IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

FAIR FIGHT ACTION, et al.,	)	
	)	
Plaintiffs,	)	
	)	
v.	)	Civ. Action No. 1:18-cv-05391-SCJ
	)	
BRAD RAFFENSPERGER, in his official capacity as Secretary of State of the State of Georgia, et al.,	)	
	)	
Defendants.	)	

EXPERT REPORT OF J. ALEX HALDERMAN

Professor of Computer Science & Engineering
Director, University of Michigan Center for Computer Security and Society
University of Michigan
Beyster Building, Room 4717
2260 Hayward Street
Ann Arbor, MI 48109-2121

February 18, 2020

J. Alex Halderman, Ph.D.
[signature to be supplied]

EXPERT REPORT OF J. ALEX HALDERMAN, Ph.D.

1. My name is J. Alex Halderman.

2. My background, qualifications, and professional affiliations are set forth in my curriculum vitae, which is attached as Exhibit A.

3. I hold a Ph.D. (2009), a master's degree (2005), and a bachelor's degree (2003), *summa cum laude*, in computer science, all from Princeton University.

4. I am Professor of Computer Science and Engineering, Director of the Center for Computer Security and Society, and Director of the Software Systems Laboratory at the University of Michigan in Ann Arbor, Michigan.

5. My research focuses on computer security and privacy, with an emphasis on problems that broadly impact society and public policy. Among my areas of research are software security, network security, and election cybersecurity.

6. I serve as co-chair of the State of Michigan's Election Security Advisory Commission, by appointment of the Michigan Secretary of State.

7. I have testified before the U.S. Senate Select Committee on Intelligence and before the U.S. House Appropriations Subcommittee on Financial Service and General Government on the subject of cybersecurity and U.S. elections.

8. I have performed security testing of electronic voting systems for the Secretary of State of California.

9. I have authored more than 85 articles and books. My work has been cited in more than 9,400 scholarly publications. I have served on the program committees for 33 research conferences and workshops. I co-chaired the USENIX Election Technology Workshop, which focuses on electronic voting security.

10. I have published numerous peer-reviewed research papers analyzing the security of electronic voting systems used in U.S. states and in other countries. I have also investigated methods for improving election security, such as efficient techniques for auditing whether computerized election results match paper ballots.

11. I regularly teach courses in computer security, network security, and election cybersecurity at the graduate and undergraduate levels. I am the creator of *Securing Digital Democracy*, a massive, open, online course about computer security and elections that has attracted more than 20,000 students.

12. I received the John Gideon Award for Election Integrity from the Election Verification Network, the Andrew Carnegie Fellowship, the Alfred P. Sloan Foundation Research Fellowship, the IRTF Applied Networking Research Prize, the Eric Aupperle Innovation Award, the University of Michigan College of Engineering 1938 E Award for teaching and scholarship, and the University of Michigan President's Award for National and State Leadership.

13. I am being compensated for my work related to this matter at my customary rate of $750 per hour. My compensation does not depend on the outcome of this litigation, the opinions I express, or the testimony I provide.

Georgia's Election Technology

14. Plaintiffs have asked me to opine on the security of Georgia's election system following the implementation of new technology from Dominion Voting Systems, Inc. ("Dominion") and KNOWiNK, LLC ("KnowInk"). The state is in the process of deploying Dominion ImageCast X Prime ("ICX") ballot marking devices (BMDs), ImageCast Precinct ("ICP") precinct-count scanners, ImageCast Central ("ICC") central-count scanners, the Democracy Suite election management system (EMS), and KnowInk Poll Pad electronic poll books. Georgia Secretary of State Brad Raffensperger certified the Dominion components in August 2019.[1]

15. I have reviewed documents provided by Dominion in response to a subpoena from Plaintiffs. These documents include technical documentation about the election system components, the company's response to Georgia's Request for Proposals for the new voting system, reports from third-party testing, and certain internal engineering memos relating to the security of the system.

[1] Georgia Dominion/KnowInk certification (Aug. 9, 2019), https://sos.ga.gov/admin/uploads/Dominion_Certification.pdf.

16. I understand that Georgia maintains its voter registration database using a system called ElectioNet ("eNet"), which was developed and is maintained by PCC Technology, Inc. Election officials use eNet to manage voter registration data and to export it to electronic poll books for each election. The Georgia My Voter Page (MVP) and Online Voter Registration (OVR) websites interface with eNet and allow voters to view and update their voter registration data. At each polling place, workers use Poll Pad electronic poll books to check in voters. The Poll Pads consist of off-the-shelf Apple iPads running custom software. The Poll Pads are also used to program "voter cards," which the voter uses to activate a ballot marking device and begin a voting session.

17. Georgia plans for all in-person voters to select candidates using Dominion ICX BMDs, which are computer tablets connected to off-the-shelf laser printers. These devices do not record votes but instead print paper ballots that are supposed to contain the voter's selections in both human-readable text and as a type of machine-readable barcode called a QR code. The voter will insert the paper ballot into a Dominion ICP optical scanner, which will store a digital scan of the printout. The scanner will process the barcode and count the votes encoded in it, and the paper ballots will be retained for use in audits or recounts. Absentee voters will not use

BMDs but will instead complete hand-marked paper ballots (HMPBs), which will be tabulated at central locations by Dominion ICC optical scanners.

18. Before every election, the Secretary of State's office will prepare election programming files using the Dominion EMS software, which is a collection of client and server programs that run on commercial-off-the-shelf (COTS) computers and servers. The Secretary of State will transmit the election programming files to county officials, who will use another instance of the Dominion EMS to prepare memory cards and USB sticks for every scanner and ballot marking device used in the county. These removable media will contain the ballot design, including the names of the races and candidates, and rules for counting the ballots. Election workers will install a memory card or USB stick into each BMD and ICP scanner prior to the start of voting.

19. After polls close, election workers will remove the memory cards from every ICP scanner and return them to the county. At that point, the memory cards will contain a digital image of each scanned ballot as well as the scanner's interpretation of the votes each ballot contains. County workers will use the Dominion EMS to retrieve data from the cards and prepare the final election results.

Threats to Georgia Elections

20. In my opinion, Georgia's election system faces a high risk of being targeted by sophisticated adversaries, including Russia and other hostile foreign governments. These adversaries could attempt to hack the election system to achieve a variety of goals, including undermining voter confidence and causing fraudulent election outcomes. Attackers could sabotage BMDs or optical scanners to prevent them from functioning on election day, or to cause obviously incorrect results. They could also infiltrate BMDs and scanners with malicious software in order to cause plausible but fraudulent election results. As I will explain, attacks by sophisticated attackers such as foreign governments could succeed despite procedural and technical protections that Georgia has in place, including a paper trail and limited post-election audits.

21. The Mueller Report outlined the scale and sophistication of Russia's efforts to interfere in the 2016 election, leaving no doubt that Russia and other adversaries will strike again.[2] The Special Counsel concluded principally that "[t]he Russian government interfered in the 2016 presidential election in sweeping and

[2] Special Counsel Robert S. Mueller, III *Report on the Investigation into Russian Interference in the 2016 Presidential Election (Volume I of II)*, United States Department of Justice (Mar. 2019), https://www.justice.gov/storage/report.pdf.

systematic fashion."[3] The report further explained that foreign actors "sought access to state and local computer networks by exploiting known software vulnerabilities on websites of state and local governmental entities."[4] The report also found that these foreign agents were successful in attacking at least one state and that their activities involved "more than two dozen states."[5] As noted prior to the Special Counsel's final report, Georgia was among the states that Russia targeted.[6]

22. Russia has sophisticated cyber-offensive capabilities, and it has shown a willingness to use them to hack elections elsewhere even before 2016. For instance, according to published reports, during the 2014 presidential election in Ukraine, attackers linked to Russia sabotaged Ukraine's vote counting infrastructure, and Ukrainian officials succeeded only at the last minute in defusing vote-stealing malware that would have caused the wrong winner to be announced.[7] Other adversarial governments have similarly advanced cyberwarfare capabilities, including China, Iran, and North Korea, and might target future Georgia elections.

---

[3] *Id.* at 1.
[4] *Id.* at 50.
[5] *Id.*
[6] *See* Indictment ¶ 75, *United States v. Netyksho*, No. 1:18-cr-00215-ABJ, , (D.D.C. July 13, 2018), ECF No. 1.
[7] Mark Clayton, "Ukraine election narrowly avoided 'wanton destruction' from hackers," *The Christian Science Monitor* (June 17, 2014), https://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers.

23. It is my opinion that Georgia's new voting technology does not achieve the level of security necessary to withstand an attack by a sophisticated adversary such as a hostile foreign government. Despite the addition of a paper trail, it suffers from serious security risks much like those of the paperless voting system it has replaced. Attackers can potentially subvert the election technology in several ways:

(a) Attackers could infiltrate the voter registration database and extract, change, or erase voter registration records. These attacks could cause voters to receive the wrong ballot or be prevented from casting a regular ballot. They could also be used to steal information that could be used to impersonate voters.

(b) Attackers could sabotage polling place equipment, including Poll Pads, BMDs, and ICP scanners, and prevent them from functioning on election day. This would cause lengthy delays and drive away many eligible voters. An attacker could target such sabotage at jurisdictions that strongly favored a particular candidate and thereby cause a partisan shift in the election outcome.

(c) Attackers could manipulate optical scanners or election management systems to cause them to report fraudulent outcomes. Attacks on the scanners could alter all digital records of the election results. The only

kind of safeguard that can reliably detect such an attack is a sufficiently rigorous manual audit or recount of the paper ballots, which Georgia does not currently require.

