Matthew Bernhard

Research Engineer, *VotingWorks*

October 9, 2022

314 S Higby St
Jackson, MI 49203 USA
umbernhard@gmail.com

mbernhard.com

Overview

My work focuses on making security theory a reality. The most common the barriers to implementing better security are a lack of tooling, training, and resources. My goal is to build security systems and products that are easy to use, provide substantial protection, and make users *feel* secure. Election systems in particular have proven to be a crucible for overcoming barriers and designing systems that satisfy substantial constraints while still providing meaningful security and intuitive user experiences.

Education

- Ph.D in Computer Science, University of Michigan, Summer 2020
  Election Security is Harder Than You Think
  Advisor: J. Alex Halderman
  Committee: Nikola Banovic, Peter Honeyman, Walter R. Mebane, Jr., Ronald L. Rivest
- M.S. in Computer Science, University of Michigan, Summer 2018
- B.A. in Computer Science, Rice University, Spring 2015
  Advisor: Dan S. Wallach

Honors and Awards

- **Election Verification Network Election Integrity Research Award** for excellence in scientific research into election integrity
- **Best Student Paper Award at IEEE Security and Privacy 2020** for Can Voters Detect Malicious Manipulation of Ballot Marking Devices?

Professional Experience

- Research Engineer at VotingWorks (September 2020–present)
  - **Product security**—deployed state-of-the-art platform security to in-the-field voting equipment, relying on UEFI Secure Boot, TPM-based attestation, and a dm-verity-protected filesystem.
  - **Operational security**—implemented organization-wide security improvements to operational security, including code signing, multifactor authentication, DDoS protection, regular penetration testing, SIEM, web application vulnerability scanning.
  - **Cutting-edge risk-limiting audit support**—implemented state-of-the-art risk-limiting audit mechanisms to enable batch-level audits, hybrid audits, and audits of instant-runoff voting.
  - **Development platform improvements**—rebuilt the voting system to run off a Debian base (from Ubuntu), relying on Debian preseed files and virtual machines to enhance the development-to-production experience.

– **Expert Witness** (2018–present)
Served as an expert witness in several lawsuits pertaining to election security. *Curling et al. v. Raffensperger*, *CGG v. Crittenden*, *Shelby Advocates for Valid Elections et al. v. Hargett et al.*, *NFB v. Lamone*

– **Software Engineering Consultant for VotingWorks** (June 2019–2020)
Implemented risk-limiting audit math for VotingWorks' open source risk-limiting audit tool Arlo.

– **Data Science Consultant for Verified Voting** (June 2018–September 2019)
Collected and interpreted 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.

– **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.

Professional Service

Program Committee

– 7th International Joint Conference on Electronic Voting (E-Vote-ID'22)
– 7th Workshop on Advances in Secure Electronic Voting (Voting'22)
– 30th USENIX Security Symposium (Sec'21)
– 32th USENIX Security Symposium (Sec'23)
– **Program co-chair**, 6th Workshop on Advances in Secure Electronic Voting (Voting'21)
– Fifth International Joint Conference on Electronic Voting (E-Vote-ID'20)
– **Program co-chair**, 5th Workshop on Advances in Secure Electronic Voting (Voting'20)

External Reviewer

– Election Law Journal
– ACM Conferences on Human Factors in Computing Systems (CHI'20)
– USENIX Security Symposium (Sec'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)

Teaching

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

Refereed Conference Publications

[1] **Risk-limiting Audits: A Practical Systematization of Knowledge**
Matthew Bernhard
In *Proceedings of the Seventh International Joint Conference on Electronic Voting* **(E-Vote-ID'21)** , October 2021.

[2] **Tales from the Trenches: Case Studies in Election Cybersecurity Preparedness in Texas**
Elizabeth Kasongo, Matthew Bernhard, and Chris Bronk
In *Proceedings of the Seventh International Joint Conference on Electronic Voting* **(E-Vote-ID'21)** , October 2021.

[3] **Can Voters Detect Malicious Manipulation of Ballot Marking Devices?**
Matthew Bernhard, Allison McDonald, Henry Meng, Jensen Hwa, Nakul Bajaj, Kevin Chang, and J. Alex Halderman
In *Proceedings of the 41st IEEE Symposium on Security and Privacy* **(Oakland'20)** , May 2020.
Best Student Paper Award

[4] **Decentralized Control: A Case Study of Russia**
Reethika Ramesh, Ram Sundara Raman, Matthew Bernhard, Victor Ongkowijaya, Leonid Evdokimov, Anne Edmundson, Steven Sprecher, Muhammad Ikram, and Roya Ensafi
In *Proceedings of the 27th Network and Distributed Systems Symposium*
(NDSS'20) , February 2020.

