Matthew Bernhard

Ph.D. Candidate,
Computer Science and Engineering
University of Michigan

2260 Hayward Street
Ann Arbor, MI 48109 USA
matber@umich.edu

mbernhard.com

June 3, 2019

Research Overview

My research focuses on areas where the security and privacy implications of sophisticated systems impacts users in the real world. My interests include election security, usability, human-computer interaction, censorship measurement and resistance, Internet measurement, cryptography, statistics, and systems security. I'm also interested in the intersection of computer science, psychology, politics, and policy.

Education

- Ph.D in Computer Science, University of Michigan, Expected Spring 2021
  Advisor: J. Alex Halderman
- M.S. in Computer Science, University of Michigan, Summer 2018
- B.A. in Computer Science, Rice University, Spring 2015
  Advisor: Dan S. Wallach

Refereed Conference Publications

[1] **On the Usability of HTTPS Deployment**
Matthew Bernhard, Jonathan Sharman, Claudia Ziegler Acemyan, Philip Kortum, Dan S. Wallach, and J. A. Halderman
In *Proceedings of the ACM Conference on Human Factors on Computing Systems* **(CHI'19)** , May 2019.

[2] **403 Forbidden: A Global View of CDN Geoblocking**
Allison McDonald, Matthew Bernhard, Luke Valenta, Benjamin VanderSloot, Will Scott, Nick Sullivan, J. A. Halderman, Roya Ensafi
In *Proceedings of the ACM Internet Measurement Conference* **(IMC'18)** , November 2018.

[3] **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
In *Proceedings of the 2nd International Joint Conference on Electronic Voting* **(E-Vote-ID'17)** , October 2017.

[4] **Understanding the Mirai Botnet**
Manos Antonakakis, Tim April, Michael Bailey, Matthew 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
In *Proceedings of the 26th USENIX Security Symposium*
(USENIX'17) , August 2017.

[5] **Implementing Attestable Kiosks**
Matthew Bernhard, J. A. Halderman, and Gabe Stocco
In *Proceedings of the 14th IEEE Conference on Privacy, Security, and Trust*
(PST'16) , December 2016.

[6] **Towards a Complete View of the Certificate Ecosystem**
Benjamin VanderSloot, Johanna Amann, Matthew Bernhard, Zakir Durumeric, Michael Bailey, J. A. Halderman
In *Proceedings of the ACM Internet Measurement Conference*
(IMC'16) , November 2016.

Refereed Workshop Publications

[7] **Bernoulli Ballot-Polling: A Manifest Improvement for Risk-Limiting Audits**
Kellie Ottoboni, Matthew Bernhard, J. A. Halderman, Ronald L. Rivest, and Philip B. Stark
In *Proceedings of the 4th Annual Workshop on Advances in Secure Electronic Voting*
(Voting'19) , February 2019.

[8] **Voting Technologies, Recount Methods and Votes in Wisconsin and Michigan in 2016**
Walter R. Mebane, Jr., Matthew Bernhard
In *Proceedings of the 3rd Annual Workshop on Advances in Secure Electronic Voting*
(Voting'18) , February 2019.

Selected Other Publications

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

Speaking

Major Invited Talks and Keynotes

- **U.S. Civil Rights Commission testimony on voter registration security**
  Michigan Advisory Committee to the U.S. Commission on Civil Rights, Detroit, Michigan, April 2019.
- **Panel: Next Generation Voting Systems (moderator)**
  Election Verification Network Conference, Washington, D.C., March 2019.

– **Panel: Usability and Voter Verification (moderator)**
Election Verification Network Conference, Washington, D.C., March 2019.

– **A Crash Course on Election Security**
2018 DEF CON Voting Village, Las Vegas, Nevada, August 2018.

– **Panel: Do We Want a Recount or Not?**
Election Verification Network Conference, Washington, D.C., March 2017.

– **Recount 2016: An Uninvited Security Audit of the U.S. Presidential Election**
2017 RoadSec, São Paulo, Brazil, November 2017.

– **Recount 2016: An Uninvited Security Audit of the U.S. Presidential Election**
33rd Chaos Communications Congress, Hamburg, Germany, December 2016.

Selected Talks

– **Cybersecurity and U.S. Elections**
Invited speaker, RoadSec Pro, São Paulo, Brazil, November 2017; Invited speaker, Workshop on Electoral Technologies, Brasilia, Brazil, June 2017;

– **Internet Pinball: The Security and Privacy Impact of Redirects**
Mozilla Security Research Summit, San Francisco, California, May 2019.