(d) Attackers could infiltrate the BMDs to cause them to sometimes print ballots that differ from voters' on-screen selections. Such an attack might change only the ballot barcode, which is the only portion of the ballot that the scanners count. The change would be invisible to voters. Unless all races are rigorously audited by inspecting the human-readable portion of the paper ballots, such attacks could go undetected.

(e) Attackers could also infiltrate the BMDs and change both the barcode *and* the human-readable text on some of the ballots. Research shows that few voters carefully review their printed ballots, and consequently fraud sufficient to change the winner of a close race might go undetected. No audit or recount could detect the change, since both the digital and paper records would be wrong.

24. One way that attackers could carry out these attacks is by introducing malicious software ("malware") into the election equipment. Malware could be introduced in several ways, including: (a) with physical access to the equipment, (b) by dishonest election workers, (c) through an attack on the hardware or software

supply-chain, or (d) by spreading from the election management systems to polling place equipment during routine pre-election procedures.

25. Critical components of Georgia's election system are directly connected to the Internet. These include the eNet voter registration system, the Georgia My Voter Page (MVP) and Online Voter Registration (OVR) websites, and the Poll Pad electronic poll books. Being connecting to the Internet exposes these systems to the threat that attackers anywhere in the world could directly target them.

26. Other components of Georgia's election system that are not directly connected to the Internet might nonetheless be targeted by attackers. Nation-state attackers have developed a variety of techniques for infiltrating non-Internet-connected systems, including by spreading malware on removable media that workers use to copy files in and out.[8] Attackers could employ this method to infect the state or county EMS and spread from there to scanners and BMDs when workers program them for the next election. In this way, an attack could potentially spread

[8] A well-known example of this ability, which is known as "jumping an air gap," is the Stuxnet computer virus, which was created to sabotage Iran's nuclear centrifuge program by attacking factory equipment that was not directly connected to the Internet. Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," *Wired* (Nov. 3, 2014), https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

form a single point of infection to scanners and BMDs across entire counties or the whole state.

Vulnerabilities in Georgia Voting Equipment

27. **Dominion components.** Dominion does not dispute that its devices can be hacked by sufficiently sophisticated adversaries.[9]

28. One reason why this is true is the complexity of the software. The Dominion software used in Georgia contains nearly 2.75 million lines of source code (equivalent to about 45,000 printed pages), excluding the Windows and Android operating systems and other off-the-shelf software packages.[10] The ICP scanner alone contains about 475,000 lines of source code, and its software is written in C/C++,[11] a programming language that is particularly susceptible to some of the most dangerous types of vulnerabilities.

29. Software of the size and complexity of the Dominion code inevitably has exploitable vulnerabilities. As a code review team working for the California

[9] Decl. of Dr. Eric Coomer, Director of Product Strategy and Security for Dominion ¶ 13, *Curling v. Raffensperger*, No 1:17-cv-2989-AT (N.D. Ga. Nov. 13, 2019), ECF No. 658-2 ("all computers can be hacked with enough time and access").
[10] SLI Compliance, "Dominion Democracy Suite 5.10 Voting System Software Test Report for California Secretary of State" 6 (Aug. 2019), https://votingsystems.cdn.sos.ca.gov/vendors/dominion/dvs510software-report.pdf.
[11] *Id*.

Secretary of State concluded in a study of a voting system with only 10% as much code as Dominion's, "If the [system] were secure, it would be the first computing system of this complexity that is fully secure."[12] Nation-state attackers often discover and exploit novel vulnerabilities in complex software.[13]

30. In addition to its complexity, the Dominion software utilizes a wide range of outdated off-the-shelf software modules, including some that perform essential security functions, such as the operating system and modules that process files an attacker might have manipulated.[14] The oldest third-party software components appear not to have been updated in more than 15 years. Old or outdated software used in Georgia's new Dominion equipment includes a version of Microsoft SQL Server dating from 2016, Adobe Acrobat from around 2015, barcode scanner software from 2015, Android operating system software from 2015, µClinux

---

[12] Joseph A. Calandrino, Ariel J. Feldman, J. Alex Halderman, David Wagner, Harlan Yu, and William Zeller, "Source Code Review of the Diebold Voting System," in *California Secretary of State's Top-to-Bottom Review of Voting Systems* (July 20, 2007), https://votingsystems.cdn.sos.ca.gov/oversight/ttbr/diebold-source-public-jul29.pdf.

[13] Andrew Springall, *Nation-State Attackers and their Effects on Computer Security* (2009), Ph.D. dissertation, University of Michigan, https://deepblue.lib.umich.edu/handle/2027.42/143907.

[14] SLI Compliance, "Dominion Voting Systems Democracy Suite 5.5-A Certification Test Plan" 16-19 (Dec. 2018), https://www.eac.gov/sites/default/files/voting_system/files/DVS_Democracy_D-Suite_5.5-A_Modification_Test_Plan_v1.2.pdf.

operating system software from 2007, COLILO bootloader software from 2004, and a version of the Apache Avalon component framework dating from 2002.

31. Outdated software components are a security risk because they frequently contain known, publicly documented vulnerabilities that have been corrected in later versions. For example, the version of the Android operating system used Georgia's ICX BMDs, Android 5.1.1, contains 254 known vulnerabilities.[15]

32. Dominion's response to Georgia's RFP lists among "key personnel" a "Chief Security Officer" (CSO) whose responsibilities for the voting system project will be "Oversight of key security development and implementation."[16] However, at the time of the RFP, the CSO position was vacant, and to my knowledge Dominion has yet to fill the role. It is unclear who at Dominion has responsibility for security development and implementation in the context of the Georgia components.

33. Georgia certified the Dominion system without performing its own security testing or source code review. The certification was preceded by tests performed that were limited to checking functional compliance with Georgia

[15] CVE Details, "Google Android 5.1.1 Security Vulnerabilities," https://www.cvedetails.com/vulnerability-list/vendor_id-1224/product_id-19997/-version_id-186573/Google-Android-5.1.1.html (last visited Feb. 10, 2020).
[16] DOM-003996.

requirements.[17] The test report states that the testing "was not intended to result in exhaustive tests of system hardware and software attributes."[18] The word "security" does not appear in the report.

34. At around the same time that Georgia certified the Dominion system, California performed tests on a more recent version of the Dominion software (version 5.10) as part of its own certification process.[19] In contrast to Georgia's tests, California's did include some source code review and security testing.

35. Like all security testing, the California tests were necessarily limited in scope and could not be expected to find all exploitable vulnerabilities. Nevertheless, they did uncover several serious flaws. In my experience, more recent versions of software tend to contain fewer security vulnerabilities than older versions, and so these problems very likely apply to the Georgia version of the Dominion system.

36. The California testers found that attackers could modify the Dominion software installation files and believed that "it would be possible to inject more lethal

---

[17] Pro V&V, "Test Report: Dominion Voting Systems D-Suite 5.5-A Voting System Georgia State Certification Testing" (Aug. 7, 2019), https://sos.ga.gov/admin/uploads/Dominion_Test_Cert_Report.pdf.
[18] *Id*. at 3.
[19] SLI Compliance, "Dominion Democracy Suite 5.10 Security and Telecommunications Test Report" (Aug. 2019), https://votingsystems.cdn.sos.ca.gov/vendors/dominion/dvs510security-report.pdf ("California Certification Security and Telecomm Test Report").

payloads into the installers given the opportunity."[20] This implies that attackers could modify the Dominion installation files to infect election system components with malicious software.

37. Furthermore, the California testers found that the Dominion system's antivirus protection was insufficient or non-existent. "[O]n the EMS server, the AVAST Antivirus (AV) File Shield (the real time AV monitor) was only able to detect and clean one of the four [test] files. This potentially leaves the system open to zipped and double zipped viruses as well as infection strings in plain text."[21] Moreover, the ICX BMD and ICP optical scanner have no antivirus software at all.[22] As a result, malware that infected the Dominion components could evade antivirus detection.

38. One way that attackers might affect election equipment is by physically accessing the devices. In the case of the BMD, the California source code reviewers found a vulnerability that can be exploited with physical access to the USB port that "would be open to a variety of actors including a voter, a poll worker, an election official insider, and a vendor insider."[23] This implies that no secret passwords or

---

[20] *Id*. at 25.
[21] *Id*. at 19-20.
[22] *Id*. at 20.
[23] California Secretary of State's Office of Voting Systems Technology Assessment, "Dominion Voting Systems Democracy Suite 5.10 Staff Report" 29

keys would be needed to exploit the problem, given physical access. California testers also found that "the ICX device does not provide monitoring of physical security,"[24] and that, for all the polling place devices, including the ICX, "[s]ecurity seals, locks, and security screws can be circumvented."[25]

39. Other weaknesses found in the California tests include that "a number of passwords were able to be recovered that were stored in plain text,"[26] that the network switch used to connect EMS clients and servers was "determined to have twelve medium vulnerabilities and four low vulnerabilities,"[27] and that, if an authentication device used by poll workers and administrators was lost or stolen shortly before an election, revoking its access would require a logistically difficult process to reprogram the election files for the polling place devices.[28] These problems indicate that the Dominion system was designed without sufficient attention to security.

(Aug. 19, 2019), https://votingsystems.cdn.sos.ca.gov/vendors/dominion/dvs510staff-report.pdf.

[24] California Certification Security and Telecomm Test Report at 11.

[25] *Id*. at 17.

[26] *Id*. at 15.

[27] *Id*. at 30.

[28] *Id*. at 15.

