Chris Inglis and Ellen Nakashima; hosts: Javed Ali and Carl Landwehr. University of Michigan, Oct. 11, 2021.

– Panelist: **President's Awards for Public Engagement.** Co-panelists: Marc A. Zimmerman, Emily Toth Martin, Margaret Dewar; moderator: Mark S. Schlissel. U. Michigan, Mar. 22, 2021.

– Panelist: **The 2020 Election: Remote Voting, Disinformation, and Audit.** Co-panelists: Ben Adida and Vanessa Teague; moderator: Avi Rubin. USENIX Security Symposium, Aug. 12, 2020.

– Panelist: **Internet Freedom in the Domestic Arena.** Co-panelists: Nadine Strossen, Milton Mueller, and Roger Dingledine; moderator: Anita Nikolich. 10th USENIX Workshop on Free and Open Communications on the Internet (FOCI), via Zoom, Aug. 11, 2020.

– Panelist: **Internet Voting.** Co-panelists: Thomas Chanussot, Carsten Schürmann, Virginia Atkinson, Robert Krimmer, and Ronan McDermott; moderator: Beata Martin-Rozumilowicz. International Foundation for Electoral Systems (IFES), via Zoom, June 16, 2020.

– Panelist: **How Adversaries Can Erode Public Trust in Democratic Institutions.** Co-panelists: Hany Farid, Ron Rivest, Suzanne Spaulding; moderator: Hon. James E. Boasberg. D.C. Circuit Judicial Conference, Cambridge, Maryland, June 26, 2019.

– Panelist: **Alumni-Faculty Forum: Cold War 2.0: Russia, Cybersecurity and Hacking.** Co-panelists: Walter Slocombe, Alexander Southwell, Ishani Sud; moderator: Jonathan Mayer. Princeton University reunions, June 1, 2018.

– Panelist: **"Critical Infrastructure" Designation for Election Operations: Risks, Mitigations, & Import for 2018**. Election Verification Network Conference, Miami, Mar. 16, 2018.

– Panelist: **The Technology of Voting: Risks & Opportunities.** U.C. Irvine Cybersecurity and Policy Research Institute, Mar. 13, 2018.

– Panelist: **Election Law Conflicts and the Vulnerability of our Election Systems.** Co-panelists: Stephen Berzon, Holly Lake, Harvey Saferstein. Ninth Circuit Judicial Conf., July 18, 2017.

– Moderator: **Apple & the FBI: Encryption, Security, and Civil Liberties.** Panelists: Nate Cardozo and Barbara McQuade. U-M Dissonance Speaker Series, Apr. 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 (Vote-ID), Bern, Switzerland, Sept. 4, 2015.
– Moderator: **Panel on Research Ethics.** USENIX Security, Washington, D.C., Aug. 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: **Work/Life Balance.** Co-panelists: Cynthia Sturton and Thorsten Holz; moderator: Kevin Fu. USENIX Security Symposium, Aug. 21, 2014.
– Panelist: **Measuring Privacy**. Big Privacy symposium, Princeton University CITP, Apr. 26, 2013 [moderator: Ed Felten].
– Panelist: **The Current State of E-Voting**. E-Voting: Risk and Opportunity symposium, Princeton University CITP, Nov. 1, 2012 [moderator: Steve Schultze].
– 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, 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 [mod.: 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.
– Panelist: **Cyber Security / Election Technology**. Overseas Voting Foundation Summit, Feb. 10, 2011 [moderator: Candice Hoke].
– 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].
– Panelist: **Tradeoffs in Electronic E2E Voting Systems**. NIST End-to-End Voting Systems Workshop (Washington, D.C.), Oct. 14, 2009.
– Panelist: **Beyond the iPhone: What Will Technology look like in 2018?** Princeton University reunions, May 30, 2008.

Advising and Mentoring

PhD Students

– Braden Crimmins (Ph.D. expected 2028)

– Allison McDonald (Ph.D. 2022; Facebook Emerging Scholar → tenure-track faculty, Boston U.)
– Matthew Bernhard (Ph.D. 2020 → VotingWorks)
– Benjamin VanderSloot (Ph.D. 2020 → tenure-track CS faculty, Detroit Mercy → Mozilla)
– David Adrian (Ph.D. 2019 → cofounder, Censys → Chrome security, Google)
– Andrew Springall (Ph.D. 2018 → Google → tenure-track CS faculty, Auburn)
– Zakir Durumeric (Ph.D. 2017; Google Ph.D. Fellow → tenure-track CS faculty, Stanford)
– Eric Wustrow (Ph.D. 2016; NSF Graduate Fellow → tenure-track CS faculty, U. Colorado)
– James Kasten (Ph.D. 2015 → Google)