– **Election Security and You**
Midwest Security Workshop, Chicago, Illinois, April 2019.

– **Coercion-resistant, Receipt-free, and Paperless Voting**
Rump session at Financial Cryptography and Data Security 2019, St. Kitts, February 2019.

– **403 Forbidden: A Global View of Geoblocking**
Rump session, 9th USENIX Workshop on Free and Open Communications on the Internet (FOCI'18), Baltimore, Maryland, August 2018.

– **A Constitutional Argument Against Burr-Feinstein**
Rump session, 25th USENIX Security Symposium (USENIX'16), Austin, Texas, August 2017.

Advising and Mentoring

Undergraduate Independent Work

– 2019: Henry Meng, Jensen Hwa, Thea Lau, Chand Rajendra-Nicolucci, Antonio Atkinson, Jeremy Wink, Kartikey Kandula

Teaching

– **Graduate Student Instructor, Introduction to Computer Security** *(Winter 2018)*
EECS 388, University of Michigan
Led discussion section, wrote and graded assignments, and lectured.

– **Graduate Student Instructor, Election Cybersecurity** *(Fall 2018)*
EECS 498, University of Michigan
Assisted with design and teaching of an undergraduate research course into election security. Lectured, wrote homework assignments, and oversaw ten undergraduate independent research projects.
– **Course Operations Liaison, Securing Digital Democracy** *(2014–2018)*
Coursera (MOOC), University of Michigan
Assisted with content maintenance and day-to-day course operations for a massive, open online course about electronic voting and Internet voting technologies.
– **Teaching Assistant, Fundamentals of Parallel Programming** *(Spring 2015)*
COMP 322, Rice University
Shaped curriculum and led lab discussions for a introductory course on parallel programming featuring Java parallelism and Apache Spark
– **Teaching Assistant, Introduction to Program Design** *(Fall 2014)*
COMP 215, Rice University
Led lab discussions and wrote and reviewed assignments and exams for an introductory course on Java and Object Oriented Programming

Professional Service

Program Committee

– **Program co-chair**, 6th Workshop on Advances in Secure Electronic Voting (Voting'21)
– **Program co-chair**, 5th Workshop on Advances in Secure Electronic Voting (Voting'20)

External Reviewer

– USENIX Security Symposium (USENIX'19)
– ACM Internet Measurement Conference (IMC'18)
– ACM Conference on Computer and Communications Security (CCS'18)
– International Symposium on Research in Attacks, Intrusions, and Defenses (RAID'18)
– ACM Conference on Computer and Communications Security (CCS'17)
– Network and Distributed System Security Symposium (NDSS'17)
– IEEE Conference on Privacy, Security, and Trust (PST'16)

Broader Impact of Selected Projects

– **Implementing Better Election Security** (2018–2019)
Currently working with the State of Michigan and municipalities across the state to pilot risk-limiting audits to help secure Michigan's elections. Developed software that interfaces with voting technology to enable ballot comparison audits.
– **Fighting Weak IoT Security** (2017)
Applied machine learning techniques to Internet measurement data to identify make and model of consumer devices that were infected by the Mirai botnet. Data has been used in ongoing legal proceedings by the Federal Trade Commission to encourage U.S. manufacturers to improve the default security of their devices.

– **2016 U.S. Presidential Election Recounts** (2016)
Supported efforts to detect vote manipulation in the 2016 election in Michigan, Wisconsin, and Pennsylvania. While progress was hindered and in places entirely halted due to political and legal reasons, what little evidence htat was generated did not show that the 2016 Presidential election was fraudulent.

Professional Experience

– **Data Science Consultant for Verified Voting** (2018–present)
Collecting and interpreting data on currently certified voting equipment in the United States to empower municipalities to make intelligent purchasing decisions. Focus on the cyber security impacts of voting technology.

– **Expert Witness** (2018–present)
Served as an expert witness in several lawsuits opposing the use of direct-recording electronic voting machines. *Curling v. Kemp*, *CGG v. Crittenden*, *Shelby Advocates for Valid Elections et al. v. Hargett et al.*

– **Cryptography Intern, Cloudflare** (2017)
Developed Certificate Transparency monitoring features. Also built an SSL detector to determine what SSL settings customer sites can support, under the advising of Nick Sullivan.

– **Microsoft Research Intern** (2015)
Explored applications of trusted platform modules (TPMs) in voting through interfaces provided by Windows 10 under the advising of Josh Benaloh.