40. Although California ultimately permitted the Dominion system to be used, its certification requirements impose much more stringent security conditions than those in Georgia.[29]

41. **Voter registration components.** Georgia has used the eNet voter registration database system for many years. I understand that the state commissioned a vendor cyber risk assessment of eNet in February 2018. The assessment encompassed a contract and documentation review, network scans and reviews of server configurations, and interviews with key personnel at PCC, the vendor that developed and (at the time) operated eNet. The assessment was limited in scope and did not include source code review or penetration testing. Even this limited review identified serious security deficiencies in both the software and PCC's network environment. In July 2019, the Secretary of State assumed operational responsibility for eNet, but development and maintenance of the software continue to be the responsibility of PCC.

42. Transferring eNet operations to the Secretary of State's office does not mitigate the full range of issues that the State's experts identified, and there is no evidence that the State has taken other steps to address them. Moreover, the 2018

[29] California Secretary of State, "Conditional Approval of Dominion Voting Systems, Inc. Democracy Suite Version 5.10 Voting System" (Oct. 18, 2019), https://votingsystems.cdn.sos.ca.gov/vendors/dominion/ds510-cert.pdf.

security assessment was of limited scope, and a more thorough assessment, including a source code review and penetration tests, would be necessary to ensure that all relevant issues are discovered and corrected.

43. The Georgia My Voter Page (MVP) and Online Voter Registration (OVR) websites that interface with eNet provide another avenue by which attackers could attempt to infiltrate the voter registration system. Serious vulnerabilities in the MVP website were discovered on the eve of the November 2018 election and reported to the Secretary of State. Unauthorized parties could have exploited these vulnerabilities to access sensitive system configuration files and voter registration data. This information would have allowed attackers to fraudulently change voters' registrations through the OVR system. Cursory security testing should have uncovered the MVP vulnerabilities, and their existence calls into question the overall security of the MVP and OVR websites.

44. **Electronic poll books.** The Poll Pads electronic poll books communicate with an Internet-based administration system called ePulse. Election workers use the ePulse website to upload lists of eligible voters for each precinct, manage Poll Pad devices, and retrieve voter history data after an election. When polls are open, Poll Pads can be configured in a fully connected mode, in which they continuously communicate with ePulse over the Internet, or in a peer-to-peer

communication mode, in which they exchange data with other Poll Pads in the polling place over a Bluetooth or WiFi wireless network.

45. Internet access and wireless capabilities expose the Poll Pads to a large variety of security risks. If attackers are able to infiltrate ePulse, they could remotely alter voter registration data before it is downloaded by the Poll Pads, or they could potentially spread malicious software to the Poll Pads. Attackers could also likely exploit the devices' wireless capabilities to disable Poll Pads during voting.

46. To my knowledge, Georgia has not performed any security testing of the Poll Pad electronic poll books. In contrast, the Secretary of State of California commissioned source code review[30] and penetration testing[31] of the Poll Pad in 2018. Among several significant deficiencies found by California were: (i) cross-site scripting vulnerabilities and insecure use of HTTP Cookies in the ePulse website, which could allow attackers to hijack election officials' accounts; (ii) the ability of the software to delete log files without this action itself being logged, which could

[30] SLI Compliance, "KNOWiNK PollPad Plus 1.0 Electronic Poll Book System Source Code Review Test Report for California" (May 6, 2018), https://votingsystems.cdn.sos.ca.gov/vendors/knowink/source-code-report.pdf.
[31] SLI Compliance, "KNOWiNK PollPad Plus 1.0 Electronic Poll Book System Security and Telecommunications Test Report for California" (May 11, 2018), https://votingsystems.cdn.sos.ca.gov/vendors/knowink/security-report.pdf.

help attackers hide evidence of their activities; and (iii) improper programming structures that apparently created the potential for inadvertent data loss.

47. Following these tests, California conditionally certified the Poll Pad subject to 19 terms and limitations that reflect the findings of the security testing.[32] Among the conditions is that Poll Pads may not be connected to smart card encoders, which ensure that there is no path for an attack to spread from the Poll Pads to BMDs.

48. Pennsylvania also evaluated and conditionally certified the Poll Pad in 2018.[33] The Pennsylvania certification is subject to 24 conditions and accompanied by five additional security recommendations. The conditions include that Poll Pads must not be configured to communicate with ePulse over the Internet during polling, and that Poll Pads and their removable media must never be connected to other voting system components, including a prohibition of using the Poll Pads to encode voter access cards.

---

[32] California Secretary of State, "Conditional Approval of KnowInk, LLC PollPad Plus Version 1.0 Electronic Poll Book System" (May 22, 2018), https://votingsystems.cdn.sos.ca.gov/vendors/knowink/cert.pdf.

[33] Commonwealth of Pennsylvania Department of State, "Results of KnowInk Electronic Poll Book Poll Pad 1.3.3 Evaluation" (Oct. 5, 2018), https://www.dos.pa.gov/VotingElections/Documents/Voting%20Systems/Knowink%20PollPag%201.3.3/Knowink%20Poll%20Pad%201.3.3%20Approval%20Report.pdf.

49. It is unclear what conditions, if any, Georgia imposes on the use of Poll Pads. However, I understand that the Poll Pad will be used to encode voter activation cards that voters use with the Dominion BMDs. California and Pennsylvania both prohibit this functionality, as it creates a path by which an attack could spread from the Poll Pads (which have Internet access) to the BMDs.

50. **Supply chain threats.** In addition to the risk that external attackers will compromise Georgia election system components by exploiting software vulnerabilities, there is also a risk that attackers could infiltrate the software development process of Dominion, KnowInk, PCC, or their suppliers. By doing so, an adversary could steal source code or other secrets in order to more easily attack the election components. An attacker could also insert vulnerabilities or malicious functionality into the election system software during development.

51. Several critical components of the Dominion systems are designed and produced overseas. Much of the election software is programmed in Serbia, a country closely allied with Russia.[34] The EMS runs antivirus software made by a Czech company, which necessitates granting that software highly privileged access

[34] Patrick Thibodeau, "One election-system vendor uses developers in Serbia," *Computer World* (Oct. 5, 2016), https://www.computerworld.com/article/3126791/one-election-system-vendor-uses-developers-in-serbia.html.

to the EMS server. The ICX BMD runs on an Android-based tablet produced by a Taiwanese company. A hostile government might attempt to plant an agent at any of these companies, blackmail honest employees, or hack into the software development environments. Although multinational supply chains are common in the technology industry, they represent a heightened threat in election contexts due to foreign governments' military, diplomatic, and economic interests in U.S. election outcomes.

Intended Safeguards Provide Insufficient Protection

52. I understand that Georgia applies or intends to apply a variety of defenses within the election system. However, even when taken together, these defenses are insufficient to thwart attacks by sophisticated adversaries, such as hostile governments.

53. **AuditMark.** When the ICP and ICC scanners process a ballot, they generate a digital image of the ballot. A feature that Dominion calls "AuditMark" appends to the image a record of the scanner's interpretation of the votes. Election officials can later review the digital records of each ballot using the EMS.

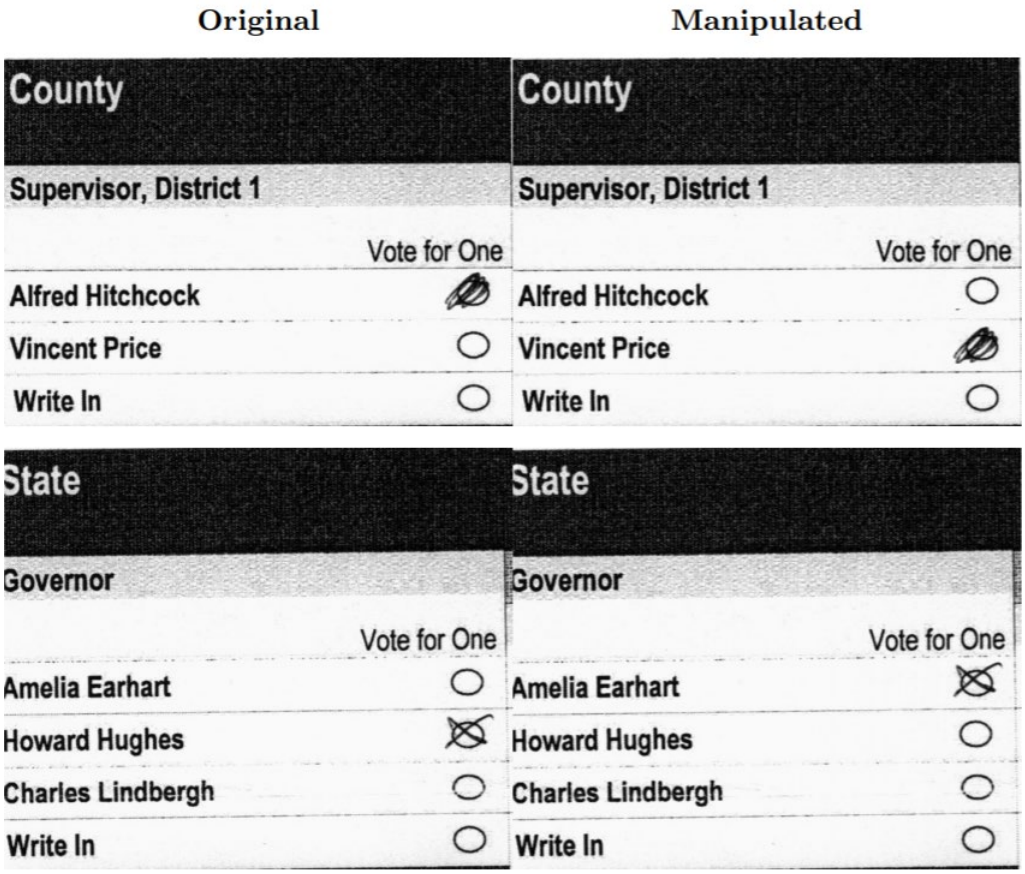
54. Digital ballot images and the AuditMark feature do not secure the electronic vote records against tampering by malicious software. My own peer-reviewed research demonstrates how malware running on an optical scanner or EMS

could automatically manipulate digital ballot images to make them appear to support a different election result.[35]

55. For ballots that are marked by hand, malware can employ computer vision techniques to manipulate ballot images while preserving the voter's original marking style, so that the manipulated marks appear consistent with other marks on the ballot. Manipulation is even more straightforward when ballots are marked by a BMD, since the BMD prints all marks in a consistent style.