[5] **UnclearBallot: Automated Ballot Image Manipulation**
Matthew Bernhard, Kartikeya Kandula, Jeremy Wink, and J. Alex Halderman
In *Proceedings of the 4th International Joint Conference on Electronic Voting*
(E-Vote-ID'19) , October 2019.

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

[7] **403 Forbidden: A Global View of CDN Geoblocking**
Allison McDonald, Matthew Bernhard, Luke Valenta, Benjamin VanderSloot, Will Scott, Nick Sullivan, J. Alex Halderman, Roya Ensafi
In *Proceedings of the ACM Internet Measurement Conference*
(IMC'18) , November 2018.

[8] **Public Evidence from Secret Ballots**
Matthew Bernhard, Josh Benaloh, J. Alex 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.

[9] **Understanding the Mirai Botnet**
Manos Antonakakis, Tim April, Michael Bailey, Matthew Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J. Alex 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.

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

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

Refereed Workshop Publications

[12] **Bernoulli Ballot-Polling: A Manifest Improvement for Risk-Limiting Audits**
Kellie Ottoboni, Matthew Bernhard, J. Alex 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.

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

Selected Other Publications

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

Speaking

Major Invited Talks and Keynotes

- **Recount 2016 and Student Voter Engagement**
  University of Pennsylvania Voter Engagement Week, Philadelphia, Pennsylvania, August 1970.
- **U.S. Civil Rights Commission testimony on voter registration security**
  Michigan Advisory Committee to the U.S. Commission on Civil Rights, Detroit, Michigan, August 1970.
- **Panel: Next Generation Voting Systems (moderator)**
  Election Verification Network Conference, Washington, D.C., August 1970.
- **Panel: Usability and Voter Verification (moderator)**
  Election Verification Network Conference, Washington, D.C., August 1970.
- **A Crash Course on Election Security**
  2018 DEF CON Voting Village, Las Vegas, Nevada, August 1970.
- **Panel: Do We Want a Recount or Not?**
  Election Verification Network Conference, Washington, D.C., August 1970.
- **Recount 2016: An Uninvited Security Audit of the U.S. Presidential Election**
  2017 RoadSec, São Paulo, Brazil, August 1970.
- **Recount 2016: An Uninvited Security Audit of the U.S. Presidential Election**
  33rd Chaos Communications Congress, Hamburg, Germany, August 1970.

Selected Talks

- **Cybersecurity and U.S. Elections**
  Invited speaker, RoadSec Pro, São Paulo, Brazil, August 1970; Invited speaker, Workshop on Electoral Technologies, Brasilia, Brazil, August 1970;
- **Internet Pinball: The Security and Privacy Impact of Redirects**
  Mozilla Security Research Summit, San Francisco, California, August 1970.
- **Election Security and You**
  Midwest Security Workshop, Chicago, Illinois, August 1970.
- **Coercion-resistant, Receipt-free, and Paperless Voting**
  Rump session at Financial Cryptography and Data Security 2019, St. Kitts, August 1970.
- **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 1970.
- **A Constitutional Argument Against Burr-Feinstein**
  Rump session, 25th USENIX Security Symposium (USENIX'16), Austin, Texas, August 1970.

Advising and Mentoring

Undergraduate Independent Work

- 2019: Henry Meng, Jensen Hwa, Thea Lau, Chand Rajendra-Nicolucci, Antonio Atkinson, Jeremy Wink, Kartikey Kandula
- 2020: Henry Meng, Jensen Hwa, Nakul Bajaj, Atreya Tata, Ryan Feng

Broader Impact of Selected Projects

- **Implementing Better Election Security** (2018–present)
  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.

References

- **Dan S. Wallach**
  Professor, CS and ECE Departments, Rice University
- **Matthew Masterson**
  Director of Information Integrity, Microsoft
- **Jonathan Brater**
  Director of Elections at the Michigan Department of State
- **J. Alex Halderman**
  Professor of Computer Science and Engineering, University of Michigan
- **Josh Benaloh**
  Senior Cryptographer, Microsoft Research,
- **Mark Lindeman**
  Policy and Strategy Director, VerifiedVoting
- **Allison McDonald**
  Assistant Professor in the Faculty of Computing and Data Sciences, Boston University
- **Zakir Durumeric**
  Assistant Professor, Stanford Univeristy, Co-Founder and Chief Scientist, Censys