Master's Students

– Braden Crimmins (M.S. 2023)
– Jack Skupski (M.S. 2022)
– Max Froehlich (M.S. 2022)
– Steve Sprecher (M.S. 2019 → Ph.D. student, Northeastern)
– Rose Howell (M.S. 2018 → AdblockPlus)
– Travis Finkenauer (M.S. 2016 → Juniper Networks)
– Scott Wolchok (M.S. 2011 → Facebook)

Post Docs

– Will Scott (2017–18)
– Colleen Swanson (2014–15)

Undergraduate Independent Work

– 2023: Anisha Aggarwal, Isabella Allada, Nakul Bajaj, Mingye Chen, Erik Chi, Jolie Kaplan, Noah Kuperberg, Anthony Li, James Maddock, Dhanya Narayanan, Andrew Plotner, Wen Plotnick, Sachin Rammoorthy, Marshall Stone, Josiah Walker, Frederick Wang, Sydney Zhong
– 2022: Nakul Bajaj, Mingye Chen, Braden Crimmins, John Jepko, Noah Kuperberg, Dhanya Narayanan, Wen Plotnick, Sachin Rammoorthy, Josiah Walker, Frederick Wang, Yuxuan Xia
– 2021: Anna Ablove, Nakul Bajaj, Sameer Barretto, William Chown, Braden Crimmins, Lukas Hazen-Bushbaker, Rebecca Hirsh, Carson Hoffman, David Meyer, Siddharth Pittie, Aditya Soni, Atreya Tata, Josiah Walker, Kevin Zhang
– 2020: Nakul Bajaj, Ryan Feng, Carson Hoffman, Jensen Hwa, Yuxuan Luo, Jacob Shreve, Atreya Tata
– 2019: Nakul Bajaj, Scott Bays, Kevin Chang, Jensen Hwa, Kartikeya Kandula, Nicholas Matton, Henry Meng, Ellen Tsao, Hassaan Ali Watoo, Jeremy Wink
– 2018: Jensen Hwa, Henry Meng, Armando Ruvalcaba
– 2017: Gabrielle Beck, Alex Holland
– 2016: Ben Burgess, Noah Duchan, Mayank Patke
– 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'Neill
– 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

Doctoral Committees

- Ramakrishnan Sundara Raman (C.S. Ph.D. expected 2024)
- Reethika Ramesh (C.S. Ph.D. expected 2023)
- Andrew Kwong (C.S. Ph.D. 2023. Michigan)
- Mert Pesé (C.S. Ph.D. 2022, Michigan)
- Duc Bui (C.S. Ph.D. 2022, Michigan)
- Allison McDonald (C.S. Ph.D. 2022, Michigan; co-chair w/ Florian Schaub)
- Chun-Yu Chen (C.S. Ph.D. 2022, Michigan)
- Matthew Bernhard (C.S. Ph.D. 2020, Michigan; chair)
- Benjamin VanderSloot (C.S. Ph.D. 2020, Michigan; chair)
- David Adrian (C.S. Ph.D. 2019, Michigan; chair)
- Arunkumaar Ganesan (C.S. Ph.D. 2019)
- Andrew Springall (C.S. Ph.D. 2018, Michigan; chair)
- Kyong Tak Cho (C.S. Ph.D. 2018, Michigan)
- Armin Sarabi (E.E. Ph.D. 2018, Michigan)
- Zakir Durumeric (C.S. Ph.D. 2017, Michigan; chair)
- Armin Sarabi (E.E. Ph.D. 2017, Michigan)
- Eric Crockett (C.S. Ph.D 2017, Georgia Tech)
- Kassem Fawaz (C.S. Ph.D. 2017, Michigan)
- Amir Rahmati (C.S. Ph.D. 2017, Michigan)
- Earlence Fernandez (C.S. Ph.D. 2017, Michigan)
- Huan Feng (C.S. Ph.D. 2016, Michigan)
- Jakub Czyz (C.S. Ph.D. 2016, Michigan)
- Denis Bueno (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)

Teaching

- **Introduction to Computer Security**, EECS 388, University of Michigan
  Terms: Fall 2023, Winter 2023, Fall 2022, Fall 2021, Winter 2020, Fall 2019, Winter 2019, Winter 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 >500 students/year. An accessible intro, teaches the security mindset and practical skills for building and analyzing security-critical systems.
- **Election Cybersecurity**, EECS 498.5/598.16, University of Michigan
  Term: Fall 2020, Fall 2018
  An in-depth examination of the past, present, and future of elections, informed by perspectives from computer security, tech policy, human factors, and more.

– **Surveillance Law and Technology** (with Margo Schlanger), EECS 598.7 / LAW 441.1, University of Michigan, Fall 2019
  Interdisciplinary seminar bringing together students and faculty from computer science and law to address current controversies in surveillance and privacy.
– **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)
  Created massive, open online course that explores the security risks—and future potential—of electronic voting and Internet voting technologies. Over 45,000 students to date, including many election officials.