56. In either case, the tampering would not be detected by the election software and would be not be apparent to a human operator reviewing the ballot images and AuditMark data. The figure below shows an example of a Dominion-style ballot image that has been manipulated using the algorithm from our research:

[35] Matthew Bernhard, Kartikeya Kandula, Jeremy Wink, and J. Alex Halderman, "UnclearBallot: Automated Ballot Image Manipulation" in *Proceedings of the Fourth International Joint Conference on Electronic Voting* (Oct. 2019), https://jhalderm.com/pub/papers/unclear-evoteid19.pdf.



Left: **Image of original Dominion-style voter-marked ballot.**

Right: **Image manipulated by malware to show fraudulent selections.**

57. **Hash comparisons.** I understand that Georgia may employ a method know an "hash comparison" to attempt to confirm that the correct software is installed on the EMS and polling place equipment. A "hash value" is a short numeric code that is calculated based on the contents of a file. The calculation method is designed so that it is difficult to figure out a way to modify the file without resulting in a different hash value. Officials might attempt to detect malware by comparing

the hash values of the software running in the election system to "known good" hash values calculated from a copy of the software that has not been altered by an attacker.

58. In response to Dominion's proposal for the election system, Georgia requested additional details about how a hash comparison can be performed during initial acceptance testing of the equipment, during pre-election processes, and immediately following an election. Dominion's responses[36] describe a hash comparison process that cannot reliably detect malicious changes to the machines.

59. There are separate comparison procedures for the EMS, ICX, ICP, and ICC. In each case, software on the equipment being tested is either responsible for calculating the hash value or for copying the files that are to be compared to removable media. If the equipment has been infected with malware, the malware could cause the machines to falsely compute the hash values of an uninfected system, or it could copy the original program files to the removable media while actually running a modified version of the files.

60. Furthermore, the hash comparisons described by Dominion for the cover only some of the software running on the devices. They fail to check the integrity of critical software such as the Windows and Android operating systems, as well as other programs and data files that could contain malware. These

[36] DOM-000143-49, 170-74, 210-11, and 239-42.

deficiencies provide multiple ways for a sophisticated attacker to conceal the presence of malware on the voting equipment even if officials practiced hash comparisons according to Dominion's instructions.

61. **Antivirus software.** As I have already described, California's security tests found that the antivirus software used on the Dominion EMS server was unable to detect some forms of malware, and that the ICP and ICX devices have no antivirus protection at all. In general, antivirus software and end-point protection software provide only a limited defense against sophisticated attackers like nation-states.

62. **Physical security.** I understand that one safeguard used in Georgia is tamper-evident seals. These seals are designed to indicate whether someone has opened the chassis of an optical scanner or BMD or accessed protected data ports or switches. Tamper evident seals do not protect against remote electronic attackers, and they provide only weak protection against attackers with physical access. The types of seals typically used for voting equipment can be bypassed without detection using readily available tools.[37] For some seals, these tools include screwdrivers and hair dryers. By bypassing the seals, an attacker with physical access to the polling place equipment can modify their internal programming and add malicious software.

[37] Andrew W. Appel, "Security Seals on Voting Machines: A Case Study," in *ACM Transactions on Information and System Security* (2011), https://www.cs.princeton.edu/~appel/voting/SealsOnVotingMachines.pdf.

63. **Logic and accuracy testing.** I understand that Georgia employs so-called "logic and accuracy" (L&A) testing. In L&A testing, officials cast a small number of ballots with known selections, then check whether the system's output reflects the correct votes. L&A testing is designed to detect errors in the ballot design or counting logic. It provides little or no benefit against deliberate attacks.

64. Much as Volkswagen's emission systems were designed to detect that they were being tested by the EPA and to only cheat while not under test, malware that has infected an optical scanner or BMD can be programmed to detect and circumvent L&A testing. For example, malware can be programmed to check the machine's clock and cheat only in the middle of election day, so that testing performed at an earlier or later time would show nothing amiss. Malware can also be programmed to cheat only after hundreds of ballots have been cast, so that more limited testing would not detect the fraud.

65. **Parallel testing.** I understand that Georgia has in the past employed a testing technique known as "parallel testing", and that the state might use this technique in the future to check whether BMDs correctly print voters' choices. In BMD parallel testing, poll workers periodically print test ballots during the election and confirm that the printouts match their selections.

66. Parallel testing cannot reliably determine that a BMD is working correctly. An attacker could program the BMD to modify the voter's selections on only certain printouts, and the selection could depend on a very large number of variables, including the time of day, the number of ballots cast, the voter's ballot selections, and whether the voter used options such as a large font size or an audio ballot. It is impossible for any practical amount of testing to examine all sets of conditions under which attackers might choose to cheat.[38]

67. In any event, investigation that occurs during the election is no help if the attacker's intention is to sabotage the voting process, such as by disabling the BMDs entirely. I am aware that Georgia's contingency plans call for having voters mark ballots by hand if BMDs are unavailable. However, an attacker might cause all BMDs to fail simultaneously over a large geographic area. To my knowledge, the state does not maintain sufficient quantities of pre-printed ballots to allow voting to continue under such a circumstance.

68. **Post-election audits.** Officials could potentially detect certain kinds of attacks by conducting a rigorous post-election audit of the paper ballots. For an audit to reliably detect vote-changing attacks, several requirements must be met. Among

[38] Philip B. Stark, "There is no Reliable Way to Detect Hacked Ballot-Marking Devices" (2019), https://www.stat.berkeley.edu/~stark/Preprints/bmd-p19.pdf.

them are: (i) the paper ballots being audited must correctly reflect voters' selections, (ii) the audit needs to be conducted manually, by having people inspect the ballots; (iii) the auditors need to inspect sufficiently many ballots to ensure that the probability that outcome-changing fraud could go undetected is low. In general, the closer the election result, the more ballots need to be audited in order to rule out fraud. Audits that limit the risk that outcome changing fraud will go undetected to no more than a pre-defined limit are called "risk-limiting audits" (RLAs).[39]

69. I understand that Georgia statute requires a state-wide post-election audit to be conducted no later than the November 2020 election.[40] However, that audit is not required to be risk-limiting. As a result, if there are close races in which an attacker changes the outcome by hacking the election equipment, there is a high probability that the audit would fail to uncover the attack.

70. Although some Georgia counties recently conducted small-scale audit pilots using risk-limiting techniques,[41] these audits achieved a low risk-limit only in

[39] Mark Lindeman and Philip B. Stark, "A Gentle Introduction to Risk-limiting Audits," in *IEEE Security and Privacy* (2012), https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf.
[40] *See* O.C.G.A. § 21-2-498(b).
[41] Georgia Secretary of State's Office, "Risk-Limiting Audit Concludes Paper-Ballot System Accurate," (https://sos.ga.gov/index.php/elections/risk-limiting_audit_concludes_paper-ballot_system_accurate (last visited Feb. 17, 2020).

specific local races. An attacker could choose to target any race in any election, and an attack would likely not be detected in an RLA if it occurred in a race for which the RLA had a high effective risk-limit. To my knowledge, the Georgia Secretary of State has not announced plans to perform an RLA of *any* state-wide race.

71. No matter what auditing procedures Georgia applies, the state's widespread use of BMDs makes it possible for an attacker to undermine the integrity of the paper trail. Malware could cause the BMDs to print fraudulent selections, both in the barcode and the human-readable text. Such an attack would be impossible to detect by auditing the ballots, even with an RLA, because all records of the voter's intent would be wrong.

BMDs Create Additional Risks

72. The ICX BMDs are computers, they run outdated and vulnerable software, and they must be programmed using the State's election management system before every election. Attackers could potentially infect Georgia's BMDs with malware in several ways, including by spreading it from the election management system (EMS).

73. An attacker who infected the BMDs with malware could change the printed ballots. On a fraction of the ballots, the attacker could cause the human-readable text, the barcode, or both to reflect fraudulent choices rather than the voter's

selections. I will discuss two kinds of such misprinting attacks: attacks that change only the barcode and attacks that change both the barcode and the text.

74. **Misprinting only the barcode.** One kind of misprinting attack is a barcode-only attack. In this attack, malware would change a fraction of the BMD printouts so that they correctly showed the voter's selections in the human-readable text but encoded a different, fraudulent set of selections in the barcode.

75. If an attacker changes only the barcode, it would be impossible for voters to detect the fraud. Voters cannot read the barcodes, so there is no practical way for them to verify that the barcodes match their intended selections. Moreover, when scanning BMD ballots, the optical scanners count only the votes encoded in the barcodes and ignore the text entirely. This means that voters cannot verify the portion of their ballots that gets counted.

76. Officials could potentially detect a mismatch between the barcodes and the ballot text using a sufficiently rigorous post-election audit. However, to my knowledge, Georgia has not announced plans to perform any kind of audit that would compare the barcodes and the printed text, nor what specific measures would be taken to render any potential audit sufficiently comprehensive and reliable.

77. **Misprinting both the barcode and the text.** Malware could also cause the BMDs to print fraudulent selections in *both* the barcode and the human-readable

text. This attack would be impossible to detect by auditing the ballots, even with an RLA, because all records of the voter's intent would be wrong. Pre-election testing and parallel testing also cannot reliably detect such cheating. The only practical way to discover the attack would be if enough voters reviewed their ballots, noticed the errors, and alerted election officials.

78. Even if some voters did notice that their ballots were misprinted, the voters would have no way to prove that the BMDs were at fault. From an election official's perspective, the voters who reported problems might be mistaken or lying. Many voters would need to report that the BMDs misprinted their ballots before officials could be sure there was a systemic problem. Even then, there are no protocols or policies in Georgia that I have found that address how many voter complaints or other conditions involving BMDs would be required to support a finding—or even a robust investigation—of a systemic problem.

79. If officials did suspect that the BMDs had been attacked, there would be no straightforward way to respond or recover. The only recourse might be to rerun the election, which could be statewide involving millions of voters across Georgia.

80. **Voter verification provides insufficient protection.** Research shows that most voters do not review their BMD printouts, and that voters will likely fail

to detect a large majority of errors caused by a BMD attack. This means that a BMD paper trail is not a reliable record of the votes expressed by the voters.

81. In one study, researchers observed voters in two polling places during an election in Sevier County, Tennessee, which uses BMDs similar to Georgia's.[42] Nearly half of voters did not review the BMD printout *at all*, and those who did review it spent an average of only 4 seconds doing so. This suggests that voters are likely to detect at most about half of misprinted ballots, and possibly far fewer.

82. A second study, conducted by my research group at the University of Michigan, measured the rate at which voters detected errors during a realistic simulated election.[43] The voters used BMDs that my research assistants and I hacked so that one selection on each printout was wrong. We recorded how many participants reviewed their ballots and how many noticed the error and reported it to a poll worker. The study was peer reviewed and published at the IEEE Symposium on Security and Privacy in January 2020.

---

[42] Richard DeMillo, Robert Kadel, and Marilyn Marks, "What Voters are Asked to Verify Affects Ballot Verification: A Quantitative Analysis of Voters' Memories of Their Ballots" (Nov. 23, 2018), https://ssrn.com/abstract=3292208.

[43] Matthew Bernhard, Allison McDonald, Henry Meng, Jensen Hwa, Nakul Bajaj, Kevin Chang, and J. Alex Halderman, "Can Voters Detect Malicious Manipulation of Ballot Marking Devices?" in *Proceedings of the 41st IEEE Symposium on Security and Privacy* (2020), https://jhalderm.com/pub/papers/bmd-verifiability-sp20.pdf.

83. In the first part of the study, subjects were not prompted to review their ballots in any way. Under that condition, 60% of voters failed to review their ballots, and voters only reported 6.6% of errors. Considering only prominent "top of the ticket" races, voters reported only 14% of errors. These results imply that for every voter who notices that their ballot is misprinted and corrects it, there will likely be many more voters who fail to notice and have their votes stolen by the attacker.

84. In the second part of the study, we tested procedural changes to see whether they improved verification. Signage instructing voters to verify their ballots (as required in Georgia) did not increase error reporting. Other changes did help, but only to a limited extent. For example, when a poll worker verbally prompted the voter to review the ballot after it was printed, voters reported 15% of errors. In my opinion, it is unlikely that any purely procedural changes can enhance voters' error detection rates sufficiently to stop outcome-changing fraud in close elections when BMDs are used by all in-person voters.

85. My coauthors and I provide a mathematical model for estimating how many voters will report problems if BMDs are attacked in a way that changes an election outcome. The model illustrates how weak a defense voter verification provides when all in-person voters use BMDs.

86. Suppose there is a close election with an apparent margin of victory of 1% in favor of candidate A. If there had been no cheating, the result would have been a one-vote victory for candidate B, but an attacker hacked the BMDs so that they misprinted a small fraction of the ballots. If voters report 14% of misprinted ballots (the rate my study found for top-of-the-ticket contests), then only about 1 in 1200 BMD voters will report a problem—roughly one per precinct—even though the election outcome is wrong due to fraud. This is likely far too few complaints to alert officials or the public that there was a major, outcome-determinative problem.

87. Election officials are unlikely to take disruptive actions, like a protracted and expensive forensic investigation or ordering a new election, unless a much larger fraction of BMD voters report problems. Suppose officials would launch an investigation if more than 1% of BMD voters reported a problem. Under the scenario above, this condition would only be met if voters verified their ballots so carefully that they reported 67% of errors. This is ten times greater than the rate of error reporting my group observed in our study.

Georgia's Voting System was Vulnerable to Cyberattacks in 2018

88. Plaintiffs have asked me to opine on the security of Georgia's election system as it was used in 2018. From 2002 until the end of 2019, Georgia's primary polling place voting equipment was Diebold AccuVote TS and TSX direct-recording

electronic (DRE) voting machines. Georgia's DREs were "paperless," in that they did not create any kind of voter-verifiable paper record of individual votes. There is a broad scientific consensus that paperless DREs do not provide adequate security against cyberattacks.[44] Moreover, Georgia's DREs and election management systems used outdated software with widely documented vulnerabilities. In my opinion, Georgia's paperless DRE system was highly susceptible to cyberattacks that could change votes, erase votes, or cast extra votes.

89. The AccuVote TS and TSX are probably the most well-studied by security researchers of any voting machines in the world. Over the past 17 years, I, and other experts have repeatedly documented serious security problems with these machines and their election management system, as part of peer-reviewed and state-sponsored research studies. The vulnerabilities that affected Georgia's DRE system include numerous hardware and software security flaws, as well as architectural weaknesses. In tests, I have demonstrated that, in just a few seconds, anyone can install vote-stealing malware on these machines that will alter all records of every vote.[45]

---

[44] National Academies of Sciences, Engineering, and Medicine, *Securing the Vote: Protecting American Democracy* (2018), http://nap.edu/25120.

[45] Ariel J. Feldman, J. Alex Halderman & Edward W. Felten, *Security Analysis of the Diebold AccuVote-TS Voting Machine*, Princeton University (2006), http://usenix.org/events/evt07/tech/full_papers/feldman/feldman.pdf.

90. In a 2006 study, collaborators and I demonstrated the vulnerabilities of the AccuVote TS by developing malware that could infect the machines and steal votes. The malware we created modifies all the vote records, audit logs, and protective counters stored by the machine, so that even careful forensic examination of the files would find nothing amiss. The malware was programmed to inspect each ballot as it was cast and modify the minimum number of votes necessary to ensure that the attacker's favored candidate always had at least a certain percentage of the vote total.

91. We also developed a voting machine virus that could spread the vote-stealing malware automatically from machine to machine during normal pre- and post-election activities. The virus propagated via the removable memory cards that election workers use to program the ballot design before every election and to offload election results. By exploiting vulnerabilities in the AccuVote software, an infected memory card can spread the voting machine virus to the machine. Once installed, the virus can copy itself to every memory card inserted into the infected machine. If those cards are inserted into other machines, they too will become infected.

92. In 2007, the Secretary of State of California organized a comprehensive election security examination, the California Top-to-Bottom Review (TTBR[46]), which examined systems including the AccuVote TSX. I was part of a team of six experts who spent approximately 30 days examining the source code to the AccuVote system. Also in 2007, the Secretary of State of Ohio conducted a similar security study and source code review (Project EVEREST[47]), which also covered the AccuVote TSX system.

93. Both studies found additional, extremely serious security vulnerabilities. The TTBR report documents 24 serious security issues in the AccuVote TSX. These include software flaws, including buffer-overflow vulnerabilities, that attackers could exploit to install malicious software on the voting machines and on the election management back-end systems used to design and tabulate ballots. These flaws could be exploited to spread a vote-stealing virus that would propagate even more efficiently and be more difficult to detect than the virus developed in my 2006 study.

---

[46] California Secretary of State, *Top-to-Bottom Review of Electronic Voting Systems* (2007), https://www.sos.ca.gov/elections/ovsta/frequently-requested-information/top-bottom-review/.

[47] Ohio Secretary of State, *EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing* (Dec. 7, 2007), http://www.patrickmcdaniel.org/pubs/everest.pdf.

94. The software that performed election functions on the AccuVote TS and TSX is called BallotStation. I understand that the machines used in Georgia used BallotStation version 4.5.2, which was developed in 2005, and that Georgia did not ever update the BallotStation software to a newer version, even though newer versions were available. This software predates the California and Ohio studies, which examined version 4.6 in 2007. In my opinion, the serious vulnerabilities discovered in these studies almost certainly remained uncorrected in the software used on Georgia's voting machines through the end of 2019.

95. The election management system that was used with the AccuVote DREs is called the Global Election Management Environment ("GEMS"). Vulnerabilities in GEMS and BallotStation make it possible for an attacker who infiltrates a GEMS installation or its data files to spread vote-stealing malware to all voting machines that are programmed from that installation.