Professional Service

Program Committees

– 2021 USENIX Security Symposium (Sec '21)
– 2019 ACM Internet Measurement Conference (IMC '19)
– 2017 ACM Conference on Computer and Communications Security (CCS '17)
– 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)

Department and University Service

– Lab Director, CSE Systems Lab (2018–present)
– Organizing Committee, Dissonance tech/policy event series (2016–present)
– Faculty Advisor, Michigan Hackers student group (2012–present)
– CSE Executive Committee (2021–2023)
– CSE Strategic Action Leadership Team (2021–2022)
– CSE Mission and Values Team (2021–2022)
– CSE Faculty Search Committee (2018–21)
– CSE Graduate Affairs Committee (2014–17)
– CSE Undergraduate Program Advising (CS/ENG) (2011–17)
– U-M Faculty Senate, Rules Committee of the Senate Assembly (2011–12)
– CSE Graduate Admissions Committee (2010–11)
– CSE Graduate Committee (2009–10)

Boards

– Board of Directors of 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 (2012–14)

Government

– Michigan Secretary of State's Election Security Advisory Commission (co-chair, 2019–present)

Broader Impact of Selected Projects

– **Analysis of the Antrim County November 2020 Election Incident** (2021)
Investigated major errors in county's election-night results, at the request of the Michigan Secretary of State and Attorney General, to counter misinformation and draw lessons for election administration. Detailed forensic analysis uncovered a chain of human error and procedural and technical shortcomings.

– **Security and Verifiability of Ballot Marking Devices** (2020)
In a mock election using hacked BMDs that secretly changed printed selections, our test voters caught only 6.6% of errors. Several states adopted changes we proposed to improve verification, but even these are likely insufficient to secure close races in states that have recently switched to BMDs for all voters.

– **Refraction Networking Enters Large-Scale Production** (2019)
Led a large multi-institutional effort to deploy advanced ISP-based censorship circumvention technology. Following years of research and development supported by the U.S. Department of State, our service is now operating in full production and available to over 1 million users in heavily censored regions.

– **Michigan Election Security Advisory Commission** (2019)
I serve as co-chair of the State of Michigan's Election Security Advisory Commission, appointed by Secretary of State Jocelyn Benson. This panel of local officials and national experts has held hearings around the state and recommend specific reforms and strategies, many of which have been implemented.

– **Censys: Attack Surface Management Company** (2018)
Co-founded Censys, now a 75-person, Ann Arbor-based cloud attack surface management company, which commercialized technology from our Internet-wide scanning research. I served as Chief Scientist until the company completed its Series A fundraising in 2020, backed by Google Ventures and Decibel.

– **Congressional Testimony on Election Cybersecurity** (2017, 2019)
Testified re election security threats and defenses to the U.S. Senate Select Committee on Intelligence and the House Appropriations Subcommittee on Financial Service and General Government. My testimony was extensively cited and helped secure $830 million in new federal funding for security improvements.

– **First International Study of the Cuban Street Network** (2017)
Cuba's SNET is a community-built IP network that reaches 10,0000s of users despite being isolated from the Internet. I collaborated with SNET operators to document the topology, demographics, and usage, draw lessons, and highlight the network's successes to the global technical community for the first time.

– **2016 U.S. Presidential Election Recounts** (2016)
Helped orchestrate election recount efforts in Michigan, Wisconsin, and Pennsylvania in an attempt to detect or deter potential outcome-alerting cyberattacks. Legal and political roadblocks prevented completion of full manual counts; the partial recounts that did occur showed no evidence of tampering.

– **Let's Encrypt: A Certificate Authority to Encrypt the Entire Web** (2016)
Co-founded HTTPS certificate authority to provide free, automatically validated certificates for all domains. Developed in partnership with EFF and Mozilla, Let's Encrypt helps secure hundreds-of-millions of sites and has issued more than half of all browser-trusted certificates worldwide.

– **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 nation-state attackers can break 1024-bit Diffie-Hellman, providing the first parsimonious explanation for how NSA can decrypt 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 nation-state 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 distributions and has been applied in nearly 1000 research studies.

– **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 new approach to circumventing Internet censorship, based on placing anticensorship technology into core network infrastructure outside the censoring country. Prototype attracted over 100,000 users, mainly in China. Subsequent development by my group and others led to Refraction Networking.

– **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, which led to the system being scrapped. Widespread media coverage alerted the public to Internet voting security risks.

– **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 Green Dam to be installed on all 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 motivated 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, 2010, 2015, 2018, 2021)
Worked with legal teams to successfully petition the U.S. Copyright Office to create and expand security research exemptions to the Digital Millennium Copyright Act. The resulting exemptions are significant steps towards addressing the long-standing chilling effects of DMCA Section 1201 for security research.

– **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 annual interdisciplinary art competition at Princeton that showcases images and videos produced in the course of scientific research and creative works that incorporate tools and ideas from science. Princeton's competition continues to this day, and the concept has spread to other universities.