96. I understand that, for the November 2018 election, Georgia programmed its DREs as follows. Individuals working as third-party contractors for the Secretary of State prepared the initial ballot programming files for every Georgia county. To do so, they used copies of GEMS installed on computers in their homes, outside the physically secured environment of the Secretary of State's office. Once an initial version of the programming for a county had been completed, it was copied

to a USB drive and delivered to Michael Barnes, Director of the Center for Election Systems, at the Secretary of State's office. Barnes used his Internet-connected computer to inspect the files. He then transferred them into the State's central GEMS server environment on another USB drive.[48]

97. As a consequence of this workflow, ballot programming files for every county passed through an Internet-connected computer. In my opinion, attackers could have exploited this weakness to spread malware to the GEMS servers, and, ultimately, to DREs across the state.

98. I understand that, after workers at the SOS office finalized the ballot programming files, they delivered them to each county on a CD. Each county maintained its own GEMS server, to which workers copied files from the CD. Workers then used the county GEMS server to prepare memory cards for each DRE within the county.

99. In my opinion, an attacker who infiltrated the SOS GEMS system could have spread malware to the county GEMS servers by infecting the CDs used to distribute the files. Similarly, an attacker who infiltrated a county GEMS system

[48] Order at 28-31, *Curling v. Raffensperger*, No. 1:17-cv-2989-AT (N.D. Ga. Aug. 15, 2019), ECF No. 579.

could have spread vote-stealing malware to all DREs in the county by infecting the memory cards.

100. I am familiar with several countermeasures that the Georgia election system employed in 2018. These include parallel testing, logic and accuracy testing, anti-virus and end-point protection, tamper-evident seals, and network isolation of GEMS servers from the Internet. In my opinion, Georgia's election security countermeasures were inadequate to stop a sophisticated attacker, such as a hostile nation state, from infiltrating the election system, spreading malware to voting machines, and altering election outcomes.

101. In principle, it might be possible to detect whether Georgia's election system was infiltrated by attackers by conducting detailed digital forensics of the election equipment. As far as I can tell, *nobody* has ever performed a forensic examination of even a single Georgia DRE or GEMS server.

I declare under penalty of the perjury laws of the State of Georgia and the United States that the foregoing is true and correct, and that this declaration was executed this 18th day of February, 2020 in Philadelphia, Pennsylvania.

J. ALEX HALDERMAN

EXHIBIT A

J. Alex Halderman

Professor, Computer Science and Engineering
University of Michigan

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

J.AlexHalderman.com

February 17, 2020

Research Overview

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

Selected Projects

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

Positions

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

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

  Director, Center for Computer Security and Society (2014–present)
- Censys; Co-founder and Chief Scientist (2017–present)
- ISRG; Co-founder and Board Member (2013–present)

Education

- Ph.D. in Computer Science, Princeton University, June 2009
  Advisor: Ed Felten Committee: Andrew Appel, Adam Finkelstein, Brian Kernighan, Avi Rubin
  Thesis: *Investigating Security Failures and their Causes: An Analytic Approach to Computer Security*
- A.B. in Computer Science, *summa cum laude*, Princeton University, June 2003

Honors and Awards

- President's Award for National and State Leadership, University of Michigan (2020)
- Andrew Carnegie Fellowship (2019)
- Merit Network's 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 Facebook Internet Defense Prize
  for "DROWN: Breaking TLS using SSLv2"
- Named one of Popular Science's "Brilliant 10" (2015) ("each year *Popular Science* honors the brightest young minds reshaping science, engineering, and the world")
- **Best Paper Award** of the 22nd ACM Conference on Computer and Communications Security
  for "Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice" (2015)
- Pwnie Award in the category of "Most Innovative Research"
  for "Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice," Black Hat 2015
- IRTF Applied Networking Research Prize for "Neither Snow Nor Rain Nor MITM... An Empirical Analysis of Email Delivery Security" (2015)
- Alfred P. Sloan Research Fellowship (2015)
- University of Michigan College of Engineering 1938 E Award (2015) ("recognizes an outstanding teacher in both elementary and advanced courses, an understanding counselor of students who seek guidance in their choice of a career, a contributor to the educational growth of the College, and a teacher whose scholarly integrity pervades his/her service and the profession of Engineering")
- Morris Wellman Faculty Development Assistant Professorship (2015)
  ("awarded to a junior faculty member to recognize outstanding contributions to teaching and research")
- **Best Paper Award** of the 14th ACM Internet Measurement Conference
  for "The Matter of Heartbleed" (2014)
- **Best Paper Award** of the 21st USENIX Security Symposium
  for "Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices" (2012)
- Runner-up for 2012 PET Award for Outstanding Research in Privacy Enhancing Technologies
  for "Telex: Anticensorship in the Network Infrastructure" (2012)
- John Gideon Memorial Award from the Election Verification Network
  for contributions to election verification (2011)
- **Best Student Paper** of the 17th USENIX Security Symposium
  for "Lest We Remember: Cold Boot Attacks on Encryption Keys" (2008)
- Pwnie Award in the category of "Most Innovative Research"
  for "Lest We Remember: Cold Boot Attacks on Encryption Keys," Black Hat 2008

- Charlotte Elizabeth Procter Honorific Fellowship, Princeton University (2007)
  ("awarded in recognition of outstanding performance and professional promise, and represents high commendation from the Graduate School")
- National Science Foundation Graduate Research Fellowship (2004–2007)
- **Best Paper Award** of the 8th International Conference on 3D Web Technology
  for "Early Experiences with a 3D Model Search Engine" (2003)
- Princeton Computer Science Department Senior Award (2003)
- Accenture Prize in Computer Science, Princeton University (2002)
- Martin A. Dale Summer Award, Princeton University (2000)
- USA Computing Olympiad National Finalist (1996 and 1997)

Refereed Conference Publications

[1] **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
To appear in *41st IEEE Symposium on Security and Privacy* ("Oakland"), May 2020.

[2] **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), Nov. 2019.
Acceptance rate: 16%, 117/722.

[3] **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), Nov. 2019.
Acceptance rate: 16%, 117/722.

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

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

[6] **403 Forbidden: A Global View of Geoblocking**
Allison McDonald, Matthew Bernhard, Benjamin VanderSloot, Will Scott, J. A. Halderman, and Roya Ensafi
Proc. 18th ACM Internet Measurement Conference (IMC), October 2018.
Acceptance rate: 24%, 43/174.

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

[8] **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
Proc. 39th IEEE Symposium on Security and Privacy ("Oakland"), May 2018.
Acceptance rate: 11%, 63/549.

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

[10] **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
Proc. 2nd International Joint Conference on Electronic Voting (E-Vote-ID), Bregenz, Austria, October 2017.

[11] **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
Proc. 26th USENIX Security Symposium, Vancouver, BC, August 2017.
Acceptance rate: 16%, 85/522.

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

[13] **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
Proc. 24th Network and Distributed Systems Symposium (NDSS), February 2017.
Acceptance rate: 16%, 68/423.

[14] **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
Proc. 24th Network and Distributed Systems Symposium (NDSS), February 2017.
Acceptance rate: 16%, 68/423.

[15] **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
Proc. 14th IEEE Conference on Privacy, Security, and Trust (PST), Auckland, NZ, December 2016.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[39] **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.

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

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

[42] **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.

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

Acceptance rate: 17%, 55/320.
Highest ranked submission.

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

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

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

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

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

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

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

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

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

Book Chapters

[53] **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, December 2016.

Journal Publications

[54] **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.

[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
Communications of the ACM, 52(5):91–98, 2009.

[56] **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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Selected Other Publications

[74] **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", February 27, 2019.

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

[76] **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.

[77] **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.

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

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

[80] **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.

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

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

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

[84] **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.

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

[86] **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.

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

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

Selected Legal and Regulatory Filings

[89] **Request for DMCA Exemption: Security Research**
Petition to the U.S. Copyright Office of Ed Felten and J. Alex Halderman, represented by Elizabeth Field, Justin Manusov, Brett Hildebrand, Alex Kimata, and Blake Reid, regarding the Seventh Triennial Section 1201 Proceeding, 2017–18.
(*Outcome:* Requested exemption granted in part.)

[90] **Request for DMCA Exemption: Security Research**
Petition to the Librarian of Congress of S. M. Bellovin, M. Blaze, E. W. Felten, J. A. Halderman, and N. Heninger, represented by Andrea Matwyshyn, regarding the U.S. Copyright Office 2014–2015 DMCA Anticircumvention Rulemaking, Nov. 2014.
(*Outcome:* Requested exemption granted in part.)

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

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

Patents

[93] **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.

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

Speaking

Major Invited Talks and Keynotes

- **U.S. House Testimony Regarding Federal Funding for Election Cybersecurity**
  Testimony before the U.S. House Appropriations Subcommittee on Financial Service and General Government, Feburary 27, 2019.
- **Election Cybersecurity Progress Report: Will the U.S. be Ready for 2020?**
  35c3, Leipzig, December 27, 2018.
- **Cyberattacks on Election Infrastructure**
  Keynote speaker, DIMVA 2018, Paris, June 29, 2018.
- **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.
- **Recount 2016: A Security Audit of the U.S. Presidential Election**
  Keynote talk, NDSS 2017, February 27, 2017.
- **Recount 2016: An Uninvited Security Audit of the U.S. Presidential Election**
  33c3, Hamburg, December 28, 2016.
- **Elections and Cybersecurity: What Could Go Wrong?**
  Keynote speaker, Merit Security Summit, Ypsilanti, MI, November 7, 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, September 9, 2016.
- **Internet Voting: What Could Go Wrong?**
  Invited speaker, USENIX Enigma, San Francisco, January 27, 2016.
- **Logjam: Diffie-Hellman, Discrete Logs, the NSA, and You**
  32c3, Hamburg, December 29, 2015.
- **The Network Inside Out: New Vantage Points for Internet Security**
  Invited talk, China Internet Security Conference (ISC), Beijing, September 30, 2015.
- **The Network Inside Out: New Vantage Points for Internet Security**
  Keynote speaker, ESCAR USA (Embedded Security in Cars), Ypsilanti, Michigan, May 27, 2015.
- **Security Analysis of the Estonian Internet Voting System**
  31c3, Hamburg, December 28, 2014.
- **The Network Inside Out: New Vantage Points for Internet Security**
  Keynote speaker, 14th Brazilian Symposium on Information Security and Computer Systems (SBSeg), Belo Horizonte, Brazil, November 4, 2014.

– **Empirical Cryptography: Measuring How Crypto is Used and Misused Online**
Keynote speaker, 3rd International Conference on Cryptography and Information Security in Latin America (Latincrypt), Florianópolis, Brazil, September 2014.

– **Healing Heartbleed: Vulnerability Mitigation with Internet-wide Scanning**
Keynote speaker, 11th Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA), London, July 10, 2014.

– **Fast Internet-wide Scanning and its Security Applications**
30c3, Hamburg, December 28, 2013.

– **Challenging Security Assumptions.** Three-part tutorial. 2nd TCE Summer School on Computer Security, Technion (Haifa, Israel), July 23, 2013.

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

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

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

Selected Talks (2009–present)

– **Let's Encrypt: An Automated Certificate Authority to Encrypt the Entire Web**
Invited speaker, OWASP Copenhagen, November 25, 2019.

– **Cybersecurity and U.S. Elections**
Invited speaker, CyberSec & AI Prague, October 25, 2019; Invited speaker, Indiana University Research, February 7, 2019; Invited speaker, Arizona State, January 16, 2019; Invited speaker, University of San Diego, November 16, 2018; Invited speaker, UMass Amherst, October 31, 2018; Invited speaker, U-M Alumni Association, October 18, 2018; Invited speaker, MIT EmTech, August 13, 2018; Invited speaker, DEFCON Voting Village, August 10, 2018; Invited speaker, U.S. Irvine Election Security Summit, Irvine, March 13, 2018; Invited speaker, Global Election Summit, San Francisco, May 17, 2017; Invited speaker, Wolverine Caucus Forum, Lansing, February 21, 2017; Invited speaker, CSE Science on Screen at Michigan Theater, Ann Arbor, January 25, 2017.

– **Congressional Briefing on Election Cybersecurity.**
Hosted by Rep. Mike Quigley and Rep. John Katko; September 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 Senator Kamala Harris and Senator James Lankford. April 12, 2018.

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

– **The Security Impact of HTTPS Interception.** Invited talk, GOTO Copenhagen, Oct. 2, 2017.
– **Congressional Briefing: Free, Automated, and Open Web Encryption.** August 8, 2017; hosted by Congressional Cybersecurity Caucus.
– **Let's Encrypt: A Certificate Authority to Encrypt the Entire Web.** Invited talk, Summer school on real-world crypto and privacy, Croatia, June 9, 2017; Invited talk, Cubaconf, Havana, April 25, 2016.
– **Congressional Briefing: Strengthening Election Cybersecurity.** Co-panelists: James Woolsey, Tony Shaffer, Lawrence Norden, Susan Greenhalgh, James Scott; moderator: Karen Greenberg. May 15, 2017.
– **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, April 8, 2016 [host: Damon McCoy]; Invited talk, UIUC Science of Security seminar, February 9, 2016 [host: Michael Bailey].
– **The Network Inside Out: New Vantage Points for Internet Security.** Invited talk, Qatar Computing Research Institute, Doha, May 24, 2015; Invited talk, University of Chile, Santiago, April 8, 2015; Invited talk, Princeton University, October 15, 2014; Invited talk, U.T. Austin, March 9, 2014.
– **Decoy Routing: Internet Freedom in the Network's Core.** Invited speaker, Internet Freedom Technology Showcase: The Future of Human Rights Online, New York, Sep. 26, 2015.
– **The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election.** 5th International Conference on E-Voting and Identity (VoteID), Bern, Switzerland, Sep. 3, 2015; Invited talk, IT Univ. of Copenhagen, Sep. 1, 2015; Invited talk (with Vanessa Teague), USENIX Journal of Election Technologies and Systems Workshop (JETS), Washington, D.C., Aug. 11, 2015.
– **Security Analysis of the Estonian Internet Voting System.** Invited talk, 5th International Conference on E-Voting and Identity (VoteID), Bern, Switzerland, Sep. 3, 2015; Invited talk, Google, Mountain View, CA, June 3, 2014; Invited talk, Copenhagen University, June 12, 2014.
– **Indiscreet Tweets.** Rump session talk; 24th USENIX Security Symposium, Washington, D.C., August 12, 2015.
– **How Diffie-Hellman Fails in Practice.** Invited talk, IT Univ. of Copenhagen, May 22, 2015.
– **Influence on Democracy of Computers, Internet, and Social Media**. Invited speaker, Osher Lifelong Learning Institute at the University of Michigan, March 26, 2015.
– **E-Voting: Danger and Opportunity**. Invited talk, University of Chile, Santiago, April 7, 2015; Keynote speaker, 14th Brazilian Symposium on Information Security and Computer Systems (SBSeg), Belo Horizonte, Brazil, November 3, 2014; Crypto seminar, University of Tartu, Estonia, October 10, 2013; Invited speaker, US–Egypt Cyber Security Workshop, Cairo, May 28, 2013; Invited speaker, First DemTech Workshop on Voting Technology for Egypt, Copenhagen, May 1, 2013; Invited keynote, 8th CyberWatch Mid-Atlantic CCDC, Baltimore, MD, Apr. 10, 2013;

Invited speaker, Verifiable Voting Schemes Workshop, University of Luxembourg, Mar. 21, 2013; Invited speaker, MHacks hackathon, Ann Arbor, MI, Feb. 2, 2013; Public lecture, U. Michigan, Nov. 6, 2012.

– **Internet Censorship in Iran: A First Look**. 3rd USENIX Workshop on Free and Open Communications on the Internet (FOCI), Aug. 13, 2013.
– **Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices**. Invited talk, NSA, Aug. 8, 2013; Invited talk, Taiwan Information Security Center Workshop, National Chung-Hsing University (Taichung, Taiwan), Nov. 16, .2012
– **Securing Digital Democracy**. U. Maryland, Apr. 8, 2013 [host: Jonathan Katz]; CMU, Apr. 1, 2013 [host: Virgil Gligor]; Cornell, Feb. 28, 2013 [host: Andrew Myers].
– **Telex: Anticensorship in the Network Infrastructure**. Invited speaker, Academia Sinica (Taipei), Nov. 14, 2012 [host: Bo-Yin Yang]; TRUST Seminar, U.C., Berkeley, Dec. 1, 2011 [host: Galina Schwartz]; Think Conference, Nov. 5, 2011; Ideas Lunch, Information Society Project at Yale Law School, Oct. 26, 2011; Invited speaker, Committee to Protect Journalists Online Press Freedom Summit (San Francisco), Sept. 27, 2011.
– **Deport on Arrival: Adventures in Technology, Politics, and Power**. Guest lecture, U-M School of Art and Design, Nov 5, 2012 [host: Osman Khan]; Invited speaker, CS4HS Workshop, U. Michigan, Aug. 21, 2012; Invited speaker, U. Michigan IEEE, Feb. 15, 2012.
– **Attacking the Washington, D.C. Internet Voting System**. Invited speaker, International Foundation for Election Systems (IFES), Nov. 2, 2012 [host: Michael Yard]; Invited speaker, IT University of Copenhagen, May 11, 2012 [host: Carsten Schürmann].
– **Voter I*Don't***. Rump session talk; 21st USENIX Security Symposium (Bellevue, WA), Aug. 8, 2012; Rump session talk; EVT/WOTE '12 (Bellevue, WA), Aug. 6, 2012 [with Josh Benaloh].
– **Reed Smith's Evening with a Hacker**. Keynote speaker (New Brunswick, NJ), Oct. 20, 2011.
– **Are DREs Toxic Waste?** Rump session talk, 20th USENIX Security Symposium (San Francisco), Aug. 10, 2011; Rump session talk, EVT/WOTE '11 (San Francisco), Aug. 8, 2011.
– **Security Problems in India's Electronic Voting Machines**. Dagstuhl seminar on Verifiable Elections and the Public (Wadern, Germany), July 12, 2011; Harvard University, Center for Research on Computation and Society (CRCS) seminar, Jan. 24, 2011 [host: Ariel Procaccia]; U. Michigan, CSE seminar, Nov. 18, 2010 [with Hari Prasad]; MIT, CSAIL CIS Seminar, Nov. 12, 2010 [with Hari Prasad; host: Ron Rivest]; Distinguished lecture, U.C. San Diego, Department of Computer Science, Nov. 9, 2010 [with Hari Prasad; host: Hovav Shacham]; U.C. Berkeley, Center for Information Technology Research in the Interest of Society (CITRIS), Nov. 8, 2010 [with Hari Prasad; host: Eric Brewer]; Google, Inc., Tech Talk (Mountain View, CA), Nov. 5, 2010 [with Hari Prasad; host: Marius Schilder]; U.C., Berkeley TRUST Security Seminar, Nov. 4, 2010 [with Hari Prasad; host: Shankar Sastry]; Stanford University, CS Department, Nov. 3, 2010 [with Hari Prasad; host: David Dill]; Princeton University, Center for Information Technology Policy, Oct. 28, 2010 [with Hari Prasad, host: Ed Felten]; University of Texas at Austin, Department of Computer Science, Aug. 27, 2010 [host: Brent Waters].

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

Selected Other Speaking (2010–present)

– Panelist: **How Adversaries Can Erode Public Trust in Democratic Institutions.** Co-panelists: Hany Farid, Ron Rivest, Suzanne Spaulding; moderator: James E. Boasberg. D.C. Circuit Judicial Conference, Cambridge, Maryland, June 26, 2019.
– **Alumni-Faculty Forum: Cold War 2.0: Russia, Cybersecurity and Hacking.** Co-panelists: Walter Slocombe, Alexander Southwell, Ishani Sud; moderator: Jonathan Mayer. June 1, 2018.
– Panelist: **"Critical Infrastructure" Designation for Election Operations: Risks, Mitigations, & Import for 2018.** Election Verification Network Conference, Miami, March 16, 2018.
– Panelist: **The Technology of Voting: Risks & Opportunities.** U.C. Irvine Cybersecurity and Policy Research Institute, March 13, 2018.
– Panelist: **Election Law Conflicts and the Vulnerability of our Election Systems.** Co-panelists: Stephen Berzon, Holly Lake, Harvey Saferstein. Ninth Circuit Judicial Conference, July 18, 2017.
– Moderator: **Apple & the FBI: Encryption, Security, and Civil Liberties.** Panelists: Nate Cardozo and Barbara McQuade. U-M Dissonance Speaker Series, April 12, 2016.

– Moderator: **Privacy, IT Security and Politics.** Panelists: Ari Schwartz and David Sobel. U-M ITS SUMIT_2015, Oct. 22, 2015.
– Panelist: **The Future of E-Voting Research.** 5th International Conference on E-Voting and Identity (VoteID), Bern, Switzerland, Sep. 4, 2015.
– Moderator: **Panel on Research Ethics.** 24th USENIX Security Symposium, Washington, D.C., August 13, 2015.
– Panelist: **Theories of Privacy in Light of "Big Data."** Michigan Telecommunications and Technology Law Review Symposium on Privacy, Technology, and the Law, University of Michigan Law School, Feb. 21, 2015.
– Panelist: **Measuring Privacy**. Big Privacy symposium, Princeton University CITP, Apr. 26, 2013 [moderator: Ed Felten].
– Panelist: **Civil Society's Challenge in Preserving Civic Participation**. The Public Voice workshop: Privacy Rights are a Global Challenge, held in conjunction with the 34th International Conference of Data Protection and Privacy Commissioners, Punta del Este, Uruguay, Oct. 22, 2012 [moderator: Lillie Coney].
– Panelist: **Election Technologies: Today and Tomorrow**. Microsoft Faculty Summit (Redmond), July 17, 2012 [moderator: Josh Benaloh].
– Panelist: **Is America Ready to Vote on the Internet?** CSPRI Seminar, George Washington University (Washington, D.C.), May 16, 2012 [moderator: Lance Hoffman].
– Panelist: **Technical Methods of Circumventing Censorship**. Global Censorship Conference, Yale Law School, Mar. 31, 2012.
– Panelist: **Internet Voting**. RSA Conference (San Francisco), Mar. 1, 2012 [moderator: Ron Rivest].
– Panelist: **The Law and Science of Trustworthy Elections**. Association of American Law Schools (AALS) Annual Meeting, Jan. 5, 2012 [moderator: Ron Rivest].
– Panelist: **Connecticut Secretary of State's Online Voting Symposium** (New Britain, CT), Oct. 27, 2011 [moderator: John Dankosky].
– Panelist: **Cyber Security / Election Technology**. Overseas Voting Foundation Summit, Feb. 10, 2011 [moderator: Candice Hoke].
– ~~Tutorial speaker/organizer: **Security Issues in Electronic Voting**, ICISS (Gandhinagar, India), Dec. 15, 2010~~ [canceled under threat of deportation].
– Invited testimony: On **D.C. Board of Elections and Ethics Readiness for the Nov. 2010 General Election**. D.C. Council Hearing, Oct. 8, 2010.
– Panelist and organizer: **India's Electronic Voting Machines**. EVT/WOTE (Washington, D.C.), Aug. 9, 2010.
– Panelist: **Ethics in Networking and Security Research**. ISOC Network and Distributed System Security Symposium (San Diego, CA), Mar. 2, 2010 [moderator: Michael Bailey].

Advising and Mentoring

Graduate Students

- Allison McDonald (Ph.D. in progress; Facebook Emerging Scholar Fellowship)
- Matthew Bernhard (Ph.D. in progress)
- Benjamin VanderSloot (Ph.D. in progress)
- David Adrian (Ph.D. 2019; went on to principal engineer at Censys)
- Andrew Springall (Ph.D. 2018; went on to tenure-track faculty position at Auburn)
- Zakir Durumeric (Ph.D. 2017; Google Ph.D. Fellowship in Computer Security; went on to tenure-track faculty position at Stanford)
- Eric Wustrow (Ph.D. 2016; went on to tenure-track faculty position at U. Colorado, Boulder)
- James Kasten (Ph.D. 2015; went on to software engineering position at Google)
- Rose Howell (M.S. 2018)
- Travis Finkenauer (M.S. 2016; went on to security position at Juniper Networks)
- Scott Wolchok (M.S. 2011; went on to software engineering position at Facebook)

Post Docs

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

Doctoral Committees

- Arunkumaar Ganesan (C.S. Ph.D. expected 2019)
- David Adrian (C.S. Ph.D. 2019, Michigan; chair)
- 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)

Undergraduate Independent Work

- 2019: Scott Bays, Kevin Chang, Jensen Hwa, Nicholas Matton, Henry Meng, Ellen Tsao, Hassaan Ali Watoo
- 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'Neil
- 2011: Yilun Cui, Alexander Motalleb
- 2010: Arun Ganesan, Neha Gupta, Kenneth Meagher, Jay Novak, Dhritiman Sagar, Samantha Schumacher, Jonathan Stribley
- 2009: Mark Griffin, Randy Yao

Teaching

- **Introduction to Computer Security**, EECS 388, University of Michigan
  Terms: 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 >750 students/year. An accessible intro, teaches the security mindset and practical skills for building and analyzing security-critical systems.
- **Surveillance Law and Technology** (with Margo Schlanger), EECS 598-007 / LAW 441-1, University of Michigan, Fall 2019.
- **Election Cybersecurity**, EECS 498, University of Michigan, Fall 2018.
- **Computer and Network Security**, EECS 588, University of Michigan
  Terms: Winter 2016, Winter 2015, Winter 2014, Winter 2013, Winter 2012, Winter 2011, Winter 2010, Winter 2009
  Redesigned core grad-level security course. Based around discussing classic and current research papers and performing novel independent work. Provides an intro. to systems research for many students.
- **Securing Digital Democracy**, Coursera (MOOC)
  Designed and taught a massive, open online course that explored the security risks—and future potential—of electronic voting and Internet voting technologies; over 20,000 enrolled students.

Professional Service

Program Committees

- 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)

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 (2011–2016)
- Advisory Council for the Princeton University Department of Computer Science (2012–2014)

Government Service

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

Department and University Service

- Lab Director, CSE Systems Lab (2018–present)
- CSE Hiring Committee (member, 2018–present)
- Faculty Advisor for Michigan Hackers student group (2012–present)
- CSE Graduate Affairs Committee (member, 2014–2017)
- CSE Undergraduate Program Advising (CS/ENG) (2011–2017)
- Faculty Senate, Rules Committee of the Senate Assembly (member, 2011–12)
- CSE Graduate Admissions Committee (member, 2010–11)
- CSE Graduate Committee (member, 2009–10)

CERTIFICATE OF SERVICE

I hereby certify that, on February 18, 2020, I caused to be served the foregoing **REPORT OF PLAINTIFFS' EXPERT WITNESS J. ALEX HALDERMAN** by filing it through the Court's ECF system, which will serve the following counsel:

Chris Carr, Esq.
Attorney General
Dennis Dunn, Esq.
Deputy Attorney General
Russell Willard, Esq.
Senior Assistant Attorney General
Georgia Office of the Attorney General
40 Capitol Square
Atlanta, GA 30334
ccarr@law.ga.gov
ddunn@law.ga.gov
rwillard@law.ga.gov

Joshua Barrett Belinfante, Esq.
Vincent Robert Russo, Jr., Esq.
Brian Edward Lake, Esq.
Carey Allen Miller, Esq.
Alexander Denton, Esq.
Special Assistant Attorneys General
Robbins Ross Alloy Belinfante Littlefield, LLC
500 Fourteenth St., N.W.
Atlanta, GA 30318
Telephone: (678) 701-9381
Fax: (404) 856-3250
jbelinfante@robbinsfirm.com
blake@robbinsfirm.com
vrusso@robbinsfirm.com
cmiller@robbinsfirm.com
adenton@robbinsfirm.com

Bryan P. Tyson, Esq.
Bryan F. Jacoutot, Esq.
Diana LaRoss, Esq.
Special Assistant Attorneys General
Taylor English Duma LLP
1600 Parkwood Circle
Suite 200
Atlanta, GA 30339
Telephone: (678) 336-7249
btyson@taylorenglish.com
bjacoutout@taylorenglish.com
dlaross@taylorenglish.com

/s/ Leslie J. Bryan
Leslie J. Bryan
Georgia Bar No. 091175